Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Leitlinie

Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf

Teil 1: Gefährdungen und Sicherheitsmaßnahmen

BSI TL-02103 - Version 2.0

Das Dokument reflektiert den Stand der Technik bis August 2014.

An der Erstellung waren folgende Mitarbeiter des BSI (Bundesamt für Sicherheit in der Informationstechnik) beteiligt: Norbert Landeck und Michael Seak

Weiterhin haben folgende Mitarbeiter der ComConsult Beratung und Planung GmbH maßgeblich mitgewirkt: Claus Elfering (†), Oliver Flüs, Leonie Herden, Dr. Simon Hoff, Dietlind Hübner, Frank Sujata, Dominik Zöller

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 228 99 9582-0
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de

Gliederung

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Kurzfassung des Gesamtdokuments

Die Komplexität von Telekommunikationslösungen (TK-Lösungen) ist in den letzten Jahren deutlich gestiegen. Bis vor einiger Zeit bestand eine TK-Anlage meist ausschließlich aus Systemen auf Basis des Integrated Services Digital Network (ISDN). Heutzutage beinhalten TK-Lösungen jedoch verschiedenste Komponenten, beispielsweise einige oder alle der folgenden Elemente:

- TK-Anlage auf Basis der klassischen Telekommunikation (ISDN-Systeme) oder auf Basis von Voice over IP (VoIP) oder eine Kombination aus beiden
- Kommunikationsdienste auf Basis von Unified Communications and Collaborations (UCC) inkl. Videokonferenzsystemen
- Spezielle Dienste und Komponenten für Kontaktcenter und Händlersysteme
- Alarmierungssysteme, die eine Kopplung an die TK-Lösung nutzen
- Nutzung Sozialer Netzwerke und Sozialer Medien (SNM)
- Nutzung von Cloud Computing

Eine solche TK-Lösung umfasst dann eine Vielzahl von Bestandteilen zur Bereitstellung der angebotenen Dienste, bestehend aus Netzwerkkomponenten, Virtualisierungsplattformen und Anwendungen, die ggf. verteilt bzw. in Form einer Mehr-Tier-Architektur mit entsprechender Middleware und Server-Infrastruktur implementiert sind. Darüber hinaus werden nicht mehr nur stationäre Telefone angebunden, sondern eine breite Palette verschiedener mobiler Endgeräte integriert, welche die genannten Dienste ebenfalls nutzen. Alle diese Aspekte einer modernen TK-Lösung sind unter Sicherheitsgesichtspunkten angemessen zu berücksichtigen.

Die verschiedenen Elemente und Schnittstellen einer TK-Lösung sind unterschiedlichsten Gefährdungen ausgesetzt: Zum einen kann die Verfügbarkeit der über die TK-Lösung angebotenen Dienste und Daten gefährdet sein, zum anderen können die Vertraulichkeit und Integrität der über die TK-Lösung ausgetauschten oder von den TK-Komponenten verwalteten Daten kompromittiert werden. Da die einzelnen Komponenten unterschiedliche Schwachstellen haben und unterschiedlichen Gefährdungen ausgesetzt sind, bietet eine moderne TK-Lösung vielfältige Angriffspunkte. Eine typische Gefährdung, welche die meisten Teilsysteme einer TK-Lösung betrifft, ist beispielsweise der unbefugte Zugriff auf personenbezogene Daten, welche auf dem System gespeichert sind. Dieser ist oft insbesondere über nicht ausreichend abgesicherte Endgeräte, z. B. Smartphones, möglich. Auf dem Endgerät gespeicherte Daten können Kontaktdaten, Bilder oder Dokumente der Organisation sein. Je nach Nutzung des Endgerätes können hiervon auch besonders schützenswerte Daten betroffen sein.

Andere Gefährdungen betreffen nur selektiv einzelne Teilsysteme der TK-Lösung und müssen daher nur berücksichtigt werden, falls die entsprechenden Teilsysteme in dem betrachteten System verwendet werden. Dies ist beispielsweise die beim Cloud Computing auftretende Gefahr der Kompromittierung von Organisationsdaten, welche bei dem Cloud-Anbieter gespeichert sind. Werden solche Cloud-Computing-Lösungen verwendet, so muss beispielsweise durch vertragliche Regelungen sichergestellt werden, dass die Organisationsdaten durch den Cloud-Anbieter ausreichend geschützt sind.

Hinzu kommt, dass die Gesamtgefährdung einer umfassenden TK-Lösung weitaus höher sein kann, als die Gefährdungen der einzelnen Teilkomponenten dies auf den ersten Blick vermuten lassen. Die Schwachstellen einzelner Komponenten und Gefährdungen, welche auf die einzelnen Teile der TK-Lösung wirken, können sich gegenseitig verstärken und so die Gesamtgefährdung der TK-Lösung deutlich erhöhen.

Zur Absicherung einer TK-Lösung ist es daher notwendig, die Gesamtheit aller Teilsysteme und die auf diese wirkenden Gefährdungen zu betrachten.

Die vorliegende Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf stellt dem Anwender der Technischen Leitlinie das Basiswissen der genannten Technologien bereit, soweit dies als Grundlage zum Verständnis der Gefährdungen oder Maßnahmen erforderlich sind. Je

TK-Technologie wird die Gefährdungslage analysiert, sowohl für einen selektiven Einsatz, z. B. ausschließliche Nutzung einer VoIP-Anlage, als auch für einen umfassenden Einsatz vielfältiger Technologien, z. B. Nutzung eines UCC-Systems auf VoIP-Basis unter Integration von Smartphones und Tablets.

Aus den auf die TK-Technologien einwirkenden Gefährdungen ergibt sich ein Maßnahmenkatalog, der ergänzend zu den IT-Grundschutz-Katalogen die wesentlichen Maßnahmen spezifiziert, welche notwendig sind, um die entsprechende TK-Technologie bei erhöhtem Schutzbedarf angemessen zu schützen. Hierbei sind auch Maßnahmen für eine Absicherung von kombiniert eingesetzten TK-Technologien dargestellt. Eine detailliertere Zusammenfassung der spezifischen Gefährdungen und Maßnahmen für die betrachteten TK-Technologien findet sich jeweils am Ende der entsprechenden Kapitel.

Auf Basis des spezifizierten Maßnahmenkatalogs kann für eine konkrete TK-Lösung eine individuelle Maßnahmenauswahl erfolgen. Es ist dabei darauf zu achten, dass Gefährdungen, welche sich durch die Kombination zweier oder mehrerer Komponenten in einer Anlage ergeben, geeignet abgesichert werden. Der Erstellung eines individuellen Maßnahmenkatalogs muss daher stets eine genaue Analyse der genutzten TK-Lösung vorausgehen.

Für die Realisierung eines umfassenden Schutzes der TK-Lösung ist die Zusammenarbeit der für die unterschiedlichen Teilsysteme verantwortlichen Personen von besonderer Bedeutung. Nur durch eine geeignete Koordination kann sichergestellt werden, dass alle Gefährdungen und Maßnahmen angemessen berücksichtigt wurden und so unerwünschte Wechselwirkungen zwischen den umzusetzenden Maßnahmen vermieden werden.

Der Maßnahmenkatalog umfasst technische und organisatorische Maßnahmen. Beispiele für technische Maßnahmen sind:

- Authentisierung der Kommunikation zwischen Server und (mobilen) Endgeräten
- Anbindung von Endgeräten über zentrale Sicherheits-Gateways
- Beschränkung der Speicherung und des Austauschs sensibler Daten auf Endgeräten

Als Ergänzung der technischen Maßnahmen sind organisatorische Maßnahmen einzusetzen. Diese beinhalten z. B. die Schulung von Mitarbeitern und Administratoren, die Regelung bestimmter Arbeitsabläufe, die vertragliche Regelung von extern erbrachten Leistungen und das Vorgehen in Notfallsituationen. Beispielsweise muss eine neue Anweisung zur angemessenen Verschlüsselung von E-Mails von einer angemessenen Information und Schulung der Mitarbeiter flankiert werden.

Die Analyse der individuellen TK-Lösung sowie die umzusetzenden Maßnahmen müssen in einem Sicherheitskonzept festgelegt und dokumentiert werden. Bei der Auswahl angemessener Maßnahmen sind neben den eingesetzten TK-Technologien auch die Größe und der Aufbau der Organisation zu berücksichtigen. Die Größe der Organisation beeinflusst beispielsweise, welche Dienste von der Organisation selbst bereitgestellt werden und bei welcher Technologie und welchen Diensten auf externe Anbieter zurückgegriffen wird.

- So wird z. B. in kleinen Organisationen mit nur einem Standort und wenigen Mitarbeitern der IT-Betrieb oft fast vollständig über externe Firmen sichergestellt. Das bedeutet, dass Schutzmaßnahmen, die vor Ort IT-kompetentes Personal voraussetzten, in diesen Organisation oft nicht umgesetzt werden können. Weiterhin sind manche Maßnahmen aus wirtschaftlichen Gründen nicht konsequent umsetzbar. Diese Maßnahmen müssen dann durch solche ersetzt werden, die im betrachteten Umfeld realisierbar sind.
- Bei großen Organisationen, beispielsweise bei einem globalen Konzern, ist die TK-Struktur deutlich komplexer und es müssen weitreichende Absicherungen getroffen werden. So ist hier beispielsweise weltweit eine sichere Kommunikation und die Vermeidung eines Datenabflusses zu gewährleisten. Darüber hinaus ist bei der Maßnahmenauswahl die gegebenenfalls unterschiedliche Gesetzeslage in verschiedenen Ländern zu berücksichtigen.

Die vorliegende Technische Leitlinie stellt die beschriebene Analyse der TK-Lösung mit der hieraus resultierender Maßnahmenauswahl für repräsentative Beispielszenarien unterschiedlicher

Größenordnung dar. Ergänzend hierzu muss ein konkretes Sicherheitskonzept für die ausgewählten Maßnahmen festlegen, wie die Maßnahmen im Detail umgesetzt werden, z. B. welche Komponenten zusätzlich beschafft oder ausgetauscht werden müssen und wie diese Komponenten installiert und konfiguriert werden müssen.

So reicht beispielsweise die Aussage, dass Endgeräte der TK-Lösung gegen den unbefugten Zugriff zu schützen sind, im konkreten Einsatzfall nicht aus, sondern es muss detailliert festgelegt werden, wie ein solcher Schutz auszusehen hat. Beispielsweise können Endgeräte durch die ausschließliche Nutzung in entsprechend zugangsbeschränkten Bereichen geschützt sein. Endgeräte, welche z. B. in öffentlich zugänglichen Bereichen untergebracht sind, müssen dahingegen durch eine angemessene Software- oder Netzkonfiguration geschützt werden.

Wird bei der Konzeptanalyse festgestellt, dass zur Umsetzung der Maßnahmen eine Neubeschaffung von Komponenten notwendig ist oder steht eine Neubeschaffung aus anderen Gründen an, so ist vor der Beschaffung der Komponenten eine Anforderungsanalyse durchzuführen. Hierbei sind in Abhängigkeit von der geplanten TK-Technologie und den umzusetzenden Maßnahmen die Anforderungen an die Komponente zu definieren, die das angestrebte Sicherheitsniveau gewährleisten.

Die vorliegende Technische Leitlinie stellt hierzu einen Beschaffungsleitfaden bereit, in dem die wesentlichen Anforderungen gelistet sind, die zur Umsetzung der spezifizierten Maßnahmen erforderlich sind, beispielsweise für eine klassische TK-Anlage:

- Eine Konfiguration der Anlage pro Port ist möglich.
- Die Möglichkeit zur Vorhaltung einer Katastrophenschaltung ist gegeben.
- Die Sperrung unerwünschter Kommunikationspartner ist pro Port möglich.

Die Anforderungen werden in einer Liste von Auswahlkriterien entsprechend UfAB V (Unterlage für die Ausschreibung und Bewertung von IT-Leistungen, Version 5) dokumentiert und können für eine Ausschreibung von TK-Lösungen auf die individuelle TK-Lösung angepasst werden. Gemäß UfAB V wird zwischen Ausschlusskriterien und Bewertungskriterien unterschieden. Im Beschaffungsleitfaden werden für die verschiedenen Größenordnungen von Szenarien beispielhaft eine Gewichtung der Kriterien vorgenommen.

Der Anforderungskatalog kann im Rahmen einer Ausschreibung genutzt werden, um eine technische Bewertung der angebotenen Lösung vorzunehmen. Um die technische Bewertung der Lösung zu verifizieren, sind für die Auswahlkriterien Prüfkriterien definiert.

Die Auswahl eines Produktes mittels Anforderungskatalog und Prüfkriterien dient der Bewertung von Produkten und ist insbesondere bei einer produktneutralen Ausschreibung relevant. Es wird so sichergestellt, dass die in der TK-Lösung eingesetzten Elemente die notwendigen Voraussetzungen für einen erhöhten Schutzbedarf erfüllen.

1 Einleitung / Vorbemerkungen

Die moderne Telekommunikation ist untrennbar mit der Informationstechnik (IT) zusammengewachsen. Dieser Wandel hat zusammen mit der Konvergenz von Festnetzen und Mobilfunknetzen fundamentale Auswirkungen auf die Sicherheit von Telekommunikationssystemen. Gefährdungen der IT springen auf die Telekommunikation über und durch das Zusammenwirken der vernetzten Komponenten entstehen unerwartete neue Bedrohungen. Auf diese komplexe, systemübergreifende Gefährdungslage muss mit einem ganzheitlichen, auf die konkrete Nutzungsweise der Telekommunikation flexibel zugeschnittenen Maßnahmenkatalog reagiert werden.

Diese Technische Leitlinie beinhaltet konkrete Handlungsempfehlungen für die Planung, Beschaffung, Installation, Konfiguration, Abnahme, Betrieb und Außerbetriebnahme von organisationsinternen Telekommunikationssystemen in Bereichen mit erhöhtem Schutzbedarf. Dabei werden auch die relevanten Datenschutzaspekte berücksichtigt.

Dieses Dokument richtet sich an alle, die mit der Absicherung eines organisationsinternen Telekommunikationssystems, sei es in der Rolle als Planer, Beschaffer, Betreiber oder Revisor, befasst sind. Die vorliegende Technische Leitlinie hat dabei Empfehlungscharakter. Verbindlichkeit entsteht erst durch individuelle Vorgabe des Bedarfsträgers, z. B. als Bestandteil von Ausschreibungsunterlagen.

Der grundsätzliche Aufbau der Technischen Leitlinie orientiert sich an dem Aufbau der IT-Grundschutz-Kataloge des Bundesamt für Sicherheit in der Informationstechnik (siehe [BSI GSK-2013]), jedoch wird der Begriff „Baustein“ in diesem Dokument bewusst vermieden, um dem Leser eine klare Differenzierung zwischen den Gefährdungen und Maßnahmen der BSI IT-Grundschutz-Kataloge und denen der Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf zu ermöglichen.

Die Technische Leitlinie ist in drei Teile aufgeteilt und umfasst

- in Teil1 die Beschreibung der betrachteten Technologien, die resultierenden Gefährdungen sowie die hieraus abgeleiteten Sicherheitsmaßnahmen,
- in Teil 2 die Darstellung von Sicherheitskonzepten für repräsentative Beispielszenarien und
- in Teil 3 einen Beschaffungsleitfaden mit Anforderungs- und Prüfkriterien.

Kapitel 2 des vorliegenden Teil 1 der Technischen Leitlinie stellt zunächst die betrachteten Telekommunikationssysteme im Überblick vor. Ausgehend von herkömmlichen ISDN-basierten TK-Anlagen werden VoIP- und Hybrid-Systeme als Basistechnologien beschrieben. Hierauf aufsetzend werden spezielle Nutzungsformen der Basistechnologien betrachtet, insbesondere auf Unified Communication and Collaboration (UCC) basierende Systeme und spezielle TK-Systeme (Videokonferenzsysteme, Kontaktcenter, Händlersysteme und Alarmierungssysteme), Social Networks and Social Media sowie Outsourcing und Cloud-Computing. Ergänzend zu den Basistechnologien und den hierauf basierenden TK-Bereichen wird die Integration von drahtlosen und mobilen Kommunikationssystemen in derartige Systeme betrachtet (siehe Abbildung 1).

Die Kapitel 3 bis 9 vertiefen die Beschreibung der genannten Basistechnologien und TK-Bereiche insbesondere durch Darstellung der in derartigen Systemen vorhandenen Sicherheitsmechanismen, analysieren die spezifische Gefährdungslage und stellen auf die Gefährdungslage zugeschnittene Sicherheitsmaßnahmen vor, die insbesondere die Anforderungen eines erhöhten Schutzbedarfs berücksichtigen.

Kapitel 10 ergänzt obige TK-Technologien um die Darstellung von generell zu ergreifenden Sicherheitsmaßnahmen, z. B. die Auslegung der passiven Netzinfrastruktur bei erhöhtem Schutzbedarf.

Ein mit den Systemen vertrauter Leser kann die Beschreibung des jeweiligen sicherheitstechnischen Basiswissens überspringen und direkt in die jeweiligen Bereiche der Gefährdungsanalyse und Sicherheitsmaßnahmen einsteigen.

Um dem Anwender dieser Technischen Leitlinie die Umsetzung der Maßnahmen zu erleichtern, werden in Teil 2 der Technischen Leitlinie zunächst die relevanten Kommunikationsschnittstellen einer Organisation spezifiziert und die in Teil 1 der Technischen Leitlinie erarbeiteten Sicherheitsmaßnahmen diesen Kommunikationsschnittstellen zugeordnet. Hierauf aufsetzend werden verschiedene repräsentative Einsatzszenarien dargestellt, für die die zu treffenden Maßnahmen im Rahmen eines beispielhaften Sicherheitskonzepts ausgewählt werden.

Zur Unterstützung bei der Beschaffung von TK-Lösungen dient der in Teil 3 der Technischen Leitlinie erarbeitete Beschaffungsleitfaden. Dieser Beschaffungsleitfaden ist in zwei Kapitel unterteilt. Das erste Kapitel spezifiziert die Kriterien für die Auswahl von Komponenten einer TK-Lösung, während das zweite Kapitel Kriterien für die Prüfung von TK-Lösungen und deren Komponenten beinhaltet.

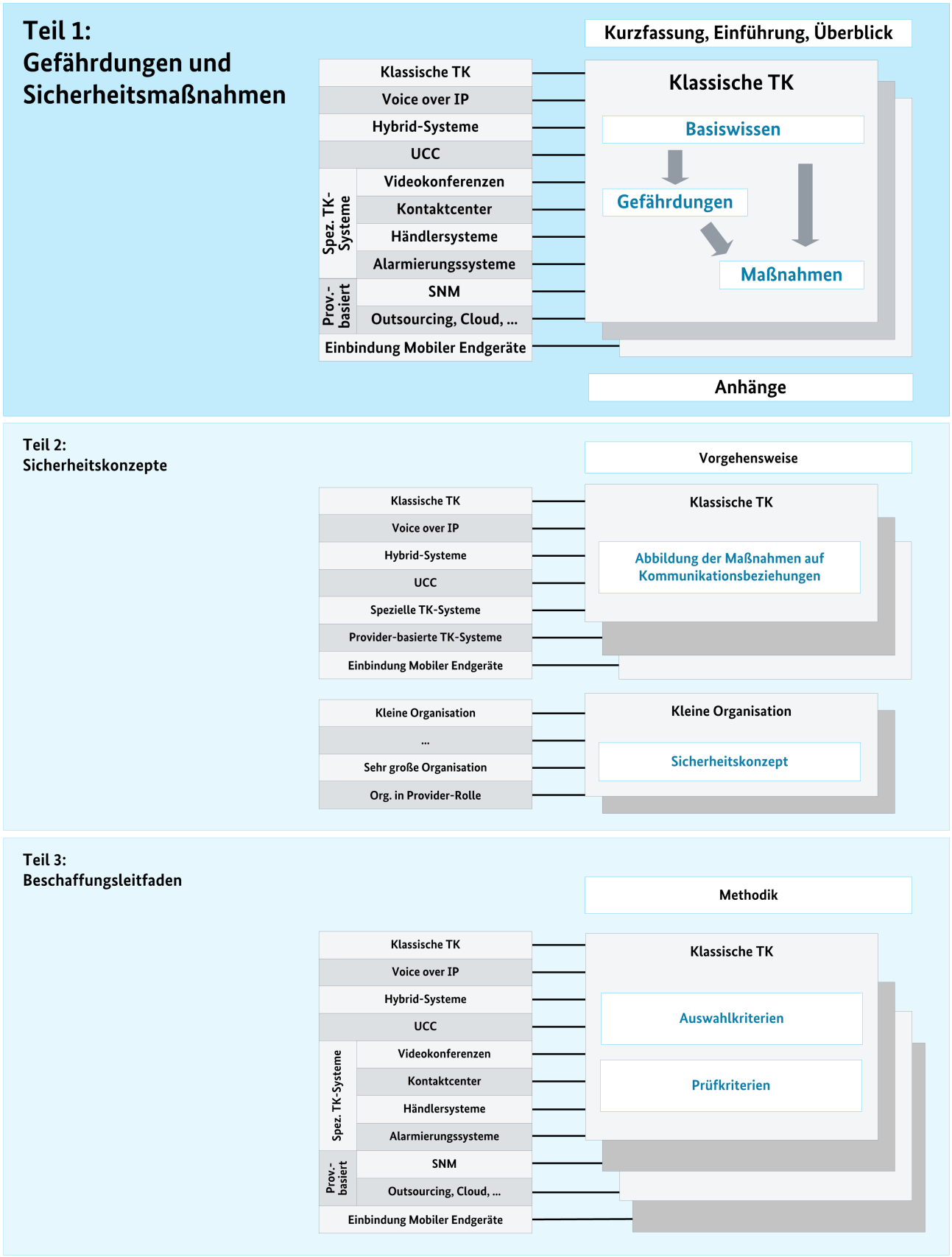


Abbildung 1: Struktur der Technischen Leitlinie

2 Einführung in die Technische Leitlinie

2.1 Navigationshilfe für verschiedene Lesergruppen

Die Technische Leitlinie beschreibt für die verschiedenen Techniken von organisationsinternen Telekommunikationssystemen mit erhöhtem Schutzbedarf in Teil 1 detailliert die technischen Grundlagen, Gefährdungen und Maßnahmen, ordnet in Teil 2 die Maßnahmen potenziellen Kommunikationsbeziehungen der Organisationen zu und erläutert die Umsetzung der relevanten Maßnahmen für repräsentative Beispielszenarien und spezifiziert in Teil 3 Auswahlkriterien und Prüfkriterien zur Beschaffung.

Die Technische Leitlinie adressiert damit alle Lesergruppen, vom Entscheider über den IT-Architekt bis zum Auditor. Jedoch sind nicht alle Detailausführungen für jede Lesergruppe gleich relevant:

- Grundsätzlich sind für eine bestimmte Lesergruppe nur die Technologien relevant, die in der jeweiligen Organisation genutzt werden. Beispielsweise sind Kapitel 3 „Klassische Telekommunikationstechnik“ und Kapitel 5 „Hybrid-Anlagen“ nicht relevant für Organisationen, die ausschließlich Voice over IP einsetzen.
- Weiterhin sind für den Leser bei der Zusammenstellung der zu betrachtenden Leitlinienanteile nur die Aspekte des jeweils abzusichernden Lebenszyklus (Planung, Beschaffung usw.) interessant. Beispielsweise sind Teil 2 „Sicherheitskonzepte“ und Teil 3 „Beschaffungsleitfaden“ nicht zwingend für Administratoren und Betreiber eines Telekommunikationssystems, sondern nur die Kapitel „Basiswissen, Gefährdungen und Maßnahmen“ in Teil 1 für die eingesetzten Technologien.
- Die Kapitel zur Beschreibung der technischen Grundlagen dienen dazu, ein einheitliches Basiswissen zum Verständnis der behandelten Technologien herzustellen. Abhängig vom Vorwissen des jeweiligen Lesers bieten diese Kapitel nicht generell neue Informationen.

Die folgende Tabelle gibt einen Überblick über die Kapitel der Technischen Leitlinie, die für die unterschiedlichen Anwender bevorzugt relevant sind.

Lesergruppe	Relevante Abschnitte der Technischen Leitlinie
Nicht-technische Entscheider	Teil 1: Kapitel „Kurzfassung des Gesamtdokuments“
Technische Entscheider	Teil 1: Kapitel „TK-Systeme und Technologien im Überblick“ Teil 1: Je individuell eingesetzter Technik Kapitel „Zusammenfassung“
IT-Planer, IT-Architekt, IT-Sicherheitsverantwortlicher	Teil 1: Je individuell eingesetzter Technik Kapitel „Basiswissen, Gefährdungen und Maßnahmen“ Teil 2: Alle Kapitel Teil 3: Je individuell eingesetzter Technik Auswahl- und Prüfkriterien
Technischer Beschaffer	Teil 1: Kapitel „TK-Systeme und Technologien im Überblick“ Teil 1: Je individuell eingesetzter Technik Kapitel „Zusammenfassung“ Teil 3: Je individuell eingesetzter Technik Auswahl- und Prüfkriterien
Administrator, Betreiber	Teil 1: Je individuell eingesetzter Technik Kapitel „Basiswissen, Gefährdungen und Maßnahmen“
Auditor	Teil 1: Je individuell eingesetzter Technik Kapitel „Basiswissen, Gefährdungen und Maßnahmen“ Teil 2: Alle Kapitel Teil 3: Je individuell eingesetzter Technik Auswahl- und Prüfkriterien

Tabelle 1: Navigationshilfe für verschiedene Lesergruppen

2.2 Grundschutz als Ausgangsbasis

Unabhängig von der Technologie und Größe einer TK-Infrastruktur für eine Organisation darf ein Mindest-Sicherheitsniveau nicht unterschritten werden. Hiermit wird verhindert, dass ein fahrlässiger Umgang die grundsätzlich zu wahrenden Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit verletzt.

Entsprechende Anforderungen finden sich unmittelbar in der klassischen Telefonie, lassen sich aber auch auf moderne TK-Infrastrukturen übertragen. Beispiele sind:

- Ein Kommunikationspartner muss sich prinzipiell darauf verlassen können, dass die Inhalte eines Informationsaustauschs nicht ohne Weiteres unberechtigten Dritten zugänglich sind.

  Eine Abwehr gezielter Versuche zum Abhören von Telefonaten ist damit noch nicht verbunden, sehr wohl aber die Vermeidung von Nachlässigkeiten wie Nutzung der Freisprechmöglichkeit eines Telefons in einem öffentlich zugänglichen Bereich oder das achtlose Liegenlassen von Faxnachrichten mit vertraulichen Inhalten zu laufenden Geschäftsvorgängen bzw. behördlichen Verfahren.

- Auch sind Kontaktinformationen wie Telefonnummern mit einer grundlegenden Sorgfalt zu behandeln, die einen unberechtigten Zugriff Dritter ausschließt. Eine Ausnahme hiervon bilden nur solche Telefonnummern, die ohnehin öffentlich zugänglich sind. Beispiel hierfür ist die Rufnummer einer Telefonzentrale, die im öffentlichen Telefonbuch, in einem öffentlichen Behördenverzeichnis oder an ähnlicher Stelle mit Billigung des Nummerninhabers jedermann zugänglich gemacht worden ist.

- Des Weiteren ist eine grundlegende Mindestverfügbarkeit sicherzustellen.

  Totalausfälle der TK-Infrastruktur innerhalb normaler Bürozeiten beispielsweise sind als anormal anzusehen, eine Nichtverfügbarkeit zu solchen Zeiten, etwa als Folge von Änderungen an der zentralen Anlage, ist zu vermeiden. Ein Wegfall der Möglichkeit zum Telefonieren zu externen Rufnummern, z. B. durch Ausfall des Zugangs zum öffentlichen TK-Netz (Public Switched Telephone Network, PSTN),

sollte innerhalb üblicher Bürozeiten ebenfalls nicht auf die zentrale Telefonielösung zurückzuführen sein.

Das Erreichen eines so geforderten Mindestniveaus bzgl. der Sicherheitsgrundwerte Vertraulichkeit, Integrität und Verfügbarkeit ist nicht Schwerpunkt der folgenden Ausführungen. Ein solches grundlegendes Sicherheitsniveau entspricht vielmehr dem Schutzbedarf „normal“. Seine Erreichung ist vorrangig Gegenstand der vom BSI veröffentlichten IT-Grundschutz-Kataloge (siehe [BSI GSK-2013]). Die Konformität zu den darin an einem betrachteten Standort einer Organisation eingesetzten Technik passenden Bausteinen und Maßnahmen wird im Weiteren als Ausgangsbasis vorausgesetzt.

Sofern im Rahmen des vorliegenden Dokuments und insbesondere in den szenarienbezogenen Empfehlungen (siehe Teil 2 der Technischen Leitlinie) anteilig Maßnahmeninhalte erwähnt werden, die bereits vom Grundschutz abgedeckt sind,

- soll dies die Unverzichtbarkeit solcher Maßnahmen unterstreichen, bzw.
- sollen gezielt Erläuterungen und Hinweise zur Auslegung solcher Maßnahmen gegeben werden, um eine solche Maßnahme szenariengerecht abzurunden bzw. den Boden für Erreichung des Sicherheitsniveaus für erhöhten Schutzbedarf optimal zu bereiten.

2.3 Telekommunikationssysteme und Technologien im Überblick

Schützenswerte Kommunikation findet in Unternehmen und Behörden auf vielfältigen Kanälen statt, die weit über die reine Sprachkommunikation via Telefon hinausgehen (siehe Abbildung 2). Die Spannbreite der genutzten Kommunikationsmedien reicht von der klassischen Telefonie, über Videotechnologie bis hin zu Instant Messaging (IM). Durch Unified Communications (UC) werden diese zahlreichen Medien in einer einheitlichen Infrastruktur und einer einheitlichen Anwenderschnittstelle für den Büro-Einsatz verschmolzen. Die tiefe Integration in die Arbeitsumgebung des Anwenders soll die Arbeit erleichtern und effizienter gestalten.

Abbildung 2: Organisationsinterne Telekommunikationssysteme

Hierdurch bewegen sich heutige Kommunikationslösungen in einem Spannungsfeld zwischen vielen angrenzenden IT-Themengebieten, die zusätzliche Auswirkungen auf die Sicherheit und Vertraulichkeit der Kommunikation haben können. Werkzeuge für die verbesserte Zusammenarbeit und die Prozessoptimierung, wie etwa Portallösungen und Dokumentenmanagementsysteme (DMS), finden sich hier ebenso wie Soziale Netzwerke und Soziale Medien als Kanal für die Kommunikation mit externen Teilnehmern. Zudem beeinflussen Trends wie zunehmende Consumerization und Bring Your Own Device (BYOD) die Applikations- und Endgerätelandschaft in Unternehmen und Behörden.

Neben der massenhaft im Einsatz befindlichen Kommunikationstechnik für Büroumgebungen werden zudem zahlreiche Spezialanwendungen – beispielsweise Kontaktcenter, Händlersysteme oder Alarmierungslösungen – an die Kommunikationsinfrastruktur angebunden. Über all diese Systeme erfolgt oft eine vertrauliche und schützenswerte Kommunikation zwischen Anwender und Systemen.

Ein wesentlicher Aspekt von modernen Kommunikationslösungen ist, dass Kommunikation nicht nur organisationsintern, sondern insbesondere über Vertrauensgrenzen hinweg ermöglicht wird. Die klassische Anschaltung an das öffentliche Telefonnetz (via Integrated Services Digital Network, ISDN) weicht zunehmend der Amtsanbindung mittels IP-Anlagenanschluss. Auch der multimediale Amts-anschluss, also eine audio-, video- und datenfähige Vernetzungsplattform für externe Teilnehmer mit standardisierter Kundenschnittstelle, materialisiert sich zusehends. Welche Rolle öffentliche Cloud-

Dienste wie Unified Communications as a Service (UCaaS) in diesem Zusammenhang spielen werden, ist noch nicht abschließend beantwortet.

Angesichts immer komplexerer Technologien und Systemabhängigkeiten zieht mancher IT-Entscheider das Outsourcing des Lösungsbetriebs in Betracht. Neben klassischen Managed Services werden zunehmend auch Cloud-Ansätze wirtschaftlich attraktiv. Ob Kommunikationslösungen nun aber in der Public Cloud oder am Standort (on premises) betrieben werden – die zugrunde liegenden Technologien zur Virtualisierung und Automatisierung der Dienstbereitstellung haben massive Auswirkungen auf die technischen Eigenschaften und den Betrieb von Kommunikationslösungen.

All diese Faktoren beeinflussen die Sicherheit, Integrität und Verfügbarkeit der internen und externen Kommunikation von Organisationen. Im Folgenden soll daher ein Überblick über die hiermit verbundenen Technologien und ihren Einfluss auf die Sicherheit gegeben werden.

2.3.1 Klassische Telekommunikationstechnik

Bei klassischer Telekommunikationstechnik handelt es sich um Systeme, welche auf analogen und digitalen Übertragungsverfahren sowie leitungsvermittelnden Techniken basieren. Für den Anschluss von Teilnehmern an das öffentliche Netz werden in der Regel Doppelader-Kupferleitungen als Übertragungsmedium genutzt, im Falle von digitaler Technologie seltener auch Glasfaserkabel. Analoge Kommunikationstechnik stellt sogenannte a/b-Schnittstellen zum Anschluss von Endgeräten und Peripherieeinheiten bereit. Diese unterstützen im Wesentlichen:

- Sprach- bzw. Datenübertragung mit einer Bandbreite von 3,1 kHz (300 Hz bis 3,4 kHz)
- Endgerätespeisung mit Gleichspannung
- Signalisierung (Anrufsignalisierung, Rufnummernübertragung, Wahlverfahren, usw.)

Die Anwendungsbereiche von analogen Schnittstellen umfassen den Anschluss von Telefonendgeräten, Gegensprechanlagen, Faxgeräten, Installationen gemäß Digital Enhanced Cordless Telecommunications (DECT) und Modems zur Datenübertragung. Auch Sonderlösungen wie Alarm-Server oder Feuerwehr-Informations-Tableaus (FIT) werden häufig über analoge Schnittstellen realisiert.

Klassische digitale Kommunikationstechnik verwendet Zeitmultiplexverfahren (Time Division Multiplex, TDM) zur Modellierung von Sprach-, Daten- und Signalisierungskanälen. Der internationale Standard Integrated Services Digital Network (ISDN) findet neben seiner Hauptanwendung im öffentlichen Festnetz auch als Teilnehmerschnittstelle in organisationsinternen Installationen Anwendung. Innerhalb des ISDN-Referenzmodells wurden Standardprotokolle wie Digital Subscriber System No. 1 (DSS1) und Q-Interface Signalling Protocol (QSIG) implementiert, um herstellerübergreifend eine Kommunikation zwischen Anlagen zu ermöglichen. Zusätzlich wurden von den Herstellern verschiedene proprietäre Netzwerkprotokolle implementiert. Diese ermöglichen bei der Vernetzung von Nebenstellenanlagen und am Teilnehmerendgerät die Bereitstellung von herstellerspezifischen Leistungsmerkmalen. In der Regel sind solche proprietären Protokolle mit Produkten anderer Hersteller nicht kompatibel. Digitale Kommunikationstechnik erweitert den Leistungsumfang analoger Technik um mindestens folgende Merkmale:

- digitale Sprachkodierung mittels Pulse Code Modulation (PCM)
- Trennung von Steuer- und Nutzdatenkanälen
- Bereitstellung mehrerer Sprach- bzw. Nutzdatenkanäle
- erweiterte Leistungsmerkmale
- integrierte Datendienste

Der primäre Anwendungsbereich digitaler Schnittstellen ist die Anbindung von Telefonendgeräten, die Amtsanbindung, die Vernetzung von Nebenstellenanlagen und die Anbindung von Sonderlösungen wie z. B. Fax-Servern.

Auch in Zeiten, in denen Voice over IP (VoIP) die verfügbaren Kommunikationsprodukte dominiert, ist klassische Telekommunikationstechnik noch weit verbreitet. Insbesondere kommt der klassischen Kommunikationstechnik als Schnittstelle im Bereich von Bestands- und Sonderlösungen weiterhin Bedeutung zu.

Durch das leitungsvermittelnde Prinzip ist klassische Kommunikationstechnik auf den ersten Blick weniger Gefährdungen ausgesetzt als die paketvermittelnde Kommunikationstechnik Voice over IP. Um ein Gespräch abhören zu können, bedarf es beispielsweise des physischen Zugriffs auf eine der Teilnehmerleitungen, eine der betroffenen Nebenstellenanlagen oder eine an der Übertragung beteiligte Vermittlungsstelle. Doch den physischen Zugriff auf diese Leitungen und Systeme zu verhindern, ist nicht immer einfach. Zudem ist eine Ende-zu-Ende-Verschlüsselung von Sprache nur über teure, proprietäre Zusatz-Hardware zu realisieren. Eine flächendeckende Absicherung der Sprachkommunikation ist somit kostenintensiv und kann nur für kleine Teilnehmergruppen bereitgestellt werden. Zur Bereitstellung von erweiterten Leistungsmerkmalen wie Computer Telephony Integration (CTI) findet zudem häufig eine Kopplung mit IP-basierten Systemen statt. Somit werden klassische Telefonanlagen vermehrt den Gefährdungen von IP-Netzen exponiert.

Kapitel 3 beschreibt klassische Telekommunikationstechnik, ihre Anwendungsbereiche sowie die zugehörigen Gefährdungen und Sicherheitsmaßnahmen.

2.3.2 Voice over IP

Seit der Entwicklung erster Grundlagen in den frühen neunziger Jahren des letzten Jahrhunderts und der ersten Spezifikation des Real-Time Protocol (RTP) sowie des ITU-Standards H.323 hat sich die Übertragung von Sprache über das Internet Protocol (IP) nahezu flächendeckend ausgebreitet. Voice over IP ist heute der De-facto-Standard der Sprachkommunikation.

Die wesentliche Eigenschaft von VoIP ist die paketvermittelte Übertragung. Hierzu wird Sprache anhand von Analog-Digital-Wandlern erfasst, auf Basis eines sogenannten Codecs (von „Code“/„Decode“) digital kodiert und dann in Form einzelner Datenpakete via IP übertragen. Dieser Nutzdatenstrom wird dabei auf Basis von RTP zwischen den Kommunikationspartnern übertragen. Die Signalisierung bildet einen zweiten separaten Kommunikationsweg, der über mehrere vermittelnde Instanzen hinweg geroutet und interpretiert wird. Für die Signalisierung haben zwei Standards weite Verbreitung gefunden:

- die Protokollsuite H.323 der International Telecommunications Union (ITU)[1]
- das Session Initiation Protocol (SIP) und das zugehörige Session Description Protocol (SDP) der Internet Engineering Task Force (IETF)

Während die Protokolle der H.323-Suite restriktiver spezifiziert wurden und einen größeren Umfang von Leistungsmerkmalen bieten, gilt SIP als das flexiblere und offenere Protokoll. Gerade die Flexibilität des SIP-Standards hat zu einem sehr hohen Verbreitungsgrad geführt, sodass sich SIP heute gegenüber H.323 durchgesetzt hat. Die Offenheit führte allerdings auch dazu, dass eine Vielzahl von Leistungsmerkmalen herstellerspezifisch implementiert wurde und der herstellerübergreifende Funktionsumfang sehr begrenzt ist. Sowohl SIP als auch H.323 werden auch bei der Vermittlung anderer Echtzeitmedien, insbesondere Video eingesetzt. Sie bilden damit eine wesentliche Grundlage für Unified Communications.

Durch die Verwendung von IP-Netzen zur Übertragung von Informationen wird die Kommunikation einer Vielzahl von IP-spezifischen Gefährdungen ausgesetzt. Somit ist VoIP im Vergleich zu klassischer, leitungsvermittelter Kommunikation stärker exponiert. Aufgrund der Protokollstrukturen, der offenen Architekturen und der Bereitstellung auf standardisierten IT-Plattformen lassen sich jedoch viele Standard-IT-Sicherheitsmechanismen mit vergleichsweise geringem Aufwand auf die Echtzeit-kommunikation übertragen. Hierdurch kann VoIP-Kommunikation in aller Regel kostengünstiger und effektiver geschützt werden als klassische Telefonie.

1 Technische Normen, Standards, und Empfehlungen für alle Gebiete der Telekommunikation werden in der ITU-Abteilung ITU-T (ITU Telecommunication Standardization Sector, bis 1993 Comité Consultatif International Téléphonique et Télégraphique, CCITT) erarbeitet.

Kapitel 4 beschreibt die Eigenschaften VoIP-basierter Kommunikationssysteme, ihre Anwendungsbereiche sowie die zugehörigen Gefährdungen und Sicherheitsmaßnahmen.

2.3.3 Hybrid-Anlagen

Hybrid-Anlagen stellen eine Kombination aus einer klassischen TDM-basierten Telekommunikationslösung (siehe Kapitel 2.3.1) mit einem VoIP-System (siehe Kapitel 2.3.2) dar. Mit einer Hybrid-Anlage können klassische digitale und analoge Telefonie und VoIP gleichzeitig betrieben werden, was eine Migration erleichtern kann. Damit vererben sich aber sowohl die Gefährdungen der klassischen Telekommunikationstechnik (siehe Kapitel 3.2) als auch von VoIP (siehe Kapitel 4.2) auf eine Hybrid-Anlage, was bei der Anwendung von Sicherheitsmaßnahmen berücksichtigt werden muss.

Kapitel 5 beschreibt die Eigenschaften von Hybrid-Anlagen, ihre Anwendungsbereiche sowie die eventuell über die zugrunde liegenden Basistechnologien hinausgehenden Gefährdungen und Sicherheitsmaßnahmen.

2.3.4 Unified Communications and Collaboration

Unified Communications beschreibt die Zusammenführung verschiedener Kommunikationsmedien auf eine IP-basierte Infrastruktur sowie auf eine einheitliche und weit verbreitete[2] Nutzerschnittstelle. Neben VoIP sind wichtigsten UC-Dienste die folgenden:

- Instant Messaging: Kurznachrichten und Chats zwischen zwei oder mehr Kommunikationspartnern
- Presence: Anzeige von und Routing anhand von Erreichbarkeits- und Ortsinformationen des Anwenders
- Unified Messaging: Einheitliches Postfach für verschiedene Nachrichtenformate, z. B. Fax, Sprachnachrichten und Short Message Service (SMS)
- Desktop-Video: Videokommunikation am PC-Arbeitsplatz oder mobilen Endgerät mit zwei oder mehreren Teilnehmern. Vermehrt auch mit Integration von Videokonferenzraum- und Telepräsenz-Systemen.
- Mobilintegration: Mobiler Zugriff auf UC-Dienste und Integration des mobilen Endgerätes in die interne Kommunikationslösung.
- Webkonferenzen, Desktop- und Application-Sharing: Konferenz zur Präsentation und Freigabe von Informationen sowie gemeinsamem Arbeiten an Dokumenten. Beinhaltet Werkzeuge für die Zusammenarbeit, verschiedene integrierte Kommunikationsdienste (Audio, Video, Instant Messaging) und die Möglichkeit zur Fernsteuerung von Anwendungen. Häufig werden Web-Clients für externe Teilnehmer unterstützt.
- Anwendungsintegration: Integration von Kommunikationsmöglichkeiten in die Arbeitsplatzanwendungen des Mitarbeiters. Erweiterung klassischer CTI-Funktionen um weitere Medien.

Die Unterstützung der Zusammenarbeit in Teams durch Kommunikationswerkzeuge wird unter dem Oberbegriff Collaboration zusammengefasst. Hierunter fallen verschiedene Techniken zur gemeinsamen Arbeit an Dokumenten und zur technisch gestützten Bearbeitung von Geschäftsprozessen. Der Fokus liegt auf der Unterstützung von räumlich und zeitlich verteilt arbeitenden Teams, wie sie in einer globalisierten Wirtschaft immer häufiger vorkommen. In der Regel handelt es sich um zentral bereitgestellte webbasierte Werkzeuge und Applikationen. Collaboration umfasst im Sinne dieser Technischen Leitlinie Technologien aus dem Bereich Portallösungen, Dokumentenmanagementsysteme, Business Process Integration (BPI) und Sozialer Software für den organisationsinternen Einsatz (Social Business Software). Collaboration bedient sich unter anderem der Integration von Kommunikationskanälen in Applikationen und Portale, weshalb es häufig in Zusammenhang mit UC eingesetzt wird und dann als Unified Communications and Collaboration (UCC) bezeichnet wird. Eine Abgrenzung zu Unified Communications ist daher nicht einfach

2 In der Fachliteratur auch häufig ubiquitär genannt.

zu treffen. Beispielsweise ließen sich Webkonferenzen sowohl dem Thema Unified Communications als auch dem Bereich Collaboration zuordnen. Da diese Technische Leitlinie Sicherheitsaspekte der Kommunikation fokussiert, werden hier vorrangig die Schnittstellen für die Integration von Unified Communications und Collaboration betrachtet.

Die verschiedenen Medien, welche mit Unified Communications zusammengeführt werden, sind den Gefährdungen IP-basierter Kommunikation ausgesetzt. Wie auch im Fall von VoIP wirken sich die paketvermittelte Übertragung und der Einsatz des SIP-Protokolls für die Signalisierung direkt auf die Gefährdungslage von Unified Communications aus. Durch die enge Verzahnung mit Applikationen und IT-Diensten ergeben sich zudem vielfältige Schnittstellen, welche durch Angreifer ausgenutzt werden können. Doch auch hier kann durch die IP-basierte Technik und die Anwendung von IT-Standardverfahren zur Verschlüsselung und Authentisierung ein Sicherheitsgewinn erzielt werden.

Da bei Collaboration insbesondere die Dokumentenzusammenarbeit im Fokus steht, sind sämtliche organisationsintern bearbeiteten Inhalte von den zugehörigen Gefährdungen betroffen. Die Gefährdungen im Bereich Collaboration ergeben sich in erster Linie aus der zentralen Bereitstellung von Inhalten über die räumlichen Grenzen der Organisation hinaus und aus dem Einsatz von Webtechnologie. Durch die zentrale, zeitunabhängige Bereitstellung sind potenziell größere Datenmengen einer Gefährdung ausgesetzt, als dies bei temporärer (Echtzeit-)Kommunikation der Fall ist. Im Gegensatz hierzu eröffnen die zentrale Datenhaltung, das strukturierte Rechtesystem für den Zugriff auf Inhalte und der Einsatz von erprobten Standard-Sicherheitsmechanismen auch viele Chancen für die Verbesserung der Informationssicherheit.

Kapitel 6 beschreibt die Eigenschaften von Lösungen für Unified Communications und Collaboration, ihre Anwendungsbereiche sowie die zugehörigen Gefährdungen und Sicherheitsmaßnahmen.

2.3.5 Spezielle TK-Systeme

Die betrachteten TK-Technologien Klassische Telekommunikationstechnik, Voice over IP und Unified Communication and Collaboration bilden die Basis für weitere TK-Lösungen, die in unterschiedlichsten Anwendungsbereichen die reine Telekommunikation ergänzen:

- Videokonferenzen (Kapitel 2.3.5.1)
- Kontaktcenter (Kapitel 2.3.5.2)
- Händlersysteme (Kapitel 2.3.5.3)
- Alarmierungssysteme (Kapitel 2.3.5.4)

2.3.5.1 Videokonferenzen

Seit der Einführung von ISDN im öffentlichen Festnetz gewinnt die audiovisuelle Kommunikation innerhalb und außerhalb von Organisationen an Bedeutung. Die Übertragung von Videodatenströmen über IP-basierte Netze hat für einen signifikanten Qualitätssprung im Vergleich zu ISDN-basierter Technologie geführt. Heutige Videokonferenzsysteme ermöglichen die gleichzeitige Teilnahme vieler, gar hunderter Raumsysteme an Konferenzen mit hochauflösenden Videoformaten mit HD (High Definition, 720p) oder sogar Full HD (1080p).

Videokonferenzraumsysteme werden für organisationsinterne, standortübergreifende oder organisationsübergreifende Besprechungen verwendet. Neben Video und Audio übertragen aktuelle Systeme auch Präsentationsinhalte. Raumbasierte Videokonferenzsysteme haben aufgrund der vergleichsweise hohen Investitionen einen hohen, aber bei weitem nicht flächendeckenden Verbreitungsgrad erreicht. Oftmals ist der Nutzerkreis auf die Leitungsebene der Organisation begrenzt. Hieraus ergibt sich häufig ein erhöhter Schutzbedarf für die transportierten Inhalte und somit für das Videokonferenzsystem.

Durch die Integration von Desktop-Video durchdringen Videokonferenzen nun zunehmend breitere Anwenderschichten. Die Anwendungsfälle sind vielfältig und reichen von der Punkt-zu-Punkt-

Kommunikation zwischen zwei Mitarbeitern einer Organisation über Massenkonferenzen zur Übertragung wichtiger organisationsinterner Ereignisse bis hin zur Unterstützung von Service-Technikern durch mobile Videokonferenzen.

Videokonferenzsysteme erzeugen vielfältige Gefährdungen für die Informationssicherheit. Teils ergeben sich diese aus den technischen Grundlagen der IP-basierten Kommunikation, teils aus dem Einsatzzweck und der Konfiguration von Videoraumsystemen. So stellen beispielsweise öffentlich erreichbare Videoraumsysteme, bei denen eine automatische Rufannahme konfiguriert ist, eine Gefährdung für alle im jeweiligen Konferenzraum besprochenen Inhalte dar. Durch die Verbreitung von Desktop-Video ergeben sich zudem vielfältige Probleme in Hinblick auf den Datenschutz. So ist der Einsatz von Desktop-Video mit kaum zu kontrollierendem Kamerablickwinkel in Großraumbüros unter Datenschutzgesichtspunkten sehr kritisch zu sehen.

Kapitel 7.1 beschreibt die Eigenschaften von Videokonferenzsystemen, die jeweiligen Anwendungsbereiche sowie die zugehörigen Gefährdungen, Sicherheitsmaßnahmen und -konzepte.

2.3.5.2 Kontaktcenter

In nahezu jeder Organisation ist die Kommunikation mit externen Kommunikationspartnern (Kunden, Partnern, Bürgern) ein wesentlicher Bestandteil des Tagesgeschäfts. Hierzu werden häufig zentrale Anlaufstellen eingerichtet, in denen Sachbearbeiter (Agenten) ein- und ausgehende Kommunikation abwickeln und Schichtleiter (Supervisoren) die Kommunikation steuern und überwachen. In der Vergangenheit wurde als Medium ausschließlich die Sprachkommunikation verwendet, weshalb diese zentralen Anlaufstellen unter dem Begriff Call Center geführt wurden. Mit dem Vormarsch des World Wide Web (WWW), der E-Mail und der Einführung von Unified Communications in Unternehmen und Behörden erweitert sich die Zahl der Kommunikationskanäle, weshalb man heute allgemeiner vom Kontaktcenter spricht.

Die Anwendungen sind vielfältig und unterscheiden sich in eingehende (engl. inbound) und ausgehende (engl. outbound) Kommunikation. Wesentliche Anwendungen für Kontaktcenter sind:

- Inbound-Anwendungen
  - Kunden- oder Bürgerinformation
  - Bestell- und Auftragsannahme
  - Störungsmanagement
  - Beschwerdemanagement
- Outbound-Anwendungen
  - Marktforschung
  - Meinungsforschung
  - Akquisition
  - Kundenpflege

Ein Beispiel für ein organisationsinternes Inbound-Kontaktcenter ist der User Help Desk der Organisations-IT, welcher Bestell- und Auftragsannahme sowie Störungs- und Beschwerdemanagement in sich vereint.

Neben der Telefonie werden in modernen Kontaktcentern viele weitere Medien eingesetzt. Insbesondere sind heute folgende Medien relevant:

- E-Mail
- SMS
- Fax
- Webchat

- Instant Messaging & Presence
- Video
- Webkollaboration

Kontaktcenter-Produkte automatisieren hierbei die Behandlung von eingehender Kommunikation durch die Verteilung der Kommunikationsanfragen auf Agentengruppen und einzelne Agenten. Hierbei ist insbesondere die Automatic Call Distribution (ACD) bzw. die automatische Verteilung multimedialer Kontaktaufnahmen sowie das E-Mail Response Management von besonderer Wichtigkeit. Systeme für Interactive Voice / Video Response (IVR) unterstützen die Kanalisierung und das zielgerichtete Routing eingehender Kontaktanfragen. Ausgehende Kampagnen werden durch Datenbank-gestütztes Anwählen von Rufnummern oder Kontaktadressen durch Wählautomaten (Dialer) realisiert. Moderne Prädiktionsverfahren gewährleisten hierbei eine gute Auslastung und geringe Wartezeiten des Agenten-Personals.

Moderne Kontaktcenter-Lösungen ermöglichen eine hohe Arbeitseffizienz der Agenten durch die tiefe Integration in weitere Applikationen und Datenbestände. Wichtige Applikationen und Systeme sind unter anderem:

- Kontaktverzeichnisse und Datenbanken
- Web-Anwendungen (z. B. Rückrufbitte-Formular, „Web Callback“)
- Customer Relationship Management (CRM)
- Enterprise Resource Management (ERM)
- Ticketsysteme
- Qualitätsmanagement-Systeme (QMS)
- Risikomanagement-Systeme (RMS)
- Personaleinsatzplanung (PEP)
- Sprachaufzeichnungs-Systeme
- Auswertungs- und Berichts-Systeme (Reporting)

Die Steuerung der ein- und ausgehenden Kommunikationskanäle und die Integration von diversen Applikationen und Systemen in Kontaktcenter-Lösungen bedingt eine Vielzahl von Schnittstellen und Integrationspunkten. Sie bilden potenzielle Schwachstellen für einen Angriff auf die Datensicherheit. Zudem werden in Kontaktcentern anwendungsbedingt vielfach personenbezogene und schützenswerte Daten verarbeitet. Ein Beispiel sind Kontaktcenter im Bereich des Versicherungs- und Gesundheitswesens. Vertrauliche Patientendaten werden an der Kundenschnittstelle ausgetauscht und durch den Agenten zur Weiterverarbeitung in diversen Systemen erfasst.

An diesem Beispiel wird ersichtlich, dass Kontaktcenter-Systeme vielfach eines besonderen Schutzes bedürfen. Die Gefährdungen im Bereich Kontaktcenter sowie die zugehörigen Sicherheitsmaßnahmen und Sicherheitskonzepte zur Absicherung der Datenhaltung, der Integrationsschnittstellen und der eigentlichen Kommunikation wird in Kapitel 7.2 beschrieben.

2.3.5.3 Händlersysteme

Händlersysteme (verbreitet auch Trading-Systeme) stellen speziell für die Arbeitsweise von Händlern optimierte Kommunikationsfunktionen zur Verfügung. Händlersysteme sind speziell für den Handel an schnelllebigen Märkten, z. B. Energiebörsen, konzipierte Kommunikationslösungen. Ihre Verbreitung beschränkt sich daher vorwiegend auf den Finanzsektor, den Energiemarkt und Händler an Rohstoffbörsen.

Die Kernfunktion klassischer und aktueller Trading-Systeme ist die Bereitstellung einer hohen Anzahl von gleichzeitig schaltbaren Telefonleitungen (teils auch Standleitungen), zwischen denen der Händler an seinem Arbeitsplatz schnell umschalten bzw. wechseln kann. Während in frühen Lösungen dem Händler

sogar ein Telefon je (analoge) Leitung am Arbeitsplatz bereitgestellt wurde, hat die digitale Kommunikationstechnik längst die Anschaltung einer Vielzahl von Sprachkanälen auf ein oder mehrere (Spezial-)Telefone möglich gemacht. Heutige VoIP-basierte Lösungen stellen diese Leistungsfähigkeit rein auf Software-Basis zur Verfügung, wodurch sich sowohl ausgefeilte Spezial-Hardware als auch PC-basierte Handelsarbeitsplätze flexibel bedienen lassen.

Zusätzlich zur reinen Punkt-zu-Punkt-Kommunikationen über statisch oder dynamisch geschaltete Leitungen sind auch Audiokonferenzen ein wesentlicher Bestandteil der Kommunikation. In Trading-Umgebungen werden oft höchste Anforderungen an die schnelle und effektive Einrichtung von dauerhaft oder ad hoc eingerichteten Konferenzen gestellt.

Neben der Sprachkommunikation haben auch andere Medien im Handelsbereich an Bedeutung gewonnen. Hierzu zählen insbesondere E-Mails und Instant Messages, aber auch Videofunktionen finden vereinzelt Verwendung.

Sowohl an die Sprachkommunikation als auch an andere Kommunikationsformen im Handelsumfeld werden von Seiten der Regulierungs- und Wettbewerbsbehörden vielfältige Anforderungen gestellt. Hierunter fällt unter anderem die revisionssichere Aufzeichnung und Archivierung von Kommunikation.

Die Sensibilität der über Händlersysteme ausgetauschten Informationen sowie die Vielzahl der rechtlichen Anforderungen resultiert in einem sehr hohen Schutzbedarf. Die Gefährdungen und Sicherheits-maßnahmen sowie Sicherheitskonzepte sind weitestgehend deckungsgleich mit klassischen und VoIP-basierten TK-Anlagen sowie mit den jeweiligen UC-Diensten. Jedoch ergeben sich einige spezifische Aspekte, welche in Kapitel 7.3 erläutert werden.

2.3.5.4 Alarmierungssysteme

Insbesondere in sicherheitskritischen Bereichen und in Produktionsbereichen werden traditionell Alarmierungssysteme an Telekommunikationsanlagen gekoppelt. Sie dienen zur Unterstützung sicherheitskritischer Anwendungen, z. B. der Evakuierung von Personal im Falle eines Unfalls in der Produktion (z. B. Chemieindustrie) oder der Abschaltung von Maschinen im Fall, dass der bedienende Mitarbeiter das Bewusstsein verliert (Totmannschaltung). Unter den Oberbegriff Alarmierungssysteme im Sinne dieser Studie fallen z. B. Personensucheinrichtungen (PSE), Totmannschaltungen, Alarm-Server oder Feuerwehr-Informations-Tableaus (FIT) sowie alle weiteren Systeme, welche zur Alarmierung im Notfall geeignet sind.

Diese Systeme verfügen neben Schnittstellen zur klassischen Telekommunikation, z. B. zum Alarmieren von Mitarbeitern via Telefonanruf oder zur Lokalisierung von Mitarbeitern via DECT-Endgerät, über verschiedene Schnittstellen zur IT- und Kommunikationsinfrastruktur.

Die Gefährdungen, denen Alarmierungssysteme ausgesetzt sind, sind auf technischer Ebene vergleichbar mit denen anderer Kommunikationssysteme. Die Risiken aller Basistechnologien, die klassische, die IP-basierte, die stationäre oder die mobile Kommunikationstechnik, akkumulieren sich. Aufgrund der speziellen, sicherheitskritischen Anwendungsgebiete von Alarmierungssystemen ergibt sich hier eine Gefährdungslage mit einer besonderen Brisanz.

Kapitel 7.4 beschreibt die wesentlichen Eigenschaften von Alarmierungssystemen, die jeweiligen Anwendungsbereiche sowie die zugehörigen Gefährdungen und Sicherheitsmaßnahmen.

2.3.6 Provider-basierte TK-Dienste

Die bisher beschriebenen organisationsinternen TK-Dienste werden in vielen Organisationen durch die Nutzung von externen TK-Diensten ergänzt, die von einem Provider bereitgestellt und betrieben werden (siehe Kapitel 2.3.6.1).

Zusätzlich können die organisationsinternen TK-Dienste vollständig oder teilweise zu einem Dienstleister ausgelagert werden, z. B. Outsourcing, Application Hosting (siehe Kapitel 2.3.6.2).

Die hier betrachteten Service Provider, die ausschließlich Dienste bereitstellen, sind abzugrenzen von Dienstleistern, die Netzverbindungen bereitstellen (engl. Network Provider). Network Provider werden im Rahmen der Technischen Leitlinie nicht als Kommunikationsendpunkte betrachtet.

2.3.6.1 Soziale Netzwerke und Soziale Medien

Die Begrifflichkeiten Soziale Netzwerke (engl. Social Networks) und Soziale Medien (engl. Social Media) umfassen insbesondere Webplattformen zur Vernetzung von Anwendern und zur Kommunikation zwischen Anwendern sowie zur Bereitstellung von nutzererzeugten Inhalten. Soziale Netzwerke und Medien bieten zudem häufig Möglichkeiten zur Echtzeitkommunikation zwischen Teilnehmern sowie zum kooperativen Arbeiten an Inhalten. Die Grenzen zu Unified Communications und Collaboration (siehe Kapitel 6) sind somit fließend.

Im Sinne dieser Studie umfassen Soziale Netzwerke und Soziale Medien ausschließlich öffentlich zugängliche Plattformen (z. B. Facebook, LinkedIn, Xing) und deren Integration in Unified-Communications- und Collaboration-Lösungen, während organisationsintern bereitgestellte Social Business Software dem Bereich Collaboration zugeordnet wird.

Öffentliche Soziale Netzwerke finden im Bereich der Organisationskommunikation verschiedenste Anwendungen. Die wesentlichen Anwendungsszenarien sind:

- Datenquelle für Kontaktverzeichnisse
- Außendarstellung und Kundenkanal der Organisation
- organisationsübergreifende Kommunikation (Föderation)
- Informationsquelle für Organisationsanwendungen

Durch die zentrale Bereitstellung als öffentlicher Cloud-Dienst, die abweichende datenschutzrechtliche Lage am Betriebsstandort des Dienstes, die Interessenslagen der Betreiber sowie den Mangel an Kontrolle über die eingesetzten Sicherheitsmechanismen sind Soziale Netzwerke und Medien vielfältigen Gefährdungen ausgesetzt. Um dem entgegenzutreten, muss daher insbesondere eine exakte Abgrenzung der Einsatzgebiete und der Schnittstellen innerhalb der Organisation vorgenommen werden. Zudem benötigt man organisationsinterne Richtlinien zum Umgang der Mitarbeiter mit diesen öffentlichen Plattformen.

Kapitel 8.1 beschreibt die Eigenschaften von Sozialen Netzwerken und Medien, die jeweiligen Anwendungsbereiche sowie die zugehörigen Gefährdungen und Sicherheitsmaßnahmen.

2.3.6.2 Outsourcing, IP-Centrex, Cloud Computing und UC as a Service

Moderne TK-Infrastrukturen und -Dienste sind oft von einer erhebliche Komplexität geprägt. Es stellt sich daher für die Telekommunikation (genauso wie für andere IT-Bereiche) oft die Frage, ob der Betrieb solch komplexer Infrastrukturen selbst geleistet werden kann und ob dies wirtschaftlich ist. Insbesondere in IT-fernen Branchen und Fachgebieten liegt die Überlegung nahe, den Betrieb einzelner oder aller TK-Dienste durch externe Dienstleister realisieren zu lassen. So soll durch Skaleneffekte, die der Dienstleister durch den Betrieb einer Vielzahl von Kundenlösungen realisieren kann, eine höhere Wirtschaftlichkeit erzielt werden. Die Auslagerung vormals selbsterbrachter Dienstleistungen wird dabei als Outsourcing bezeichnet. Mit dem allgemeinen Outsourcing von IT-Diensten hat auch das Outsourcing von TK-Diensten an Popularität gewonnen. Viele IT-Dienste werden heutzutage als sogenannte Cloud Services am Markt angeboten. Die wesentlichen Eigenschaften einer Cloud sind

- die geteilte Nutzung einer gemeinsamen Infrastruktur durch mehrere Kunden bzw. Mandanten,
- die weitgehende Automatisierung des Betriebs und der Provisionierung,
- die Virtualisierung zur Abstraktion von der darunterliegenden Hardware-Plattform,
- die hochgradige Standardisierung von Diensten,
- das flexible, nutzungsbasierte Preismodell sowie

- ein potenziell niedriger Grad an Interaktion mit dem Betreiber, z. B. durch Selbstbedienungsportale.

Durch die vier erstgenannten Aspekte unterscheidet sich eine Cloud-Lösung essenziell von bis dato üblichen "hosted" (von engl. beherbergt) Angeboten. Bei diesen handelt es sich meist um dedizierte Systeme je Kunde, welche nicht derart automatisiert, virtualisiert und standardisiert sind wie ein Cloud-Angebot.

Zu unterscheiden sind Public Clouds und Private Clouds. Eine Public Cloud bezeichnet dabei Cloud Services, die ein externer Dienstanbieter über das Internet zur gemeinsamen Nutzung durch die Kunden bereitstellt. Demgegenüber steht die Private Cloud, bei der dem Kunden eine dedizierte Infrastruktur zur Verfügung bereitgestellt wird, entweder in den eigenen Rechenzentren des Kunden ("on premises") oder in den Rechenzentren des Cloud-Anbieters.

Im Bereich der VoIP gibt es IP-Centrex als Outsourcing-Modell. Bei IP-Centrex stellt der Anbieter den Dienst Telefonie und die damit verbundenen Leistungsmerkmale netzseitig zur Verfügung. Im Gegensatz zu klassischen ISDN-basierten Centrex-Lösungen wird die Telefonanlage auf Basis von IP betrieben. Der Netzübergang in das öffentliche Festnetz wird durch den Provider sichergestellt. Der Vorteil einer solchen Lösung ist, dass innerhalb der Gebäude nur ein Kabelnetz, nämlich das IP-Netz, betrieben werden muss und der Kunde keinerlei eigene Systeme betreiben und warten muss. Viele IP-Centrex-Lösungen werden heute unter dem Oberbegriff Cloud vermarktet, auch wenn es sich in Wirklichkeit um klassische gehostete Systeme handelt.

Bei Unified Communication as a Service (UCaaS) werden die grundlegenden Funktionalitäten ebenfalls von einem Cloud-Anbieter in seinem Rechenzentrum betrieben. Der Zugriff auf die entsprechenden Dienste erfolgt ebenfalls über die Internetverbindung. Außerdem werden die Nutzer- und Anwendungsdaten auf Servern des Cloud-Anbieters gespeichert, sodass im eigenen Rechenzentrum hierzu keine Kapazität vorgehalten werden muss.

Mittlerweile haben sich verschiedene Anbieter von Cloud-basierten Diensten im Bereich Unified Communications etabliert. Diese Dienste versprechen verschiedene Vorteile:

- potenzielle Kostenersparnis
- weitreichende Flexibilität in Bezug auf die räumliche Verteilung der Anwender
- kurze Zeiträume für Implementierung und Inbetriebnahme
- hohe Skalierbarkeit
- einfache Einrichtung und Bedienung durch webbasierte Administrationsoberflächen

Jedoch gibt es gerade in Bezug auf die Sicherheit einige Aspekte, die zu beachten sind: Datensicherheit, Zugriffsbeschränkungen und Verfügbarkeit.

Das Thema Datensicherheit ist besonders relevant, wenn schützenswerte Daten nicht mehr im eigenen Rechenzentrum, sondern beim jeweiligen Anbieter gespeichert sind. Der genaue Speicherort der Daten unterliegt dabei der Verantwortung des Anbieters und entzieht sich meist vollständig der Kontrolle des Kunden. Dies hat zur Folge, dass sensible Daten außerhalb Deutschlands gespeichert werden könnten und sich somit der in Deutschland gültigen Rechtslage entziehen. Es gelten vorrangig nationale Gesetzgebungen zur Herausgabe von Anwenderdaten desjenigen Landes, in dem die Daten gespeichert sind. So unterliegen beispielsweise Daten in US-amerikanischen Rechenzentren und ggf. sogar generell Daten bei Diensten US-amerikanischer Unternehmen dem Patriot Act.

Zudem obliegt die Sicherung der Daten in vielen Fällen nicht mehr dem Kunden, sondern dem Dienstbetreiber. In der Praxis bedeutet dies, dass der Kunde keine Handhabe gegen einen unberechtigten Zugriff durch Dritte hat. Dieser Zugriff könnte durch den Anbieter selbst oder – im Falle einer unzureichenden Sicherung der Infrastruktur durch den Anbieter – auch durch einen externen Angreifer erfolgen.

Des Weiteren muss die Frage der Verfügbarkeit von Diensten und Daten gestellt werden. Fallen nämlich beim Anbieter zentrale Infrastrukturen aus, so kann der entsprechende Dienst nicht genutzt werden. Im Falle von IP-Centrex käme dies dem Ausfall der gesamten Telefonie-Funktion gleich, sofern der Kunde

nicht eine TK-Anlage als Backup vorhält. Der Anbieter muss also die Hochverfügbarkeit des Dienstes aus der Cloud geeignet sicherstellen. Zudem müssen die Netzübergänge des Kunden (Internet- bzw. WAN-Anbindung) hochverfügbar gestaltet sein. Die Netzinfrastruktur zwischen lokaler Netzanbindung und Provider-Rechenzentrum muss eine ausreichend hohe Verfügbarkeit und Dienstqualität aufweisen. Während dies im Wide Area Network (WAN) zumeist in Abstimmung mit dem WAN-Provider realisierbar ist, entzieht sich das öffentliche Internet dem Einfluss von Kunde und Provider.

Kapitel 8.2 beschreibt die wesentlichen Eigenschaften von Outsourcing und Cloud-basierten Diensten, die jeweiligen Anwendungsbereiche sowie die zugehörigen Gefährdungen und Sicherheitsmaßnahmen.

2.3.7 Einbindung Mobiler Endgeräte

Mobile Endgeräte sind aus dem Arbeitsalltag vieler Arbeitnehmer nicht mehr wegzudenken. Durch die Weiterentwicklung von klassischen Mobiltelefonen und Personal Digital Assistants (PDA) zu intelligenten mobilen Endgeräten (sogenannten Smartphones und Tablets) ist der Einsatzzweck nicht mehr nur auf die mobile Sprachkommunikation beschränkt. Möglich machte dies der sukzessive Umbau der Mobilfunknetze von leitungsvermittelten Sprachdiensten hin zu paketvermittelten Datendiensten. Durch das Universal Mobile Telecommunications System (UMTS) und seine Erweiterungen sowie den Nachfolger Long Term Evolution (LTE) hat eine Konvergenz von Sprach- und Datendiensten im Mobilfunk stattgefunden, während gleichzeitig immer höhere Datenraten bereitgestellt wurden.

Heute finden mobile Endgeräte viele Anwendungen im Bereich der Organisationskommunikation. Einige Anwendungsfälle sind:

- mobile Sprachkommunikation
- mobile Videokommunikation und Unified Communications
- mobiler Zugriff auf E-Mails und Groupware-Dienste
- mobiler Zugriff auf Collaboration-Lösungen
- mobiler Zugriff auf Organisationsanwendungen
- ortsabhängige Dienste (Location-based Services)

Die Verbreitung von Smartphones und Tablets und der zugehörigen Applikations-Software bedingt, dass zunehmende auch klassische PC-Arbeitsplätze durch mobile Endgeräte ergänzt oder gar ersetzt werden. Mobile Endgeräte sind somit nicht mehr nur Kommunikationsendpunkte, sondern gleichzeitig vollwertige IT-Clients. Aus dieser Verzahnung und der hohen Mobilität der Endgeräte ergeben sich vielfältige Gefährdungen, denen durch geeignete Sicherheitsmaßnahmen begegnet werden muss. So lassen sich viele Gefährdungen beispielsweise durch den Einsatz von Management-Lösungen (Mobile Device Management, MDM) minimieren. In Bereichen mit erhöhtem Schutzbedarf kann zudem von einem Einsatz von Standard-Endgeräten abgesehen werden. Sogenannte Cryptophones bieten ein erhöhtes Maß an Informationssicherheit durch die generelle Verschlüsselung der Sprach- und Datenkommunikation und der gespeicherten Daten. Während es sich bei Cryptophones in der Vergangenheit oft um vollständige Sonderentwicklungen handelte, wird heute verstärkt auf den Einsatz von ggf. modifizierter Standard-Hardware gesetzt. Diese werden mit speziell gehärteten Betriebssystemen betrieben, die im Gegensatz zu den meisten am Markt verfügbaren Standard-Betriebssystemen keinen Black-Box-Charakter haben und ein deutlich höheres Schutzniveau aufweisen sollen. Zudem wird eine umfassende Sicherheitsarchitektur implementiert, welche unter anderem Maßnahmen wie z. B. die Datenträgerverschlüsselung, ein Sprachverschlüsselungsmodul, Virtual Private Network (VPN) und Management-Funktionen umfasst. Die Sicherheitsarchitektur für Cryptophones umspannt im Regelfall nicht nur die Endgeräte selbst, sondern auch verbundene Systeme und Dienste wie z. B. E-Mail-Server, Dokumentenmanagementsystem oder MDM-Lösung.

In der Kommunikation von Behörden und Unternehmen spielt neben der standortübergreifenden auch die standortinterne Mobilität eine große Rolle. Insbesondere in der Produktion und in Service-intensiven Bereichen werden hier schon seit Jahrzehnten Techniken zur mobilen Kommunikation eingesetzt. Hier spielt DECT und die Nachfolgetechnologie IP-DECT eine große Rolle. Die hiermit verbundenen

Gefährdungen resultieren aus der tiefen Durchdringung von sicherheitskritischen Bereichen mit dieser Technologie, die Funkabdeckung über kontrollierte Bereiche hinaus sowie unzureichende technische Mechanismen zur Verschlüsselung und Authentisierung.

Aus diesen Gründen und aufgrund von Konvergenzbestrebungen in Richtung IP gewinnen Wireless Local Area Networks (WLANs) in vielen Bereichen an Attraktivität. Insbesondere für UCC und andere TK-Anwendungsbereiche, die auf IP-basierten Diensten aufbauen, sind WLAN inzwischen eine wesentliche Zugangstechnik geworden. Da sichere WLAN-Aufbauvarianten seit Jahren im Betrieb bewährt sind, wird zunehmend auch die (Sprach-)Kommunikation auf WLAN portiert. Auch wenn Voice over WLAN (VoWLAN) hohe Qualitätsanforderungen an das WLAN stellt und damit verbunden hohe Kosten verursacht, ist diese Technologie ein sehr wichtiger Bestandteil der mobilen Kommunikation auf dem Campus, der zukünftig eine große Rolle bei der Ablösung von DECT-Infrastrukturen spielen kann. Insbesondere die höheren Datenraten, die neue WLAN-Standards wie IEEE 802.11ac (siehe [IEEE 802.11ac-2013]) bieten, machen WLAN attraktiv für die Übertragung von Multimedia-Kommunikation. Wie auch andere Funknetze sind WLANs gemäß dem Standard IEEE 802.11 vielfältigen Gefährdungen ausgesetzt, die sich auf die darauf betriebenen Dienste vererben. Außerdem haben die aus der IP-Kommunikation vererbten Gefährdungen Auswirkungen für die Sicherheit der drahtlosen Kommunikation.

Speziell im Zusammenhang mit modernen Smartphones und Tablets ist die private Nutzung dienstlicher Geräte sowie die dienstliche Nutzung privater Geräte (Bring Your Own Device, BYOD) in den Vordergrund gerückt. Dies impliziert spezielle Sicherheitsproblematiken, die primär in der Trennung dienstlicher und privater Daten liegen.

Kapitel 10 beschreibt die Eigenschaften von mobilen Plattformen und Techniken zur mobilen Sprachkommunikation, die jeweiligen Anwendungsbereiche sowie die zugehörigen Gefährdungen und Sicherheitsmaßnahmen.

2.3.8 Übergreifende Themen/Techniken

Die Kapitel 3 bis 9 behandeln Anwendungsgebiete, Gefährdungen und Sicherheitsmaßnahmen verschiedenster Kommunikationssysteme und derer Schnittstellen. Für viele dieser Systeme gelten auch übergreifende technische Aspekte, welche für die einzelnen TK-Technologien jeweils systemspezifisch betrachtet werden. Drei dieser übergreifenden technischen Aspekte werden im Folgenden kurz erläutert.

2.3.8.1 Amtsanschlüsse und SIP-Trunking

Die Unternehmens- und Behörden-übergreifende Kommunikation wird klassischerweise über das öffentliche Festnetz für Telefonie oder auch Public Switched Telephone Network (PSTN) abgewickelt. Hierzu werden Amtsanschlüsse durch einen Telefonnetzbetreiber (engl. Carrier) bereitgestellt. Während Amtsanschlüsse für Sprachkommunikation in der Vergangenheit vorrangig auf Basis des Integrated Services Digital Network (ISDN) oder als analoge Anschlüsse realisiert wurden, findet auch hier eine Verschiebung zu IP-basierter Kommunikation statt. Der IP-Anlagenanschluss (umgangssprachlich wegen der Verwendung des Session Initiation Protocol auch SIP-Trunk genannt) stellt den direkten Nachfolger eines ISDN-Anlagenanschlusses in einem konvergenten Netz dar. Während viele Organisationen heute noch klassische ISDN-basierte Anlagenanschlüsse verwenden, führt mit dem bereits vollzogenen Technologie-Wechsel in den Telefonnetzen mittelfristig kein Weg an dem Einsatz von IP-basierten Anlagenanschlüssen vorbei.

Der Amtsanschluss stellt einen Übergang in ein Netz mit anderem Schutzniveau dar. Während die öffentlichen Telefonnetze von vielen fast schon reflexartig als vertrauenswürdig angesehen werden, sind diese in Wahrheit die Quelle vielfältiger Gefährdungen. Zum einen endet die Vertraulichkeit der Kommunikation mit dem Übergang in das öffentliche Netz. Eine Verschlüsselung der Kommunikation ist im Standardumfang nicht verfügbar. Eine Authentisierung von Teilnehmern kann nur auf Basis von manipulierbaren Rufnummern oder Nebenstellenkennungen erfolgen. Zum anderen öffnen sich durch die definierten Abhörschnittstellen für behördliche Intervention und durch den Fremdbetrieb vielfältige Gefährdungen für die Vertraulichkeit der Kommunikation. Diese Gefährdungen der Amtsanschlüsse gelten

zunächst auch für IP-basierte Anlagenanschlüsse. Darüber hinaus sind IP-basierte Anlagenanschlüsse noch den Gefährdungen ausgesetzt, die sie von der zugrunde liegenden IP-basierten Kommunikation erben.

2.3.8.2 Kommunikation über Vertrauensgrenzen

Bei den zuvor beschriebenen Amtsanschlüssen findet eine Kommunikation über Vertrauensgrenzen hinweg statt. Die Kommunikation verlässt das eigene, vertrauenswürdige Netz und somit den direkten Kontroll- und Einflussbereich der Verantwortlichen für die Behörden- und Unternehmens-kommunikation. Aber nicht nur der Übergang in das öffentliche Netz, sondern auch Netzübergänge innerhalb von Organisationen und zu Partnernetzen realisieren Kommunikation über Vertrauensgrenzen hinweg. Ein Beispiel hierfür ist die zentrale Bereitstellung von UC-Diensten durch die zentrale Konzern-IT für ein Konzernunternehmen mit einem Local Area Network (LAN) im Eigenbetrieb. Hier passiert mindestens die Signalisierung, oft aber auch der Inhalt der Kommunikation, die Vertrauensgrenze zwischen eigenem Netz und dem Netz des Dienstbetreibers.

Hier stellt sich die Frage nach der Vertraulichkeit der kommunizierten Inhalte und dem Umgang mit ihnen an diesen Vertrauensgrenzen. Durch Verschlüsselung von Kommunikation und Signalisierung sowie der Authentisierung von Kommunikationsteilnehmern bieten gerade IP-basierte Kommunikationsmedien viele Möglichkeiten, um diesen Gefährdungen zu begegnen. Auch die Segmentierung der Vertrauensbereiche durch Elemente zur Netztrennung und zur Kontrolle der Kommunikation, z. B. Firewalls und Intrusion Prevention Systems (IPS), bietet Chancen zur Erhöhung des Schutzniveaus.

2.3.8.3 Virtualisierung von Server- und Desktop-Systemen

Klassische Telekommunikationslösungen waren oftmals monolithische, rein Hardware-basierte Systeme. Mit dem Einzug von IP-basierter Kommunikation wurden diese proprietären Systeme durch IT-Lösungen ersetzt, welche auf Standard-Server-Infrastrukturen betrieben werden. Parallel zur Netzkonvergenz entwickelten sich hier Verfahren zur Virtualisierung von Netz- und Rechnerinfrastrukturen. Sie abstrahieren von den tatsächlichen physischen Gegebenheiten einer Infrastruktur und ermöglichen hierdurch ein hohes Maß an Flexibilisierung und Automatisierung beim Server-Betrieb. Diese Technologien werden mittlerweile in nahezu allen Anwendungsbereichen der IT und der Kommunikationstechnik eingesetzt und von vielen namhaften Herstellern unterstützt.

Durch die Einführung von Server-Virtualisierung und Netzvirtualisierung entstehen jedoch zusätzliche Gefährdungen, die aus der notwendigen Abstraktionsschicht (Hypervisor, virtuelle Switches usw.) resultieren. Beispielsweise können Server-Instanzen durch Sicherheitslücken in der Virtualisierungsschicht kompromittiert werden. Zudem müssen manche Sicherheitsparadigmen wie z. B. die Zonierung von Netzen in voll virtualisierten Umgebungen neu gestaltet werden.

Zudem wird in vielen Unternehmen und Behörden die Virtualisierung von Arbeitsumgebungen (oder auch Desktop-Virtualisierung) genutzt. Durch den zentralen Betrieb können sich betriebliche und wirtschaftliche Vorteile ergeben. Darüber hinaus wird die Desktop-Virtualisierung auch als Sicherheitsmechanismus zur Entkopplung der Datenhaltung von lokalen Clients eingesetzt.

Problematisch wird die Desktop-Virtualisierung, wenn Kommunikationsdienste am Desktop (z. B. Unified Communications Clients) genutzt werden. Aus Gründen der Performance sollte eine lokale Auskopplung der Mediendaten aus dem Desktop-Virtualisierungsprotokoll stattfinden. Dies hat aber zur Folge, dass auch die Maßnahmen zum Schutz des Medienstromes am lokalen Endpunkt getroffen werden müssen. Derartige Maßnahmen sind aber beispielsweise in einer Thin-Client-Umgebung nicht immer möglich. Die Desktop-Virtualisierung, die an anderer Stelle sicherheitstechnische Vorteile hat, birgt hier also zusätzliche Risiken für die Informationssicherheit.

3 Klassische Telekommunikationstechnik

Unter klassischer Telekommunikationstechnik werden meist Systeme auf Basis des Integrated Services Digital Network (ISDN) bzw. allgemein von Time Division Multiplex (TDM) verstanden. Diese Systeme werden zwar immer seltener und verstärkt durch Voice over IP (VoIP) ersetzt, jedoch bilden sie gerade für Hybrid-Anlagen eine sehr wichtige Migrationsbasis. Außerdem haben wichtige Grundkonzepte moderner Telekommunikationssysteme hier ihre Wurzeln, was sich auch in der Wiederverwendung von Sicherheitsmaßnahmen zeigt.

3.1 Basiswissen

Eine digitale TK-Anlage besteht vereinfacht aus folgenden Komponenten (siehe auch Abbildung 3):

- Das digitale Koppelfeld kann Verbindungen zwischen Ports schalten.
- Die Anschlusseinheiten stellen die Ports bereit.
- Die Steuereinheit hat unter anderem die Aufgabe Rufnummern und Kommandos, die von den angeschlossenen Telefonen gewählt werden, zu analysieren und entsprechende Kommandos an das Koppelfeld zu geben.
- Über die Wartungseinheit erfolgt der administrative Zugriff zur Anlage. Die Wartung kann über ein Wartungsapparat oder einen Personal Computer (PC) erfolgen. Der Wartungszugang für einen PC kann durch eine Telekommunikationsverbindung oder IP-basiert realisiert werden.

Der Anschluss einer TK-Anlage an das öffentliche Telefonnetz (Public Switched Telephone Network, PSTN) erfolgt meist auf Basis von ISDN, d. h. über einen ISDN-Anlagenanschluss. Auch an einem modernen Next Generation Network (NGN), das auf Basis des Session Initiation Protocol (SIP) und Voice over IP (VoIP) operiert, können ISDN-basierte TK-Anlagen angeschlossen werden. Dies erfolgt dann über ein Integrated Access Device (IAD). Ein IAD enthält unter anderem ein Media Gateway, das als Bindeglied für Signalisierung und Datentransport im ISDN und im NGN dient. Details zu VoIP können in Kapitel 4 nachgelesen werden.

Endgeräte können kabelgebunden oder drahtlos an die TK-Anlage angeschlossen werden.

Der kabelgebundene Anschluss an die Ports der TK-Anlage erfolgt je nach System meist digital über einen ISDN S_0-Bus oder über eine systemspezifische Schnittstelle. Grundsätzlich ist auch heute noch für bestimmte Geräte ein analoger Anschluss gängig (z. B. für Fax). Bei der Verbindung über Kabel wird oft eine strukturierte Verkabelung vorgenommen, die gleichermaßen für das Telekommunikationsnetz und das (Ethernet-basierte) Datennetz genutzt wird.

TK-Anlagen mehrerer Standorte innerhalb einer größeren Organisation können über Standleitungen (seltener Wählleitungen) zu einem Verbund vernetzt werden. Für die Kommunikation zwischen den TK-Anlagen werden systemspezifische Protokolle oder das standardisierte QSIG-Protokoll verwendet. QSIG ist eine Abkürzung für die Signalisierung am Q-Referenzpunkt, der eine Schnittstelle für die Kopplung organisationsinterner Vermittlungssysteme darstellt.

Für die drahtlose Anbindung wird auch heute noch meist DECT (Digital Enhanced Cordless Telecommunications) verwendet (siehe Kapitel 9.1.7).

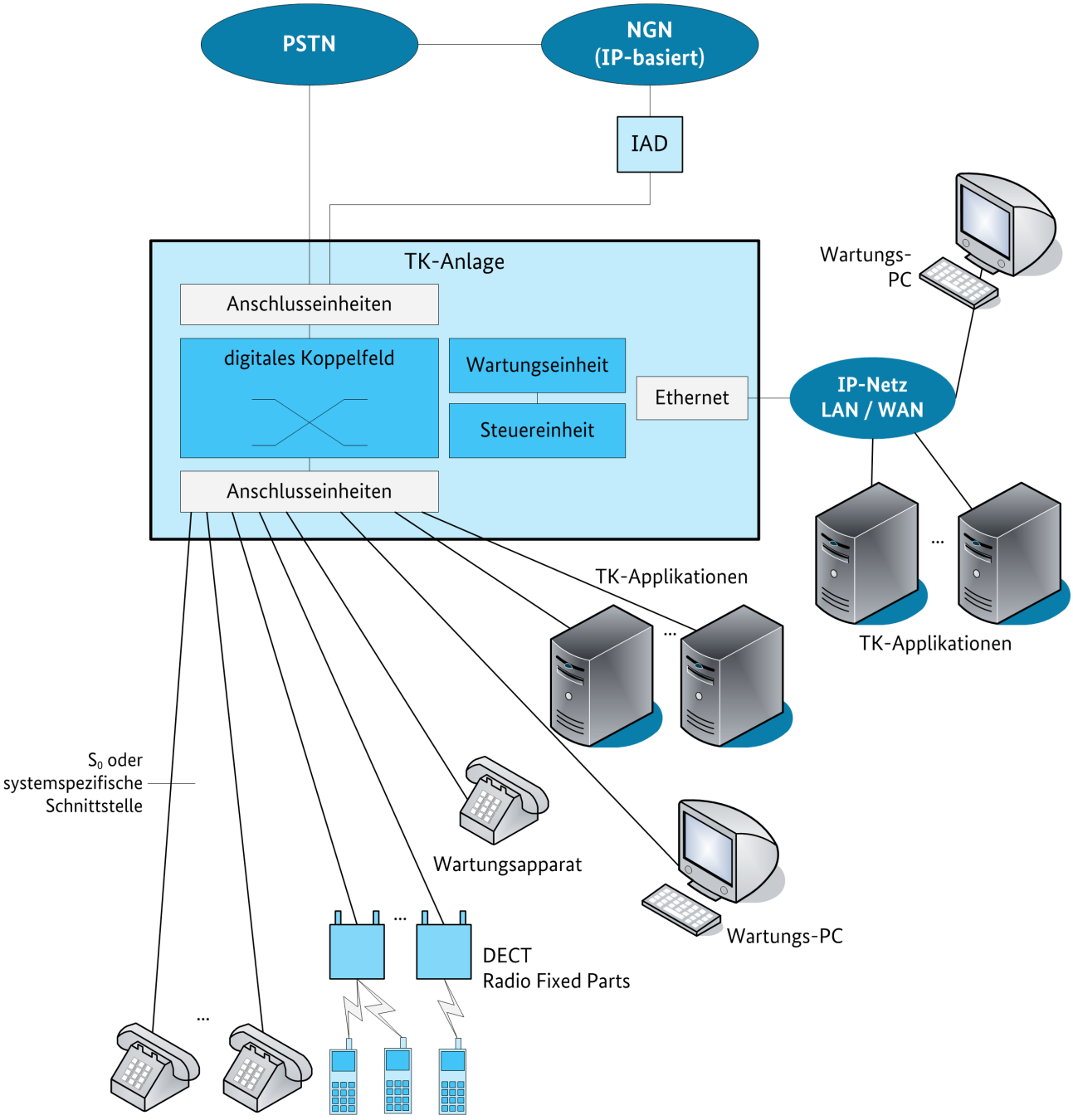


Abbildung 3: Traditionelle TK-Anlage im Überblick

TK-Anlagen verfügen über Fernwartungszugänge für Management-Funktionen. Über diese Zugänge können alle Administrations- und Wartungstätigkeiten sowie sonstige Management-Funktionalitäten wie z. B. Alarmsignalisierung und -bearbeitung abgewickelt werden. Solche Remote-Zugänge sind besonders in TK-Anlagen-Verbünden (Corporate Networks) nützlich und teilweise unverzichtbar.

Der Remote-Zugang kann über folgende Techniken realisiert werden:

- Zugang über dedizierte Management-Ports per Modem
- direkte Einwahl über Direct Inward System Access (DISA)[3]

[3] DISA ist ein Dienst von TK-Anlagen, über den externe Anrufer von außen unter Angabe eines Passcodes auf die TK-Anlage zugreifen können. Dabei erhält der externe Anrufer den internen Wählton und kann darüber wie ein

- Zugang über ein IP-Netz

Für die Absicherung von TK-Anlagen muss besonders beachtet werden, dass verstärkt Anwendungen aus dem Bereich der Computer Telephony Integration (CTI) eingesetzt werden, die eine entsprechende Anbindung der TK-Anlage an eine IT-Infrastruktur erfordern, wie in Kapitel 4 beschrieben.

Zu erwähnen sind in diesem Zusammenhang auch Gegensprechanlagen und Türöffnungssysteme, die als Endgeräte einer TK-Anlage ausgelegt sein können. Bei Betätigen des Klingelknopfes wird eine Verbindung zu einem Telefon hergestellt; sowohl die Gegensprechfunktion als auch die Türöffnung können dann über das Telefon erfolgen. Rein funktional unterscheiden sich solche Gegensprechsysteme nicht von konventionellen Telefonen. Da es sich jedoch um öffentlich zugängliche Apparate handelt, müssen entsprechende Maßnahmen zur Absicherung dieses Zugangs getroffen werden. Dies reicht von der Einschränkung der wählbaren Rufnummern, um einen Gebührenmissbrauch zu vermeiden, bis hin zur Absicherung des Ethernet-Zugangs, um einen direkten Zugriff auf das Netz zu verhindern.

Die Beschreibung der traditionellen TK-Anlagentechnik ist bewusst kurz gehalten, da sich dieser Bereich der Telekommunikationstechnik seit geraumer Zeit nicht geändert hat und eine Vielzahl guter Veröffentlichungen verfügbar ist. Außerdem ist festzustellen, dass Systeme basierend auf VoIP vermehrt die traditionelle ISDN-basierte Telekommunikation bereits verdrängt haben.

3.2 Gefährdungen

Historisch betrachtet ist mit der Digitalisierung die Informationstechnik (IT) in den TK-Anlagenbereich eingezogen. Diese Technik brachte als Begleiterscheinung bei der Einführung ein - im Vergleich zu der derzeit kaum noch genutzten analogen Technik - neues Bedrohungspotenzial mit. Während die analoge Welt primär Gefährdungen auf physikalischer Kommunikationsebene ausgesetzt war, kamen nun Bedrohungen auf logischer Ebene hinzu, deren Komplexität und Gefährdungsgrad mindestens proportional mit dem Einsatz der Informationstechnik gewachsen ist.

Heute ist man übrigens in einer ähnlichen Situation. Die leitungsvermittelnde Telekommunikation ist im organisationsinternen und im öffentlichen Sektor durch paketvermittelnde Techniken mit dem Internet Protocol (IP) als Träger im Wesentlichen abgelöst worden. Im Vergleich gilt dabei die traditionelle digitale TK-Anlage allgemein als eine vergleichsweise sichere Technologie.

Trotzdem sollte man sich gerade für den erhöhten Schutzbedarf die Gefährdungslage traditioneller TK-Anlagen vergegenwärtigen. Dieses Kapitel analysiert die Gefährdungslage für traditionelle digitale TK-Anlagen, die mit leitungsvermittelnder, digitaler Technik auf Basis von ISDN arbeiten.

Für die im Folgenden beschriebene Gefährdungsanalyse ist generell auch der Gefährdungskatalog des Bausteins B 3.401 „TK-Anlage“ der IT-Grundschutz-Kataloge (siehe [BSI GSK-2013]) anwendbar.

3.2.1 Höhere Gewalt

Auf digitale TK-Anlagen treffen allgemein die Gefährdungen durch höhere Gewalt, die in den IT-Grundschutz-Katalogen genannt sind, zu. Dies beinhaltet beispielsweise Gefährdungen durch Feuer, Wasser, Blitzeinschlag, Staub und Verschmutzung.

3.2.2 Organisatorische Mängel

Die Bedrohung der Vertraulichkeit, Verfügbarkeit und Integrität einer digitalen TK-Anlage durch organisatorische und konzeptionelle Mängel ist vergleichbar mit anderen der Kommunikation dienenden IT-Systemen. Dies betrifft beispielsweise die Gefährdung durch einen unbefugten Zutritt zu dem Technikraum, in dem die TK-Anlage installiert ist (siehe Gefährdung G 2.6 „Unbefugter Zutritt zu schutzbedürftigen Räumen“ der IT-Grundschutz-Kataloge, siehe [BSI GSK-2013]). Einige Gefährdungen

interner Teilnehmer mit den Berechtigungen eines internen Apparats Gespräche aufbauen.

besitzen allerdings spezifische Ausprägungen im Kontext von TK-Anlagen. Insbesondere können spezifische Gefährdungen über die Wartungsschnittstelle auftreten. Weiterhin ist bei TK-Anlagen generell der Aspekt des Datenschutzes bei der Aufzeichnung von personenbezogenen Daten zu berücksichtigen.

3.2.2.1 Wartung einer TK-Anlage

G-TK-1 Unzureichende oder fehlende Konzepte für die Wartung einer TK-Anlage

Durch unzureichend abgesicherte Wartungszugänge bestehen vielfältige Gefährdungen. Hier müssen geeignete Konzepte den technischen Aufbau und den Betrieb von Wartungszugängen regeln und sichern.

Besondere Sorgfalt ist für die Einrichtung von Fernwartungszugängen erforderlich, da hier ein Zugang von außen auf die TK-Anlage ermöglicht werden muss. Bei der Wartung einer TK-Anlage durch Externe kann eine besondere Gefährdungslage durch Mängel in sicherheitsrelevanten Teilen von Verträgen oder Service Level Agreements (SLAs) und deren Kontrolle entstehen.

Für IP-basierte Wartungszugänge überträgt sich generell die Gefährdungslage von Systemen, die per IP im Local Area Network (LAN), Wide Area Network (WAN) oder Internet kommunizieren, automatisch auf die TK-Anlage. Dabei besteht außerdem die unmittelbare Gefahr eines unberechtigten Zugangs zur TK-Anlage (ggf. sogar über den Standort hinaus).

G-TK-2 Ungeeignete Aufstellung eines Wartungsapparats

Bei den meisten digitalen TK-Anlagen kann eine Konfiguration der Anlage über ein Systemtelefon oder einen Wartungsapparat erfolgen. Ist dieser Apparat durch eine ungeeignete Aufstellung einem nicht zur Wartung befugten Personenkreis zugänglich, so kann es zu absichtlichen oder unabsichtlichen Konfigurationsänderungen kommen.

G-TK-3 Unzureichende Passwort-Policy für einen administrativen Zugang

Durch unzureichende Regelungen für den regelmäßigen Wechsel und eine angemessene Komplexität von Passwörtern entstehen unmittelbare Gefährdungen:

Leicht zu erratende Default-Passwörter und PINs bilden eine Gefährdung für TK-Anlagen, da sie einen unbefugten Zugriff erleichtern. Dies gilt insbesondere für Wartungs- bzw. Systemtelefone, die in öffentlich zugänglichen Bereichen aufgestellt sind. Dies gilt sinngemäß auch für den Zugang zu PCs, die für die Wartung einer TK-Anlage verwendet werden.

3.2.2.2 Datenschutz und rechtliche Rahmenbedingungen

G-TK-4 Unzureichender Schutz personenbezogener Daten

Für die Rechnungserstellung zeichnen TK-Anlagen in der Regel Verbindungsdatensätze auf, die mindestens Informationen über die gerufene Teilnehmernummer, den Anrufzeitpunkt und die Dauer des Gesprächs enthalten. Hieraus lassen sich Kommunikationsprofile für einzelne Endgeräte bzw. Nutzer ableiten. Verbindungsdaten sind potenziell zumindest für die Zeit ihrer Existenz zugreifbar und müssen vor einem unautorisierten Zugriff geschützt werden.

Als Grundlage wird organisationsübergreifend und im Einvernehmen mit dem Datenschutzbeauftragten meist festgelegt, welche Benutzeraktivitäten aus Sicherheitsgründen überwacht und aufgezeichnet werden sollen und wie Nutzer hierüber zu informieren sind. Durch Mängel in einer solchen Festlegung besteht die Gefahr, über den notwendigen Umfang hinaus personenbezogene Daten aufzuzeichnen und auszuwerten, was neben datenschutzrechtlichen Bedenken zunächst zu einer unnötigen Vergrößerung der Angriffsfläche führt.

Es ist zudem möglich, dass über einen ungeeignet abgesicherten Wartungszugang temporäre Protokolldateien erstellt werden, die z. B. im wenig geschützten Bereich für temporäre Dateien abgelegt werden.

G-TK-5 Verstöße gegen das Urheberrecht

Verstöße gegen das Urheberrecht können im Kontext von TK-Anlagen nicht nur durch den Einsatz von nicht-lizenzierter Software (z. B. für die Wartung) entstehen. Eine zusätzliche Gefährdung entsteht durch den Einsatz urheberrechtlich geschützter musikalischer Werke für Wartemusik (Music on Hold) ohne eine entsprechende Lizenzvergütung an die GEMA (Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte).

3.2.3 Menschliche Fehlhandlungen

Die im Folgenden genannten Gefährdungen sind nicht spezifisch für TK-Anlagen, sie haben jedoch bedingt durch die hohen Schutz- und Verfügbarkeitsanforderungen an Telekommunikationsdienste einen besonderen Stellenwert.

G-TK-6 Unzureichende Prüfung der Identität von Kommunikationspartnern

Die Identität des Kommunikationspartners wird aus Höflichkeitsgründen oft nicht hinterfragt. Dies wird auch beim Social Engineering ausgenutzt (siehe hierzu G 5.42 „Social Engineering“ der BSI IT-Grundschutz-Kataloge, siehe siehe [BSI GSK-2013]).

Diese Bedrohung wird durch das Leistungsmerkmal Rufnummernanzeige begünstigt, da die Anzeige der vermeintlichen richtigen Telefonnummer den Benutzer in Sicherheit wiegt. Dabei kann der Anrufer lediglich ein kurzzeitig unbeaufsichtigtes Endgerät unbefugt verwenden.

G-TK-7 Funktionsstörung oder Ausfall der TK-Anlage durch Fehlkonfiguration

Durch die absichtliche oder unabsichtliche Fehlkonfiguration einer TK-Anlage kann es zu einem Ausfall des Telefoniedienstes kommen. Zum Beispiel können einzelne Anschlüsse durch eine Veränderung der Durchwahl so konfiguriert werden, dass sie von außen nicht mehr erreichbar sind. Wenn nach außen bei einer solchen Störung ein Freizeichen signalisiert wird, kann es einige Zeit dauern, bis eine solche Funktionsstörung bemerkt wird.

G-TK-8 Nachlässigkeiten bei der Verwendung eines PCs für die Administration einer TK-Anlage

Durch Nachlässigkeit bei der Nutzung von PCs, die für die Administration einer TK-Anlage verwendet werden, können Gefährdungen entstehen. Dies gilt insbesondere dann, wenn der PC nicht nur für die Anlagenkonfiguration, sondern auch für andere Zwecke verwendet wird. Beispielsweise können Benutzerwechsel bei solchen PCs eine Gefährdung darstellen. Erfolgen dabei An- und Abmeldevorgänge nicht ordnungsgemäß, können unberechtigte Benutzer Zugang zur Anlage erhalten und sicherheitsrelevante Daten kompromittieren (z. B. die Konfiguration ändern oder personenbezogene Daten einsehen).

3.2.4 Technisches Versagen

Die primäre Funktion von TK-Anlagen wird im Prinzip nur durch technisches Versagen in direktem Zusammenhang mit der Anlage bedroht. Zu diesen Gefährdungen zählen etwa der Ausfall der Stromversorgung, einer Netzkomponente oder ein Defekt der Verkabelung.

Durch die meist geringe Integration mit anderen IT-Systemen sind traditionelle TK-Anlagen zumindest für Basis-Telefoniedienste in der Regel nicht von Ausfällen anderer Infrastrukturkomponenten (z. B. Verzeichnisdiensten) betroffen.

G-TK-9 Software-Fehler

Software-Fehler können auch in TK-Anlagen vorkommen, und mit steigendem Funktionsumfang erhöht sich entsprechend die Wahrscheinlichkeit, von einem Software-

Fehler betroffen zu werden. Für digitale TK-Anlagen wird zwar allgemein eine höhere Stabilität und geringere Fehlerhäufigkeit als für andere IT-Systeme angenommen, jedoch ist die Abdeckung durch Tests seitens der Hersteller nie 100 Prozent. Insbesondere in den Implementierungen von selten genutzten Leistungsmerkmalen können sich Fehler befinden.

G-TK-10 Undokumentierte Funktionen

TK-Anlagen können undokumentierte Funktionen enthalten. Solange diese Funktionen nicht offen gelegt sind, kann nicht ausgeschlossen werden, dass mit ihnen auch Schaden angerichtet werden kann.

Dies ist insbesondere dann problematisch, wenn die undokumentierten Funktionen Sicherheitsmechanismen des Produktes betreffen, beispielsweise den Zugriffsschutz oder die Aufzeichnung von Daten.

Solche Funktionen dienen oft als Hilfsmittel für die System-Entwicklung oder als Hintertür für die Wartung des Systems durch den Hersteller.

3.2.5 Vorsätzliche Handlungen

Die größten Gefährdungen für TK-Anlagen und ihre Nutzung gehen von vorsätzlichen Handlungen aus; dabei hängen Gefährdungen oft zusammen. Beispielsweise können organisatorische Mängel eine vorsätzliche Handlung erleichtern oder sogar erst ermöglichen.

G-TK-11 Abhören von Verbindungen

Für unverschlüsselte Telefongespräche besteht grundsätzlich die Gefahr, dass Angreifer alle Informationen mithören, indem ein Telefonkabel angezapft oder an einer zwischen den Teilnehmern vermittelnden TK-Anlage mitgehört wird. Für TK-Anlagen, die per IAD an die IP-Infrastruktur eines Dienstleisters angeschlossen werden, ist dieses Risiko deutlich erhöht (siehe hierzu auch Kapitel 4).

Weiterhin können unter Umständen auch durch die missbräuchliche Verwendung von Leistungsmerkmalen Gespräche im Kollegenkreis mitgehört werden. Ein Beispiel hierfür ist die Dreierkonferenz: Erhält der Teilnehmer A einen Anruf für den Teilnehmer B, so könnte er, anstatt den Anruf zu übergeben, versuchen, heimlich eine Dreierkonferenz herzustellen. Besitzt Teilnehmer B ein Telefon ohne Display, würde er diese Tatsache nicht bemerken.

Denkbar ist ebenfalls das Mithören von Gesprächen durch das Aktivieren von gesperrten, in Deutschland zum Teil unzulässigen Leistungsmerkmalen. Als ein Beispiel sei hier die Zeugenschaltung erwähnt. Eine derartige Aktivierung erfordert jedoch neben einem Konfigurationszugang zur TK-Anlage genauere Systemkenntnisse.

G-TK-12 Manipulation der Signalisierung

Eine Manipulation einer digitalen TK-Anlage kann grundsätzlich auch über das Einspielen von eventuell modifizierten Signalisierungssequenzen auf einem Signalisierungskanal (Signalisierung über den D-Kanal bzw. über das Signalisierungssystem Nr. 7, SS7) erfolgen. Die Auswirkungen solcher Aktionen können vielfältig sein. Voraussagen über das Verhalten der Software auf bestimmte, z. B. bewusst fehlerhafte Befehlssequenzen sind meist nicht möglich. Es ist auch denkbar, dass undokumentierte Funktionen über diesen Weg aktiviert werden können. Daher ist dies gerade für den erhöhten Schutzbedarf als erhebliches Sicherheitsdefizit anzusehen.

Bei TK-Anlagen, die per IAD an die IP-Infrastruktur eines Dienstleisters angeschlossen werden, erfolgt im Netz des Dienstleisters die Signalisierung über das SIP und erst in dem IAD wird auf die in ISDN verwendete Signalisierung auf dem D-Kanal umgesetzt. Daher vererben sich Gefährdungen von SIP zumindest in einem gewissen Umfang auch auf eine ISDN-basierte TK-Anlage (siehe hierzu auch Kapitel 4). Daher ist hier mit einem erhöhten Risiko der Manipulation der Signalisierung zu rechnen.

G-TK-13 Abhören von Räumen

Über Mikrofone in Endgeräten können grundsätzlich auch Räume abgehört werden. Dabei können zwei Varianten unterschieden werden.

Bei der ersten Variante wird bei intelligenten Endgeräten per Fernsteuerung (z. B. über das öffentliche Netz) das Mikrofon aktiviert.

In der zweiten Variante wird durch die missbräuchliche Verwendung des Leistungsmerkmals „direktes Ansprechen“ in Kombination mit der Option „Freisprechen“ die Funktion einer Wechselsprechanlage realisiert, über die unter gewissen Umständen der entsprechende Raum abgehört werden kann. Im Normalfall wird ein kurzer, einmaliger Warnton bei Aktivierung des Mikrofons abgegeben. Warntöne können aber durch eine entsprechende Konfiguration unterbunden werden. Die Konsequenz ist, dass im Prinzip jeder, der in der Lage ist eine TK-Anlage zu administrieren, jeden Raum, in dem ein entsprechend ausgerüstetes Telefon steht, von jedem Ort innerhalb der Anlage (oder des Anlagenverbundes) abhören kann.

G-TK-14 Missbrauch von Wartungszugängen

Die Möglichkeit eines Missbrauchs von lokalen Wartungszugängen und von Fernwartungszugängen ist mit massivsten Gefährdungen von Vertraulichkeit, Integrität und Verfügbarkeit verbunden. Der entstehende Schaden kann sich vom vollständigen Anlagenausfall über schwerste Betriebsstörungen, den Verlust der Vertraulichkeit aller auf der Anlage vorhandenen Daten bis hin zum großen direkten finanziellen Schaden, z. B. durch Gebührenbetrug, erstrecken.

Durch die mangelhafte Durchsetzung einer Passwort-Richtlinie oder durch eine zu schwache Passwort-Richtlinie kann die PIN für einen Wartungsapparat oder das Passwort für einen Wartungs-PC durch systematisches Raten, d. h. durch eine Wörterbuchattacke, ermittelt werden. Nach Überwindung des Anlagenpasswortes kann ein Hacker dann Zugang zu den Management-Programmen des TK-Systems erlangen.

G-TK-15 Gebührenbetrug

Unter Gebührenbetrug versteht man die missbräuchliche Nutzung einer TK-Anlage mit dem Ziel, die Kosten für geführte Telefonate auf jemand anderen zu übertragen. Entsprechende Manipulationen sind auf verschiedene Weisen durchführbar.

Zum einen kann versucht werden, vorhandene Leistungsmerkmale einer TK-Anlage für diese Zwecke zu missbrauchen. Geeignet hierfür sind beispielsweise aus der Ferne umprogrammierbare Rufumleitungen oder Dial-In-Optionen. Zum anderen können die Berechtigungen so vergeben werden, dass kommende Amtsleitungen abgehende Amtsleitungen belegen können. Auf diese Weise kann bei Anwahl einer bestimmten Rufnummer von außen der Anrufer automatisch wieder mit dem Amt verbunden werden, wobei dies allerdings auf Kosten des TK-Anlagenbetreibers geschieht.

Weiterhin kann auf unterschiedliche Arten wie z. B. durch das Telefonieren von fremden Apparaten, Auslesen fremder Berechtigungscodes (Passwörter) oder Verändern der persönlichen Berechtigungen versucht werden, auf Kosten des Arbeitgebers oder der anderen Beschäftigten zu telefonieren.

G-TK-16 Schadenstiftende Software auf Wartungs-PCs

Durch ein Trojanisches Pferd auf einem für die Wartung und Konfiguration einer TK-Anlage eingesetzten PC oder Notebook kann ein Angreifer an Zugangs-, Konfigurations- oder Verbindungsdaten einer Telefonanlage kommen.

Spyware in Form von Keylogger kann eine Gefährdung der TK-Anlage darstellen, wenn sie auf den eingesetzten Wartungsrechnern installiert ist. Keylogger zeichnen Tastatureingaben auf und übermitteln diese möglichst unbemerkt an den Angreifer. Auf diese Weise kann das Passwort der Management-Schnittstelle einer Anlage in unbefugte Hände geraten und z. B. einen Angriff über die Fernwartungsschnittstelle ermöglichen.

G-TK-17 Verschleierte Identifizierung zwischen Gesprächsteilnehmern

Die verschiedenen Leistungsmerkmale zur Übertragung und Unterdrückung von Rufnummern haben ein grundsätzliches Gefährdungspotenzial, das auch zur Verschleierung der Identität verwendet werden kann.

Beispielsweise kann über das Leistungsmerkmal „CLIP[4] no screening“ neben der netzseitigen Rufnummer des Anrufers noch eine vom Anrufer selbst festgelegte kundenspezifische Rufnummer (z. B. eine Service-Nummer) an den Angerufenen übertragen werden. Diese selbst festgelegte Rufnummer wird von den vermittelnden Anlagen nicht überprüft (no screening). Welche Rufnummer dann am Gerät auf der Empfängerseite angezeigt wird (ggf. sogar beide Rufnummern), ist von den jeweils aktivierten Leistungsmerkmalen, der Art des Anschlusses und der Gerätekonfiguration abhängig.

In diesem Zusammenhang muss darauf hingewiesen werden, dass Telefonnummern nicht als Identifikationsmerkmal für einen Teilnehmer geeignet sind.

3.3 Sicherheitsmaßnahmen

Der Maßnahmenkatalog zur Absicherung von Nutzung und Betrieb von ISDN-basierten TK-Anlagen ist in die folgenden Blöcke aufgeteilt:

- Zentrale Anlage, siehe Kapitel 3.3.1
- Endgeräte, siehe Kapitel 3.3.2
- Netzwerk, siehe Kapitel 3.3.3
- Netz- und Systemmanagement, siehe Kapitel 3.3.4

Grundsätzlich wird die Umsetzung der generell zu ergreifenden Maßnahmen (siehe Kapitel 10) vorausgesetzt.

3.3.1 Zentrale Anlage

Die folgenden Maßnahmen sind schwerpunktmäßig im Bereich der zentralen Anlage umzusetzen, vor allem mit Blick auf die Steuereinheit, den Anschluss an das PSTN und gegebenenfalls einen zum Zwecke der Anbindung an Zusatzlösungen vorhandenen LAN-Anschluss der Anlage. Dabei konzentrieren sich die Maßnahmen auf sichere Konfiguration und sicheren Betrieb der Anlage: Es wird davon ausgegangen, dass bei Neubeschaffungen entsprechend dem Marktangebot in der Regel keine reinen ISDN-basierten TK-Anlagen in die engere Wahl gezogen werden bzw. zur Wahl stehen. Sofern dies ausnahmsweise doch der Fall sein sollte, ist es ratsam, bei der Produktauswahl gezielt auf die Unterstützung der im Weiteren benannten Maßnahmen durch entsprechende technische Funktionalitäten zu achten.

Grundsätzlich sind im Falle erhöhten Schutzbedarfs für ISDN-basierte TK-Anlagen die Maßnahmen sinngemäß umzusetzen, die sich für solchen Schutzbedarf für beliebige Telefonie-Lösungen als systemübergreifende Aspekte anbieten.

Speziell bei einer ISDN-basierten TK-Anlage sind auf diesen Grundsätzen aufbauend folgende Maßnahmen im Bereich der zentralen Anlage selbst bedeutsam:

M-TK-1 Sperrung nicht benötigter oder sicherheitskritischer Leistungsmerkmale

Soweit ISDN-Leistungsmerkmale nicht benötigt werden bzw. bewusst nicht verwendet werden sollen, sind diese zu sperren. Auf diese Weise wird verhindert, dass die Anlage über

4 Unter Calling Line Identification Presentation (CLIP) versteht man die Anzeige der Rufnummer des Anrufers auf dem Gerät des Angerufenen, sofern die rufende Seite dies nicht selbst durch das Leistungsmerkmal Calling Line Identification Restriction (CLIR) explizit unterdrückt.

solche Merkmale unnötig möglichen Angriffen ausgesetzt wird (siehe hierzu auch M-TK-17 „Aktivierung einer Warnung bei Nutzung unsicherer Merkmale“).

Bestimmte (ISDN-)Leistungsmerkmale können zu gezielten Angriffen, insbesondere auf Vertraulichkeit oder Verfügbarkeit, missbraucht werden. Neben der Gefährdung dieser Sicherheitsgrundwerte können im Zuge eines derartigen Missbrauchs außerdem (vom Anlagenbesitzer ungewollte) Anrufgebühren generiert werden. Merkmale mit Missbrauchspotenzial sind vor allem:

- Direktes Ansprechen bzw. automatische Rufannahme ist in Verbindung mit Freisprechfunktionalität des Telefons zum Abhören des Raums missbrauchbar.
- Der Amtszugang birgt bei leicht zugänglichen Apparaten die Gefahr der Nutzung durch Unbefugte für Amtsgespräche mit resultierendem Mehraufkommen an Anrufgebühren.
- Bei einer Rufumleitung kann z. B. durch versehentliche oder böswillige Fehlnutzung die Nichterreichbarkeit des Nutzers eines Telefonanschlusses die Folge sein.
- Dial-In-Möglichkeiten sollten im Endteilnehmer-Umfeld grundsätzlich abgeschaltet werden, da die Nutzung hier nur missbräuchlichen Hintergrund haben kann.
- Export-Merkmale sind zu Angriffen auf Vertraulichkeit nutzbar (z. B. „Zeugenschaltung“ oder „Abhören“).

Für offen zugängliche Geräte sollten derartige Merkmale bei erhöhtem Schutzbedarf in jedem Fall zwingend gesperrt werden. Bei gesichert aufgestellten Endgeräten sollten mindestens die Merkmale, deren Sperrung Angriffe von außen abwehrt (vor allem direktes Ansprechen, automatische Rufannahme, Dial-In), so behandelt werden.

Sofern Endgeräte mit geeigneter Sicherheitsintelligenz eingesetzt werden, kann in Abhängigkeit von der konkreten Risikobewertung zwischen einer vollständigen Deaktivierung solcher Merkmale und einer Sperrung bis zur erfolgreichen Authentisierung am Endgerät abgewogen werden.

Auch sollte im Fall entsprechend intelligenter Endgeräte im Rahmen der produkttechnisch gegebenen Möglichkeiten gezielt eine Konfiguration vorgenommen werden, auf Grund derer eine Warnung erfolgt, sofern sicherheitskritische Merkmale genutzt werden (siehe M-TK-17 „Aktivierung einer Warnung bei Nutzung unsicherer Merkmale“).

Die Abschaltung von nicht benötigten bzw. wegen ihres Missbrauchspotenzials als kritisch eingestuften und daher zur Abschaltung vorgesehenen Leistungsmerkmalen ist so weit wie möglich an der zentralen Anlage vorzunehmen. Bietet diese nur eingeschränkte bzw. nicht ausreichend differenzierte Möglichkeiten, so kann eine Sicherheitskonzeption für die TK-Lösung Konfigurationsvorgaben für die zentrale Angabe gezielt mit entsprechenden Sperreinstellungen auf Endgeräten kombinieren. Voraussetzung für die Maßnahmen-umsetzung ist in einem solchen Fall eine gezielte Beschaffung ausreichend sicherheits-intelligenter Endgeräte, siehe M-TK-16 „Einsatz sicherheitsintelligenter Endgeräte“.

M-TK-2 Schaffung eines zusätzlichen TK-Ersatzanschlusses für Notrufe

Bei Ausfällen im Bereich der zentralen Anlage ist es fraglich, ob an dieser Anlage angeschlossene Telefone noch Notrufe absetzen können. Als Ausweichlösung kann hier ein separater PSTN-Anschluss mit direkt angebundenem Telefon eingesetzt werden. Bei einer Umsetzung dieser Maßnahme ist entsprechend der räumlichen Ausdehnung des betrachteten Standorts auf geeignete Platzierung und Anzahl solcher Telefone und Anschlüsse zu achten.

Die Notrufmöglichkeiten müssen von allen Räumen aus auf ausreichend kurzen Wegen erreichbar sein. Eine einzige zentrale Lösung kann dazu führen, dass Notrufe nicht rechtzeitig abgesetzt werden können, um Schaden zu minimieren bzw. Gefahr für Leib und Leben geeignet abzuwenden.

Die Verkabelung für den TK-Ersatzanschluss sollte auf von der zentralen Anlage separierten Kabelwegen erfolgen.

Selbstverständlich können auch Mobiltelefone für Notrufe verwendet werden. Für den erhöhten Schutzbedarf muss jedoch die im Vergleich zum PSTN geringere Verfügbarkeit von Mobilfunknetzen berücksichtigt werden.

M-TK-3 Katastrophenschaltung

Sofern die ISDN-Anlage eine entsprechende Konfiguration ermöglicht, kann dafür gesorgt werden, dass in Ausnahmesituationen die vorhandenen kommenden und gehenden Leitungen des ISDN-PSTN-Anschlusses bestimmten Telefonie-Endgeräten fest zugeordnet sind.

Hierbei müssen die weiterhin zur Anlagennutzung berechtigten Apparate bedarfsgerecht auf die Organisationseinheiten verteilt werden.

Die Umsetzung dieser Maßnahme bedarf dabei einer kontinuierlichen Pflege: In regelmäßigen Abständen sollte die Festlegung der entsprechenden Zuordnungen inhaltlich überprüft werden. Wegen eines Wechsels von Aufgaben bzw. Umzug des Personals, das an den ursprünglich in die Katastrophenschaltung eingebundenen Apparaten gesessen hat, kann eine Anpassung der Konfiguration an neue Gegebenheiten von Zeit zu Zeit notwendig werden.

Es bietet sich an, diese Thematik in die allgemeine Notfallplanung einzubetten und die entsprechenden aktuell gültigen Festlegungen in den zugehörigen Dokumenten festzuhalten.

M-TK-4 Erhöhter Zutrittsschutz

Bei erhöhtem Schutzbedarf ist es angezeigt, die zentrale Anlage gezielt gegen Zugriff durch Unbefugte auch mit den Mitteln des Zutrittsschutzes besonders zu schützen. Typische Vorkehrung ist dabei die Aufstellung der Anlage in einem Raum nur mit Zugang für das Anlagen-Betriebspersonal.

Es sind Räume zu wählen, die mindestens mit denselben Maßnahmen gegen unbefugten Zutritt gesichert sind wie die Aufstellungsorte kritischer zentraler IT-Systeme.

Sofern die räumlichen Gegebenheiten dies nicht zulassen, empfiehlt sich zumindest die Kombination aus folgenden Punkten:

- Die Aufstellung der Anlage erfolgt in einem Raum, der nur einem eingeschränkten Personenkreis zugänglich ist.
- Die Unterbringung der Anlage erfolgt in einem separaten abschließbaren Schrank.
- Das Schließsystem des Schranks sollte angesichts des erhöhten Schutzbedarfs so ausgelegt sein, dass passende Schlüssel auf das Betriebspersonal der TK-Anlage beschränkt werden können.
- Der Zugang für Externe zur Anlage erfolgt nur unter Aufsicht. Minimum ist dabei die Beaufsichtigung durch Personal, das auf die Unterbindung von nicht vorgesehenen physischen Eingriffen an der Anlage eingewiesen bzw. fallweise über die Notwendigkeit solcher Eingriffe vorab informiert ist. Bevorzugt sollte bei erhöhtem Schutzbedarf die Aufsicht durch Personal erfolgen, das mit der Anlage technisch vertraut ist und so besser beurteilen kann, ob eine vom Externen vorgenommene Änderung an der Anlage unschädlich und auftragsgemäß ist.
- Eine Protokollierung des Aufenthalts im Raum wird durchgeführt. Mindestens protokolliert wird der Aufenthalt Externer (Name, Firma, Zeitraum).

  Ist die Anlage zusammen mit anderem technischen Equipment untergebracht, sodass der Raum für verschiedenes Betriebspersonal zugänglich sein muss, bietet sich bei erhöhtem Schutzbedarf eine Protokollierung jeglicher Anwesenheit im Raum an. Ist der Raum durch

ein entsprechendes elektronisches Schließsystem geschützt, können zu diesem gehörende Protokollierungsfunktionen bei der Umsetzung dieser Vorkehrung hilfreich sein.

M-TK-5 Geeignete Aufstellung der TK-Anlage

Ideal ist eine Aufstellung in einem räumlich separaten Sicherheitsbereich. Die Anforderungen eines erhöhten Zutrittsschutzes lassen sich auf dieser Basis mit minimalem Zusatzaufwand realisieren.

Darüber hinaus ist eine Aufstellung in einer Umgebung wichtig, die durch entsprechende Vorkehrungen den erhöhten Anforderungen an Verfügbarkeit besonders genügt. Dies betrifft die folgenden Infrastrukturaspekte:

- Stromversorgung / Überspannungsschutz
- Klimatisierung / Schutz vor Wasserschäden
- Brandschutz
- Verwendung von Sicherheitstüren und Fenstern
- Einbindung des Raums in eine vorhandene Gefahrenmeldeanlage

Am Aufstellungsort der TK-Anlage sind mindestens dieselben Vorkehrungen zu treffen, die am selben Standort für kritische IT-Systeme realisiert sind (Unterbrechungsfreis Stromversorgung (USV), Klimatisierung, Brandschutz usw.). Jedoch ist eine gemeinsame Nutzung derselben Versorgungslösungen durch die TK-Anlage und durch andere IT-Systeme kritisch zu prüfen (z. B. ggf. zwingende separate USV für die TK-Anlage).

Als Basis für die Einleitung und Koordination notwendiger Maßnahmen kommt gerade bei Großstörungen bzw. in Notfallsituationen einer möglichst unterbrechungsfreien Verfügbarkeit der Telefonie und damit auch der zentralen TK-Anlage besondere Bedeutung zu.

Diesem Umstand sollte durch die genannten Maßnahmen gezielt Rechnung getragen werden. In notfallbedingten Engpass-Situationen ist es außerdem empfehlenswert, der Versorgung der TK-Anlage nochmals erhöhte Priorität einzuräumen (Wiederanlaufreihenfolge bzw. Maßnahmenpriorisierung in Notfällen).

M-TK-6 Sichere Ablage von Kontaktinformationen

Sofern sich der erhöhte Schutzbedarf insbesondere auf den Grundwert Vertraulichkeit bezieht, ist zu prüfen, inwieweit in der TK-Anlage gespeicherte Rufnummern- und sonstige Kontaktinformationen besonders geschützt abgelegt werden können.

Dies betrifft neben gezieltem Schutz vor unberechtigtem Zugriff von beliebigen angeschlossenen Apparaten aus auch den Aspekt eines Zugriffs bei administrativen Tätigkeiten.

M-TK-7 Sicherer Umgang mit Daten zur Anlagennutzung

Daten zur Anlagennutzung werden zu Abrechnungs- und Nachweiszwecken typischerweise protokolliert und zumeist zuerst auf der Anlage selbst gespeichert.

Bei erhöhtem Schutzbedarf sind insbesondere bezüglich Vertraulichkeit, etwa aus Gründen des Datenschutzes, im Rahmen der technischen Möglichkeiten der Anlage die folgenden technischen und organisatorischen Vorkehrungen zu erwägen und geeignet zu kombinieren:

- Löschung derartiger Daten auf der TK-Anlage nach erfolgter vorgesehener Auswertung bzw. nach Auslagerung auf ein Auswertesystem
- verschlüsselte Ablage auf der ISDN-basierten TK-Anlage (z. B. zum Schutz vor Zugriff durch externes Support-Personal)

- verschlüsselte Ablage außerhalb der Anlage

  Je nach Alter der TK-Anlage kann eine Verschlüsselungsoption nicht grundsätzlich als gegeben vorausgesetzt werden. Hingegen ist bei entsprechendem Schutzbedarf im Falle einer Auslagerung von Daten zur Anlagennutzung für das Zielsystem eine verschlüsselte Ablage verbindlich zu fordern.

  Ergänzend zur verschlüsselten Ablage auf einem solchen externen System sind die Vorkehrungen zur Absicherung der zugehörigen Kommunikation zu beachten (siehe Maßnahme M-TK-8 „Absicherung eines LAN-Anschlusses der ISDN-basierten TK-Anlage“).

M-TK-8 Absicherung eines LAN-Anschlusses der ISDN-basierten TK-Anlage

ISDN-basierte TK-Anlagen können einen LAN-Anschluss zur Verfügung stellen, um über diesen administrative Zugriffe oder ein Zusammenspiel mit Telefonie-Mehrwert-Lösungen (z. B. Abrechnungssystem, CTI-Lösung) zu ermöglichen.

Um einer Gefährdung der Anlage über diesen Anschluss entgegenzuwirken, sind mindestens bei erhöhtem Schutzbedarf die folgenden Vorkehrungen umzusetzen:

- Deaktivierung von ICMP[5] für die IP-Software der Anlage
- Abschaltung von Diensten bzw. Funktionen, die über die LAN-Schnittstelle nutzbar sind, aber nicht benötigt werden
- Nutzung gesicherter Kommunikationskanäle zu Drittsystemen
- Bevorzugt ist hier der Einsatz von Verschlüsselung zu sehen. Alternativ ist gezielt eine angemessene Netztrennung zu realisieren.

M-TK-9 Absicherung der Kommunikation über ein IAD

Bei Nutzung eines IAD befindet man sich im Grenzbereich zwischen klassischer Telekommunikation und VoIP-Kommunikation.

Falls ein IAD genutzt wird und der Anschluss an das NGN durch Ethernet erfolgt, sind SIP-basierte schadenstiftende Zugriffe aus einem Provider-Netz oder bei entsprechendem Anschluss der TK-Anlage auch aus dem LAN möglich.

Daher muss der Zugriff auf ein IAD über einen Paketfilter kontrolliert werden. Bei einem erhöhten Schutzbedarf muss hier eine Firewall im Sinne eines dynamischen, zustandsbehafteten Paketfilters verwendet werden (siehe Abbildung 4). Die zusätzliche Funktion eines Intrusion Prevention System (IPS) ist an dieser Stelle ebenfalls vorteilhaft, sofern das IPS auch SIP-basierte Angriffe erkennen kann. Weiterhin kann der zusätzliche Einsatz eines Session Border Controller (SBC, siehe Kapitel 4) in Betracht kommen.

5 Das Internet Control Message Protocol (ICMP) ermöglicht die Übermittlung von Informations- und Fehlermeldungen über IP. Die bekannteste ICMP-Meldung ist der Echo Request („Ping“) mit der die Erreichbarkeit von Netzwerk-Endgeräten geprüft werden kann.

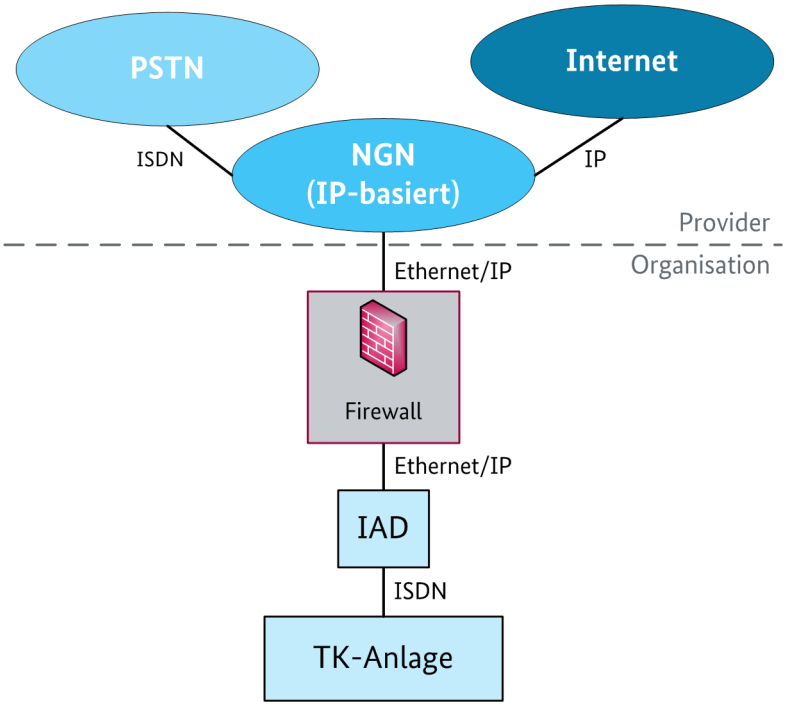


Abbildung 4: Absicherung des Zugriffs über ein IAD mit einer Firewall

3.3.2 Endgeräte

Bei Endgeräten, die im Zusammenspiel mit einer ISDN-basierten TK-Anlage zum Einsatz kommen, kann zwischen folgenden Endgerätetypen unterschieden werden:

- Teilnehmerendgeräte, d. h. vom Telefonie-Nutzer verwendete Endgeräte, insbesondere
  - Faxgeräte
  - Multifunktionsgeräte mit Faxfunktion
  - Kabelgebundene Telefone
  - Drahtlose Telefone
- Endgeräte zu Administrationszwecken, insbesondere
  - Wartungsapparate (Telefone)
  - Wartungs-PCs

3.3.2.1 Faxgeräte und Multifunktionsgeräte mit Faxfunktion

Die nachfolgenden Ausführungen beziehen sich im Wesentlichen auf Faxgeräte und Multifunktionsgeräte mit Faxfunktion, die über eine zentrale (ISDN-)Telefonielösung an das PSTN angeschlossen werden. Im Falle erhöhten Schutzbedarfs wird dringend empfohlen, Faxgeräte möglichst nicht direkt, sondern über eine TK-Anlage an das PSTN heranzuführen, um die sicherheitsrelevanten Möglichkeiten der TK-Anlagenlösung bei der Maßnahmenumsetzung gezielt mit nutzen zu können.

Faxgeräte mit Direktanschluss an das PSTN sollten bei erhöhtem Schutzbedarf bewusst auf notfallspezifische Lösungen beschränkt bleiben.

Werden dennoch Faxlösungen mit direktem PSTN-Anschluss eingesetzt, so sind die nachfolgend benannten technischen Maßnahmen sinngemäß mit den entsprechenden Konfigurationsmöglichkeiten

des Faxgerätes zu realisieren. Es ist bei der Produktauswahl auf Unterstützung entsprechender Funktionalitäten zu achten.

Für Faxgeräte und Multifunktionsgeräte mit Faxfunktion sind bei erhöhtem Schutzbedarf die folgenden Maßnahmen besonders herauszustellen:

M-TK-10 Sperrung bestimmter Fax-Rufnummern

Faxgeräte, die in den Bereich erhöhten Schutzbedarfs fallen, können gezielt gegen Blockieren durch minder wichtigen Eingang (Werbung o. Ä.) geschützt werden.

Andererseits kann es im Sinne der Vertraulichkeit wünschenswert sein, den Faxversand technisch auf bestimmte Empfänger-Nummern zu beschränken, um einen versehentlichen Versand an Dritte zu verhindern.

Beide Aufgaben bedeuten eine gezielte Beschränkung der als Kommunikationspartner eines Faxgerätes in Frage kommenden Rufnummern.

Liegen derartige Detailanforderungen im Rahmen des erhöhten Schutzbedarfs vor, so stehen bei ISDN-basierter Telefonie insgesamt als Basis für die Umsetzung zur Verfügung:

- Sperrung unerwünschter Rufnummern als Kommunikationspartner mit den Hilfsmitteln der ISDN-basierten TK-Anlage (zu bevorzugender Weg)

  Vorteile der Nutzung solcher Funktionalitäten der ISDN-Anlage bestehen in der Möglichkeit zur Übernahme entsprechender, einmal getroffener Festlegungen für mehrere/alle Ports mit Faxanschlüssen sowie im besseren Schutz solcher Einstellungen durch den Zugriffsschutz für die Gesamtkonfiguration der ISDN-Anlage. Weiterhin bleiben derartige Festlegungen auf der zentralen Anlage auch bei notwendigem Austausch eines Faxgerätes erhalten.

- Vornahme entsprechender Einstellungen auf dem einzelnen Faxgerät

  Diese Form der Umsetzung ist etwa notwendig, wenn die Möglichkeiten der zentralen Anlage die notwendigen Festlegungen gar nicht erlauben bzw. eine als notwendig gesehene Unterscheidung nach verschiedenen Faxanschlüssen nicht unterstützen.

- (Gebührenpflichtige) Bereitstellung einer entsprechend konfigurierten Zusatzeinrichtung durch den PSTN-Betreiber

  Dieser Lösungsweg besteht als Alternative, sofern weder TK-Anlage noch Faxgeräte die notwendigen Konfigurationsmöglichkeiten aufweisen. Die anfallenden Gebühren sind sorgsam gegen die Kosten einer geeigneten Ersatzbeschaffung im Bereich Faxgerät abzuwägen (oft nur als Überbrückung bis zu einer vorgesehenen Ablösung der vorhandenen TK-Lösung sinnvoll).

- Bildung einer geschlossenen Benutzergruppe unter ISDN

  Dieser Schritt ist schon wegen der damit verbundenen Gebühren nicht als Alternative zu den vorherigen Umsetzungsformen zu sehen, sondern als Verstärkung bei Bedarf.

  Insbesondere die Sperrung unerwünschter eingehender Faxsendungen wird hier verstärkt: Eine auf der Rufnummer des Senders basierende Annahmeblockierung bleibt wirkungslos, sofern durch die sendende Seite die Übermittlung der Faxnummer unterdrückt oder diese durch eine Sammelnummer maskiert wird.

M-TK-11 Gesicherte Aufstellung der Faxlösung

Bei erhöhtem Schutzbedarf bzgl. Vertraulichkeit und Integrität muss eine Aufstellung so erfolgen, dass die Faxlösung nur dem Personal zugänglich ist, das zum Zugang zu versendender bzw. etwaig auf einem solchen Gerät eingehender Informationen berechtigt ist.

Der entsprechende Zugangsschutz muss konsequent technisch (abschließbare Räume, Sicherheitsbereich mit besonderem Schließ- oder Zutrittssystem) und organisatorisch

(Regelungen zum Verschließen, Zutritt für Dritte nur unter Aufsicht) realisiert sein. Voraussetzung hierfür ist die Festlegung berechtigter Nutzer des jeweiligen Gerätes.

M-TK-12 Verhinderung der Faxfunktionsnutzung bei ungeschützten Multifunktionsgeräten

Werden Multifunktionsgeräte mit Faxfunktion in einer Umgebung genutzt, in der eine gesicherte Aufstellung gemäß der vorigen Maßnahme nicht gewährleistet werden kann, so sollten derartige Geräte keinen Telefonie-Anschluss erhalten. Ergänzend ist die Faxfunktion nach Möglichkeit abzuschalten.

M-TK-13 Sichere Nutzung von Faxgeräten und Multifunktionsgeräten mit Faxfunktion

Bei erhöhtem Schutzbedarf müssen getroffene technische Maßnahmen unbedingt durch angemessene organisatorische Regelungen ergänzt werden.

In Abhängigkeit von den besonderen Risiken, die zur Feststellung des erhöhten Schutzbedarfs geführt haben, sind folgende mögliche Elemente einer solchen organisatorischen Regelung zu erwägen:

- Fertigung von Kopien eingehender Faxnachrichten für längere Aufbewahrung

  Soweit Faxinhalte unter einzuhaltende Verpflichtungen zur längeren Aufbewahrung von Korrespondenz fallen, muss sichergestellt werden, dass die Inhalte nicht durch Verbleichen oder ähnliche materialbedingte Erscheinungen vorzeitig unlesbar werden. Nötigenfalls sind Kopien unter Verwendung geeigneter Technik anzufertigen.

  Sofern vorhanden, kann alternativ zur Papierkopie auch auf Möglichkeiten der (manipulationssicheren) Umwandlung in Dateiform und Archivierung mit Mitteln der Dokumentenverwaltung und elektronischen Archivierung zurückgegriffen werden. Diese elektronische Archivierung muss dann so gestaltet sein, dass die Erfüllung der Aufbewahrungspflichten gewährleistet ist. Die organisatorischen Festlegungen müssen umfassen:

  - Festlegung, für welche Art von Faxeingängen eine Kopie anzufertigen ist
  - Festlegung des Ablaufs, über den eine Kopie erzeugt wird, die im Sinne der Aufbewahrungspflicht dem Original gleichwertig ist
- Umgang mit dem Original nach Anfertigung der Kopie
- (Verpflichtung zur) Nutzung eines vorbereiteten Faxdeckblatts

  Bei erhöhtem Schutzbedarf kann die Anforderung bestehen, sicherzustellen, dass bei ausgehenden Faxsendungen die notwendigen Informationen zum Integritätsnachweis mitgegeben werden und alle notwendigen Inhalte enthalten sind, die der Faxnachricht die notwendige Rechtsgültigkeit verleihen. Hierzu kann ein einheitlich zur Benutzung vorgeschriebenes Faxdeckblatt mit folgenden typischen Inhalten vorbereitet werden:

  - Identifikation des Absenders über Rufnummer des Faxgerätes, Name, Telefonnummer der Person und vollständige Adresse
  - Telefonnummer eines Ansprechpartners bei Übertragungsproblemen
  - Identifikation des beabsichtigten Empfängers mindestens über Rufnummer des Faxgerätes, eventuell zusätzlich über vollständige Anschrift
  - Seitenzahl der Faxsendung einschließlich Faxdeckblatt
  - Gegebenenfalls Dringlichkeitsvermerk mit vorgegebenen Stufungen (möglichst zum Ankreuzen vorbereitet, sofern eine solche Stufung benötigt wird)
  - Unterschrift des Absenders
  - Festgelegte Verfahrensweisen zur telefonischen Begleitung von Faxsendungen

- Bei erhöhtem Schutzbedarf kann es sinnvoll sein, den Faxversand durch telefonische Kooperation mit dem externen Sender bzw. Empfänger zu begleiten. Entsprechende organisatorische Regelungen müssen hierzu beschreiben, wann und wie die folgenden Begleitmaßnahmen ergriffen werden sollen:
  - telefonische Ankündigung einer Faxsendung
  - telefonische Rückversicherung über korrekten Faxempfang durch den Empfänger
  - telefonische Rückversicherung über Authentizität einer empfangenen Faxnachricht durch Rückfrage beim angegebenen Absender

M-TK-14 Sichere Aufbewahrung eingegangener Faxnachrichten

Bei erhöhtem Schutzbedarf bzgl. Vertraulichkeit von Faxnachrichten ist durch geeignete Aufbewahrung sicherzustellen, dass Unbefugte die Inhalte eingegangener Faxnachrichten nicht einsehen können.

Hierbei sind als Phasen der Verbleib im Gerät und die Aufbewahrung nach Entnahme aus dem Faxgerät zu unterscheiden. In diesem Sinne können je nach Einschätzung des Risikos ergänzend zum grundlegenden Zutrittsschutz folgende Vorkehrungen getroffen werden:

- organisatorische Auflage zur umgehenden Entnahme von Faxeingängen, die durch den Absender telefonisch vorangekündigt wurden
- Auflage zum Sperren bzw. Ausschalten des Gerätes bei längerem Verlassen des Raums (technische Gestaltung der Variante Ausschalten dabei: Empfangsbereitschaft nach Wiedereinschalten erst nach ausdrücklichem Entsperren am Gerät)
- Einsatz eines Faxgerätes mit automatischer Eingangskuvertierung

  Ein derartiges Gerät erschwert durch automatische Faltung (nur noch Faxkopf sofort lesbar) und Verschweißung in transparenter Folie den schnellen Zugriff durch Unbefugte. Es handelt sich um eine Ergänzungsmaßnahme zum Schutz in kurzen Momenten, in denen ein im Raum Anwesender unbeobachtet auf das Faxgerät Zugriff hat und Inhalte eingehender Faxnachrichten absichtlich oder zufällig „aufschnappen“ könnte.
- Regelungen zur unmittelbaren und sicheren Ablage von Faxnachrichten

  Derartige Regelungen schreiben vor, welche Formen der Aufbewahrung nach Entnahme aus dem Gerät zulässig sind (z. B. Verschluss im Schreibtisch bis zur endgültigen Bearbeitung).

3.3.2.2 Kabelgebundene Telefone

Die nachfolgend benannten Maßnahmen für den erhöhten Schutzbedarf sind je nach Einstellmöglichkeiten und Leistungsmerkmalen der Endgeräte schwerpunktmäßig am Endgerät, über die TK-Anlage auferlegte Beschränkungen oder eine Kombination aus beidem zu realisieren. Bei manchen Maßnahmen ist die Machbarkeit grundsätzlich von den Einstellmöglichkeiten am Endgerät abhängig. Falls nötig, muss bei erhöhtem Schutzbedarf eine Einführung geeigneter Endgeräte als Vorbereitung vorausgehen, d. h. eine entsprechend gezielte Beschaffung.

Für die zwecks Anbindung der Telefone an die ISDN-Anlage mitgenutzte universelle Verkabelung gelten die für den erhöhten Schutzbedarf systemübergreifend beschriebenen Maßnahmen zur Verkabelung.

Außerdem wird einem erhöhten Schutzbedarf durch folgende Maßnahmen gezielt entsprochen:

M-TK-15 Sicherung von Telefonie-Endgeräten in frei zugänglichen Räumen

Bei der Aufstellung von an eine ISDN-Anlage angeschlossenen Telefonie-Endgeräten in frei zugänglichen Räumen sollten für einen erhöhten Schutzbedarf nur Endgeräte mit eingeschränktem (als unkritisch befundenem) Funktionsumfang eingesetzt werden.

Ist dies nicht möglich, muss das Endgerät durch mechanische Sicherung vor unbefugtem Entfernen geschützt werden. Dies verhindert Diebstähle solcher Geräte. Ein solcher Diebstahl birgt neben dem reinen finanziellen Verlust die Gefahr, dass der lokale Schutz auf dem Apparat gespeicherter sensibler Informationen (z. B. Rufnummern häufig gewählter Teilnehmer) mit Hilfe von Zusatzausstattung des Diebs überwunden werden kann. Auch kann ein Diebstahl dazu dienen, das Telefon für Angriffe auf die Vertraulichkeit zu präparieren (Einbau von Abhöreinrichtung), um es dann wieder zurückzustellen und so die geplanten Angriffe durchzuführen.

M-TK-16 Einsatz sicherheitsintelligenter Endgeräte

Eine derartige Endgeräteintelligenz umfasst mindestens die Möglichkeit zur Sperrung des Gerätes (bis auf Minimalfunktionen wie Notruf) durch lokale PIN oder lokalen Kennwortschutz.

Einem erhöhten Schutzbedarf angemessener ist die Möglichkeit zur Unterscheidung zwischen einem Standard-Leistungsumfang (z. B. rein internes Telefonieren, ohne Zugriff auf Telefonbuchfunktionen o. Ä.) und Freischaltung erweiterten Leistungsumfangs nach Eingabe von Authentisierungsinformationen am Gerät. Diese Unterscheidung kann je nach eingesetzten Produkten und Zusammenspiel zwischen Telefon und TK-Anlage rein über entsprechende Funktionalitäten des Endgerätes stattfinden oder mittels über die TK-Anlage verwalteter Berechtigungsfestlegungen für den Endgeräteanschluss.

M-TK-17 Aktivierung einer Warnung bei Nutzung unsicherer Merkmale

Für den erhöhten Schutzbedarf sollten Endgeräte so konfiguriert werden können, dass ein eindeutiger Hinweis gegeben wird, sobald auf unsichere Merkmale zurückgegriffen wird. Ein wichtiges Beispiel ist ein Warnsignal in dem Fall, dass gerade eine Aufschaltung durch einen Dritten auf ein zurzeit geführtes Telefonat erfolgt.

M-TK-18 Sicherer Umgang mit Schnittstellen am Telefonie-Endgerät

Neuere Telefone weisen neben der Anschlussmöglichkeit an die Telefonie-Verkabelung zum Teil weitere Schnittstellen auf, z. B. Bluetooth zur Anbindung von drahtlosen Headsets oder WLAN-Anschlussmöglichkeit zwecks alternativer Verwendung als drahtlos angebundenes VoIP-Telefon.

Derartige Schnittstellen sind zu deaktivieren, sofern sie nicht genutzt werden sollen. Ist ihre Nutzung vorgesehen, typischerweise zum Anschluss drahtloser Zusatzausstattung, so sind die entsprechenden Sicherheitsvorkehrungen für diese Art von Schnittstelle zu treffen.

Ein notwendiges Minimum stellt in jedem Fall der Schutz solcher Schnittstellen gegen unbefugten Zugriff mittels vorgeschalteter Authentisierung dar. Einem erhöhten Schutzbedarf angemessener ist der ergänzende Einsatz von

- Verschlüsselung auf dem Endgerät gespeicherter Daten wie Rufnummern zu häufig angewählten Teilnehmern zum Schutz gegen Auslesen über nur schwach absicherbare Schnittstellen sowie
- Verschlüsselung der Kommunikation zwischen Telefonie-Endgerät und drahtlosem Zusatzequipment zum Schutz gegen Abhören oder störende Einflussnahme durch Dritte zum Zwecke eines Denial-of-Service-Angriffs (DoS-Angriff).

Nähere Einzelheiten zu Schnittstellen für Drahtlosanbindungen finden sich ergänzend im Kapitel zur Einbindung mobiler und drahtloser Systeme (siehe Kapitel 9) und sind sinngemäß auf solche Schnittstellen an Endgeräten zur ISDN-basierten TK-Anlage anzuwenden.

M-TK-19 Geschützte Übertragung von Sprachdaten

Im Falle erhöhten Schutzbedarfs bzgl. Vertraulichkeit sollte für Telefonate mit Partnern, in deren Verlauf sensiblen Inhalte besprochen werden, eine geschützte Übertragung von Sprachdaten erfolgen. Derartige Telefonate erfolgen zum Beispiel:

- bei Gesprächen zwischen Teilnehmern an der ISDN-basierten TK-Anlage, für deren Telefonate der erhöhte Schutzbedarf bzgl. Vertraulichkeit maßgeblich ist (siehe Abbildung 5)
- zwischen Teilnehmern an der ISDN-basierten TK-Anlage und Mitgliedern der gleichen Organisation im Home-Office oder in kleineren Außenstellen ohne eigene TK-Anlage (siehe Abbildung 6)
- zwischen Teilnehmern an der ISDN-basierte TK-Anlage und Mitgliedern der gleichen Organisation auf Geschäfts- oder Dienstreise, z. B. aus dem Hotelzimmer (siehe Abbildung 6)

Telefonate mit anderen Standorten der gleichen Organisation bzw. mit Partner-Organisationen stellen Szenarien der Vernetzung von ISDN-basierten TK-Anlagen dar und werden in Kapitel 3.3.3 behandelt.

Einem Endgerät, das eine verschlüsselte ISDN-basierte Übertragung von Sprachdaten durchführen muss, ist eine entsprechende Verschlüsselungsbox vorzuschalten. Für die Verwendung in externen Lokalitäten (Beispiele: Home-Office oder auf Reisen) gibt es für den mobilen Einsatz geeignete Produkte dieser Art.

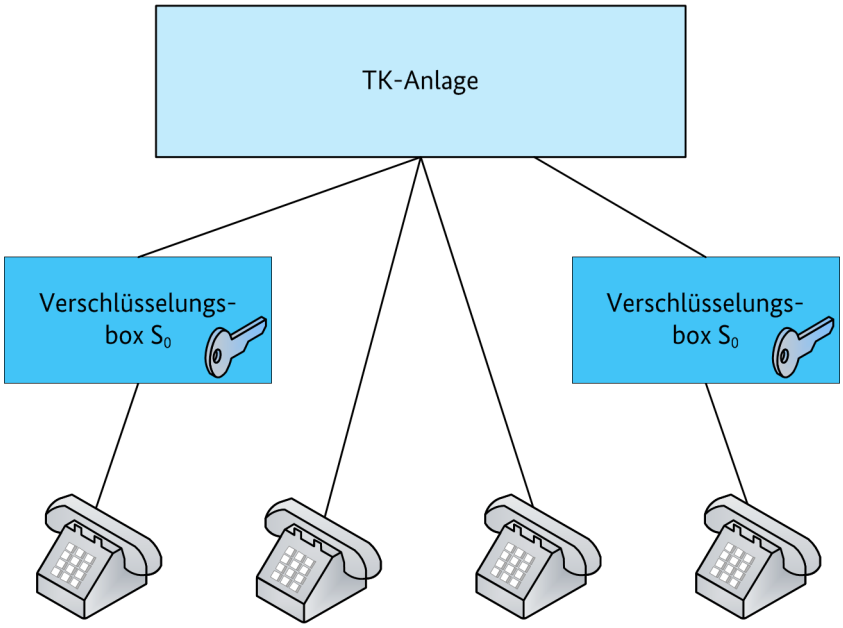


Abbildung 5: Verschlüsselung zwischen einzelnen Teilnehmern an der TK-Anlage

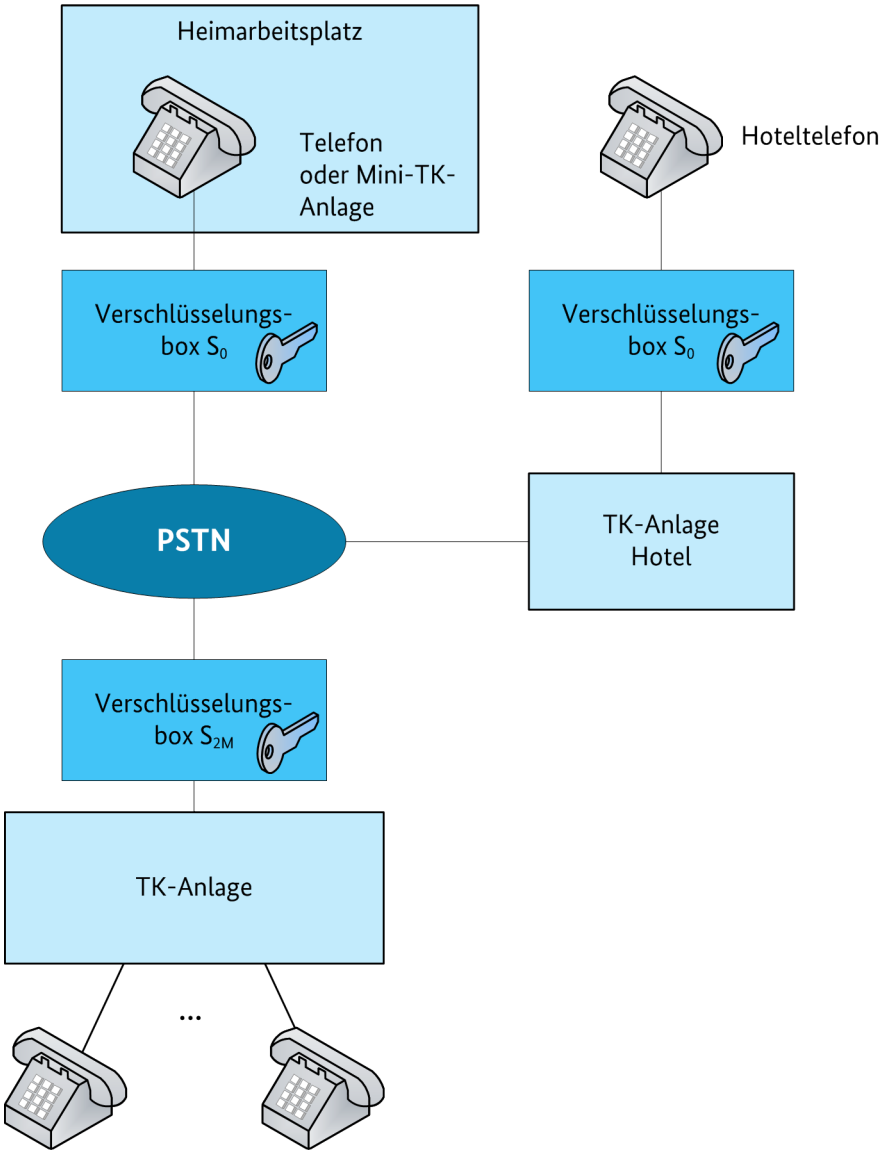


Abbildung 6: Verschlüsselung für Geräte am Heimarbeitsplatz und auf Reisen

3.3.2.3 Drahtlose Telefone

Werden im Zusammenhang mit einer zentralen ISDN-Anlage drahtlose Telefone eingesetzt, so handelt es sich typischerweise um DECT-Telefone, deren Basisstation kabelbasiert an die zentrale Anlage angeschlossen ist. Hier sind die Ausführungen zum Umgang mit DECT-Lösungen in Kapitel 9 zu beachten und die dort genannten Maßnahmen zu berücksichtigen.

3.3.2.4 Wartungsapparate

Im Falle erhöhten Schutzbedarfs ist der Einsatz von Wartungsapparaten hochgradig bedenklich. Der für diese Form der Fernadministration realisierbare Schutz des Administrationszugangs gegen unbefugten Zugriff ist zu schwach. Entsprechend werden die folgenden Maßnahmen vorgesehen:

M-TK-20 Verzicht auf Einsatz von Wartungsapparaten

Da der für Wartungsapparate realisierbare Schutz des Administrationszugangs gegen unbefugten Zugriff zu schwach ist, sollte möglichst auf den Einsatz von Wartungsapparaten verzichtet werden.

M-TK-21 Sperrung der Wartungsmöglichkeit per Wartungsapparat an der Anlage

Sofern von der Anlagen-Software unterstützt, sollte gezielt die Software-Funktionalität deaktiviert werden, über die Wartungsapparaten ein administrativer Durchgriff auf die ISDN-Anlage gewährt wird.

Auf diese Weise wird z. B. verhindert, dass externe Support-Techniker versehentlich die Regelung zum Verzicht auf Einsatz von Wartungsapparaten verletzen.

3.3.2.5 Wartungs-PCs

Wartungs-PCs können sein:

- PCs mit spezieller Client-Software zur Administration der Anlage
- vom Anlagenbetreiber genutzte PCs mit Web-Browser bei Administration der Anlage über eine Web-Schnittstelle

Für diese gelten die im Kapitel 3.3.4 dem Stichwort Netz- und Systemmanagement folgenden Ausführungen zum Anlagenmanagement. Die auf Wartungs-PCs anzuwendenden Maßnahmen regeln den angesichts erhöhten Schutzbedarfs vorzusehenden Umgang mit Administrationsendgeräten.

3.3.3 Netzwerk

Von Netzwerk ist im Falle von ISDN-basierten TK-Anlagen in mehrerlei Hinsicht zu sprechen:

- Anbindung von Endgeräten an die ISDN-Anlage

  Die hier für erhöhten Schutzbedarf zu berücksichtigenden Maßnahmen sind im Rahmen der Ausführungen zu kabelbasiert angebundenen Endgeräten benannt worden.

- LAN-Anbindung der ISDN-Anlage zum Datenaustausch mit Applikations-Servern (CTI, Abrechnungssystem u. Ä.)

  Maßnahmen für den erhöhten Schutzbedarf zum letzten Punkt sind im Zusammenhang mit Aspekten zur zentralen Anlage benannt worden, siehe Kapitel 3.3.1.

- LAN-Anbindung der ISDN-Anlage zum Zwecke des Anlagenmanagements

  LAN-Anbindungen zum Zwecke des Anlagenmanagements sind Gegenstand des Kapitels 3.3.4.

- Anbindung der ISDN-Anlage an das PSTN für externe Telefonate
- Anbindung der ISDN-Anlage in Form von Kommunikation mit Teilnehmern an weiteren ISDN-Anlagen der gleichen Organisation bzw. vertrauenswürdiger Partner

Für die beiden letzten Punkte sind im Sinne erhöhten Schutzbedarfs die folgenden Maßnahmen hervorzuheben:

M-TK-22 Gesicherte Übertragung der Sprachdaten zwischen Partnerstandorten durch Leitungsverschlüsselung

Technisch gesehen gleichen die hier einzusetzenden Lösungen den zur gesicherten Sprachdatenübertragung für kabelbasiert angebundenen Endgeräte verfügbaren Lösungen (siehe M-TK-19 „Geschützte Übertragung von Sprachdaten“). Allerdings kommt bei größeren Anlagen die Anforderung der Anschlussmöglichkeit an einen S2M-PSTN-Zugang hinzu (siehe Abbildung 7). Außerdem ist auf ausreichende Leistungsfähigkeit des Gerätes zu achten.

Falls der Partnerstandort nicht Teil der eigenen Organisation ist, kann es vorkommen, dass eine Leitungsverschlüsselung auf Partnerseite nicht umsetzbar ist.

Bei der Produktauswahl ist auf Kompatibilität der an der Anlage und im Endgerätebereich eingesetzten Verschlüsselungslösungen zu achten. Für die Kopplung eigener Anlagen an verschiedenen Standorten ist die Verwendung einheitlicher Geräte empfehlenswert.

Sollen Partner-Standorte mit ISDN-Anlagen derart abgesichert angebunden werden, ist darauf zu achten, dass die Partner-Organisation ein Produkt mit Unterstützung gleicher Verschlüsselungsgüte verwendet. Andernfalls ist die organisatorische Freigabe zur Übermittlung vertraulicher Informationen in Telefonaten mit einem solchen Partner sorgfältig zu prüfen.

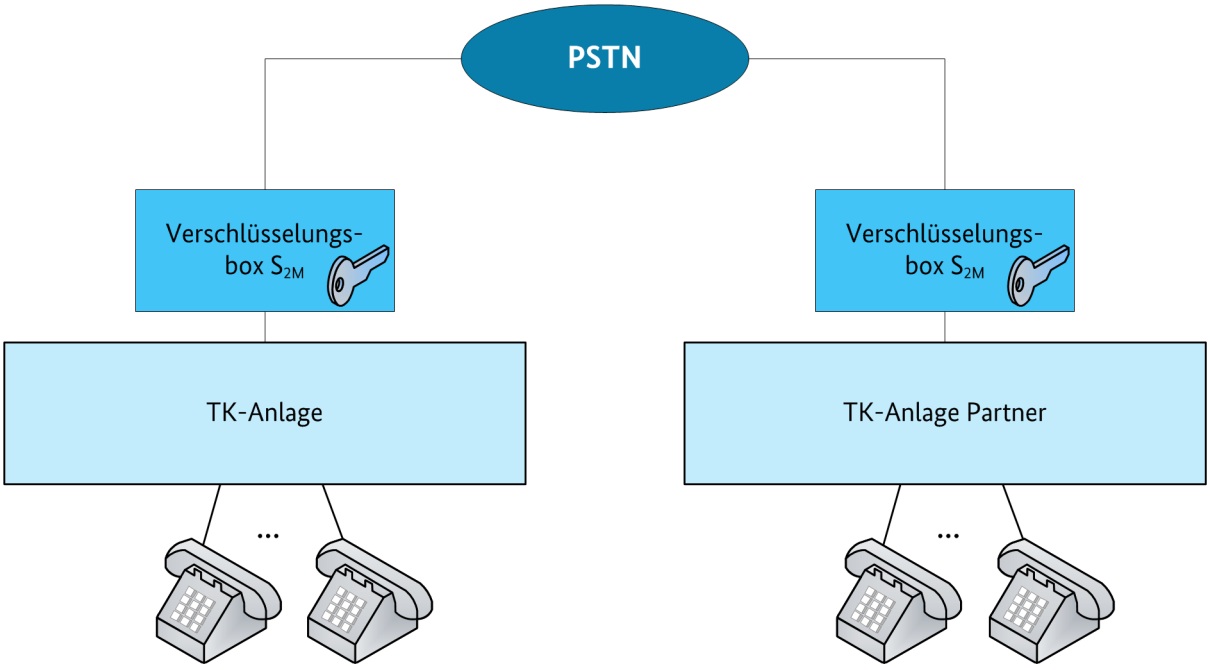


Abbildung 7: Verschlüsselung der Kommunikation zwischen Partnerstandorten

3.3.4 Netz- und Systemmanagement

Das Netz- und Systemmanagement wird bei ISDN-basierten TK-Anlagen auch als Anlagenmanagement bezeichnet. Im Sinne erhöhten Schutzbedarfs sind hier die folgenden Maßnahmen besonders zu nennen:

M-TK-23 Restriktive Einbindung externer Wartung

Wartungs- und Support-Arbeiten erfordern eine Zugriffsberechtigung zur Anlage, mit der leicht Angriffe auf alle Grundwerte der Sicherheit möglich sind. Je nach konkreter Risikobewertung lassen sich für die restriktive Einbindung externer Wartung verschiedene Stufen unterscheiden:

- gezielte Absicherung von Fernwartungszugriffen durch Externe

  Hier sind alle in Kapitel 3.3.3 „Netzwerk“ beschriebenen Maßnahmen empfehlenswert (z. B. Verschlüsselung). Die Maßnahmen dieser Stufe sollten in jedem Fall eingesetzt werden, sofern für die ISDN-basierte Telefonie ein erhöhter Schutzbedarf festgestellt wurde.
- Freischaltung des Fernwartungszugriffs für externen Support nur bei konkretem Bedarf
- Verzicht auf Fernwartungszugriff durch Externe
- Vier-Augen-Prinzip bei Vor-Ort-Wartung durch Externe

M-TK-24 Sichere Aufstellung von Administrationsendgeräten

Als Administrationsendgeräte zu ISDN-basierten TK-Anlagen werden im Zusammenhang mit erhöhtem Schutzbedarf eigene Administrations-PCs betrachtet. Diese zeichnen sich durch das Vorhandensein spezieller Software (Administrations-Client) zur Administration der Anlage oder bei Administration über Web-Browser dadurch aus, dass nur Nutzer dieser PCs zur Kommunikation mit der Management-Schnittstelle der TK-Anlage berechtigt sind.

Die sichere Aufstellung solcher Administrationsendgeräte gemäß den Anforderungen erhöhten Schutzbedarfs wird durch Vorkehrungen der folgenden Art realisiert:

- Aufstellung in abschließbaren Büros ohne freien Publikumsverkehr

  Dies stellt eine Minimalvorkehrung dar.

- Betreten dieser Räume durch Externe (z. B. Reinigungspersonal) nur unter Aufsicht

- Trennung vom übrigen LAN

  Durch diese Vorkehrung wird das Gerät zu einem reinen TK-Administrations-PC. Eine Nutzung zu anderen Zwecken ist nicht möglich, eine Kompromittierung im Rahmen solcher alternativer Nutzungszwecke mit nachfolgend missbräuchlichem Zugriff Unbefugter auf die TK-Anlage fällt nicht an.

- Aufstellung des Administrations-PCs am Standort der TK-Anlage

  Auf diese Weise wird der physische Zugangsschutz zu diesem Gerät maximiert und die Vernetzung zwischen Administrations-PC und TK-Anlage hat minimale Ausdehnung. Anonyme Angriffe auf diese „lokale Vernetzung“ aus dem Anwenderbereich des Organisations-LANs sind ausgeschlossen.

Alternativ kann mit Virtualisierungstechniken gearbeitet werden. Entweder werden die Administrationsanwendungen über einen Terminal-Server oder der Administrations-PC selbst wird komplett als zentral laufende Virtuelle Maschine (VM, engl. Virtual Machine) über eine Virtual Desktop Infrastructure (VDI) bereitgestellt. Dies hat die Vorteile, dass die Kommunikation entkoppelt wird (d. h. das Endgerät des Nutzers kommuniziert nur mit Terminal-Server-Protokollen), die Administrationsanwendungen an zentraler Stelle ausgeführt werden und die Administrationsaktivitäten dort leichter überwacht und protokolliert werden können.

M-TK-25 Sichere Konfiguration von Administrationsendgeräten

Im Sinne des erhöhten Schutzbedarfs ist durch gezielte Konfiguration der Administrationsendgeräte die unbefugte Nutzung technisch möglichst zu erschweren. Die nachfolgend benannten Vorkehrungen sollten in jedem Fall getroffen werden, unabhängig von der gewählten Form der sicheren Aufstellung:

- technische Beschränkung des Zugangs zu solchen Endgeräten auf das TK-Betriebspersonal

  Dieser Ansatz ist (mindestens) mit der üblichen Verwendung von Nutzerkonten und Kennwortschutz zu realisieren. Im Falle eines erhöhten Schutzbedarfs ist dabei nach Möglichkeit mit personenbezogenen Nutzerkonten zu arbeiten.

- Verwendung eines Bildschirmschoners mit an das Anmeldepasswort gekoppeltem Kennwortschutz und automatischer Aktivierung

- Logging aller Anmeldeversuche

- sinngemäße Anwendung der in M-TK-236 „Einbindung der Server der TK-Lösung in das Patch-Management der Organisation“ (siehe Kapitel 10.2) für Server formulierten Maßnahme zu Software-Sicherheit inklusive Patch-Management

- regelmäßige Integritäts-Checks für die auf solchen Geräten eingesetzte Software

  Diese Vorkehrung sollte getroffen werden, wenn ein Administratorendgerät so vernetzt ist, dass es auch mit anderen Geräten als der TK-Anlage kommunizieren kann und zu anderen Nutzungszwecken verwendet wird. Im Zuge solcher alternativer Nutzungszwecke bzw. bei Angriffen auf zugehörige Dienste und Schnittstellen erfolgte unbefugte Veränderungen am Gerät werden so frühzeitig entdeckt.

M-TK-26 Regelungen für sichere TK-Administration

Die empfohlenen Vorkehrungen zur sicheren Konfiguration können nur ihre volle Wirkung entfalten, wenn mit ihnen dem erhöhten Schutzbedarf entsprechend umgegangen wird. Personen, die zur Nutzung von Administrations-PCs berechtigt sind, müssen organisatorisch zu Folgendem verpflichtet werden:

- Abmeldepflicht, sobald die Administrationsmaßnahmen abgeschlossen sind
- manuelle Sperrung des Bildschirms, sofern der Raum zum Administrations-PC vorübergehend verlassen wird
- Abmeldepflicht, sofern der Raum zum Administrations-PC für längere Zeit verlassen wird
- Verwendung „starker" Kennwörter gemäß den Vorgaben einer entsprechenden Sicherheitsrichtlinie
- regelmäßige Kennwortänderung

M-TK-27 Sichere Konfiguration des Management-Zugangs zur TK-Anlage

Anstelle einer unbefugten Verwendung von Administrations-PCs können Versuche unberechtigter Manipulationen an der Anlage auch direkt über Angriffe auf Schnittstellen zur Anlagen-Fernadministration erfolgen. Die nachfolgend benannten Ansätze zur Minimierung des durch solche Schnittstellen gegebenen Risikos gelten sowohl für Fernadministration von extern als auch für Fernadministrationszugriffe aus der Umgebung der Organisation, z. B. LAN-basiert über eine entsprechende LAN-Anbindung der ISDN-basierten TK-Anlage.

Die im Falle eines erhöhten Schutzbedarfs zu treffenden besonderen Vorkehrungen sind dabei zum Teil von den Konfigurationsmöglichkeiten der Anlage abhängig:

- Sperrung des DISA-Zugriffs

  Die Absicherung dieser für ein Management via Telefon-Wartungsapparat gedachten Management-Schnittstelle ist für erhöhten Schutzbedarf zu schwach bzw. die Möglichkeiten des Missbrauchs sind zu groß. Daher ist die Schnittstelle abzuschalten.

- Netztrennung: Beschränkung von LAN-basierten Administrationszugriffen auf die ISDN-basierte TK-Anlage auf ein (physisch oder logisch) separates Netz zum Anlagenmanagement
- Abschaltung sonstiger, nicht zur Verwendung vorgesehener Schnittstellen, hier sind mindestens zu nennen:
  - Web-Interface, sofern keine Administration via Browser erfolgt
  - Telnet-Zugang
  - Simple Network Management Protocol (SNMP) v1/v2/v3

  Im Falle erhöhten Schutzbedarfs ist die Verwendung dieser Schnittstellen bedenklich, sofern die Kommunikationsmöglichkeiten nicht mit den Mitteln der Netztrennung ausschließlich auf TK-Administrations-PCs und TK-Anlage beschränkt werden können. Es sollte dann für diese Dienste eine verschlüsselte Variante verwendet werden oder eine Abschaltung erfolgen.

- Kennwortschutz und Rechteverwaltung

  Sofern die ISDN-basierte TK-Anlage entsprechende Möglichkeiten im Sinne des erhöhten Schutzbedarfs bietet, sollten hier die folgenden Vorkehrungen auf Seiten der Anlage konfiguriert werden:

  - Beschränkung des Zugriffs auf personenbezogene Administratorkonten
  - (starker) Kennwortschutz für solche Konten
  - Verwendung von SNMPv3 unter Nutzung von Authentication und Privacy, falls SNMP-basierte Zugriffe erfolgen sollen

  Unterstützt die Anlage diese Möglichkeiten nicht, so sind stattdessen folgende Punkte vorzusehen:

  - Einsatz einer der Anlage vorgelagerten Authentisierungslösung
  - maximaler Schutz der Administratorarbeitsplätze (konsequente Umsetzung aller in der Einsatzumgebung möglichen Vorkehrungen gemäß Maßnahmen M-TK-24 „Sichere Aufstellung von Administrationsendgeräten“ und M-TK-25 „Sichere Konfiguration von Administrationsendgeräten“)

M-TK-28 Protokollierung und regelmäßige Kontrolle von Fernwartungszugriffen

Im Rahmen der Möglichkeiten der eingesetzten TK-Anlagen-Software sind Anmeldungen bzw. Zugriffe auf die Anlage über Administrationsschnittstellen und zugehörige Konten automatisch zu protokollieren. Sofern der Administrationszugang nicht bei Bedarf freigeschaltet wird, sondern permanent möglich ist, sind die entsprechenden Log-Files regelmäßig (bei erhöhtem Schutzbedarf ggf. mit höherer Frequenz, z. B. mindestens einmal täglich) einer Sichtkontrolle zu unterziehen. Gehäuften fehlerhaften Anmeldeversuchen ist gezielt nachzugehen, bei erfolgreichen Anmeldungen ist im Zweifel ein Abgleich der Zeitpunkte mit der Dokumentation durchgeführter Wartungsmaßnahmen durchzuführen.

Sofern von der Anlage unterstützt, sollte bei erhöhtem Schutzbedarf bei Häufungen fehlerhafter Anmeldeversuche automatisch ein Alarm ausgelöst werden (siehe M-TK-29 „Verfügbarkeitssicherung durch (automatisierte) Zustandsüberwachung“).

Bei Auffälligkeiten muss sofort entsprechend den für die IT bestehenden Regelungen für einen vermuteten Sicherheitsvorfall verfahren werden, bis ein Angriffsverdacht schlüssig widerlegt ist.

M-TK-29 Verfügbarkeitssicherung durch (automatisierte) Zustandsüberwachung

Im Falle erhöhten Schutzbedarfs bezüglich Verfügbarkeit muss eine ISDN-basierte TK-Anlage zwingend unter Nutzung einer Schnittstelle zum Anlagenmanagement einer zumindest teilautomatisierten Zustandsüberwachung unterzogen werden. Eine Einbindung in bereits für andere IT-Systeme verwendete zentrale Lösungen zu Monitoring, Logging und Alarming ist einer isolierten Überwachung für die TK-Anlage vorzuziehen.

Unabhängig von der realisierten Konstellation ist die im Rahmen solcher Permanentüberwachung und Ereignisprotokollierung erfolgende Kommunikation gemäß den generell zu ergreifenden Maßnahmen (siehe Kapitel 10.3) abzusichern.

M-TK-30 Abschluss eines Support-Vertrags inklusive externer Beratungskompetenz

Im Falle erhöhten Schutzbedarfs muss man sich zur Sicherstellung ausreichender Verfügbarkeit sowie zur Reaktion auf neu erkannte Sicherheitsrisiken durch geeignete Präventivmaßnahmen gezielt auf externe Unterstützung mit direktem Zugriff auf den Hersteller abstützen können. Basis hierfür ist ein Support-Vertrag, der mindestens Folgendes umfasst:

- Hardware-Wartung (Ersatzteillieferung, Einbau durch Wartungstechniker)

- Software-Pflege (Information über bzw. Bereitstellung von Bugfixes, Sicherheits-Updates und ähnlicher Software-Korrekturen)
- 3rd-Level-Support bei komplexen, in Eigenleistung nicht behebbaren Störungen
- Beratung bei Bedarf zu Anpassungen an der aktuellen Konzeption/Konfiguration, z. B. zur Gefahrenabwehr oder als Notfallvorsorge

Für Leistungen im Störungs- bzw. Notfall müssen der genauen Risikobewertung angemessene Service-Level-Vereinbarungen getroffen werden. Darüber hinaus ist vertraglich sicherzustellen, dass der Externe im Rahmen seiner Vertragsleistungen ein Sicherheitsniveau aufrecht erhält, dass dem Schutzbedarf angemessen ist (Güte des Sicherheitsmanagement des Externen, Einhaltung von in der Einsatzumgebung der TK-Anlage maßgeblichen, sicherheitsrelevanten Regelungen). Durch gezielte Vertragsgestaltung muss zudem dafür gesorgt werden, dass bei Unzuverlässigkeit in Form wiederholter Verletzungen des Service Level ohne finanziellen Schaden kurzfristig der Vertragspartner gewechselt werden kann.

3.4 Zusammenfassung

Mit dem Begriff klassische Telekommunikationstechnik werden meist Systeme auf Basis von ISDN verstanden. Die Endgeräte werden kabelgebunden oder drahtlos an die TK-Anlage angebunden. Bei klassischen TK-Anlagen sind folgende Angriffspunkte gezielt zu berücksichtigen:

- die eigentliche zentrale Anlage
- Schnittstellen der Anlage zu TK-Anwendungssystemen, TK-Wartungssystemen und Endgeräten
- Kommunikationswege zwischen verschiedenen Anlagen (Anlagenkopplung)

Die Angriffsrisiken sind in Abhängigkeit von den genutzten Leistungsmerkmalen und den Vertraulichkeits- bzw. Verfügbarkeitsanforderungen zu bewerten und zu minimieren.

Besonders zu beachten sind dabei aus Sicht der Zielumgebung:

- Vertraulichkeit der Gesprächsinhalte und allgemein der übertragenen Informationen
- eigene Verfügbarkeitsansprüche, ggf. auch einzuhaltende gesetzliche oder ähnliche Auflagen, bzgl. Verfügbarkeit der TK-Anlagennutzung für Notrufe und zur Begleitung von Notfallsituationen
- ggf. erhöhte Verfügbarkeitsanforderungen der Telefoniefunktion an bestimmten Arbeitsplätzen und damit an bestimmten Endgeräten
- Umfang einer Speicherung personenbezogener Daten im Rahmen der Lösung zu internen Zwecken bzw. ggf. zur Erfüllung gesetzlicher oder ähnlicher Auflagen und des angemessen sicheren Umgangs damit.

Die Erarbeitung und Umsetzung einer Sicherheitskonzeption umfasst neben den generell zu ergreifenden Maßnahmen (siehe Kapitel 10) die folgenden Aspekte.

Absicherung der zentralen TK-Anlage

Generell sind die TK-Anlage, ggf. angekoppelte Anwendungssysteme und mit der Anlage zu Wartungszwecken kommunizierende Systeme gezielt zu härten und mit Blick auf Sicherheitsaspekte im Netzwerk zu positionieren.

Angriffen durch unbefugte Zugriffe ist durch eine Absicherung der zugehörigen Schnittstellen gezielt entgegen zu wirken. Nicht benötigte und nicht geeignet absicherbare Schnittstellen sollten vermieden bzw. deaktiviert werden. Dies gilt für Schnittstellen zur internen Kopplung ebenso wie für Übergänge zu öffentlichen TK-Netzen (Public Switched Telephone Network, PSTN).

TK-Leistungsmerkmale, die nicht benötigt werden, sind durch gezielte Konfiguration der TK-Anlage abzusichern bzw. zentral an der Anlage zu sperren.

Absicherung der Kommunikation zwischen Anlagenelementen

Falls die Schnittstellen der TK-Anlage nicht so abgesichert werden können, dass das geforderte Schutzniveau erreicht wird, sollte ergänzend eine Verschlüsselung der Datenströme zwischen den Anlagenelementen erfolgen. Dies gilt insbesondere bei standortübergreifender Kopplung zwischen TK-Anlagen und für die Kommunikation zwischen TK-Anlage und Wartungs-PCs oder ähnlichen Wartungs-Endgeräten.

Sicherheitsmaßnahmen im Bereich Endgeräte und Endgerätenutzung

Leistungsmerkmale und Funktionalitäten, die für Angriffe missbraucht werden können, müssen am Endgerät zugriffsgeschützt bereitgestellt werden. Müssen Endgeräte in nicht zugangsgeschützten Bereichen aufgestellt werden, kann eine Deaktivierung kritischer Nutzungsmöglichkeiten an den zugehörigen TK-Anlagenports erfolgen. Alternativ sind Endgeräte zu nutzen, bei denen diese Nutzungsformen nicht möglich sind.

Eine ungesicherte Drahtlosanbindung von Endgeräten ist nach Möglichkeit zu deaktivieren. Drahtlose Schnittstellen sind generell gemäß den entsprechenden Maßnahmen (siehe Kapitel 9.3.2) abzusichern.

Soll von bestimmten Endgeräten aus die Kommunikation besonders vertraulicher Inhalte möglich sein, steht als gezielte Zusatzmaßnahme die Option zur Absicherung mittels Ende-zu-Ende-Verschlüsselung der Sprachkommunikation zur Verfügung. Bei Entscheidung zu dieser Maßnahme sollte das Endgerät neben der reinen Unterstützung der Verschlüsselung den Nutzer gezielt und zuverlässig über den aktuellen Verschlüsselungszustand informieren.

Gezielte Ausstattung, externe Leistungen

Produkte für zentrale Anlagenelemente und Endgeräte müssen mit Blick auf die anzuwendenden Maßnahmen (insbesondere hinsichtlich der Vertraulichkeit der Kommunikation) ausgewählt werden. Zentrale Installationen und deren Vernetzung sind den Verfügbarkeitsanforderungen angemessen redundant auszulegen. Außerdem sind Wartungsverträge und Detailvereinbarungen zu schnellen Ersatzlieferungen bedarfsgerecht zu gestalten.

Für Notfallsituationen sind Optionen bzgl. einer Notbetriebsausstattung gezielt zu prüfen und im beschlossenen Umfang geeignet vorzubereiten, sodass alle besonders wichtigen Nutzungszwecke der TK-Lösung über die Notbetriebsform geeignet abgedeckt werden können.

Organisatorische Maßnahmen

Administratoren der TK-Anlage (und vorhandener TK-Anwendungen) sind geeignet auf Konfiguration und Betrieb der Sicherheitsmaßnahmen zu schulen. Sie müssen zu einem angemessenen Umgang mit vertraulichen Daten, Authentisierungsmerkmalen und administrativen Zugängen verpflichtet werden.

Nutzer von TK-Endgeräten müssen im Umgang mit sicherheitsrelevanten Aspekten geschult werden, sodass jeder Nutzer für ihn freigegebene Funktionalitäten einerseits erreicht und andererseits den Schutz der Anlage nicht unnötig schwächt. Ergänzend ist eine Sensibilisierung bzgl. eines angemessenen Umgangs mit besonders vertraulichen Informationen im Rahmen von Telefonaten notwendig.

4 Voice over IP

Unter dem Begriff der konvergenten Netze wird allgemein die Portierung von Spezialsystemen und deren für das Spezialsystem zugeschnittenen spezifischen Kommunikationssysteme auf das Internet Protocol (IP) verstanden. IP wird hier als gemeinsamer Träger für alle Kommunikationsdienste genutzt. Sprache ist hier keine Ausnahme und Voice over IP (VoIP) ist inzwischen ein klassisches Beispiel für eine gelungene Netzkonvergenz. Die Bedeutung von VoIP hat in den vergangenen Jahren immer mehr zugenommen und VoIP stellt inzwischen eine bewährte Basistechnologie zur Übertragung von Sprache und allgemein von Multimedia-Datenströmen dar. Die dabei eingesetzten Techniken und Protokolle werden in Kapitel 4.1 beschrieben.

Der Träger IP bedingt eine spezifische Gefährdungslage, bei der zusätzlich VoIP-spezifische Gefährdungen berücksichtigt werden müssen, wie in Kapitel 4.2 dargestellt. Der Maßnahmenkatalog für die Basistechnologie VoIP, der diesen Gefährdungen entgegenwirkt, wird in Kapitel 4.3 spezifiziert.

4.1 Basiswissen

Voice over IP, d. h. die Sprachübertragung über IP-Netze, hat sich fest in der Architektur moderner Kommunikationsdienste etabliert und löst die Techniken klassischer TK-Anlagen, d. h. Leitungsvermittlung, ab. Dieses Kapitel beschreibt die technischen Grundlagen der IP-Telefonie, die wesentlichen Elemente eines VoIP-Systems und die verschiedenen Sicherheitsmechanismen für VoIP-Systeme.

4.1.1 IP als Träger für Sprache

Da das IP-Protokoll grundsätzlich verbindungslos und paketorientiert ist, steht VoIP im Gegensatz zur klassischen Telekommunikationstechnik, welche verbindungsorientiert und leitungsvermittelnd arbeitet. In IP-Netzen bestehen technologiebedingt Bandbreitenschwankungen für die einzelnen Kommunikationsbeziehungen und außerdem können einzelne IP-Pakete über Routing verschiedene Wege durch das Netz nehmen und dadurch sogar in unterschiedlicher Reihenfolge beim Empfänger eintreffen. Dadurch drohen in IP-Netzen Qualitätsverluste in der Sprachübertragung durch Paketverluste, Verzögerungen (Delay) und durch Jitter, d. h. der Schwankung des Delay. Allgemein gilt: Je höher Delay oder Jitter sind, desto schlechter ist die realisierbare Sprachqualität. Abbildung 8 zeigt die wesentlichen für VoIP-Systeme verwendeten Protokolle im Überblick[6]. Beschreibungen hierzu finden sich im Anhang in Kapitel 13.1.

Bei einer klassischen TK-Anlage wird die gesamte Kommunikation, d. h. Signalisierung und Nutzdaten zwischen Endgerät und TK-Anlage, stets über eine einzelne Kabelstrecke geführt. Außerdem werden in klassischen TK-Anlagen stets getrennte Kanäle für die Signalisierung und Nutzdatenübertragung verwendet. VoIP geht hier auf eine andere Weise vor, indem Signalisierungsdaten zwischen Endgeräten und Telefonie-Server übertragen werden und die Nutzdaten im Normalfall als Peer-to-Peer-Kommunikation zwischen den Endgeräten selbst. Dabei werden Signalisierungs- und Nutzdaten als einzelne Pakete über ein gemeinsames IP-Netz übertragen und enthalten lediglich die Angaben zur Sende- und Empfangsadresse. Die Pakete werden also nicht mehr über dedizierte Signalisierungs- und Nutzkanäle übertragen, sondern werden individuell anhand der im Paket spezifizierten Informationen vermittelt. Bei der Übertragung wird vom Netz zunächst kein Unterschied zwischen IP-Datagrammen für VoIP und Datagrammen für andere Anwendungen gemacht.

6 Formal korrekt ist die Bezeichnung DoD-Modell für das TCP/IP-Modell, jedoch hat sich umgangssprachlich die Bezeichnung TCP/IP-Modell eingebürgert.

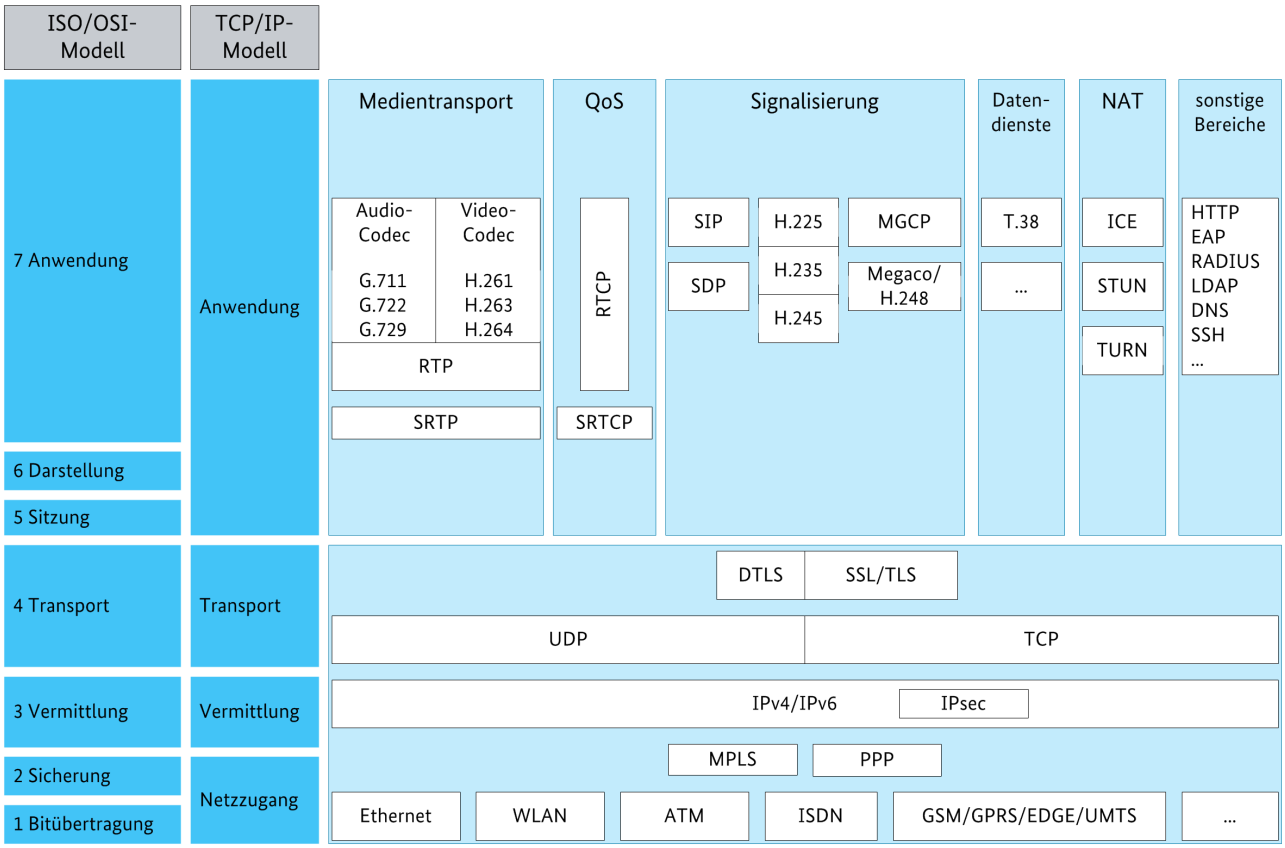


Abbildung 8: Protokolle für VoIP-Systeme im Überblick

4.1.2 Anwendungsgebiete von VoIP

VoIP findet im Wesentlichen in vier unterschiedlichen Bereichen moderner Telekommunikation Anwendung:

- VoIP im Local Area Network (LAN)
- IP-Anlagenanschluss
- VoIP auf Weitverkehrsstrecken
- Internettelefonie

Diese werden im Folgenden kurz erläutert.

4.1.2.1 VoIP im LAN

Innerhalb von Firmen und Behörden wird die getrennte Infrastruktur für Daten und Telekommunikation verstärkt von einer IP-basierten konvergenten Netzarchitektur abgelöst, die Daten- und TK-Dienste über eine gemeinsame LAN-Infrastruktur unterstützt. Eine Telefonanlage wird dabei durch ein IP-fähiges System, eine sogenannte Internet Protocol - Private Branch Exchange (IP-PBX), ersetzt, das sogar als reine Software-Lösung (sogenannter Soft-Switch) vorliegen kann. Eine IP-PBX kann als Hardware-Appliance, Software-Appliance, virtuelle Maschine (VM) oder als Software auf einem Standardbetriebssystem vorliegen. Dieser Wandel bringt entsprechende Einsparungen in den Bereichen Verkabelung, Netzinfrastruktur, Administration und Wartung mit sich. Nach außen wird das interne VoIP-Netz über ein Gateway direkt an das Public Switched Telephone Network (PSTN) oder über ein rein IP-basiertes

Koppelelement (z. B. Router oder Firewall) an andere VoIP-Netze bzw. über einen VoIP-Provider an externe Netze angebunden.

Durch die Übertragung von Sprache und Daten über eine gemeinsame LAN-Infrastruktur ergeben sich zusätzliche Anforderungen an die Sicherheit.

4.1.2.2 IP-Anlagenanschluss

Die Kopplung einer VoIP-Anlage an das PSTN kann zunächst durch Gateways innerhalb der lokalen Infrastruktur erfolgen. Dem steht die Entwicklung in den Netzen der Netzdienstanbieter (Carrier) gegenüber, welche mehr und mehr IP-basierende Netze aufbauen. Ziel der Carrier ist, im Rahmen der Umstellung auf das Next Generation Network (NGN), die Schaffung einer einheitlichen, auf IP basierenden Netzinfrastruktur. Als Konsequenz kann der Übergabepunkt zum Carrier unmittelbar durch VoIP-Komponenten realisiert werden und notwendige Übergänge zum PSTN leistet dann der Carrier.

4.1.2.3 VoIP auf Weitverkehrsstrecken

VoIP wird auch über Wide Area Networks (WANs) übertragen, um kostengünstig eine standortübergreifende interne Telefonie zu realisieren. Eine bestehende IP-Infrastruktur kann dabei für Telekommunikationsdienste mitverwendet werden.

Da hier VoIP auf einer gemeinsamen Infrastruktur eines WAN-Anbieters zusammen mit anderen Daten, auch denen anderer Kunden, übertragen wird, ist die Zusicherung einer angemessenen Dienstgüte (Quality of Service, QoS) wesentlich. Außerdem kommt bei der Übertragung von VoIP über WAN-Strecken der Verschlüsselung der Daten eine besondere Bedeutung zu, wobei bei internationalen Übertragungen ggf. auch regulatorische Aspekte berücksichtigt werden müssen.

4.1.2.4 Internettelefonie

Der Begriff der Internettelefonie bezeichnet allgemein die Telefonie über öffentliche IP-Netze. Internettelefonie wurde in der Vergangenheit vornehmlich von Privatpersonen (z. B. Skype) eingesetzt, jedoch ist insbesondere mit der verstärkten Nutzung von Smartphones und Tablets im dienstlichen Bereich auch hier der Einsatz von Internettelefonie gestiegen. Zum Einsatz kommen oft sogenannte Softphones, d. h. Dienstprogramme, welche auf einem Computer installiert in Verbindung mit einem Headset das Telefonieren ermöglichen. Dabei lehnen sich die Softphones in ihrer Struktur an Messenger- und Chat-Dienste an bzw. werden teilweise als Zusatzfunktion in diese Programme integriert.

Im Vordergrund steht bei Internettelefonie meist nicht eine mit herkömmlicher Telefonie vergleichbare hohe Qualität, sondern die flexible Nutzung von VoIP, die Integration mit anderen Anwendungen auf PC, Tablet oder Smartphone sowie auch eine Gebühreneinsparung.

4.1.3 Übertragung von Signalisierungsdaten

Zur Übertragung der Signalisierungsdaten werden unterschiedliche Protokolle eingesetzt. Zu nennen sind hier insbesondere:

- Session Initiation Protocol (SIP), siehe Kapitel 13.1.1.1
- H.323, siehe Kapitel 13.1.1.2
- Media Gateway Control Protocol (Megaco und MGCP), siehe Kapitel 13.1.1.3
- Inter-Asterisk eXchange (IAX), siehe Kapitel 13.1.1.4

Das Verfahren E.164 Telephone Number Mapping (ENUM, siehe Kapitel 13.1.1.5) realisiert die Übersetzung von Telefonnummern in Namen des Domain Name System (DNS) und umgekehrt. Hierüber können die für die Signalisierung benötigten Informationen verwaltet werden.

4.1.4 Übertragung der Nutzdaten

Die Übertragung der Nutzdaten erfolgt bei VoIP über das Real-Time Transport Protocol (RTP), das in [IETF RFC3550-2003] spezifiziert ist. RTP setzt auf dem User Datagram Protocol (UDP) auf und dient der Übertragung echtzeitsensitiver Daten für Unicast- und Multicast-Anwendungen. Vornehmlich wird RTP für die Übertragung von Medienströmen in Form von Sprach- und Videodaten eingesetzt.

Bei RTP-Sitzungen werden im Fall von Paketverlusten Daten nicht erneut übertragen. Stattdessen werden Datenverluste und damit verbundene Qualitätsschwankungen bewusst in Kauf genommen, um zu verhindern, dass Delay und Jitter durch wiederholtes Senden der Pakete erhöht werden.

Kontrollinformationen für RTP, die beispielsweise zur Bewertung der Übertragungsqualität und als Grundlage für eine dynamische, qualitätsorientierte Anpassung der Übertragung dienen, werden über das Real Time Control Protocol (RTCP) übertragen.

Weitere Informationen zu RTP und RTCP finden sich in Kapitel 13.1.2.

4.1.5 Sicherheitsmechanismen in VoIP

Die Absicherung einer VoIP-Kommunikation kann letztendlich auf allen Protokollebenen vorgenommen werden, von einer physischen Netztrennung bis zur Absicherung der Sprachübertragung auf Anwendungsebene. VoIP-Sicherheit besteht aus zwei wesentlichen Bestandteilen:

- Sicherer Medientransport: Zum sicheren Medientransport (z. B. Sprache oder Video) wird vor allem das Secure Real-Time Transport Protocol (SRTP) eingesetzt (siehe Kapitel 13.1.3.1). Es kommen aber auch andere Verfahren wie IPsec[7] und allgemein Techniken wie Virtual Private Network (VPN) in Frage (siehe Kapitel 13.1.3.2).
- Sichere Signalisierung: VoIP-Sitzungen werden über Signalisierungsprotokolle auf- und abgebaut sowie gesteuert. Die Absicherung dieser Protokolle erfolgt bei VoIP meist auf der Transportschicht über Transport Layer Security (TLS, siehe Kapitel 13.1.3.3) oder auf der Vermittlungsschicht über IPsec. Im Detail unterscheiden sich die verschiedenen Signalisierungsprotokolle hinsichtlich ihrer Absicherung (siehe Kapitel 13.1.3.4 für SIP und Kapitel 13.1.3.5 für H.323).

4.1.6 IP-Anlagenanschluss

Die Entwicklung von der klassischen Telefonietechnik hin zu IP-basierter Sprachkommunikation betrifft nicht nur die organisationsinterne Infrastruktur in Unternehmen und Behörden, sondern auch die Infrastruktur der Carrier.

VoIP findet beispielsweise auf Basis von SIP eine zunehmende Verbreitung in Unternehmens- und Behördennetzen. Telefonanlagen mit herkömmlicher TK-Technik werden nach und nach durch Soft-Switches bzw. IP-PBX ersetzt. Die Anbindung an das PSTN erfolgt dabei oft durch eine Gateway-Komponente als Bestandteil der lokalen VoIP-Anlage, wie in Abbildung 9 dargestellt.

7 Bei IPv6 sind die in IP Security (IPsec) spezifizierten Mechanismen ein fester Bestandteil des Standardumfangs.

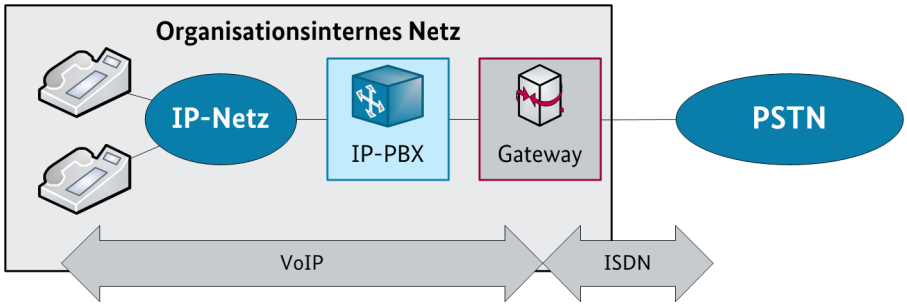


Abbildung 9: Traditionelle PSTN-Anbindung über ein Gateway der lokalen VoIP-Anlage

Außerdem stellen die Carrier mit NGNs verstärkt ihre Netze auf IP um, damit eine einheitliche, paketvermittelnde und IP-basierte Netzwerktechnik alle Dienste bereitstellen kann[8].

Beide Entwicklungen haben eine logische Konsequenz: Der Übergabepunkt zwischen organisationsinternem Nutzer und Carrier wird auch für die Telekommunikation letztendlich IP-basiert sein. Der Nutzer wird insbesondere keine PSTN-Gateway-Komponente mehr benötigen und hat dann nach außen lediglich einen IP-Anlagenanschluss. Auf Basis des verwendeten Signalisierungsprotokolls (in der Regel SIP) wird dazu eine VoIP-Verbindung zwischen der IP-fähigen Telefonanlage des Unternehmens bzw. der Behörde und dem VoIP-Anbieter (genauer gesagt dem Internet Telephony Service Provider, ITSP) über das Internet hergestellt. Der ITSP kann dabei auch dem Internet Service Provider (ISP) entsprechen. Bei SIP wird diese Verbindung als SIP-Trunk bezeichnet[9].

Die Anbindung an das PSTN erfolgt also anstatt über einen lokalen Anschluss, z. B. S_{2M}-Anschluss, über entsprechende Media Gateways beim ITSP, inklusive des im Folgenden beschriebenen Sicherheitselements Session Border Controller (SBC), wie in Abbildung 10 gezeigt. Eine zusätzlich zu pflegende lokale TDM-Infrastruktur entfällt. Bei einem IP-Anlagenanschluss kann die Zahl der Sprachkanäle (begrenzt durch die zur Verfügung stehende Bandbreite) im Prinzip frei dem Bedarf angepasst werden.

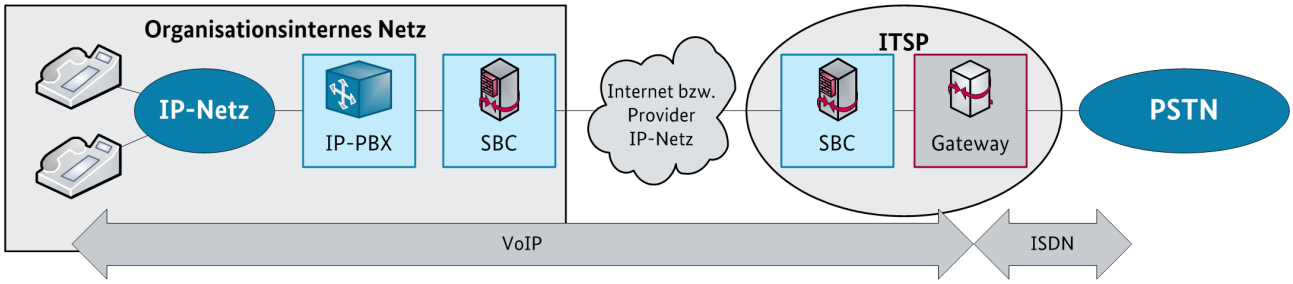


Abbildung 10: IP-Anlagenanschluss

Eine IP-basierte Telekommunikations-Schnittstelle zu einem ITSP erfordert die Berücksichtigung folgender Punkte:

- Schutz des organisationsinternen Netzes vor dem ITSP und umgekehrt
- Schutz der Datenübertragung zwischen organisationsinternem Netz und ITSP
- Bereitstellung von öffentlichen IP-Adressen
- Bereitstellung von Abrechnungsfunktionen

8 NGN werden vom European Telecommunications Standards Institute (ETSI) unter der Bezeichnung Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN) standardisiert. Neben der Architektur (siehe [ETSI ES282001-2009]) sind unter anderem auch Sicherheitsanforderungen (siehe [ETSI TS187001-2011]) spezifiziert und eine zugehörige Sicherheitsarchitektur für NGN erarbeitet worden (siehe [ETSI TS187003-2011]).

9 Das Herstellerkonsortium SIP Forum hat im Januar 2008 hierzu eine Empfehlung für die Interoperabilität zwischen IP-PBX und der Infrastruktur eines ITSP herausgegeben und 2011 überarbeitet (siehe [SIP TR-2011]).

- Bereitstellung von Zugangskontrollfunktionen
- Bereitstellung von Funktionen zur Sicherstellung der Dienstgüte (QoS)

Zur Unterstützung dieser Funktionen dient der oben erwähnte Session Border Controller. Ein SBC ist ein Netzelement, das ein Provider-Netz oder ein organisationsinternes IP-basiertes Telekommunikationsnetz abschließt, d. h. es begrenzt alle abgehenden und ankommenden Gespräche und terminiert demzufolge die entsprechenden Protokollsitzungen.

Grundsätzlich realisiert der SBC eine Protokollvalidierung für alle übertragenen Daten (Signalisierungs- und Nutzdaten), wobei die Kommunikation auch über Network Address Translation (NAT) hinweg erfolgen kann. Werden verschiedene Protokolle im VoIP-Netz genutzt, erfolgt die Umsetzung dieser Protokolle im SBC.

Solche Grundfunktionalitäten werden ergänzt um eine Firewall-Funktion für die VoIP-Protokolle, die gegebenenfalls durch einen Signalisierungs- und RTP-Proxy ergänzt wird und Schutz vor Attacken, z. B. vom Typ Denial of Service (DoS), bietet.

Im Rahmen der Signalisierung wird die erforderliche Gesprächsqualität durch folgende Funktionen gewährleistet:

- Limitierung der Bandbreite für alle Gespräche insgesamt bzw. je Gespräch, die dann ggf. von Call Admission Control (CAC) genutzt wird
- Call Admission Control

  Mittels CAC können Verbindungsanforderungen nach festgelegten Regeln (z. B. der verfügbaren Bandbreite) akzeptiert oder abgelehnt werden, um eine geforderte Dienstgüte für die Sprachübertragung gewährleisten zu können.
- Traffic Shaping

  Über Traffic Shaping wird die Übertragungsrate der Pakete gesteuert, um die Latenz der Nutzdatenpakete zu kontrollieren und den Anforderungen anzupassen. Dabei werden die Pakete klassifiziert und je nach Priorität bevorzugt weitergeleitet.

Bei der Übertragung der Nutzdaten, d. h. des Medienstroms, übernimmt der SBC die folgenden Funktionen:

- Umwandlung von Sprach-Codecs (Transcoding)

  Die nutzbaren Sprach-Codecs können eingeschränkt werden, sodass z. B. nur G.711 A-law und G.729 verwendet werden dürfen
- Entfernung bzw. Modifikation VoIP-spezifischer Header
- Priorisierung von markierten IP-Paketen entsprechend den Festlegungen während der Signalisierung

Diese Funktionen gelten allgemein für alle VoIP-Standards, neben SIP sind hier H.323 oder Megaco zu nennen.

Aus dem Blickwinkel des Nutzers eines IP-Anlagenanschlusses kommen zusätzlich zur Gefährdungslage eines VoIP-Systems die Gefährdungen durch die Schnittstelle zum ITSP, die ja jetzt IP-basiert ist, sowie durch den ITSP selbst, der die Anbindung an das PSTN bereitstellt, hinzu.

Da der SBC sowohl Signalisierung als auch den Medienstrom terminiert, muss der SBC bei verschlüsseltem VoIP zwingend als Verschlüsselungsendpunkt dienen können. Daher ist insgesamt der SBC eine entscheidende Sicherheitskomponente, die eine entsprechende Vertrauenswürdigkeit haben muss.

4.1.7 Standortübergreifende Kommunikation

4.1.7.1 Allgemeine Aspekte

Wesentliche Techniken bei der standortübergreifenden Kommunikation über ein WAN sind Multi-Protocol Label Switching (MPLS) und vermehrt auch Carrier Ethernet.

Bei MPLS werden dem Kunden durch einen Provider bzw. Carrier ein oder mehrere sogenannte MPLS Virtual Private Networks (MPLS-VPNs) bereitgestellt. Dabei muss beachtet werden, dass es sich bei einem MPLS-VPN zwar um ein virtuelles privates Netz handelt, jedoch ohne Zusatzinstrumente keine Verschlüsselung der Kommunikation wie bei einem IPsec-VPN stattfindet. Innerhalb des MPLS-Netzes erfolgt die Trennung der verschiedenen MPLS-VPNs zwischen Layer 3 und Layer 2 durch virtuelle Routing-Instanzen (Virtual Routing and Forwarding, VRF) und durch ein sogenanntes Label, das als Zusatzinformation in den Paketen übertragen und einem MPLS-VPN zugeordnet wird. Am Übergang zu den Kundennetzen werden diese MPLS-VPNs dann auf dem Kunden bereitgestellten Routing-Instanzen terminiert. Mehrere Kunden bzw. mehrere MPLS-VPNs teilen sich also eine gemeinsame Infrastruktur, wie in Abbildung 11 dargestellt. Die Übertragung von VoIP-Daten eines Kunden kann grundsätzlich zusammen mit den anderen Daten auf einem gemeinsamen MPLS-VPN des Kunden erfolgen. Bei höheren QoS-Anforderungen oder bei der Forderung einer allgemeinen Trennung von VoIP und Daten kann auch ein dediziertes MPLS-VPN für VoIP verwendet werden.

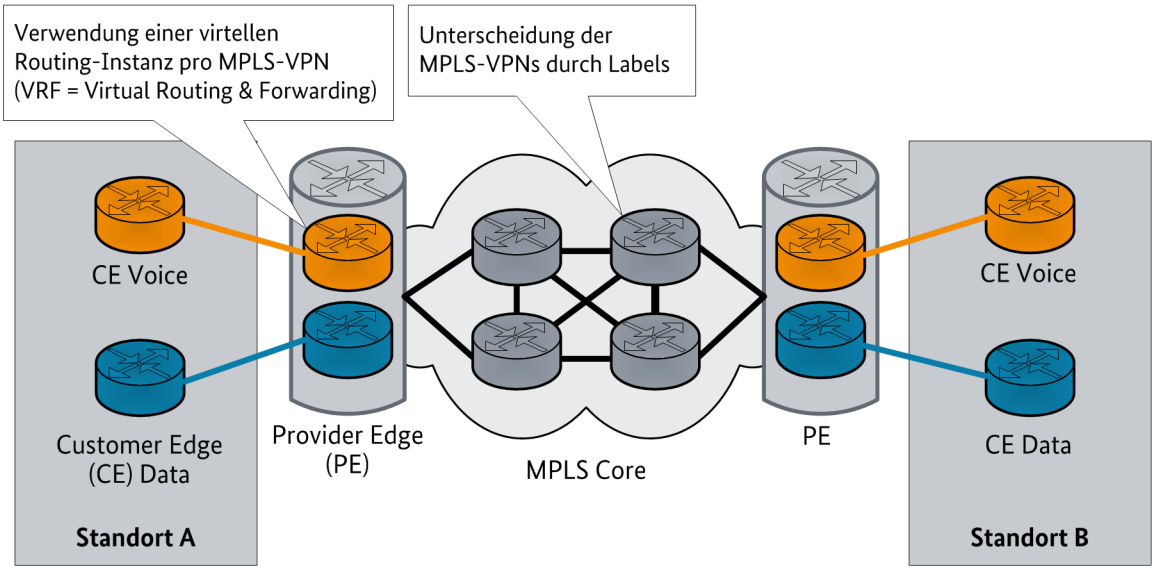


Abbildung 11: Exemplarische Darstellung der Trennung von Mandanten (Gruppen) bei MPLS durch MPLS-VPN

Bei Carrier Ethernet erfolgt die Trennung der Kundennetze auf eine ähnliche Weise wie in einem LAN durch Virtual LAN (VLAN). Dabei wird auf Layer 2 ein entsprechender Tag dem Paket zugefügt. Analog zu MPLS kann VoIP auf einem VLAN gemeinsam mit anderen Kundendaten transportiert werden oder es wird ein eigenes VLAN für VoIP für einen Kunden durch den Provider bereitgestellt.

Bei der Übertragung von VoIP über eine WAN-Strecke sind Delay und Jitter besonders wichtige Parameter. Es kann erforderlich sein, dass zumindest am WAN-Übergang und ggf. auch im WAN selbst durch den Provider die VoIP-Übertragung priorisiert werden muss.

Die Sicherheitsaspekte von MPLS wurden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in einer Kurzstudie analysiert (siehe [BSI MPLS-2009]). Hierbei wurden zwar keine in MPLS direkt verwurzelten Gefährdungen festgestellt, es besteht jedoch eine Vielzahl von generellen Gefährdungen, die aus der von den Kunden gemeinsam genutzten Infrastruktur resultieren. Es ist beispielsweise nicht ausgeschlossen, dass durch eine Fehlkonfiguration des Provider ein Paket unbeabsichtigt in ein falsches

MPLS-VPN ausgekoppelt wird. Grundsätzlich lassen sich viele der für MPLS betrachteten Gefährdungen auch auf Carrier Ethernet übertragen.

Aus diesen Gründen sind WANs stets als Netze mit eingeschränkter Vertrauenswürdigkeit zu werten.

Daher ist bei erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit und Integrität stets eine Verschlüsselung der Daten bei Übertragung über eine WAN-Strecke notwendig. Dies gilt auch für VoIP. In den BSI IT-Grundschutz-Katalogen (siehe [BSI GSK-2013]) wird beispielsweise im Baustein B 4.7 „VoIP“ in Maßnahme M 2.374 „Umfang der Verschlüsselung von VoIP“ eine angemessene Verschlüsselung von VoIP zwingend gefordert, sobald VoIP-Pakete das geschützte LAN verlassen.

Zur Verschlüsselung von VoIP über WAN-Strecken kommen unterschiedliche Optionen in Frage:

- Die Verschlüsselung kann auf Ebene der VoIP-Lösung mit SRTP für den Medienstrom und z. B. mit TLS für die Signalisierung erfolgen.
- Eine Verschlüsselung kann auf Ebene des Netzes durch den Aufbau eines eigenen Site-to-Site-IPsec-VPN (siehe hierzu Kapitel 13.3.4.3) erreicht werden. Eine solche Lösung kann vorteilhaft sein, wenn neben VoIP noch andere Daten zu verschlüsseln sind, da im Extremfall pauschal alle Daten, die über das WAN übertragen werden, per VPN abgesichert werden.
- Eine Verschlüsselung auf Ebene des Netzes kann auch durch den WAN-Provider durchgeführt werden. Dabei ist allerdings zu klären, ob dabei der Provider das Schlüsselmaterial verwaltet. Generell ist es sicherer, wenn ausschließlich der Kunde Kenntnis der Schlüssel hat.
- Bei Carrier Ethernet kommt zusätzlich als Option die Möglichkeit einer Verschlüsselung auf Layer 2 durch proprietäre Kryptoboxen und künftig auch durch IEEE 802.1AE „MAC[10] Security“ (siehe [IEEE 802.1AE-2006]) in Betracht.

Die Forderung einer Verschlüsselung gilt natürlich selbstverständlich auch für das Internet bzw. für alle Netze, die keinerlei Vertrauenswürdigkeit besitzen. Nur wird man hier noch höhere Anforderungen an die Absicherung der Kommunikation stellen müssen, was Stärke von Authentisierung und Verschlüsselung anbelangt.

Für international operierende Organisationen muss beachtet werden, dass dem Einsatz von Verschlüsselungstechniken zumindest in gewissen Ländern regulatorische Grenzen gesetzt werden. Wenn hierdurch ein Zwang zum Einsatz schwächerer Verfahren oder sogar zur Offenlegung von Schlüsseln besteht, muss durch technische Maßnahmen diese Schwächung lokal begrenzt werden und darf sich keinesfalls über die gesamte standortübergreifende Kommunikation erstrecken.

4.1.7.2 Verbindung verschiedener Standorte

Werden verschiedene Standorte einer Organisation über ein Netzwerk (z. B. WAN) verbunden, sind die in Kapitel 4.1.7.1 beschriebenen Techniken relevant. Sobald es sich bei der Organisation z. B. um einen Verbund von unterschiedlichen Gesellschaften handelt, kann es jedoch vorkommen, dass an den Standorten bereits eigene VoIP-Lösungen installiert sind, die ggf. sogar unterschiedliche Produkte von verschiedenen Herstellern nutzen können.

Bei der Verbindung unterschiedlicher Standorte muss in einer solchen Situation eine Kopplung von VoIP-Anlagen erfolgen.

Diese Kopplung kann beispielsweise durch Etablierung einer abgesicherten Verbindung zwischen den Telefonie-Servern der beteiligten Standorte (z. B. über einen mit IPsec oder TLS verschlüsselten SIP Trunk) realisiert werden, wie in Abbildung 12 dargestellt. Wenn dies allerdings herstellerübergreifend vorgenommen werden muss, ist mit Einschränkungen in den zur Verfügung stehenden Leistungsmerkmalen zu rechnen.

10 MAC = Media Access Control

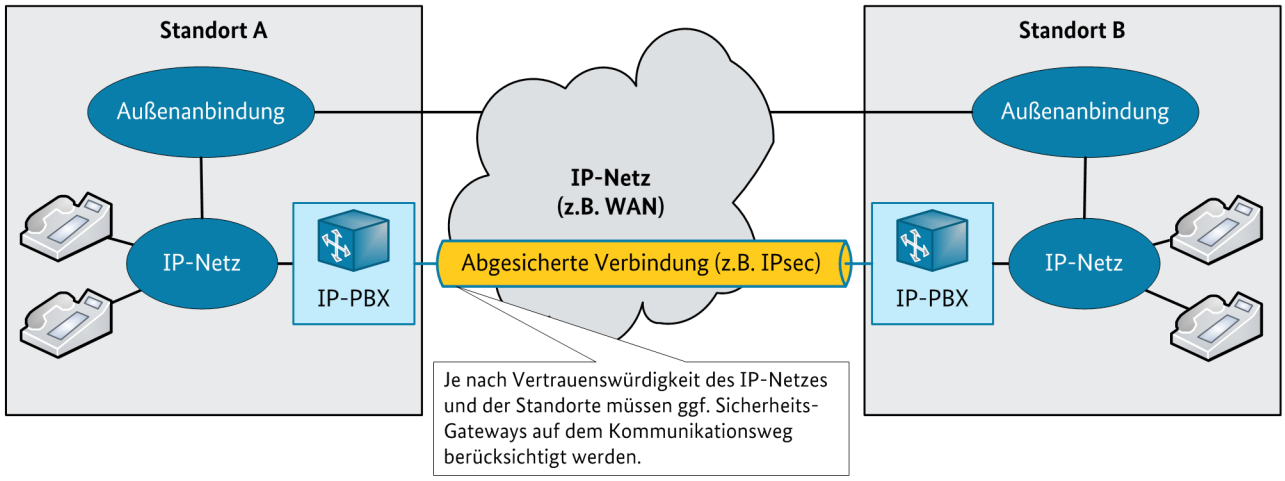


Abbildung 12: Anlagenkopplung über ein IP-Netz

4.1.7.3 Anbindung von Außenstellen

Für ein Szenario, in dem eine größere Zahl meist kleineren Außenstellen einer Organisation über VPN oder über eine WAN-Verbindung an eine Zentrale angebunden wird, muss eine VoIP-Lösung geeignet gestaltet werden. Solche Außenstellen betreiben in der Regel keine eigenständigen TK-Systeme (Filialen) oder maximal abgesetzte rudimentäre TK-Installationen (kleine Standorte).

Wesentliches Element ist die Sicherstellung der Verfügbarkeit der Telefonie in einer Außenstelle auch bei einem Ausfall von Verbindungen zur Zentrale.

Typischerweise verwendet man zentrale VoIP-Server und die Signalisierung der IP-Telefone erfolgt über WAN bzw. VPN. Für die Anbindung an das PSTN werden oft zentrale Gateways genutzt. Gespräche von den Filialen in das PSTN laufen dann grundsätzlich über die Zentrale. Hierzu sind die Übertragungswege dem Schutzbedarf der Telekommunikation entsprechend abzusichern. Neben dem Einsatz gesicherter VPNs (z. B. IPsec-VPNs) ist auch eine Verschlüsselung der Signalisierung und des Medienstroms, d. h. die Verwendung von z. B. TLS für die Signalisierung und SRTP für den Medienstrom, möglich.

Wenn für die Absicherung der Kommunikation ein Site-to-Site-VPN mit IPsec verwendet werden soll, ist Folgendes zu beachten: Die Kommunikation zwischen den VoIP-Endgeräten ist eine Peer-to-Peer-Kommunikation, da der RTP-Medienstrom direkt zwischen den beteiligten Endgeräten übertragen wird. Für VoIP wäre daher eine direkte VPN-Verbindung zwischen Außenstellen wünschenswert, was ein vollvermaschtes Site-to-Site-VPN zur Folge hätte. Bei einem vollvermaschten Site-to-Site-VPN entspricht die Anzahl der aufzubauenden Security Associations (SAs) und damit der Realisierungsaufwand der Anzahl der möglichen Kommunikationsbeziehungen zwischen den Außenstellen sowie zwischen Zentrale und Außenstellen. Da diese Anzahl quadratisch mit der Anzahl der Außenstellen anwächst, ist eine solche Lösung bereits bei einer kleineren Anzahl von Außenstellen sehr aufwendig.

Als Optionen kommt dann der Aufbau eines Hub-and-Spoke-VPN in Frage, d. h. die VoIP-Kommunikation (auch zwischen Außenstellen) wird stets über die Zentrale geleitet, wie in Abbildung 13 dargestellt. In diesem Fall entspricht die Anzahl der SAs der Anzahl der Außenstellen. Alternativ können herstellerspezifische Lösungen in Betracht gezogen werden, die es gestatten, SAs in einem IPsec-VPN gruppenweise aufzubauen (z. B. gemäß [IETF RFC6407-2011]) und so den Aufwand zu reduzieren.

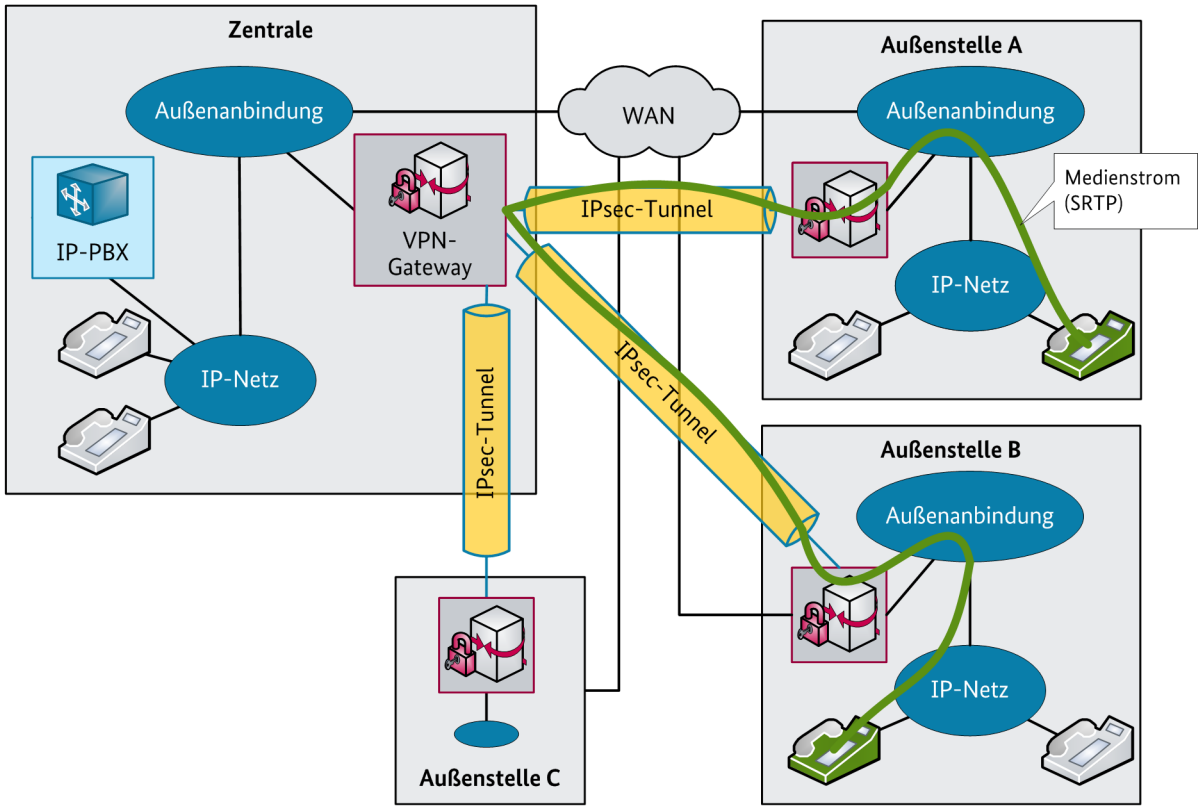


Abbildung 13: Verwendung eines Hub-and-Spoke-VPN zur Übertragung von VoIP

Bei Ausfall der Anbindung an die Zentrale kann es erforderlich sein, dass zumindest ein Notbetrieb der Telefonie sichergestellt werden kann. Hierzu bieten die TK-Ausrüster unterschiedliche Lösungen an, die auf einem gemeinsamen Prinzip basieren. Auf einer herstellerspezifischen Plattform werden ein meist rudimentärer Telefonie-Server und ein PSTN-Gateway realisiert (siehe Abbildung 14). Diese Komponenten können auf einer gemeinsamen Hardware laufen oder in getrennten Elementen untergebracht werden. Bei Ausfall der Verbindung zur Zentrale übernimmt automatisch das lokale Notsystem und die IP-Telefone in der Außenstelle kommunizieren über das Notsystem. Zu beachten ist, dass Funktionsumfang und Kapazität der Notversorgung meist erheblich reduziert sind und sich auf die reine Telefonie beschränken. Es ist wichtig, dass ein solcher Notbetrieb dem Nutzer signalisiert wird, um auf das ggf. geringere Sicherheitsniveau und die eingeschränkte Funktion hinzuweisen.

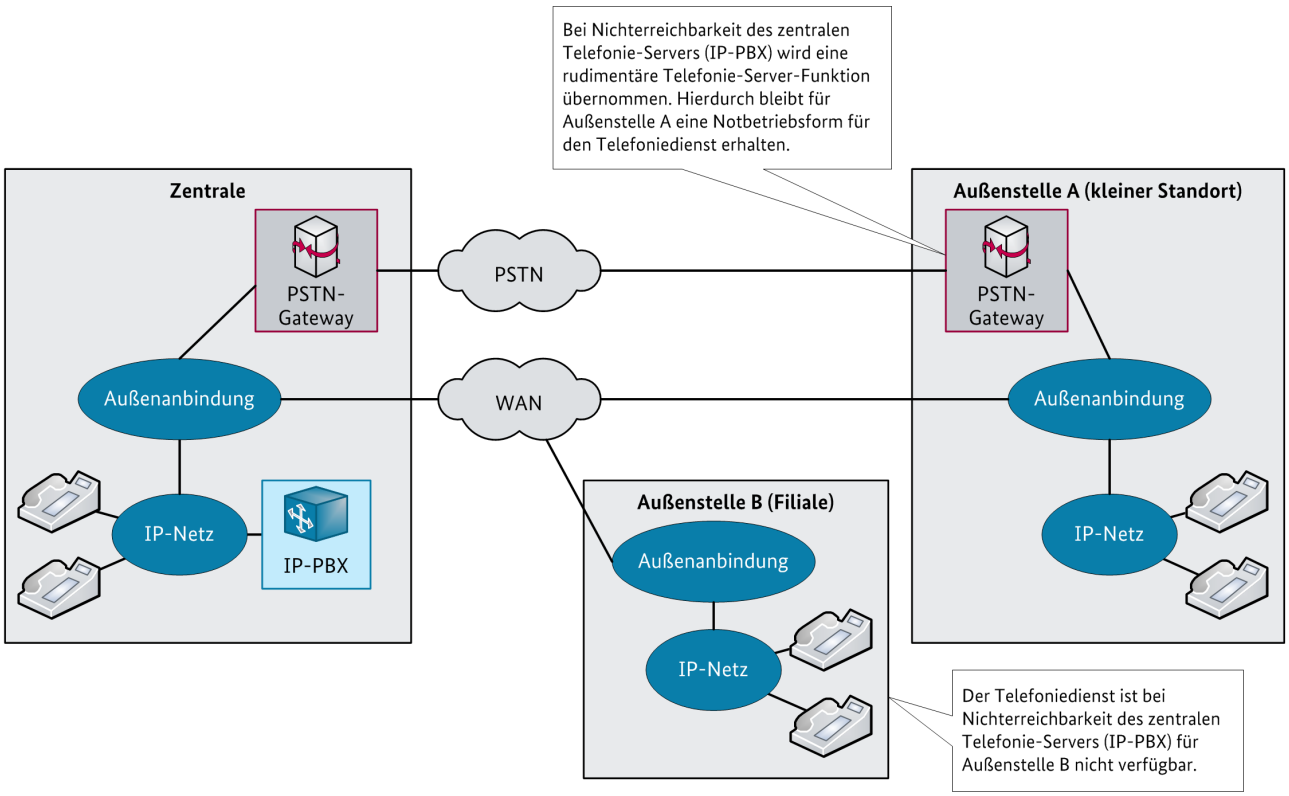


Abbildung 14: Notbetriebsfunktion für Außenstellen am Beispiel eines PSTN-Gateway mit rudimentärer Telefonie-Server-Funktion

4.1.7.4 Anbindung von Telearbeitsplätzen

Eine sichere Anbindung von Telearbeitsplätzen kann für die Unterstützung von VoIP auf unterschiedliche Weisen vorgenommen werden, die im Folgenden kurz dargestellt werden.

Absicherung auf Ebene des Netzwerks

Über ein konventionelles Client-to-Site-VPN, bei dem die Clients (z. B. PCs) einen VPN-Client als Software-Komponente erhalten, kann – unter der Voraussetzung einer angemessenen Leistung von VPN und zugrunde liegendem Netzwerk – grundsätzlich auch VoIP genutzt werden. Die Härtung der Endgeräte ist für eine solche Lösung von besonderer Bedeutung, da diese bei einem Client-to-Site-VPN ggf. direkt an ein unsicheres Netz (z. B. an das Internet) angebunden sind. Hier unterscheidet sich VoIP nicht von anderen IT-Anwendungen.

Als Alternative ist auch der Einsatz von kleinen VPN-Gateways als Kryptoboxen am Telearbeitsplatz möglich, um Telearbeitsplätze über ein Site-to-Site VPN zu integrieren. Dabei ist die Sicherheit der Kryptoboxen natürlich von entscheidender Bedeutung. Außerdem muss beachtet werden, dass das lokale Netzwerk am Telearbeitsplatz aus dem Blickwinkel einer Site-to-Site-VPN-Lösung als vertrauenswürdig zu sehen ist.

Absicherung auf Ebene von VoIP

Über einen zentralen SBC der Organisation (oder durch eine vergleichbare Lösung) können auch die IP-Telefone und Softphones anderer Standorte der Organisation und insbesondere Telearbeitsplätze sowie mobile Endgeräte angebunden werden, wie in Abbildung 15 exemplarisch gezeigt. Hierzu wird das IP-Telefon bzw. das Softphone am Telearbeitsplatz oder im mobilen Endgerät so konfiguriert, dass es beispielsweise für einen ausgehenden Ruf den SBC kontaktiert, der dann die Anfrage an den zentralen Telefonie-Server der Organisation weiterleitet. Die Signalisierung kann dann beispielsweise mit TLS abgesichert werden und wenn die Sitzung aufgebaut ist, kann der Medienstrom zwischen IP-Telefon und

SBC mit SRTP abgesichert werden. Auf diese Weise kann auch ein unsicheres Netz zwischen Heimarbeitsplatz und dem Standort des SBC der Organisation genutzt werden.

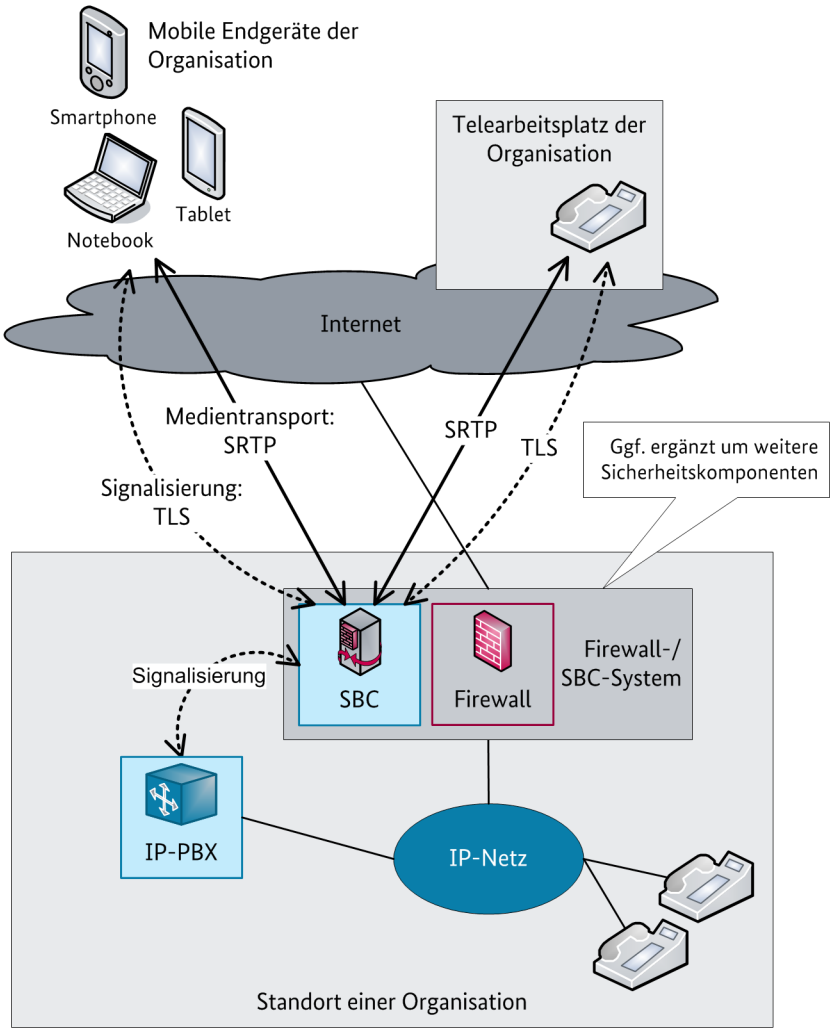


Abbildung 15: Verwendung eines SBC zur Anbindung von Telearbeitsplätzen und mobilen Endgeräten

4.1.8 VoIP über Vertrauensgrenzen hinweg

Für die VoIP-Kommunikation über Vertrauensbereiche hinaus ist es erforderlich, den VoIP-Verkehr (Signalisierung und Medientransport) an einem Sicherheits-Gateway zwischen den Vertrauensbereichen geeignet zu filtern, wie in Abbildung 16 illustriert.

Beispiele sind die Kommunikation zwischen unterschiedlichen Organisationen oder die Kommunikation zwischen einem Softphone, das dem Datennetz zugeordnet ist, und einem IP-Telefon in einem abgetrennten VoIP-Netz.

Die Filterung kann aus zwei Perspektiven erfolgen:

- Erkennung und Weiterleitung erlaubter Kommunikation durch eine Firewall-Funktion
- Erkennung und Blockierung von Kommunikationsanomalien (insbesondere von Angriffen) durch ein Intrusion Prevention System (IPS)

Diese Funktionen können in einem Gerät oder in getrennten Geräten realisiert werden.

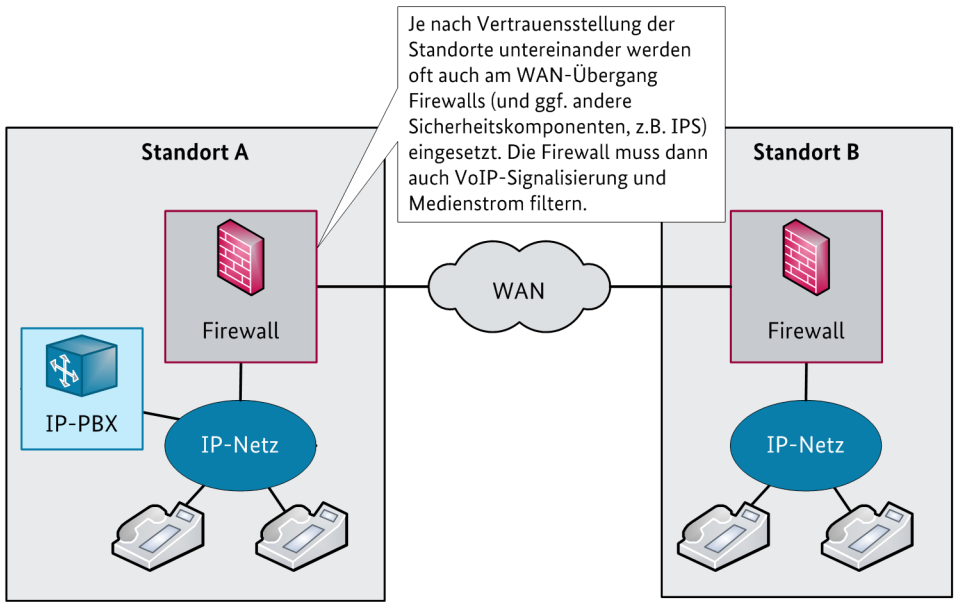


Abbildung 16: Filterung von Medienstrom und Signalisierung bei VoIP-Kommunikation über Vertrauensgrenzen hinweg

Die für eine RTP-Übertragung zu verwendenden RTP-Ports werden im Rahmen der Signalisierung (z. B. per Session Description Protocol, SDP) zwischen den Endpunkten ausgetauscht. Diese Ports variieren in der Regel bei jedem neuen Gespräch. Eine auf einem dynamischen Paketfilter basierende Firewall stößt hier an Grenzen, denn große Portbereiche müssten für RTP-Pakete dauerhaft freigeschaltet werden. Dies stellt ein erhebliches Risiko dar, da eine sehr große Angriffsfläche für DoS- und andere Attacken geschaffen wird.

Eine Firewall mit VoIP-Applikationsintelligenz ist daher zu empfehlen.

Dabei sind für das verwendete Signalisierungsprotokoll entsprechende Parser zu unterstützen. Durch die Analyse der Signalisierung kann die Firewall die für eine Sitzung zu verwendenden Ports feststellen und diese dynamisch für die Dauer der Sitzung freischalten. Die Feststellung der Zuordnung von Sitzungen und Ports ist für eine IPS-Funktion ebenfalls relevant.

Falls die Signalisierung verschlüsselt übertragen wird, hat eine Firewall oder ein IPS zunächst keine Möglichkeit, die Signalisierungsinformationen zu analysieren und insbesondere die Ports für die RTP- bzw. SRTP-Kommunikation zu ermitteln. Die Firewall muss in diesem Fall einen Endpunkt der Verschlüsselung realisieren. Manche Hersteller von Firewalls und IPS bieten hierzu die Funktion eines Proxy für Secure Socket Layer (SSL-Proxy) bzw. TLS-Proxy an, der im Sinne eines vertrauenswürdigen, „freundlichen“ Man-in-the-Middle zwischen den Kommunikationspartnern die TLS-Kommunikationsbeziehung in beide Richtungen terminiert, wie in Abbildung 17 dargestellt. Diese Funktion ist aus der Sicherheitsperspektive allerdings kritisch zu bewerten, da keine Ende-zu-Ende-Verschlüsselung zwischen den eigentlichen Signalisierungsinstanzen besteht.

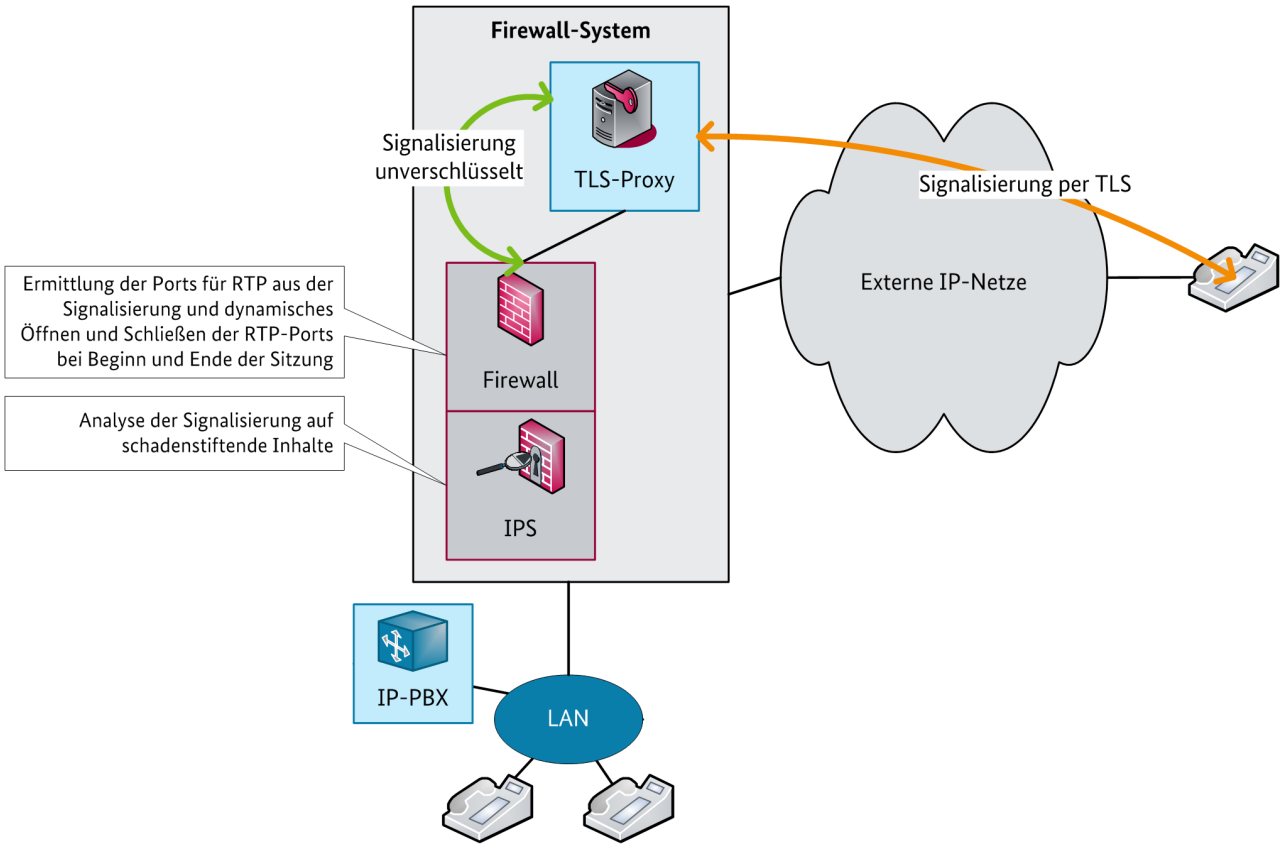


Abbildung 17: Verwendung einer Proxy-Funktion zur Entschlüsselung der Signalisierung, um Analyse des Verkehrs durch Firewall-System zu ermöglichen

Alternativ kann die Firewall auch als Session Border Controller (SBC) aktiver Bestandteil des VoIP-Systems werden und so automatisch zum Endpunkt einer verschlüsselten Signalisierungssitzung werden, siehe hierzu auch das Kapitel 4.1.6 zum IP-Anlagenanschluss.

Weiterhin ist die Verwendung von Network Address Translation (NAT) bei der Übertragung von VoIP problematisch, da in einigen VoIP-Signalisierungspaketen die IP-Adresse verwendet wird.

[IETF RFC5389-2008] definiert einen Ansatz zur Lösung dieses Problems unter der Bezeichnung Session Traversal Utilities for NAT (STUN). Dabei kann ein NAT Binding, d. h. die öffentliche (externe) IP-Adresse und die Abbildungsvorschrift zwischen den internen und den externen Ports, über einen STUN-Server von einem STUN-Client im Endgerät abgefragt werden. Weitere Ansätze, die allerdings noch nicht in standardisierter Form, d.h. als RFC (Request for Comment) vorliegen, sind Traversal Using Relay NAT (TURN, siehe [IETF RFC5766-2010]) und Interactive Connectivity Establishment (ICE, siehe [IETF RFC5245-2010]). ICE ist für SIP spezifiziert, funktioniert aber auch mit H.323.

4.1.9 Virtualisierung von VoIP-Systemen

Grundsätzlich können die zu einem VoIP-System gehörenden zentralen Komponenten auch als VM auf einem Virtualisierungs-Host betrieben werden, sofern der Hersteller diese Betriebsform unterstützt. Dies gilt sogar für Telefonie-Server. Dabei sind jedoch die im Folgenden beschriebenen Aspekte zu berücksichtigen.

Die VMs konkurrieren bei Überbuchung des Virtualisierungs-Host um Ressourcen, was sich negativ auf die Leistung des VoIP-Systems auswirken und im schlimmsten Fall für den Nutzer spürbar sein kann.

Die zentralen Komponenten eines VoIP-Systems verarbeiten schützenswerte Daten, die häufig mit einem erhöhten Schutzbedarf hinsichtlich der Vertraulichkeit und Integrität verbunden sind. Hier ist insbesondere die Frage zu klären, ob die Schutzmaßnahmen der Virtualisierungslösung ausreichen, um solche VMs mit anderen ggf. unsicheren VMs zusammen auf einem Virtualisierungs-Host betreiben zu dürfen, oder ob hier eine physische Trennung notwendig ist.

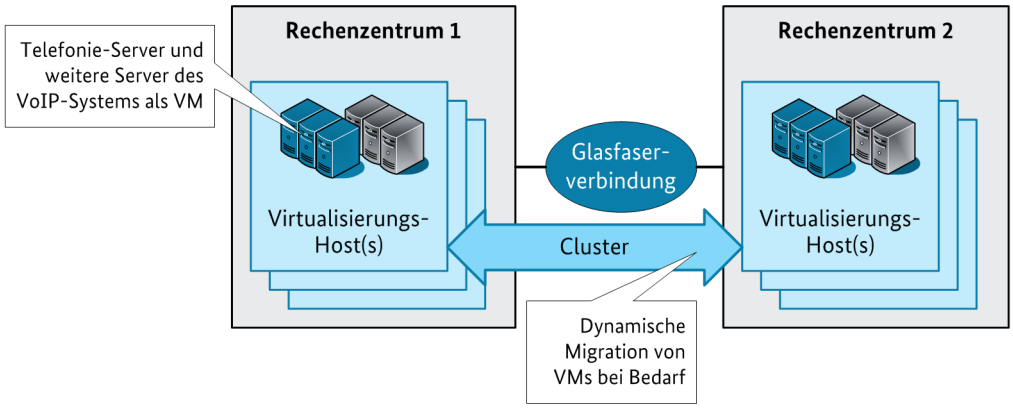


Abbildung 18: Virtualisierung von VoIP- und UCC-Servern

Außerdem können Softphone-Anwendungen prinzipiell auch über Terminal-Server oder im Rahmen der Virtualisierung von Clients durch eine Virtual Desktop Infrastructure (VDI) bereitgestellt werden. Bei einer solchen Nutzungsform sind Signalisierung und Medienstrom im Terminal-Server bzw. in der zentralen VDI-Lösung terminiert. Zum physischen Endgerät des Nutzers (sogenannter Thin Client) werden nur Mikrofon-, Video-, Tastatur- und Mausdaten über das verwendete Terminal-Server-Protokoll übertragen. Beispiele für solche Protokolle sind die Independent Computing Architecture (ICA) und das Remote Desktop Protocol (RDP). Abbildung 19 illustriert das Grundprinzip. Sofern die Qualität der Kommunikationsverbindung zwischen Thin Client und Terminal-Server akzeptabel ist, kann ein solcher Ansatz sich grundsätzlich als praktikabel erweisen.

Aus der Terminal-Server-Kommunikation kann ein Angreifer jedoch grundsätzlich in einem gewissen Umfang und mit entsprechender Mühe auch die Nutzdaten extrahieren. Dies ist insbesondere bei Sprachkommunikation der Fall. Wenn ein Terminal-Server-Protokoll über eingeschränkt vertrauenswürdige Netze übertragen wird, muss daher insbesondere bei einem erhöhten Schutzbedarf hinsichtlich der Vertraulichkeit die Kommunikation zusätzlich z. B. mit TLS verschlüsselt werden.

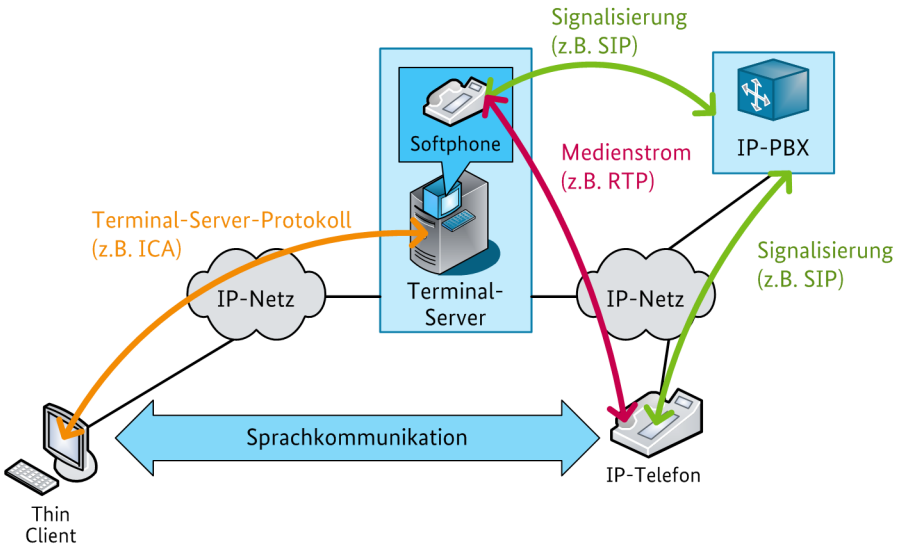


Abbildung 19: Nutzung von VoIP über Terminal-Server über zentrales Hosting einer Softphone-Anwendung (vereinfacht)

Terminal-Server-Protokolle waren ursprünglich nicht für Sprach- und Multimediakommunikation mit hoher Qualität gedacht. Es kann daher z. B. für VoIP durchaus vorkommen, dass die Terminierung von Signalisierung und Medienstrom in einem zentralen Desktop-Server zu signifikanten Qualitätseinbußen führt und je nach System sind auch funktionale Einschränkungen nicht ausgeschlossen. Dies wird auch als Hairpinning-Problem bezeichnet. Abhilfe kann hier eine Auskopplung der Medienströme am Endgerät schaffen, die die Belastung des Netzes und der Netzübergänge zwischen Terminal-Server und Thin Client sowie des Terminal-Servers reduziert.

Hierzu muss ein Teil der Applikationslogik des Softphones, der für die Codierung und Decodierung des Medienstroms zuständig ist, auf dem Thin Client ausgeführt werden. Dies kann durch Verteilung dieser Applikationslogik als Plug-in für den Thin Client realisiert werden. Ergänzend zu der traditionellen zentralen Ausführung (Hosting) von Anwendungen über Terminal-Server bzw. eine VDI-Lösung unterstützen zudem manche Lösungen in einem gewissen Umfang das sogenannte Anwendungs-Streaming von Anwendungen oder Anwendungskomponenten auf die Thin Clients. In beiden Fällen wird in einem gewissen Umfang auch Anwendungslogik auf dem Thin Client ausgeführt. Damit vererben sich natürlich alle Gefährdungen, die die Anwendungskomponenten und die verwendeten Kommunikations-protokolle betreffen, auf den Thin Client. Diese müssen bei der Planung von Sicherheitsmaßnahmen entsprechend berücksichtigt werden. Wenn im Rahmen von Streaming beispielsweise auch Softphone-Bestandteile auf dem Thin Client ausgeführt werden und dabei die RTP-Kommunikation auf dem Thin Client terminiert wird (siehe Abbildung 20), ist es wesentlich, dass diese Kommunikation wie bei einem Fat Client abgesichert werden kann, etwa durch die Verwendung von SRTP.

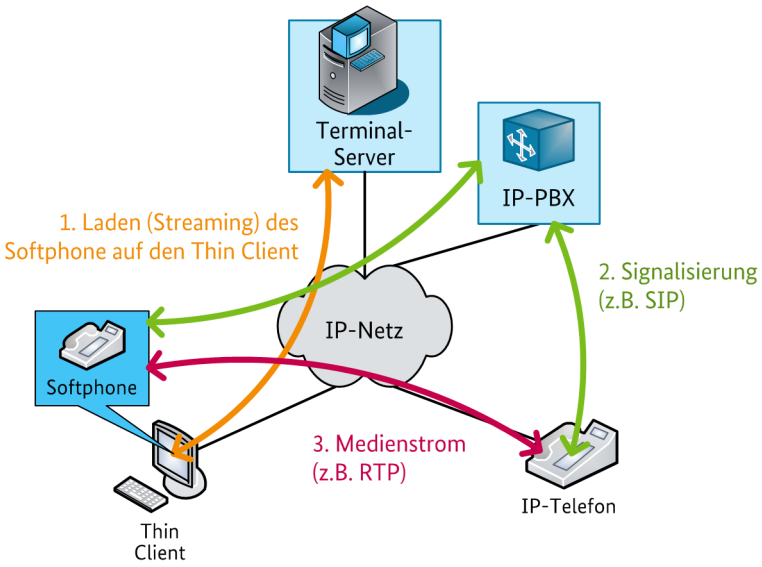


Abbildung 20: Streaming eines Softphone und Terminierung des Medienstroms auf dem Thin Client (vereinfacht)

4.2 Gefährdungen

Im Folgenden werden die VoIP-spezifischen Gefährdungen inkl. des IP-Anlagenanschlusses auf Basis der in Kapitel 4.1 beschriebenen technischen Grundlagen analysiert.

4.2.1 Höhere Gewalt

Auf VoIP-Installationen treffen wie für alle digitalen Anlagen-Lösungen allgemein die Gefährdungen durch höhere Gewalt zu, die in den BSI IT-Grundschutz-Katalogen (siehe [BSI GSK-2013]) genannt sind.

Spezifische Ausprägungen bei einem VoIP-Einsatz innerhalb eines Unternehmens oder einer Behörde ergeben sich im Sinne folgender Besonderheiten:

- Abhängigkeiten von der durch VoIP mitgenutzten IP-Infrastruktur

  VoIP stützt sich auf Basisdienste wie DNS und Dynamic Host Configuration Protocol (DHCP) sowie auf Netzwerkinfrastrukturen in LAN und WAN. Hieraus ergeben sich Gefährdungsketten, die sich auf VoIP-Installationen mittelbar auswirken.

- Nutzung drahtloser Kommunikationsformen

  Die in diesem Zusammenhang für VoIP auf drahtloser Kommunikationsbasis zu berücksichtigenden Gefährdungen sind identisch mit den entsprechenden Betrachtungen in Kapitel 9.2.

Für eine Organisation, die einen IP-Anlagenanschluss verwendet, bestehen Gefährdungen durch höhere Gewalt primär in den Bereichen der Anbindung und der Übertragungswege zum ITSP sowie in der Infrastruktur des ITSP selbst. Die Gefährdungslage entspricht hier weitgehend den in den IT-Grundschutz-Katalogen (siehe [BSI GSK-2013]) beschriebenen Gefährdungen eines Internetzugangs sowie den Gefährdungen für ein VoIP-System mit PSTN-Übergang über ein ISDN-Gateway. Unterschiede bestehen aber darin, dass die Übertragung IP-basiert erfolgt und die Infrastruktur des ITSP gemeinsam mit anderen Kunden des ITSP genutzt wird. Auf diese Weise können sich Seiteneffekte ergeben.

G-TK-18 Ausfall der mitgenutzten IP-Infrastruktur

Eine spezielle Gefährdung ergibt sich bei VoIP durch die Abhängigkeit von IT-Lösungen, die nicht vom TK-Betreiber selbst verantwortet werden:

- Abhängigkeit von vorgelagerten Diensten (DNS, DHCP usw.), die teilweise nicht in Hand des TK-Systembetreibers liegen
- Abhängigkeit von einer Netzwerkinfrastruktur, die nicht in Hand des TK-Systembetreibers liegt

Je nach Betriebskonstellation kommt verschärfend hinzu, dass die Störungsbehandlung über die Grenzen einer einzelnen inhaltlichen Zuständigkeit hinweg (VoIP-Installationen, von VoIP mitgenutzte IT) erfolgen muss, zum Teil sogar über die Grenzen von Abteilungen bzw. Behördeninstanzen hinweg.

G-TK-19 Ausfall eines für VoIP mitgenutzten Weitverkehrsnetzes

Wird ein Standort über ein Weiterverkehrsnetz (Wide Area Network, WAN) mit den übrigen Standorten einer Organisation verbunden und über diesen Weg auch die interne Telefonie mittels VoIP realisiert, so kommt der Verfügbarkeit des WAN eine erhöhte Bedeutung zu.

Häufig ist die VoIP-Lösung so ausgelegt, dass der Boot-Vorgang von Telefonen oder die Ruf-Signalisierung nur mit Hilfe von Servern in einem zentralen Standort erfolgen kann. Hier bedeutet der Ausfall der Weitverkehrsanbindung aus Sicht eines Standortes ohne eigene derartige Server auch den Verlust der Telefoniermöglichkeit.

Dies ist umso bedeutsamer, als dass davon auch wichtige telefonische Notrufmöglichkeiten betroffen sind. Außerdem ist eine Kommunikation des vom WAN abgeschnittenen Standorts mit den IT-Betreibern über die Störung und das weitere Vorgehen per VoIP nicht mehr möglich.

4.2.2 Organisatorische Mängel

Organisatorische Mängel treffen VoIP-Lösungen grundsätzlich genauso wie beliebige andere IT. Allerdings muss berücksichtigt werden, dass beim Einsatz von VoIP die Kommunikationsinfrastruktur und teilweise auch die Endgeräte gemeinsam mit IT-spezifischen Anwendungen genutzt werden. Im organisatorischen Bereich müssen daher VoIP-Systeme als Anwendungen mit besonderen Anforderungen aufgefasst werden.

Bei einem IP-Anlagenanschluss muss primär beachtet werden, dass mit IP die Sprach- bzw. allgemein die Multimedia-Kommunikation zum ITSP über ein grundsätzlich unsicheres Protokoll abläuft. Hier müssen beide Parteien, d. h. der ITSP und das Unternehmen bzw. die Behörde, die sich daraus ergebende

Gefährdungslage beachten. Die Auslagerung des PSTN-Übergangs hat darüber hinaus auch Konsequenzen für die lokale Infrastruktur.

Mit der VoIP-Einführung müssen bestehende Entscheidungen und Konzepte für eine solche durch VoIP mitgenutzte IT gezielt überprüft werden. Dies beinhaltet insbesondere:

- die Schutzbedarfsfeststellung
- die zentralen Elemente von Sicherheitskonzepten
- die organisatorischen Regelungen im Bereich Technik-Betrieb

Ein ordnungsgemäßer Betrieb der Telefonie ist zu gewährleisten und dabei ist die von VoIP mitgenutzte Infrastruktur entsprechend zu verwalten. Hierzu gehören Regelungen in den Bereichen:

- Wartungsfenster
- Verhalten bei Sicherheitsvorfällen (z. B. Sperrung aller nicht-VoIP-spezifischen Ports auf Firewalls statt vollständiger Stilllegung der Außenanbindung)
- Change Management: Abstimmung zwischen Telefonie-Betreiber und den Betreibern der weiteren IT-Infrastrukturkomponenten bei der Planung und Durchführung von Changes bezüglich des IP-Netzes, grundlegenden Infrastrukturdiensten wie DNS und DHCP sowie Endgeräte-Installationen

Ausgehend von diesen Überlegungen lassen sich neben den in den BSI IT-Grundschutz-Katalogen (siehe [BSI GSK-2013]) im Baustein B 4.7 „VoIP“ genannten Gefährdungen folgende VoIP-spezifischen Gefährdungen ermitteln, die insbesondere in Bereichen mit erhöhtem Schutzbedarf zu beachten sind.

G-TK-20 Unzureichende Regelungen für den Einsatz von VoIP

Für den Einsatz von VoIP sind Regelungen zu treffen und einzuhalten, die der Bedeutung der Telefonie für ein Unternehmen bzw. Behörde gerecht werden.

Wird dieser Bedeutung nicht oder nur unzureichend entsprochen oder werden die entsprechenden Regelungen nicht konsequent umgesetzt, so besteht die Gefahr, dass die Grundwerte Verfügbarkeit, Vertraulichkeit und Integrität sowie gegebenenfalls weitere Grundwerte nicht oder nur unzureichend erreicht werden. Dies hat neben einer möglichen Ablehnung durch die Nutzer auch akute Sicherheitslücken zur Folge.

Beispiele zu Regelungsaspekten und Gefährdungen bei VoIP-Lösungen sind:

- Regelungen zur Wahrung der Vertraulichkeit von Nachrichten einer Sprach-Mailbox in Dateiform

  Nachrichten einer Sprach-Mailbox können im Rahmen von VoIP-Lösungen als Multimedia-Dateien vorliegen. Gefahren drohen bei unüberlegtem Anlegen von Kopien solcher Dateien, z. B. bei lokaler Speicherung auf einem Notebook, der Speicherung in Nutzer- und/oder Projektablagen auf einem File-Server oder der Aufbewahrung als Anlage einer E-Mail im Postfach des Anwenders. Hieraus kann ein Vertraulichkeitsverlust erfolgen. Weiterhin kann in Summe der Ressourcenverbrauch enorm sein.

- Einsatz von Messtechnik im Umfeld von Netzwerk-Bereichen, die durch VoIP mitgenutzt werden

  Mit Hilfe von Analysator-Software, wie sie zur Diagnose in Netzwerken (LAN und WAN) eingesetzt wird, ist es möglich, den Inhalt des Telefonats aufzuzeichnen und nachträglich anzuhören. Der Einsatz solcher Diagnosetechnik muss so geregelt sein, dass keine Verletzung von Datenschutz- und Persönlichkeitsrechten des Telefonie-Anwenders droht.

G-TK-21 Unzureichende Harmonisierung zwischen IT- und VoIP-Betrieb

Falls vor der VoIP-Einführung IT- und TK-Betrieb getrennt waren und der bisherige TK-Betreiber den Betrieb der VoIP-Lösung wahrnimmt, muss die Kooperation dieser beiden Verantwortungsbereiche erst etabliert werden. Dies betrifft den kompletten Lebenszyklus der Installationen von der Planung bis zur Außerbetriebnahme.

Durch eine unzureichende Harmonisierung zwischen IT- und VoIP-Betrieb ist mindestens die Verfügbarkeit der IP-Telefonie stark gefährdet.

G-TK-22 Fehlende, ungeeignete und inkompatible Betriebsmittel für VoIP

VoIP-Lösungen bringen einerseits neue Geräte in das IP-Netz ein, andererseits besteht durch diese Vernetzung die Möglichkeit, sie in vorhandene IT-Betriebslösungen wie Backup und Restore einzubinden. Dies setzt allerdings voraus, dass die VoIP-Geräte (Telefone, Server und Gateways) in den IT-Planungen zu Betriebsmitteln ausreichend berücksichtigt werden. Typische Gefahrenmomente sind hier:

- unzureichende Auslegung des Access-Bereichs mit für Telefonie geeigneten Anschlüssen (insbesondere inklusive Power over Ethernet, PoE)
- bei Einsatz von VoIP-Endgeräten mit eigenem Netzteil zur Spannungsversorgung: Fehlen der notwendigen Steckdosen am Arbeitsplatz
- nicht ausreichende Adresskonzeption zur Versorgung der VoIP-Endgeräte
- nicht ausreichende Kapazitäten im Bereich Speicherplatzbedarf und Ressourcen sowie unzureichende Zeitplanung für die Backup-Restore-Lösung zur Sicherung von Dateien der Sprachmailbox

Die genannten Punkte können zu einer eingeschränkten Verfügbarkeit sowie zu einem Datenverlust führen. Als Beispiel kann hier eine unzureichende Stromversorgung von IP-Telefonen genannt werden.

G-TK-23 Unzureichende Verwaltung und Kontrolle von Zugangs- und Zugriffsmöglichkeiten auf VoIP-Endgeräte

Durch die Möglichkeit zum Abrufen von Kontaktinformationen auf VoIP-Endgeräten, bei Softphones sogar zum Abspeichern solcher Informationen, werden diese Geräte relevant für den Datenschutz.

Während bei mobilen Datenendgeräten (z. B. Notebooks) eher von geeigneten, vom Nutzer nicht umgehbaren Sicherheitsvorkehrungen Gebrauch gemacht werden kann, sind die Möglichkeiten im Bereich IP-fähiger mobiler Telefonie-Endgeräte noch begrenzt.

Bei solchen Telefonie-Endgeräten kommt der Sorgfalt des Anwenders im Umgang mit (Schutzmechanismen für) Kontaktdaten und ähnlichen Daten verstärkte Bedeutung zu.

Bei frei zugänglichen Telefonen besteht die Gefahr, dass über das gewünschte Dienstspektrum hinaus (z. B. Notruf) Funktionen am Gerät genutzt werden können.

Außerdem besteht auf VoIP-Endgeräten typischerweise die Möglichkeit, lokal am Gerät Konfigurationsänderungen vorzunehmen. Diese sind ab Werk durch Default-Kennwörter bzw. -PINs geschützt. Werden diese nicht vor Freigabe für den Anwender abgeändert, drohen Manipulationen am VoIP-Endgerät.

G-TK-24 Kein ordnungsgemäßer Benutzerwechsel für VoIP-Endgeräte

Für IP-Telefone kann bei Verzicht auf personenbezogene Nutzerprofile ein Nutzer die Möglichkeit zur Nutzung von Leistungsmerkmalen erlangen, die nicht für diesen Nutzer bestimmt sind, sondern für den vorherigen Nutzer freigeschaltet waren. Weiterhin ermöglichen ungelöschte Anruflisten einem nachfolgenden Nutzer, Informationen über zuletzt vom Vorgänger geführte Telefonate zu erlangen. Dies kann z. B. zur Verletzung des Datenschutzes führen.

Auch bei Verwendung von Nutzerprofilen auf IP-Telefonen kann ein nicht ordnungsgemäßer Benutzerwechsel dazu führen, dass dem Nachfolgenutzer nicht alle Leistungsmerkmale zur Verfügung stehen, die für ihn vorgesehen sind.

Die für ein IP-Telefon beschriebene Gefährdung ist bei einem ungeordneten Benutzerwechsel an einem PC in folgenden Punkten für VoIP relevant:

- Einsatz einer Softphone-Lösung
- Browser-basiert nutzbare VoIP-Funktionen, die wegen ungelöschten Informationen (z. B. URL-Historie, Bookmarks, Cookies) eine Gefährdung darstellen können
- lokal gespeicherte personenbezogene Daten (z. B. Kontaktinformationen von Gesprächspartnern des bisherigen PC-Nutzers)

G-TK-25 Mangelhafte Behandlung der Archivierung von Sprachnachrichten und elektronischen Faxnachrichten

Datenarchivierung kann bei VoIP-Lösungen primär in folgenden Bereichen anfallen:

- Archivierung von Verbindungsdaten und Abrechnungen
- Archivierung von Protokollen der Telefonate in Form von Multimedia-Dateien
- Archivierung von Dateien der Sprach-Mailbox
- Archivierung von Faxein- und -ausgängen sowie von Faxausdrucken

Werden diese Archivierungsformen nicht ausreichend geregelt und berücksichtigt, so drohen einerseits Verletzungen der Vertraulichkeit oder des Datenschutzes. Weiterhin sind Verletzungen von Aufbewahrungspflichten möglich, etwa durch ungeeignete Lösungen, die nicht für die Archivierung von VoIP-Multimedia, insbesondere Dateien der Sprach-Mailbox und Faxnachrichten ausgelegt sind.

G-TK-26 Unzulängliche vertragliche Regelungen für externe Leistungen zur VoIP-Lösung

Eine Gefahr besteht hier vor allem bei allzu unreflektierter Anlehnung an Dienstleistungs- bzw. Wartungsverträge für bestehende ältere TK-Anlagen:

- Durch die veränderte technische Basis und den im Vergleich zu einer älteren TK-Anlage erhöhten Software-Anteil können bei unreflektierter Übernahme von Inhalten aus Verträgen zur alten TK-Lösung wichtige Aspekte ungeregelt bleiben.
- Ältere Verträge zu TK-Dienstleistungen berücksichtigen häufig nicht die heute im IT-Bereich üblichen Service Level.
- Durch die Einbindung der VoIP-Komponenten in das IP-Netzwerk müssen typische für LAN-basierte Systeme geltende Sicherheitsauflagen erfüllt werden (z. B. sicherer Remote-Administrations-Zugriff). Hierzu sind entsprechende vertragliche Regelungen erforderlich.

Werden die Wartungsverträge nicht entsprechend diesen Aspekten gezielt gestaltet, so drohen beispielsweise Verfügbarkeitsprobleme mangels ausreichender Support-Qualität bzw. Sicherheitslücken z. B. mangels Zugriff auf Sicherheits-Patches.

G-TK-27 Unzureichende Regelungen für das Ende der externen Dienstleistungen für eine VoIP-Lösung

Wartungsverträge für TK-Anlagentechnik wurden in der Vergangenheit häufig an den Abschreibungszeitraum gebunden. Regelungen für einen vorzeitigen Ausstieg waren in derartigen Verträgen gar nicht vorhanden oder auf eine vollständige Stilllegung der fraglichen Anlage als Berechtigungsgrund beschränkt.

Dies ist für VoIP so pauschal ungeeignet, da ein VoIP-Wartungsvertrag sich wegen des deutlich erhöhten Software-Anteils nicht mehr auf reine Hardware-Instandhaltung konzentriert. Änderungen in diesem Software-Anteil sind im Vergleich zu traditionellen TK-Systemen deutlich häufiger und gravierender. Über die gesamte Standzeit der VoIP-Installation muss ein Dienstleister die für die Software-Pflege notwendige Kompetenz und den entsprechenden Service Level zusichern.

Bei unzureichenden Regelungen für die Kündigung von Dienstleistungen besteht hier die Gefahr, dass ein Vertrag nicht bedarfsgerecht gelöst werden kann.

G-TK-28 Unzureichende Regelungen für den IP-Anlagenanschluss mit dem ITSP

Die Sicherheitsmaßnahmen, die seitens des ITSP ergriffen werden sollen, müssen durch geeignete Regelungen vereinbart und überprüft werden. Sind diese Regelungen beispielsweise nicht eindeutig, besteht die Gefahr, dass ein zu niedriges Sicherheitsniveau hinsichtlich der Sicherheitsziele Vertraulichkeit und Integrität implementiert wird oder die Verfügbarkeit unter den Erfordernissen bleibt.

G-TK-29 Unzureichende oder fehlende Planung der Absicherung für die Erweiterung der Außenanbindung um eine VoIP-Komponente

Bei Einsatz eines IP-Anlagenanschlusses muss der Schutz der eigenen Infrastruktur um Maßnahmen gegen Gefährdungen durch die Übertragung von VoIP von und zum ITSP erweitert werden. Ist die Planung der Sicherheitsmaßnahmen hier unzureichend, kann beispielsweise über VoIP-Protokolle ein unberechtigter Zugriff auf die eigene Infrastruktur und der dort verwalteten Daten erlangt werden. Die Planung der Sicherheitsmechanismen muss auch berücksichtigen, dass Signalisierungs- und Nutzdaten über Koppelelemente mit Sicherheitsfunktionalität (z. B. Firewall, SBC) geleitet werden, die daher geeignet dimensioniert sein müssen.

G-TK-30 Unzureichende Kontrolle auf Kommunikationsstrecken bei standortübergreifender Kommunikation

Die Absicherung der standortübergreifenden Kommunikationsstrecken entzieht sich oft sehr stark ggf. sogar vollständig der eigenen Kontrolle. Für eine Dark-Fiber-Strecke mag zwar noch eine vergleichsweise hohe Kontrolle bestehen, bereits bei einem MPLS-VPN besteht jedoch kaum noch eine Möglichkeit als Kunde auf die Absicherung der Kabelstrecken und der verbindenden aktiven Komponenten Einfluss zu nehmen. Die betrifft alle Sicherheitsziele, d. h. es besteht die Gefahr eines Verlusts der Vertraulichkeit, der Integrität und auch der Verfügbarkeit.

4.2.3 Menschliche Fehlhandlungen

Menschliche Fehlhandlungen kommen bei jeglicher Form von IT-Lösungen vor, so auch für VoIP-Lösungen. Dabei sind Fehlhandlungen der Telefonie-Nutzer ebenso zu berücksichtigen wie solche des IT-Personals, z. B. der VoIP-Administratoren. Für einen IP-Anlagenanschluss sind die Gefährdungen durch menschliche Fehlhandlungen für einen Zugang zu einem ITSP identisch zu den in den BSI IT-Grundschutz-Katalogen genannten Gefährdungen für einen Internetzugang (siehe Baustein B 5.19 „Internet-Nutzung“ in [BSI GSK-2013]).

Neben den in den BSI IT-Grundschutz-Katalogen im Baustein B 4.7 „VoIP“ genannten Gefährdungen sind bei einem erhöhten Schutzbedarf folgende Gefährdungen durch menschliche Fehlhandlungen zu beachten.

G-TK-31 Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten der VoIP-Benutzer

Vertraulichkeitsverluste mit solcher Ursache können insbesondere bei Mehrwert-Funktionalitäten von VoIP-Lösungen auftreten, z. B.:

- Zugänglichkeit von Kontaktinformationen für Dritte durch schlecht oder gar nicht geschützte Speicherung auf mobilen Medien
- Zugänglichkeit von Kontaktinformationen durch Drucken auf einem zentralen Drucker (Netzwerkdrucker), die dann nicht zeitnah abgeholt werden

G-TK-32 Unstrukturierte Datenhaltung durch VoIP-Nutzer

Bei VoIP-Lösungen kommt diese Gefährdung insbesondere im Zusammenhang mit Mehrwertfunktionalitäten zur reinen Telefonie zum Tragen. Beispiele sind:

- In Form von Multimediadateien festgehaltene Inhalte der Sprach-Mailbox werden gleichzeitig an mehreren Stellen vorgehalten:
  - im Rahmen des entsprechenden VoIP-Systems
  - als Dateianlage von E-Mails, die bei Eingang der Sprachnachricht automatisch generiert und an den Posteingang des Telefonnutzers gesendet wurden
  - als Kopie in einer Dateiablage zum Gesamtvorgang, in den die jeweilige Sprachnachricht einzuordnen ist
- Kontaktdaten werden sowohl zentral im VoIP-Gesamtsystem als auch lokal von den Benutzern gepflegt.

Durch derartige Formen unstrukturierter Datenhaltung wird einerseits unnötig der Speicherplatzbedarf vervielfacht. Andererseits können unterschiedlich aktuelle Datenbestände mit vergleichbaren Inhalten zu Konsistenzproblemen führen. Zudem ist fraglich, ob alle Ablageorte das gleiche Sicherheitsniveau aufweisen, d. h. es können Vertraulichkeit und Integrität gefährdet werden.

G-TK-33 Konfigurationsfehler und Bedienungsfehler bei VoIP-Lösungen

Konfigurationsfehler an VoIP-Servern und ähnlichen zentralen Komponenten können zu Fehlfunktionen, Vertraulichkeitsverlusten, Nicht-Verfügbarkeit von Leistungsmerkmalen oder Absturz der Server und damit Nicht-Verfügbarkeit der Telefonie als Ganzes führen.

Dies lässt sich ausweiten auf Komponenten der IP-Infrastruktur, soweit sie auch für die VoIP-Telefonie genutzt werden, aber in ihrer Konfiguration nicht bzw. nicht vollständig auf die Anforderungen der Sprachkommunikation umgestellt wurden. Man vergleiche in diesem Zusammenhang auch die Gefährdung G-TK-21 „Unzureichende Harmonisierung zwischen IT- und VoIP-Betrieb“.

Eine Gefährdung durch Konfigurations- und Bedienfehler besteht auch im Endgerätebereich.

G-TK-34 Fehlerhafte Administration von Zugangs- und Zugriffsrechten zu VoIP-Installationen

Diese Gefährdung ist für VoIP relevant im Zusammenhang mit folgenden Punkten:

- Zugang zu VoIP-Mehrwertfunktionen und zugehörigen Datenbeständen
- Nutzungsberechtigungen für Telefone (Benutzerprofile)
- Konfigurationsmöglichkeiten des Nutzers für seine VoIP-Nutzungsumgebung (z. B. Tastenbelegung, PIN-Code): Bei Änderung durch unbefugte Dritte kann ein berechtigter Anwender mangels Wissens um die Änderung „ausgesperrt“ werden.

Im Zusammenhang mit fehlerhafter Freischaltung von Amtsberechtigungen können ungewollte Kosten entstehen, je nach Ziel (Handy-Nummer, Auslandsziele) auch in kurzer Zeit in beträchtlicher Höhe (Gebührenbetrug).

4.2.4 Technisches Versagen

Die Gefährdungen der Kategorie „Technisches Versagen“ treffen für VoIP grundlegend zu, soweit die durch eine Gefährdung bedrohte Technik eingesetzt wird:

- Netzwerk-Technik (LAN, WAN, ggf. auch Wireless LAN)
- Server-Betriebssystem(e) der im Rahmen einer konkreten VoIP-Lösung eingesetzten Art

- Endgeräte-Betriebssysteme, soweit im Telefonie-Endgerätebereich eingesetzt (Softphone-Lösungen eingeschlossen)

Eine Einordnung als VoIP-spezifische Gefährdung ist nur dann angemessen, wenn VoIP ein besonderes Angriffsziel im Rahmen einer Gefährdung darstellt bzw. auf Grund seiner technischen Besonderheiten (z. B. Anforderungen an die Netzwerkinfrastruktur und Kommunikationseigenschaften von Netzwerk-Strecken) besonders gefährdet ist oder vorzugsweise im Sinne dieser Gefährdung angegriffen wird. Weiterhin kann eine besondere Ausprägung der Gefährdung im Falle von VoIP besondere Maßnahmen notwendig machen.

Die hier speziell für VoIP relevanten Gefährdungen sind bereits in den BSI IT-Grundschutz-Katalogen (siehe [BSI GSK-2013]) enthalten und beschrieben. Sie werden hier gezielt vom Baustein B 4.7 „VoIP“ referenziert:

- G 4.56 „Ausfall der VoIP-Architektur“
- G 4.57 „Störungen beim Einsatz von VoIP über VPNs“
- G 4.58 „Schwachstellen beim Einsatz von VoIP-Endgeräten“
- G 4.59 „Nicht-Erreichbarkeit von VoIP durch NAT“

Angesichts der hohen Bedeutung der Telefonie-Verfügbarkeit (mindestens an bestimmten Arbeitsplätzen z. B. für Notruffunktionen) darf man sich im Zusammenhang mit VoIP bei erhöhtem Schutzbedarf nicht nur auf diese spezifischen Gefährdungen konzentrieren. Vielmehr müssen konsequent alle VoIP-relevanten Gefährdungen im Bereich „Technisches Versagen“ behandelt werden.

Falls ein IP-Anlagenanschluss genutzt wird, steht bei den Gefährdungen durch technisches Versagen neben den VoIP-relevanten Gefährdungen die zentrale Rolle des SBC im Mittelpunkt, der beim ITSP und ggf. auch bei einem Kunden des ITSP installiert ist. Dabei übertragen sich im Wesentlichen die in den BSI IT-Grundschutz-Katalogen (siehe [BSI GSK-2013]) genannten Gefährdungen, denen allgemein eine Firewall oder ein Application Layer Gateway (ALG) ausgesetzt sind, auf den SBC.

4.2.5 Vorsätzliche Handlungen

Gerade in der Gefährdungskategorie „Vorsätzliche Handlungen“ ist es wichtig zu beachten, dass VoIP mit dem IP-Netzwerk eine Infrastruktur mitnutzt, die nicht integraler Teil der VoIP-Lösung ist und von anderen Kommunikationsformen mitgenutzt wird:

- Gefährdungen, die auf andere Nutzungsformen eines IP-Netzes zutreffen, müssen auch für VoIP berücksichtigt werden.

  Solche Gefährdungen kommen also zu den direkt auf die VoIP-Installationen wirkenden Gefährdungen hinzu.

- Lösungen zur Entkräftung von Gefährdungen, die anderen Nutzungsformen genügen, sind für VoIP nicht per se ausreichend.

VoIP hat besondere Ansprüche an die Kommunikationsparameter, die insbesondere eine Denial-of-Service-Attacke erleichtern, denn es genügt eine mutwillige Verschlechterung der Übertragungsqualität im Bereich der für VoIP relevanten Größen (insbesondere Jitter und Delay).

Die Anforderungen des Datenschutzes für die Sprachdaten müssen berücksichtigt werden und zudem muss davon ausgegangen werden, dass von jedem VoIP-Endgerät aus anteilig vertrauliche Gespräche geführt werden. Der Schutzbedarf bezüglich der Vertraulichkeit muss höher als normal eingestuft werden, auch wenn für alle anderen Datenübertragungen vom selben Anwenderarbeitsplatz eine Einstufung als normal erfolgt ist.

Weiterhin ist mindestens für einen Teil der Telefone zur Sicherstellung von Notrufmöglichkeiten der Schutzbedarf hinsichtlich der Verfügbarkeit als erhöht einzustufen, d. h. vorsätzliche Handlungen, die solche Telefone unbrauchbar machen sollen, sind als besonders brisant anzusehen. Dies betrifft sowohl die

Verfügbarkeit des Telefons selbst als auch der Pfade im IP-Netzwerk, über das ein solches Telefon Sprachdaten versendet.

Die BSI IT-Grundschutz-Kataloge listen im Baustein 4.7 „VoIP“ folgende Gefährdungen durch vorsätzliche Handlungen (siehe [BSI GSK-2013]):

- G 5.11 „Vertraulichkeitsverlust von in TK-Anlagen gespeicherten Daten“
- G 5.12 „Abhören von Telefongesprächen und Datenübertragungen“
- G 5.13 „Abhören von Räumen über TK-Endgeräte“
- G 5.14 „Gebührenbetrug“
- G 5.15 „Missbrauch von Leistungsmerkmalen von TK-Anlagen“
- G 5.134 „Fehlende Identifizierung zwischen Gesprächsteilnehmern“
- G 5.135 „SPIT und Vishing“
- G 5.136 „Missbrauch frei zugänglicher Telefonanschlüsse“

Bei erhöhten Schutzbedarf wird ergänzend bzw. konkretisierend auf die folgenden Gefährdungen hingewiesen.

G-TK-35 Denial-of-Service-Angriffe auf VoIP

Hierunter fallen sowohl vorsätzliche Handlungen, die VoIP-Equipment und VoIP-Teilkomponenten vorübergehend oder dauerhaft der vorgesehenen Nutzung durch den Anwender entziehen als auch Angriffe auf die von VoIP mitgenutzten Elemente eines IP-Netzwerks.

Zu Diebstahl und Angriffen vom Typ Denial of Service (DoS), die sich zerstörerisch direkt gegen die VoIP-Komponenten richten, kommen Angriffsformen hinzu, bei denen über eine LAN- oder WLAN-Verbindung bzw. über das Internet angegriffen wird. Der physische Zugangsschutz zum angegriffenen Objekt ist daher weniger wichtig, entscheidender ist der Netzzugang des Angreifers.

Typische Angriffsszenarien haben entsprechend eine wie folgt zu beschreibende Grundcharakteristik:

- Zunächst findet der Angreifer einen Weg, von außen in den Netzwerkbereich einzudringen, in dem er ein VoIP-relevantes Objekt angreifen will.
- Nun wird der eigentliche (Last-)Angriff durchgeführt. Das angegriffene Objekt wird gezielt für VoIP unbrauchbar gemacht, ohne physisch in seine Nähe gekommen zu sein.

Telephony DoS (TDoS) ist dabei eine typische Angriffsform, die sich ursprünglich gegen klassische TK-Anlagen gerichtet hatte, jedoch ebenso gegen VoIP-Anlagen einsetzbar ist. Dabei werden zunächst über das PSTN durch den Angreifer systematisch Anrufe erzeugt und damit Leitungen bzw. Kanäle belegt. Ist die maximale Anzahl von Kanälen der PSTN-Anbindung der TK-Anlage erreicht, ist für die eigentlichen Nutzer kein Gespräch mehr möglich.

Ist eine VoIP-basierte TK-Anlage zudem über (interne oder externe) IP-Netze erreichbar, wird TDoS deutlich erleichtert, da der Angreifer über IP zielgerichtet und einfach den entsprechenden Signalisierungsverkehr und sogar den Medienstrom erzeugen kann. Hier unterscheidet sich VoIP von der ISDN-basierten Telekommunikation drastisch, da bei VoIP TDoS auch in LANs möglich ist.

Gerade die Signalisierung in VoIP eignet sich für DoS. Hier ist speziell SIP zu nennen. Einerseits ist es sehr einfach möglich über SIP eine TDoS zu realisieren (SIP Flooding) andererseits bietet SIP (auch durch die Ähnlichkeit zum Hypertext Transfer Protocol, HTTP) weitere Angriffsmöglichkeiten für DoS, indem z. B. Pakete bewusst so konstruiert werden, dass beim Parsing der Pakete besonders viel CPU-Zeit benötigt wird oder versucht wird durch fehlerhafte Pakete das System zum Absturz zu bringen.

Neben DoS-Angriffen, die spezifisch für Telefonie und VoIP sind, müssen bei VoIP DoS-Angriffe berücksichtigt werden, die auf Ebene des IP-Netzes wirken und sich so auf VoIP vererben. Ein typisches Beispiel ist ein auch als „DHCP Starvation" bezeichneter Angriff bei dem ein Angreifer systematisch kontinuierlich per DHCP neue IP-Adressen anfordert, bis der Pool an dynamisch vergebenen IP-Adressen aufgebraucht ist. Damit stehen am Ende auch keine IP-Adressen mehr für IP-Telefone zur Verfügung und damit für die betroffenen Geräte auch keine Telekommunikationsdienste. Weiterhin müssen Schwächen von DNS beachtet werden, die es beispielsweise einem Angreifer erlauben, sich als DNS-Server auszugeben und DNS-Anfragen schadenstiftend zu beantworten (als DNS Spoofing bezeichnet).

DoS-Angriffe, die über das Netzwerk erfolgen, können nur dann erfolgreich geblockt werden, ohne dass das Netzwerk insgesamt nutzlos wird, wenn man gezielt zwischen „berechtigter" und „unberechtigter" Netzwerk-Nutzung unterscheiden kann. Typische Angriffsformen versuchen daher in einem ersten Schritt, eine Identität anzunehmen bzw. zu simulieren, deren Aktivität nicht sinnvoll geblockt werden kann. Auf dieser Basis wird dann der eigentliche DoS-Angriff durchgeführt.

Vergleichbar zu Spam mittels E-Mail wird mit zunehmender Verbreitung von Internet Telephony auch die missbräuchliche Nutzung dieses Dienstes, als Spam over Internet Telephony (SPIT) bezeichnet, für Marketingzwecke oder als Denial-of-Service-Angriff stark zunehmen.

G-TK-36 Abhören der VoIP-Kommunikation durch Schwachstellen in Netzwerkprotokollen

Ähnlich wie bei gegen die Verfügbarkeit gerichteten DoS-Angriffen auf VoIP ist auch bei Angriffen auf die Vertraulichkeit der typische Angriff ein Mehrschritt-Ansatz:

- Zunächst wird die Umgebung ausspioniert, um Identitäten im Netzwerk zu identifizieren, auf die bzw. über die der angestrebte Abhörangriff erfolgen kann.
- Nun wird missbräuchlich vom Angreifer eine Identität bzw. Rolle angenommen, über die er in den Sprachdatentransfer eingebunden wird, ohne dass dies auffällt.
- Der Angreifer übt dann die unberechtigt übernommene Rolle aus und gelangt so in die Position, die Sprachdaten mitzulesen und zur Abhörung aufzubereiten.

Ein Beispiel für einen solchen Angriff ist das sogenannte Address Resolution Protocol Spoofing (ARP Spoofing, auch ARP Poisoning genannt, siehe Gefährdung G 5.112 „Manipulation von ARP-Tabellen" der IT-Grundschutz-Kataloge, siehe [BSI GSK-2013]). Dieser Angriff gestattet es, durch missbräuchliche, aber standardkonforme Verwendung des Address Resolution Protocol (ARP) innerhalb einer Broadcast-Domäne eines LAN jeglichen Kommunikationsverkehr eines Endgerätes über den Angreifer zu leiten. Der Angreifer muss sich hierzu lediglich an einen Netzwerkport des LAN anschließen.

Dabei muss sich der Angreifer nicht notwendig im LAN des angegriffenen VoIP-Systems befinden. Es ist genauso möglich, dass der Lauschangriff ausgehend von einem Computer im LAN, von dem aus das angegriffene VoIP-System erreichbar ist, über ein Trojanisches Pferd erfolgt. Die Sprachdaten werden dann von dem infizierten Computer über eine erlaubte Kommunikationsbeziehung per Internet an den eigentlichen Angreifer übermittelt (siehe Abbildung 21). Eine Infizierung mit einem Trojanischen Pferd ist insbesondere bei Softphones möglich.

Eine weitere typische Angriffsvariante ist das Einrichten eines DHCP-Servers durch den Angreifer, der auf DHCP-Anfragen mit falschen Antworten reagiert und so beispielsweise dem angegriffenen Gerät mitteilt, dass der Angreifer selber das Default Gateway sei. Das angegriffene Gerät würde dann den gesamten Subnetz-übergreifenden Verkehr über den Angreifer leiten.

Außerdem muss auf die Gefährdung durch DNS Spoofing im Zusammenhang mit der Nutzung von ENUM hingewiesen werden. Die Schwächen von DNS vererben sich auf ENUM und ein Angreifer ist grundsätzlich in der Lage, über DNS Spoofing falsche Bindungen

zwischen einer Telefonnummer und einem Dienst zu verbreiten. Das auf diese Weise angegriffene Gerät kann dann beispielsweise ohne es zu bemerken zu einem Kommunikationsziel geleitet werden, das unter der Kontrolle des Angreifers steht.

Zum Zwecke des Ausspionierens (Schritt 1) können Auswertungsmöglichkeiten der VoIP-Lösung (Accounting-, Billing- und Logging-Funktionen) mit den umfangreichen Möglichkeiten der Auswertung von IP-basierter Kommunikation kombiniert werden.

Die Durchführung solcher Angriffe wird zudem erleichtert, wenn Wartungs- und Administrationszugänge zum IP-Netz oder zu einzelnen Netzwerk- bzw. VoIP-Komponenten Schwachstellen aufweisen, über die Unbefugte solche Zugänge nutzen können.

Da VoIP-Pakete mit den Mitteln der Protokollanalyse dekodiert und insbesondere Sprachdaten in Multimedia-Dateien umgewandelt werden können, ist eine VoIP-Kommunikation ohne einen gezielten Schutz durch Verschlüsselung als „Klartext"-Kommunikation einzustufen. Die Daten liegen somit offen, sobald ein Lauschzugriff mit den Mitteln der Protokollanalyse erfolgen kann.

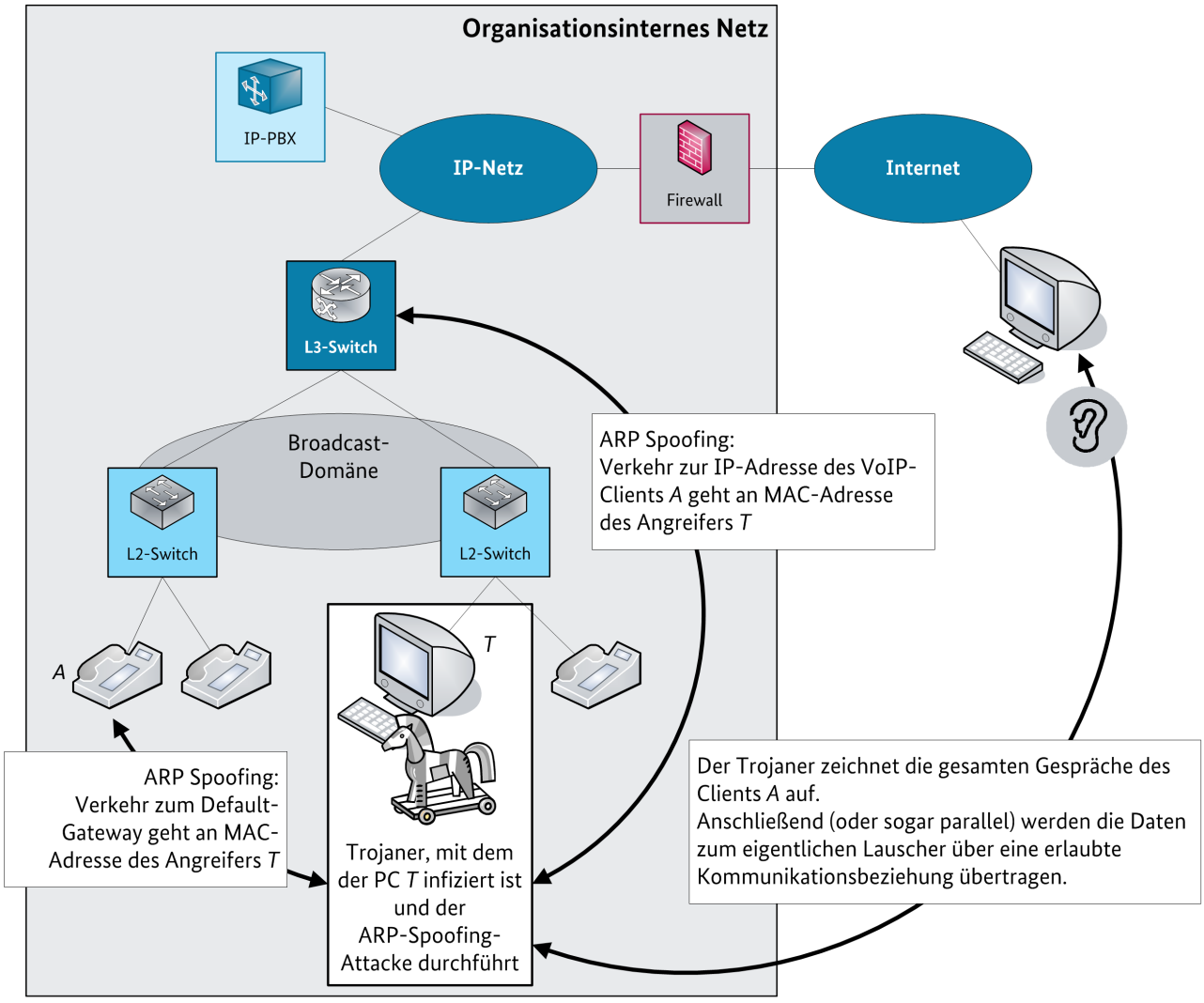


Abbildung 21: ARP Spoofing durch einen Trojaner zum Abhören eines Gesprächs

G-TK-37 Missbräuchlicher Zugriff auf VoIP-Geräte

Die Kombination von reiner Telefonie mit einer Vielzahl von Mehrwertfunktionen führt bei VoIP dazu, dass auch die Endgeräte selbst immer mehr Funktionalitäten mitbringen. IP-Telefone enthalten einen Computer, auf dessen Betriebssystem neben der VoIP-Software beispielsweise oft auch ein Web-Browser und zu Konfigurationszwecken ein Web-Server läuft. Damit überträgt sich eine Vielzahl von Gefährdungen auf IP-Telefone. Entsprechende Angriffe auf IP-Telefone, die einen Zugriff auf Daten und Konfigurationen sowie deren Manipulation ermöglichen, sind bereits bekannt.

Die Durchführung solcher Angriffe wird zudem erleichtert, wenn Wartungs- und Administrationszugänge zum IP-Netz oder zu einzelnen Netzwerk- bzw. VoIP-Komponenten Schwachstellen aufweisen, über die Unbefugte solche Zugänge nutzen können.

Eine weitere potenzielle Gefährdung ergibt sich bei der Verwendung von Signalisierungsprotokollen, die – wie es bei SIP der Fall ist – HTTP entlehnt sind und HTML- und XML-ähnliche[11] Sprachen verwenden. Beispielsweise könnte durch systematisch manipulierte Nachrichten Kommandos auf VoIP-Geräten ausgeführt oder über einen provozierten Pufferüberlauf ein missbräuchlicher Zugriff ermöglicht werden.

Bei Softphones bestehen Gefährdungen zudem über Verwundbarkeiten im Betriebssystem und den installierten Anwendungen. Hierdurch entsteht eine Plattform für eine ganze Palette von Angriffen, z. B. von der Aufzeichnung von Sprachinformationen bis hin zum Abhören von Räumen.

Die BSI IT-Grundschutz-Kataloge (siehe [BSI GSK-2013]) beschreiben eine Reihe von Gefährdungen durch vorsätzliche Handlungen, die sich auf VoIP-Systeme und Firewalls beziehen. Diese bestehen auch für IP-Anlagenanschlüsse, wodurch insbesondere ein weiterer Pfad für die Übertragung von schadenstiftender Software (Infektionspfad) zu berücksichtigen ist.

G-TK-38 Übertragung von schadenstiftender Software über die IP-Kommunikation mit VoIP-Netzelementen des ITSP

Über die VoIP-Kommunikation mit dem ITSP kann grundsätzlich auch schadenstiftende Software in die eigene Infrastruktur gelangen. Dabei können prinzipiell das VoIP-Endgerät und sogar die TK-Anlage als Wirt oder als Opfer dienen.

4.3 Sicherheitsmaßnahmen

Dieses Kapitel beschreibt Maßnahmen zur Absicherung von VoIP-Systemen unter besonderer Berücksichtigung eines erhöhten Schutzbedarfs.

Generell können zunächst die in Kapitel 3.3 beschriebenen Maßnahmen für ISDN-basierte TK-Anlagen sinngemäß auf ein VoIP-System übertragen werden. Dies gilt insbesondere für den PSTN-Übergang und die ISDN-Leistungsmerkmale. In diesem Sinne ist beispielsweise die Maßnahme M-TK-1 „Sperrung nicht benötigter oder sicherheitskritischer Leistungsmerkmale“ unmittelbar als Härtungsmaßnahme auf ein VoIP-System anzuwenden.

Im Folgenden werden die VoIP-spezifischen Maßnahmen beschrieben, wobei es sich teilweise um Ansätze handelt, die auch für andere vernetzte IT-Systeme greifen können. Je nach Szenario und insbesondere für den erhöhten Schutzbedarf kommt es darauf an, aus diesem Baukastensystem von Maßnahmen jeweils angemessene Pakete zu bilden. Der Maßnahmenkatalog zur Absicherung von Nutzung und Betrieb von VoIP-Systemen ist in die folgenden Blöcke aufgeteilt:

- Server und Anwendungen, siehe Kapitel 4.3.1
- Endgeräte, siehe Kapitel 4.3.2
- Netzwerk, siehe Kapitel 4.3.3

11 HTML = HyperText Markup Language, XML = Extensible Markup Language

- Netz- und Systemmanagement, siehe Kapitel 4.3.4
- Übergreifende Aspekte, die allgemein für VoIP-Systeme gelten, siehe Kapitel 4.3.5

Grundsätzlich wird die Umsetzung der generell zu ergreifenden Maßnahmen (siehe Kapitel 10) vorausgesetzt.

4.3.1 Server und Anwendungen

M-TK-31 Durchgängige Verschlüsselung des Medienstroms

Für den erhöhten Schutzbedarf muss der Medienstrom durchgängig zwischen den Kommunikationspartnern verschlüsselt werden. Dabei sollte möglichst weitgehend mit einer Ende-zu-Ende-Verschlüsselung des Medienstroms gearbeitet werden. Verschlüsselungsendpunkte dürfen nur an Vertrauensbereichsgrenzen in streng kontrollierter Umgebung vorliegen.

Auf eine Verschlüsselung darf nur in besonders geschützten Bereichen (z. B. in einem entsprechend abgesicherten Rechenzentrum) verzichtet werden, wenn das Risiko eines Vertraulichkeits- oder Integritätsverlusts mit anderen Mitteln effektiv erreicht werden kann.

Die Verschlüsselung sollte möglichst über SRTP respektive Secure RTP Control Protocol (SRTCP) nach [IETF RFC3711-2004] erfolgen. Die Schlüssellänge muss mindestens 128 Bit betragen. Weiterführende Empfehlungen sind in [BSI TRKrypto-2013] in der jeweils aktuellen Fassung zu finden. Alternativ kann eine gleichwertige, beispielsweise auf VPN-Techniken basierende Verschlüsselungstechnik eingesetzt werden (siehe Kapitel 13.3.4 zum Thema VPN und die Hinweise zur Nutzung von TLS in Kapitel 13.3.3).

Die Verschlüsselung erfolgt zwischen den Endgeräten bzw. zwischen Endgerät und einem Gateway, das den Medienstrom terminiert (z. B. PSTN-Gateway, Media Gateway, SBC oder Konferenz-Server), wie in Abbildung 22 gezeigt, und ggf. zwischen Gateways. Die an der Verschlüsselung beteiligten Instanzen müssen ein dynamisches Schlüsselmanagement unterstützen, das eine sichere Aushandlung des Schlüsselmaterials erlaubt (siehe Kapitel 13.1.3).

Eine Verschlüsselung des Medienstroms ist bereits für den normalen Schutzbedarf zu empfehlen bzw. bei einer Standort-übergreifenden Kommunikation sogar zwingend erforderlich. Siehe hierzu auch folgende Maßnahmen des Bausteins 4.7 „VoIP“ der BSI IT-Grundschutz-Kataloge (siehe [BSI GSK-2013]):

- M 2.374 „Umfang der Verschlüsselung von VoIP“
- M 5.135 „Sicherer Medientransport mit SRTP“

Hinweis: Unter speziellen Rahmenbedingungen kann bei Verwendung von Sprach-Codecs mit Variable Bit Rate (VBR) in Verbindung mit SRTP oder anderen Verschlüsselungsverfahren, bei denen die Längeninformation erhalten bleibt und somit unter anderem auch Sprechpausen ausgewertet werden können, in einem gewissen eingeschränkten Umfang auf den Klartext zurückgeschlossen werden (siehe [IETF RFC6562-2012]). Dies ist anwendungsspezifisch und betrifft primär Anwendungen, bei denen mit einem kleinen, vordefinierten und bekannten Wortschatz gearbeitet wird. Typische Beispiele können im Umfeld von IVR-Anwendungen gefunden werden. Bei derartigen Anwendungen mit erhöhtem Schutzbedarf hinsichtlich der Vertraulichkeit sollte daher auf solche verwundbare VBR-Sprach-Codecs verzichtet und die VoIP-Lösung entsprechend konfiguriert werden. Alternativ kann, sofern verfügbar, auch ein Verschlüsselungsverfahren eingesetzt werden, bei dem die Längeninformation nicht erhalten bleibt und Sprechpausen nicht mehr sinnvoll ausgewertet werden können.

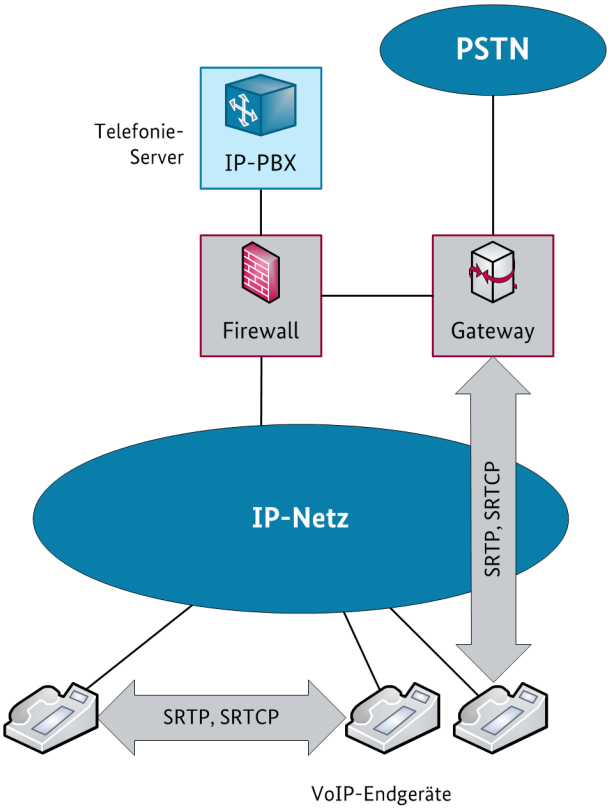


Abbildung 22: Endpunkte bei Verschlüsselung mit SRTP

M-TK-32 Durchgängige Verschlüsselung der Signalisierung

Für den erhöhten Schutzbedarf muss die VoIP-Signalisierung durchgängig zwischen Endgerät bzw. einem Gateway und dem Telefonie-Server verschlüsselt werden. Auf dem Signalisierungspfad erfolgt die Verschlüsselung Hop-by-Hop, d. h. an einem Proxy im Signalisierungspfad wird jeweils eine Verschlüsselungsstrecke terminiert.

Hinweis: Wenn der Signalisierungspfad Bereiche außerhalb der eigenen administrativen Verantwortung enthält, kann eine durchgängige Verschlüsselung nicht mehr erzwungen werden. In diesem Fall muss eine entsprechender Risikobetrachtung durchgeführt werden und ohne zusätzliche Sicherheitsmaßnahmen (z. B. entsprechende Vertragsgestaltungen mit einem Provider) ggf. hier sogar auf den Einsatz von VoIP verzichtet werden.

Auf eine Verschlüsselung darf nur in besonders geschützten Bereichen (z. B. einem entsprechend abgesicherten Rechenzentrum) verzichtet werden, wenn das Risiko eines Vertraulichkeits- oder Integritätsverlusts mit anderen Mitteln effektiv erreicht werden kann.

Die Verschlüsselung sollte mit einer sicheren Variante von TLS (unter Beachtung der Hinweise für den Einsatz von TLS in Kapitel 13.3.3) erfolgen. Dabei muss beachtet werden, dass gravierende Unterschiede im Sicherheitsniveau zwischen verschiedenen TLS-Varianten bestehen. Alternativ kann eine gleichwertige, beispielsweise auf IPsec oder auf einer anderen VPN-Technik basierende, Verschlüsselungstechnik eingesetzt werden (siehe Kapitel 13.3.4 zum Thema VPN).

Ergänzend ist (sofern technisch möglich) bei Verwendung von SIP für die Absicherung von Signalisierungselementen, die Ende-zu-Ende übertragen werden, eine Verschlüsselung über Secure Multipurpose Internet Message Extensions (S/MIME) zu empfehlen (siehe Kapitel 13.1.3.4.2).

Eine Verschlüsselung der Signalisierung ist bereits für den normalen Schutzbedarf zu empfehlen bzw. bei einer Standort-übergreifenden Kommunikation sogar zwingend

erforderlich. Siehe hierzu auch folgende Maßnahmen des Bausteins 4.7 „VoIP“ der BSI IT-Grundschutz-Kataloge (siehe [BSI GSK-2013]):

- M 2.374 „Umfang der Verschlüsselung von VoIP“
- M 5.134 „Sichere Signalisierung bei VoIP“

Falls die Maßnahmen M-TK-31 „Durchgängige Verschlüsselung des Medienstroms“ und M-TK-32 „Durchgängige Verschlüsselung der Signalisierung“ nicht zufriedenstellend umgesetzt werden können, muss eine ausgleichende Maßnahme auf Ebene des Netzwerks zum Schutz der Kommunikation zumindest über eingeschränkt vertrauenswürdige Netze angewandt werden (siehe Maßnahme M-TK-66 „VPN zur Kommunikation über eingeschränkt vertrauenswürdige Netze“).

M-TK-33 Absicherung von VoIP bei der Verwendung von Thin Clients

Die Übertragungsstrecke zwischen dem Server, der die Client-Anwendung bereitstellt, und einer Partnerinstanz für Signalisierung und/oder Medienstrom, ist außerhalb eines besonders geschützten Rechenzentrums stets abzusichern (siehe Maßnahmen M-TK-31 „Durchgängige Verschlüsselung des Medienstroms“und M-TK-32 „Durchgängige Verschlüsselung der Signalisierung“).

Bei traditionellem Hosting ist die Kommunikation zwischen Thin Client und Terminal-Server zusätzlich zu betrachten. Für die Übertragung der Sprachinformationen oder sofern durch den Nutzer im Rahmen der Signalisierung kritische Daten (z. B. ein Passwort) anzugeben sind, muss auch das Terminal-Server-Protokoll angemessen (z. B. mit TLS) verschlüsselt werden.

Wenn im Rahmen von Streaming VoIP-bezogene Anwendungselemente (im Extremfall ein vollständiges Softphone) auf dem Thin Client ausgeführt werden, ist die Kommunikation, wie in Maßnahmen M-TK-31 und M-TK-32 für einen Fat Client beschrieben, abzusichern (d. h. beispielsweise Verwendung von TLS für die Signalisierung und SRTP für den Medienstrom).

M-TK-34 Authentisierung zwischen Endgeräten und Servern des VoIP-Systems

Für den erhöhten Schutzbedarf muss zwischen den Endgeräten und den Servern des VoIP-Systems, mit denen das Endgerät kommuniziert (insbesondere Telefonie-Server) eine Authentisierung erfolgen. Dabei sollte nach Möglichkeit eine gegenseitige Authentisierung stattfinden. Empfohlen wird der Einsatz von Mutual TLS (MTLS) unter Beachtung der Hinweise für den Einsatz von TLS in 13.3.3.

M-TK-35 Authentisierung zwischen Servern

Sofern die Server des VoIP-Systems in einer gemeinsamen Sicherheitszone von anderen Elementen der IT-Infrastruktur nicht geeignet isoliert sind, ist für den erhöhten Schutzbedarf eine Authentisierung zwischen den Servern erforderlich. Empfohlen wird der Einsatz von MTLS unter Beachtung der Hinweise für den Einsatz von TLS in 13.3.3.

M-TK-36 Redundanz der Telefonie-Server

Telefonie-Server müssen redundant ausgelegt werden. Bei der Umschaltung zwischen Telefonie-Servern sollten möglichst keine Gespräche bzw. Sitzungen unterbrochen werden.

M-TK-37 Redundanz der Server und Gateways, von denen die Funktion des Telefonie-Servers und des Telefonie-Dienstes unmittelbar abhängt

In Ergänzung zu M-TK-36 „Redundanz der Telefonie-Server “ müssen für den erhöhten Schutzbedarf alle Server und Gateways (inklusive PSTN-Gateways), von denen die Funktion des Telefonie-Servers und des Telefonie-Dienstes unmittelbar abhängt, redundant ausgelegt werden bzw. eine genügend hohe Verfügbarkeit aufweisen. Ein typisches Beispiel ist DNS.

M-TK-38 Schaffung eines zusätzlichen PSTN-Ersatzanschlusses für Notrufe

Auch bei Ausfällen des VoIP-Systems müssen noch Notrufe erfolgen können. Hierzu muss ein separater PSTN-Anschluss mit direkt angebundenem Telefon eingesetzt werden. Dabei ist auf eine geeignete Anzahl, Platzierung inklusive Ausschilderung und Markierung, d. h. einfache

Erreichbarkeit von allen Räumen auf ausreichend kurzen Wegen, solcher Telefone und Anschlüsse zu achten.

Für einen solchen PSTN-Anschluss und die zugehörigen Endgeräte gelten allgemein die in Kapitel 3.3 beschriebenen Maßnahmen.

M-TK-39 Automatische PSTN-Umschaltung für kleinere Außenstellen

Für kleinere Außenstellen, die über WAN oder VPN an zentrale Telefonie-Server angebunden werden, ist für den Ausfall der Verbindung zur Zentrale eine lokale Lösung vorzusehen, die wie in Kapitel 4.1.7.3 beschrieben, als Notbetrieb für die lokalen IP-Telefone eine Kommunikationsmöglichkeit inklusive PSTN-Anbindung schafft. Über einen solchen Notbetrieb muss der Nutzer über die IP-Telefone oder über einen anderen Weg möglichst automatisiert informiert werden und so auf das ggf. geringere Sicherheitsniveau und die eingeschränkte Funktion hingewiesen zu werden. Wenn eine automatische Information nicht möglich ist, muss eine manuelle Benachrichtigung der Nutzer durch einen Administrator z. B. über E-Mail durchgeführt werden.

M-TK-40 Absicherung von Telefonie-Daten im Verzeichnisdienst

Gewisse telefoniebezogene Daten werden manchmal über einen Verzeichnisdienst verwaltet. Dies beinhaltet insbesondere auch Teilnehmerdaten (z. B. das Dienstprofil, nutzerspezifische Einstellungen, ggf. sogar eine PIN zur Freischaltung von Diensten).

Die Berechtigungen für den Zugriff auf diese Daten müssen so eingestellt sein, dass nur die notwendigen Zugriffe für autorisierte Parteien gestattet sind. Die Protokolle für den Zugang auf Telefonie-Daten im Verzeichnisdienst müssen hinsichtlich Vertraulichkeit und Integrität abgesichert sein.

PINs und sonstige Daten mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit und Integrität müssen verschlüsselt hinterlegt werden.

M-TK-41 Verfügbarkeit kritischer Telefonie-Daten

Für kritische TK-Daten, wie Teilnehmerprofile oder aktuelle teilnehmerbezogene Einstellungen (z. B. Rufumleitungen), die zentral verwaltet werden, muss eine dem Schutzbedarf angemessene Verfügbarkeit sichergestellt werden. Wenn beispielsweise die Datenhaltung der aktuellen teilnehmerbezogenen Einstellungen auf einem speziellen Server erfolgt, kann für den erhöhten Schutzbedarf die Datenhaltung voll redundant ausgelegt werden.

M-TK-42 Einschränkungen von DNS für VoIP

Es sollte ein interner DNS-Server für die ausschließliche Verwendung von VoIP aufgesetzt werden. Dynamic DNS (DDNS), Caching und Forwarding von DNS-Anfragen sind zu deaktivieren. IP-Telefone werden so konfiguriert, dass sie nur diesen DNS-Server ansprechen.

Sofern möglich, sollten die Domain Name System Security Extensions (DNSSEC) gemäß [IETF RFC4033-2005], [IETF RFC4034-2005] und [IETF RFC4035-2005] eingesetzt werden[12].

Bei erhöhtem Schutzbedarf sollten Softphones in Verbindung mit DNS nach Möglichkeit nicht verwendet werden. Ist die Nutzung von Softphones und DNS unbedingt erforderlich, dann muss auf dem bestehenden internen DNS-Server, welcher die PC-Infrastruktur bedient, folgendes beachtet werden: VoIP-spezifische Anfragen müssen so an eine DNS Subdomain delegiert werden, dass nur der eben erwähnte interne VoIP-DNS-Server diese Anfragen beantwortet.

Das bestehende Restrisiko durch DNS Spoofing und DoS muss bei Verwendung von DNS in jedem Fall abgewogen werden.

12 Über DNSSEC können die Antworten eines DNS-Servers mit dem privaten Schlüssel des DNS-Servers signiert und die Server-Antworten so authentisiert werden. DNSSEC ist allerdings in der Praxis noch selten anzutreffen.

Bei erhöhtem Schutzbedarf sollte man daher auch in Betracht ziehen, auf den Einsatz von DNS für VoIP zu verzichten.

M-TK-43 Einschränkung von ENUM

Bei erhöhtem Schutzbedarf sollte auf den Einsatz von ENUM möglichst verzichtet werden, da sich das erhebliche Gefährdungspotenzial von DNS automatisch auf ENUM und damit auf die Telekommunikation vererbt.

Ist eine ENUM-Nutzung unbedingt erforderlich, muss ENUM auf ausschließlich interne Nutzung eingeschränkt und M-TK-42 „Einschränkungen von DNS für VoIP“ umgesetzt werden.

Folgende Maßnahmen sind für den Fall der Nutzung eines IP-Anlagenanschlusses zusätzlich relevant:

M-TK-44 Redundante Internetanbindung für den IP-Anlagenanschluss

Sofern es erhöhte Anforderungen an die Verfügbarkeit des IP-Anlagenanschlusses und damit auch der Internetanbindung gibt, ist eine redundante Internetanbindung über verschiedene Internet-Provider zu realisieren. Bei Ausfall einer Verbindung sollte möglichst ein automatischer Wechsel auf den alternativen Internet-Provider erfolgen. Diese Anbindung muss geeignet dimensioniert sein, um eine vollständige Versorgung sicherzustellen. In diesem Zusammenhang sind auch die Maßnahmen M-TK-82 „VoIP-Tauglichkeit der IP-Infrastruktur für einen IP-Anlagenanschluss“ und M-TK-83 „Überwachung der VoIP-Anbindung zum ITSP“ entsprechend zu berücksichtigen.

M-TK-45 Zusätzlicher IP-Anlagenanschluss

Die Verfügbarkeit der PSTN-Anbindung durch einen IP-Anlagenanschluss kann in Anlehnung an Maßnahme M-TK-44 „Redundante Internetanbindung für den IP-Anlagenanschluss“ weiter erhöht werden, indem ein zusätzlicher IP-Anlagenanschluss bei einem unterschiedlichen ITSP beauftragt wird. Bei Ausfall eines IP-Anlagenanschlusses sollte möglichst ein automatischer Wechsel auf den alternativen ITSP erfolgen. Dieser Anschluss muss geeignet dimensioniert sein, um eine vollständige Versorgung sicherzustellen.

M-TK-46 Zusätzlicher PSTN-Anschluss

Genügen die Maßnahmen M-TK-44 „Redundante Internetanbindung für den IP-Anlagenanschluss“ und M-TK-45 „Zusätzlicher IP-Anlagenanschluss“ den Anforderungen an die Verfügbarkeit des IP-Anlagenanschlusses nicht oder lassen sich aufgrund anderer Gründe nicht vollständig umsetzen, ist sicherzustellen, dass eine zusätzliche Anbindung an das PSTN erfolgt. Hier können z. B. TDM-basierte Anschlüsse in Form von S_0- oder S_{2M}-Anschlüssen in Erwägung gezogen werden. Nach Möglichkeit sollte auch hier ein automatischer Wechsel auf den TDM-basierten Anschluss erfolgen, sofern der IP-Anlagenanschluss nicht verfügbar ist. In diesem Zusammenhang ist auch die Maßnahme M-TK-83 „Überwachung der VoIP-Anbindung zum ITSP“ entsprechend zu berücksichtigen. Je nach geforderter Verfügbarkeit kann auch eine Anbindung an die Mobilfunknetze als ausreichend angesehen werden.

M-TK-47 Verwendung eines Session Border Controller zur Absicherung eines IP-Anlagenanschlusses

Wie in Kapitel 4.1.6 beschrieben, sind zwischen Unternehmen bzw. Behörde und ITSP weitere Maßnahmen zur Absicherung erforderlich.

Für den erhöhten Schutzbedarf ist ein lokaler SBC im Unternehmen bzw. in der Behörde dringend erforderlich (siehe Kapitel 4.1.6). Der SBC ist dann für die Verbindung zwischen dem Unternehmen bzw. der Behörde und dem ITSP zuständig und terminiert, im Unterschied zu einer Firewall mit VoIP-Applikationsintelligenz, die Signalisierungs- und Nutzdaten, wodurch weitergehende sicherheitsrelevante Funktionen ermöglicht werden. Am lokalen SBC können auch andere Standorte der Organisation und insbesondere Telearbeitsplätze angekoppelt werden, wie in Abbildung 23 exemplarisch gezeigt.

Der SBC terminiert die Sitzungen und ist damit stets der Verschlüsselungsendpunkt, wie in Abbildung 23 illustriert. Der SBC muss daher als vertrauenswürdig eingestuft werden können und angemessen gehärtet sein. Sofern für den SBC zutreffend, gelten hierfür die Maßnahmen der IT-Grundschutz-Kataloge (siehe [BSI GSK-2013]) für ein Sicherheits-Gateway gemäß Baustein B 3.301 „Sicherheits-Gateway (Firewall)“. Eine typische Härtungsmaßnahme ist beispielsweise die Deaktivierung aller nicht benötigten Funktionen.

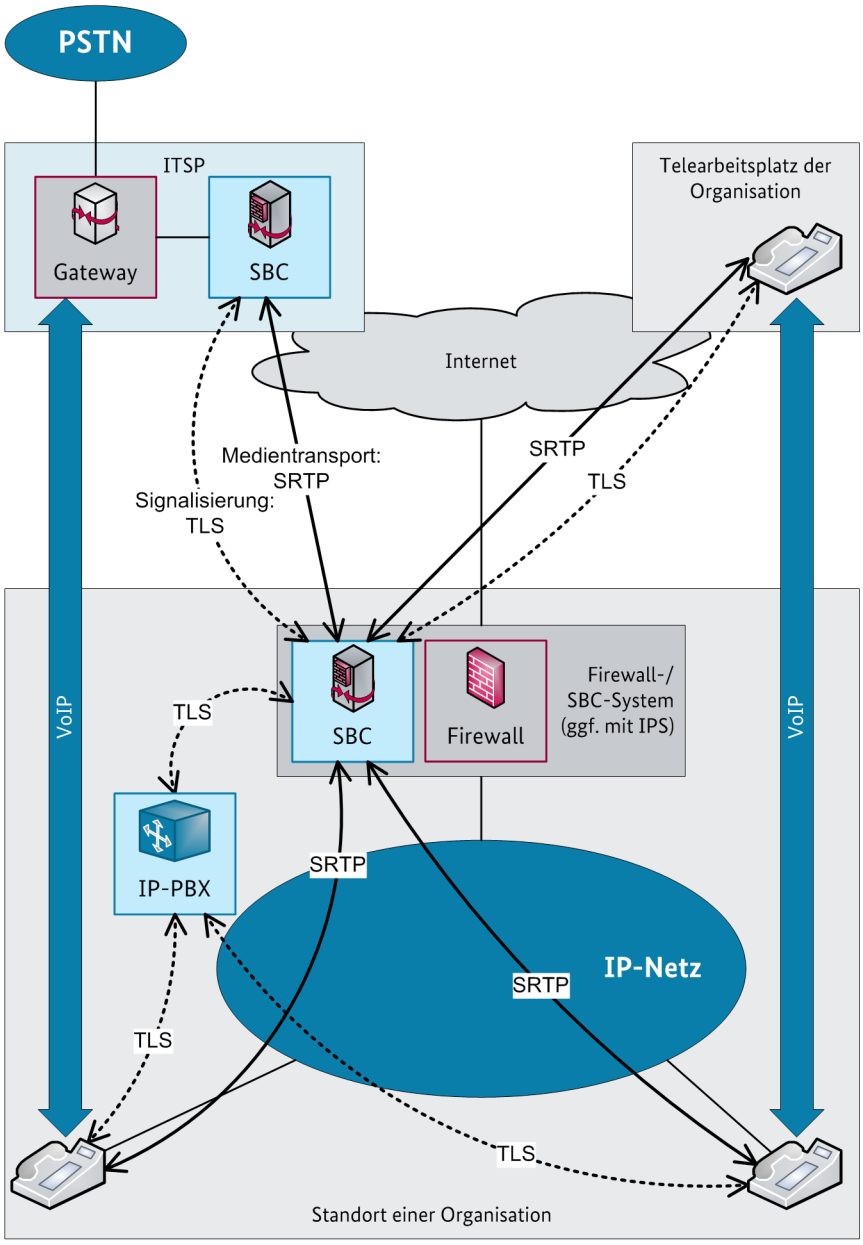


Abbildung 23: Absicherung mittels TLS und SRTP bei Verwendung eines SBC

4.3.2 Endgeräte

Bei erhöhtem Schutzbedarf insbesondere hinsichtlich der Vertraulichkeit müssen generell speziell gehärtete und entsprechend geprüfte IP-Telefone verwendet werden. Die Grundlage bilden die hier genannten Maßnahmen. Diese Maßnahmen sind bei Bedarf durch organisatorische Maßnahmen zu ergänzen. Ein Beispiel ist, dass vertrauliche Gespräche nur über hierzu vorgesehene und entsprechend gekennzeichnete Geräte geführt werden dürfen.

M-TK-48 Sicherung von IP-Telefonen in unübersichtlichen Umgebungen

Für IP-Telefone, die in unübersichtlichen Umgebungen oder in Bereichen mit erhöhtem Publikumsverkehr (z. B. in Besprechungsräumen oder öffentlich zugänglichen Räumen, etwa in Lobbys) aufgestellt werden, sollten nach Möglichkeit nur Endgeräte mit eingeschränktem (als unkritisch befundenem) Funktionsumfang eingesetzt werden. In diesem Sinne sollten auch keine IP-Telefone mit integriertem Ethernet Switch oder ggf. vorhandenem USB-Port aufgestellt werden (zumindest sollte die entsprechende Funktion im Telefon deaktiviert werden), da man diesen für den Zugang zum Netzwerk missbrauchen könnte.

Weiterhin sollte man einen mechanischen Diebstahlschutz vorsehen, sofern auf dem Gerät vertrauliche Daten gespeichert werden oder mit Hilfe des Gerätes (bzw. entsprechender Identitätsinformationen) auf vertraulicher Informationen in der Infrastruktur zugegriffen werden kann.

M-TK-49 Warnung bei unsicheren Einstellungen

Für den erhöhten Schutzbedarf sollten Endgeräte so konfiguriert werden können, dass ein eindeutiger Hinweis auf unsichere Einstellungen, insbesondere auf eine deaktivierte Ende-zu-Ende-Verschlüsselung, erfolgt (siehe auch M-TK-17 „Aktivierung einer Warnung bei Nutzung unsicherer Merkmale“).

M-TK-50 Prozess zur Behandlung des Verlusts eines VoIP-Endgerätes

Werden auf VoIP-Endgeräten vertrauenswürdige Daten gespeichert, muss ein Prozess zur Behandlung des Verlusts eines VoIP-Endgerätes implementiert werden, der den Umgang mit diesen Daten bei Beeinträchtigung von Vertraulichkeit und Integrität regelt. Dies beinhaltet beispielsweise, dass Zertifikate eines IP-Telefons sofort zurückgezogen werden.

M-TK-51 Absicherung der Firmware

Bevor eine neue Firmware auf ein IP-Telefon übertragen wird, sollte die Integrität und Authentizität der Datei überprüft werden. Falls der Hersteller seine Firmware digital signiert und eine Prüfsumme zur Verfügung stellt, so müssen die Signatur sowie die Prüfsumme überprüft werden. Bei der Übertragung der Firmware vom Telefonie-Server auf die IP-Telefone sollte ebenfalls eine digitale Signatur verwendet werden.

M-TK-52 Absicherung von Konfigurationsdateien

Zur Konfiguration von IP-Telefonen existieren unterschiedliche Mechanismen. Dazu zählen die manuelle Konfiguration am Endgerät, die Konfiguration per Web-Interface des IP-Telefons und das Verfahren, bei dem sich das Telefon automatisch eine Konfiguration von einem Server via HTTP oder Trivial File Transfer Protocol (TFTP) lädt.

Für den erhöhten Schutzbedarf muss die Konfiguration über einen gesicherten Übertragungsweg erfolgen, der eine Authentisierung dem Telefon gegenüber ermöglicht. Beispielsweise kann ein HTTPS[13]-Server mit Authentisierung verwendet werden.

Da Konfigurationsdateien sensible Daten, wie beispielsweise Passwörter enthalten können, sollten für den erhöhten Schutzbedarf die Konfigurationsdateien vom Telefonie-Server signiert und verschlüsselt an das IP-Telefon übertragen werden.

13 HTTPS steht umgangssprachlich für HTTP Secure, ist aber von der IETF als HTTP over TLS bzw. HTTP/TLS spezifiziert (siehe [IETF RFC2818-2000]).

M-TK-53 Sicherheit von Softphones

Für den erhöhten Schutzbedarf sollte man möglichst auf Softphones verzichten, da für einen PC zu viele kritische Angriffsmöglichkeiten (Trojaner, Cross-Site Scripting usw.) bestehen. Durch die Ausnutzung von Sicherheitsschwachstellen ist es z. B. möglich Anrufprotokolle und Adressbucheinträge des Softphones zu manipulieren oder das Mikrofon des PCs zum Abhören des Raums zu benutzen.

Falls der Einsatz von Softphones gefordert ist, so muss auf dem PC mit dem Softphone neben einer Personal Firewall und einem Virenschutz in jedem Fall ein Host-basiertes IPS installiert werden.

Weiterhin müssen im Sinne erhöhten Schutzbedarfs die folgenden Einzelmaßnahmen umgesetzt werden:

- Verschlüsselung der Signalisierungs- und Nutzdaten gemäß Maßnahmen M-TK-31 „Durchgängige Verschlüsselung des Medienstroms“ und M-TK-32 „Durchgängige Verschlüsselung der Signalisierung“
- Härtung des Betriebssystems
- Härtung des Web-Browsers

  Skriptsprachen, beispielsweise JavaScript und Virtual Basic Script (VBScript) sollten deaktiviert werden. Weiterhin sollten ActiveX, Java und Plug-in-Programme, z. B. Macromedia Flash, auf dem PC mit dem Softphone nicht benutzt werden dürfen.

Die Administration des PCs sollte von einer zentralen Stelle erfolgen, um die unkontrollierte Installation von Software zu verhindern.

Hinweis zur Nutzung von Thin Clients: Sofern auf Thin Clients z. B. über Streaming ein Softphone oder andere TK-Komponenten laufen, sind die Maßnahmen zur Absicherung des Softphone und der jeweiligen TK-Komponenten anzuwenden. Außerdem ist der Thin Client selbst (ggf. wie ein konventioneller Fat Client) entsprechend abzusichern.

M-TK-54 Sichere Konfiguration von Ethernet-Ports für den PC-Anschluss an IP-Telefonen

IP-Telefone bestimmter Hersteller umfassen die Möglichkeit, an einem im Telefon eingebauten PC-Port (Ethernet-Port) ein PC-Endgerät anzuschließen. Dies kann ein Sicherheitsrisiko darstellen, mit dem bei erhöhtem Schutzbedarf durch gezielte Konfiguration umzugehen ist. Es ergeben sich folgende Prüf- und Aktionspunkte:

- Deaktivierung der Weiterleitung aller Pakete auf den PC-Port

  Etliche IP-Telefone leiten zurzeit in der Default-Konfiguration alle Pakete, die zwischen dem Telefon und anderen Stationen ausgetauscht werden, auch an den PC-Port des Telefons weiter. Dies sollte in jedem Fall geändert werden, sodass ein Abhören und Aufzeichnen von Telefonaten mit Hilfe von Software auf einem am PC-Port angeschlossenen Gerät unmöglich ist.

- Deaktivierung von PC-Ports an IP-Telefonen

  Werden die PC-Ports an den IP-Telefonen in der betrachteten Umgebung nicht genutzt, d. h. werden für die PC-Endgeräte separate Netzwerk-Anschlusspunkte zur Verfügung gestellt, so sollten die PC-Ports an den IP-Telefonen gezielt deaktiviert werden (Vermeidung ungesicherter Netzzugänge über die PC-Ports).

Hinweis: IP-Telefone stellen in der Regel keine vollwertigen Ethernet Switches gemäß IEEE 802.1D dar. Daher kann insbesondere die VLAN-Trennung von Voice- und Daten-VLAN Schwachstellen aufweisen.

M-TK-55 Sichere Konfiguration von IP und von IP-basierten Diensten

Diese Maßnahme ist im Sinne einer Systemhärtung der IP-Telefone zu sehen und dient der gezielten Abwehr von Angriffen auf diese Endgeräte. Derartige Angriffe können über IP und IP-basierte Dienste sowie deren Schnittstellen am Telefon erfolgen. Typische, je nach Produkt in unterschiedlichem Umfang konfigurierbare Prüf- und Aktionspunkte sind:

- Deaktivierung der Reaktion auf Gratuitous ARPs

  Durch eine solche Konfiguration am IP-Telefon wird vermieden, dass der ARP-Cache des Telefons durch Gratuitous ARPs (Sonderform von ARP-Nachrichten) kompromittiert und so z. B. ein Lauschangriff auf das Telefon vorbereitet werden kann.

- Deaktivierung des Versendens von Gratuitous ARPs

  Gratuitous ARPs werden von (Telefonie-)Endgeräten vorrangig versandt als Versuch IP-Adresskonflikte zu ermitteln. Kritisch ist dabei der Broadcast-basierte Versand solcher Pakete, der dazu führt, dass ein Angreifer in der Broadcast-Domäne des Telefons auf diese Weise IP- und MAC-Adresse des Telefons erfährt und diese Information gezielt für einen Angriff missbrauchen kann (Aufhebung der Anonymität des Telefons).

- Deaktivierung des Web-Servers am IP-Telefon

  Durch die Deaktivierung des Web-Servers am IP-Telefon wird verhindert, dass mit einem Web-Browser oder Vergleichbarem über das Netz auf das Telefon zugegriffen wird. Die Webschnittstelle ist gerade bei Endgerätelösungen nur schwach gesichert und damit ein bevorzugtes Angriffsziel.

M-TK-56 Einschränkung des lokalen Zugriffs auf die Konfiguration des IP-Telefons

Das IP-Telefon stellt meist einen Zugang über Bedientasten am Gerät bereit, über den verschiedene Einstellungen am Telefon vorgenommen und geändert werden können.

Dabei müssen grundsätzlich zwei Einstellbereiche unterschieden werden:

- Im ersten Bereich der Einstellungen kann der Benutzer z. B. Klingeltöne einstellen und den Kontrast des Displays ändern.

  Dieser Bereich sollte grundsätzlich bei jedem IP-Telefon freigegeben sein (Bedienzugang für den Anwender).

- In einem weiteren Bereich besteht Zugang zu den Netzwerkeinstellungen des Telefons.

  Nach einer Prozedur zum Entsperren der Einstellungen können diese auch geändert werden (lokaler Administrationszugang zum Telefon). So könnte z. B. die IP-Adresse des Telefons oder des TFTP-Servers geändert werden. Der Zugriff auf diesen Bereich muss eingeschränkt werden. Die vom Hersteller voreingestellte PIN für administrative Zugriffe bzw. ein voreingestelltes Kennwort (typisch sind leicht zu erratende PINs wie 0000 oder der Herstellername als Default-Kennwort) muss geändert werden. Die Komplexität von PIN oder Kennwort muss dabei möglichst hoch sein.

M-TK-57 Benutzerabhängige Berechtigungen

VoIP-Lösungen unterstützen oft eine Funktion, die eine Anmeldung eines Benutzers am IP-Telefon über eine personenbezogene PIN ermöglicht. Der Benutzer veranlasst mit dieser Funktion die Übertragung eines Profils auf das Telefon, mit dem die Konfiguration des Telefons hinsichtlich Kurzwahllisten, Berechtigungen, Durchwahlnummer usw. durchgeführt wird.

Hiermit können benutzerabhängige Berechtigungen für die Nutzung der VoIP-Lösung erteilt werden. Für den erhöhten Schutzbedarf kann auf diese Weise ein differenziertes und gestuftes Berechtigungskonzept umgesetzt werden.

In Ergänzung zu Maßnahme M-TK-16 „Einsatz sicherheitsintelligenter Endgeräte“ sind dabei folgende Punkte im Einzelfall zu entscheiden:

- Abwägung zwischen zeitgesteuerter oder expliziter Abmeldung (Sicherheit versus Verfügbarkeit)
- Standard-Profil, das nach der Abmeldung eines Nutzers auf dem Telefon aktiviert wird, (Logout-Profil) mit folgenden denkbaren Basisfunktionalitäten:
  - nur Notruf
  - nur interne Telefonie
  - übertragene Durchwahlnummer
- Übertragung einer allgemeinen oder nutzerabhängigen Durchwahlnummer
- nutzerabhängige Freigabe eines schreibenden Zugriffs auf die Konfigurationsdatenbank des Telefonie-Servers

M-TK-58 Schutz von teilnehmerspezifischen Daten auf einem IP-Telefon

Auf IP-Telefonen werden lokal diverse Daten abgespeichert. Ein Teil dieser Daten umfasst teilnehmerspezifische Daten wie z. B. das Rufjournal, persönliche Kontakte und Leistungsmerkmale. Diese Daten müssen durch eine sichere Verwaltung der Profile auf dem Telefon geschützt werden. Zur sicheren Verwaltung von den auf dem IP-Telefon lokal abgespeicherten Nutzerprofilen sollten benutzerabhängige Berechtigungen für die Nutzung der VoIP-Lösung erteilt werden. Für den erhöhten Schutzbedarf kann auf diese Weise ein differenziertes und gestuftes Berechtigungskonzept umgesetzt werden, siehe Maßnahme M-TK-57 „Benutzerabhängige Berechtigungen“.

Falls eine sichere Verwaltung der Daten technisch nicht möglich ist, so müssen bei erhöhtem Schutzbedarf folgende Maßnahmen beachtet werden:

- Das IP-Telefon muss mindestens mit einer PIN geschützt werden.
- Es sollten keine IP-Telefone eingesetzt werden, die Nutzer- und Nutzungs-spezifische Daten lokal speichern. Eine Ausnahme stellen IP-Telefone dar, bei denen man explizit die Speicherung solcher Daten deaktivieren kann.
- Nutzer-spezifische Daten sollten auf dem Telefon manuell löschbar sein.
- Räume, in denen IP-Telefone aufgestellt sind, sollten beim Verlassen des Raums immer abgeschlossen werden, sofern nicht der Raum selbst bereits Bestandteil eines Sicherheitsbereichs ist.

M-TK-59 Einschränkung von Internettelefonie auf dedizierte, gehärtete Endgeräte

In Umgebungen mit erhöhtem Schutzbedarf muss eine Internettelefonie insbesondere wegen Gefährdungen der Vertraulichkeit strikt eingeschränkt werden. Wenn eine Internettelefonie zwingend erforderlich sein sollte, muss diese auf dediziert hierfür vorgesehene PCs eingeschränkt werden, die strikt gehärtet werden und nur einen minimalen Funktionsumfang bieten. Dabei kann auch eine VM eingesetzt werden, die entsprechend gekapselt wird und deren Kommunikationsmöglichkeiten z. B. durch eine Host-basierte Firewall auf Internet-telefonie reduziert werden.

4.3.3 Netzwerk

M-TK-60 Sichere Konfiguration der Netzwerk-Komponenten

Zum Schutz der VoIP-Infrastruktur sollten neben den Servern des Telekommunikationssystems auch die übrigen Netzwerk-Komponenten, z. B. Router und Switches, angemessen abgesichert werden. Hierzu sind insbesondere die folgenden Einstellungen zu konfigurieren:

- Um Informationen über die vorhandene Netzwerk-Topologie zu schützen, sollten die Nachrichtentypen ICMP Destination Unreachable, ICMP Redirect und ICMP Address Mask Request deaktiviert werden. An dieser Stelle muss darauf hingewiesen werden, dass durch die Umsetzung dieser Maßnahme eine ggf. erforderliche Fehlersuche erschwert wird.
- IP Source Routing ist eine Technik, bei der der Sender die Route für ein IP-Paket zu einem Ziel beeinflussen kann. Da IP Source Routing für Angriffe missbraucht werden kann, sollte es deaktiviert werden.
- Die Einstellung Proxy ARP sollte abgeschaltet werden, da sie zur Informationsgewinnung über das Netzwerk und zur Durchführung von Denial-of-Service-Angriffen missbraucht werden kann.

M-TK-61 Sicheres Routing

Die zwischen den vernetzten Systemen ausgetauschten Routing-Informationen müssen angemessen geschützt werden[14]. Bei der Auswahl des verwendeten Routing-Protokolls ist darauf zu achten, dass das Protokoll beim Austausch von Routing-Informationen ein verschlüsseltes Authentisierungsverfahren verwendet, um die Integrität der Informationen zu schützen. Vergleichbares ist bei allen Routing-nahen dynamischen Mechanismen zu nutzen. Protokolle mit Klartext-Authentisierung sind in jedem Fall zu vermeiden. Weiterhin ist darauf zu achten, dass in regelmäßigen Abständen das bei der Authentisierung genutzte Passwort gewechselt wird.

Eine weitere Möglichkeit zur Erhöhung der Sicherheit wird durch die Konfiguration von Access Control Lists (ACLs) erzielt. Durch diese Maßnahme wird der Austausch von Routing-Updates auf die definierten IP-Adressen beschränkt.

In einer Demilitarisierten Zone (DMZ) sollten keine dynamischen Routing-Protokolle, sondern nur statische Routen verwendet werden. Falls es einem Angreifer gelingt Zugriff auf die in der DMZ ausgetauschten Routing-Informationen zu erlangen, so könnte er daraus auf die Netzstruktur des internen Netzwerks schließen.

M-TK-62 Absicherung von Switch-Ports

Sofern an einem Access-Port keine Zugangskontrolle gemäß Maßnahme M-TK-64 „Zugangskontrolle zum Netzwerk“ realisiert werden kann, sollten Protokolle wie LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Discovery) nur in den Fällen aktiviert werden, wo sie unbedingt benötigt werden. Ansonsten sollte auf derartige Protokolle zwischen Endgeräten (inklusive IP-Telefonen) und Switches verzichtet werden, da sie keine Authentisierungsverfahren unterstützen.

Weiterhin sollte ein Schutz vor bewusst durch einen Angreifer in das Netz gesendeten Paketen des Spanning Tree Protocol (STP) aktiviert werden[15].

Protokolle, die eine dynamische Aushandlung von VLANs gestatten (z. B. VLAN Trunking Protocol, VTP), sollten möglichst nicht verwendet werden.

14 Durch die Erzeugung und Einschleusung von manipulierten Routing-Informationen ist es beispielsweise möglich, gezielt Routing-Tabellen zu manipulieren und somit den Übertragungsweg von Paketen zu verändern.

15 Bei diesem Angriff sendet ein Angreifer manipulierte BPDUs (Bridge Protocol Data Units), um das Netzwerk zu stören oder eine Veränderung der Topologie herbeizuführen.

Funktionen zur Blockierung von DHCP-basierten Angriffen (auch als DHCP Snooping bezeichnet), die inzwischen von vielen Herstellern angeboten werden, sollten auf den Switches aktiviert werden[16].

Funktionen zur Blockierung von ARP Spoofing (auch als Dynamic ARP Inspection bezeichnet), sollten auf den Switches aktiviert werden.

M-TK-63 Quality of Service im Netzwerk

Zur Vermeidung einer punktuellen Überlastung von Verbindungen oder Netzressourcen sollte generell für das LAN eine ausreichende Dimensionierung der Netz-Komponenten vorgesehen werden.

Beim Einsatz von VoIP über ein WAN sollte bei der Auswahl eines Providers darauf geachtet werden, dass der Provider mit seiner Technik Service-Klassen unterstützen kann[17]. Es sollte weiterhin vertraglich fixiert werden, dass die Sprachkommunikation immer in der höchsten Service-Klasse stattfindet.

Beschreibungen einzelner Techniken zur Realisierung von QoS findet man im Baustein B 4.7 „VoIP“ in der Maßnahme M 5.136 „Dienstgüte und Netzmanagement bei VoIP“ der IT-Grundschutz-Kataloge (siehe [BSI GSK-2013]).

M-TK-64 Zugangskontrolle zum Netzwerk

Der LAN-Anschluss für VoIP-Endgeräte sollte bei erhöhtem Schutzbedarf durch eine Netzzugangskontrolle abgesichert werden. Für Anschlüsse in unübersichtlichen Umgebungen oder in Bereichen mit erhöhtem Publikumsverkehr (z. B. In Besprechungsräumen oder öffentlich zugänglichen Räumen, etwa in Lobbys) muss eine Netzzugangskontrolle vorgesehen werden.

Wenn eine Netzzugangskontrolle verwendet werden soll, muss bei erhöhtem Schutzbedarf als Mechanismus zur Netzzugangskontrolle IEEE 802.1X verwendet werden (siehe Kapitel 13.3.2). Dabei ist die Verwendung von einer zertifikatsbasierten Authentisierung mit Extensible Authentication Protocol – Transport Layer Security (EAP-TLS) zu bevorzugen und einfache Passwort-Hash-basierte Mechanismen wie Extensible Authentication Protocol – Message-Digest Algorithm 5 (EAP-MD5) möglichst zu vermeiden. Eine MAC-Adress-basierte Zugangskontrolle kommt für den erhöhten Schutzbedarf nicht in Frage.

M-TK-65 MAC Security im Anschlussbereich für Endgeräte

Der Einsatz einer Netzzugangskontrolle gemäß Maßnahme M-TK-64 „Zugangskontrolle zum Netzwerk“ sichert ggf. nicht zu, dass die Pakete auch tatsächlich von dem Endgerät stammen, das sich authentisiert hat. Wenn keine Ende-zu-Ende-Verschlüsselung gemäß Maßnahme M-TK-31 „Durchgängige Verschlüsselung des Medienstroms“ eingesetzt werden kann, muss die Kommunikation zwischen Endgerät und dem Switch in der Infrastruktur, an den das Endgerät angeschlossen ist (Access Switch), anderweitig abgesichert werden. In diesem Fall kann - sofern technisch möglich - eine Verschlüsselung, Authentisierung und Integritätsprüfung der Pakete gemäß IEEE 802.1AE eingesetzt werden. Das hierzu erforderliche Schlüsselmanagement sollte über IEEE 802.1X gemäß der Fassung von 2010 erfolgen.

16 Bei diesen Funktionen werden die Ports der Switches in vertrauenswürdige Ports und nicht vertrauenswürdige Ports eingeteilt. Antworten auf eine DHCP-Anfrage werden nur auf vertrauenswürdigen Ports, d. h. auf Ports, über die potenziell ein DHCP-Server als erreichbar angenommen wird, gestattet. DHCP-Antworten auf einem nicht vertrauenswürdigen Port werden verworfen, da angenommen wird, dass an einem solchen Port nur Clients angeschlossen werden. Weiterhin wird typischerweise ein Schutz vor DHCP Starvation (siehe G-TK-35) geboten, indem die maximale Rate von DHCP-Anfragen auf eine vorgegebene Grenze eingeschränkt werden kann.

17 Diese Maßnahme ist im Rahmen des verfügbaren Marktangebots anzuwenden.

M-TK-66 VPN zur Kommunikation über eingeschränkt vertrauenswürdige Netze

Diese Maßnahme ist insbesondere in Betracht zu ziehen, wenn die Maßnahmen M-TK-31 „Durchgängige Verschlüsselung des Medienstroms“ und M-TK-32 „Durchgängige Verschlüsselung der Signalisierung“ nicht zufriedenstellend umgesetzt werden können.

Bei einem erhöhten Schutzbedarf hinsichtlich Vertraulichkeit oder Integrität ist die über eingeschränkt vertrauenswürdige Netze geführte VoIP-Kommunikation zwingend zu verschlüsseln. Dies betrifft speziell die Standort-übergreifende Kommunikation z. B. über ein WAN oder das Internet. Zur Verschlüsselung kann ein Site-to-Site-VPN auf Basis von IPsec oder einer vergleichbaren Technik eingesetzt werden. Alternativ können die betroffenen Übertragungsstrecken auf Layer 2 mit IEEE 802.1AE MAC Security geschützt werden. Eine angemessene Authentisierung zwischen den Partner-Instanzen wird vorausgesetzt.

Hinweis: Bei der Umsetzung dieser Maßnahme muss beachtet werden, dass ein VPN zwischen unterschiedlichen Organisationen oft nur mit erheblichem und ggf. sogar mit einem nicht vertretbaren organisatorischem Aufwand möglich ist.

M-TK-67 Netztrennung für VoIP

Etliche Gefährdungen für VoIP resultieren aus der Tatsache, dass mit einem IP-Netz eine Kommunikationsbasis genutzt wird, die auch von anderen Anwendungen genutzt werden kann und wegen der Offenheit der TCP/IP-Protokolle einer Vielzahl von Angriffsformen ausgesetzt ist.

Hier kann der Aufbau von Sicherheitszonen mit den Mitteln des Netzwerks eine sinnvolle Sicherheitsmaßnahme darstellen, die unter gewissen Rahmenbedingungen in Betracht gezogen werden muss. Eine Sicherheitszone ist dabei ein IP-Netz, das aus Sicherheitsgründen von anderen IP-Netzen getrennt wird und bei dem die Kommunikation zu und/oder von der Sicherheitszone durch Sicherheitselemente kontrolliert und ggf. reglementiert wird.

Für den Aufbau solcher Sicherheitszonen ist zunächst zu unterscheiden, ob ausschließlich zentrale Komponenten (Server und Appliances) oder auch Clients von der Trennung betroffen sind.

Für zentrale Komponenten gilt:

- Wenn zentrale Komponenten der VoIP-Lösung (z. B. Telefonie-Server) nicht angemessen dahingehend gehärtet werden können, dass sie mit anderen Systemen in einem gemeinsamen IP-Netz liegen können, müssen diese je nach Sicherheitsanforderungen in einer oder in mehreren Sicherheitszonen von anderen Systemen getrennt werden, wie in Abbildung 24 illustriert. Als Sicherheitselement zur Kontrolle der Kommunikation kommen üblicherweise eine Firewall und/oder ein Intrusion Prevention System (IPS) in Frage.
- Für den netztechnischen Aufbau von Sicherheitszonen können unterschiedliche Techniken eingesetzt werden (für Details siehe Kapitel 13.3.1). Für eine logische Trennung der Sicherheitszonen kann auf Layer 2 mit VLANs und auf Layer 3 mit virtuellen Routing-Instanzen über „Virtual Routing and Forwarding“ (VRF) gearbeitet werden.
- Alternativ kann eine Sicherheitszone (je nach eingesetzten Produkten) auch mit kryptografischen Techniken aufgebaut werden. Hier ist beispielsweise IEEE 802.1AE MACsec (Media Access Control Security) zu nennen. Mit dieser Technik können in einem Netz durch Verschlüsselung auf Layer 2 auch unterschiedliche Gruppen voneinander getrennt werden.
- Eine physische Trennung der Systeme in der Sicherheitszone kann aus Gründen der Verfügbarkeit sinnvoll sein. In vielen Fällen wird man bedingt durch den Aufbau moderner Rechenzentren eine logische Netztrennung anstreben.

Für eine flächendeckende Trennung von VoIP und anderen Daten, die auch die VoIP-Endgeräte berücksichtigt, sind folgende Punkte zu beachten:

- Zunächst ist eine Zuordnung von Desktop-IP-Telefonen in ein separates VLAN (Voice-VLAN) zur Trennung der Broadcast-Domänen üblich. Der Sicherheitsgewinn besteht primär darin, dass eine Störung auf Layer 2, z. B. ein Broadcast-Sturm, in einer anderen Broadcast-Domäne, d. h. einem anderen VLAN, sich nicht auf die IP-Telefone im Voice-VLAN auswirkt.
- Für den erhöhten Schutzbedarf kann eine weitergehende netztechnische Separierung der VoIP-Geräte (IP-Telefone, IP-PBX usw.) und ihrer Kommunikation in einer flächendeckenden VoIP-Sicherheitszone in Betracht gezogen werden. Dies ist sinnvoll, wenn keine angemessene Verschlüsselung (die ja einen besonders effektiven Trennungsmechanismus auf Ebene der Daten darstellt) der VoIP-Kommunikation gemäß Maßnahmen M-TK-31 „Durchgängige Verschlüsselung des Medienstroms“ und M-TK-32 „Durchgängige Verschlüsselung der Signalisierung“ bzw. M-TK-66 „VPN zur Kommunikation über eingeschränkt vertrauenswürdige Netze“ möglich ist. Ggf. werden dabei im Rahmen einer Client-Server-Trennung gewisse VoIP-Server, wie oben beschrieben, in einer zusätzlichen Sicherheitszone separiert.
  - Der Aufbau einer solchen flächendeckenden Sicherheitszone kann im LAN analog zu der Separierung zentraler Komponenten durch eine logische oder eine physische Trennung erfolgen. Eine physische Trennung kann beispielsweise aus Gründen der Verfügbarkeit oder einer strikten organisatorischen Trennung der Netzbereiche angestrebt werden. Bei einer logischen Trennung im LAN können VLAN und VRF zum Einsatz kommen (siehe Abbildung 25).
  - Wenn im WAN mit Multi-Protocol Label Switching gearbeitet wird, kann für VoIP ein eigenes MPLS-VPN vorgesehen werden.
  - Beim Aufbau einer Sicherheitszone, die auch IP-Telefone beinhaltet, ist sicherzustellen, dass Clients auch korrekt zu der zu ihnen gehörenden Sicherheitszone zugeordnet werden. In vielen Fällen erfolgt der Anschluss von VoIP-Geräten und anderen Endgeräten (z. B. PCs), die nicht zur VoIP-Sicherheitszone gehören, an benachbarten Netzwerk-Ports, d. h. es ist keine geografische Trennung der Nutzergruppen möglich. Es muss trotzdem ausgeschlossen werden, dass ein Endgerät, das unberechtigterweise an einem Switch-Port der VoIP-Sicherheitszone angeschlossen wird, über diesen Port auf Ressourcen der Sicherheitszone zugreifen kann. Eine effektive Netztrennung erfordert also meist eine Netzzugangskontrolle gemäß Maßnahme M-TK-64 „Zugangskontrolle zum Netzwerk“.

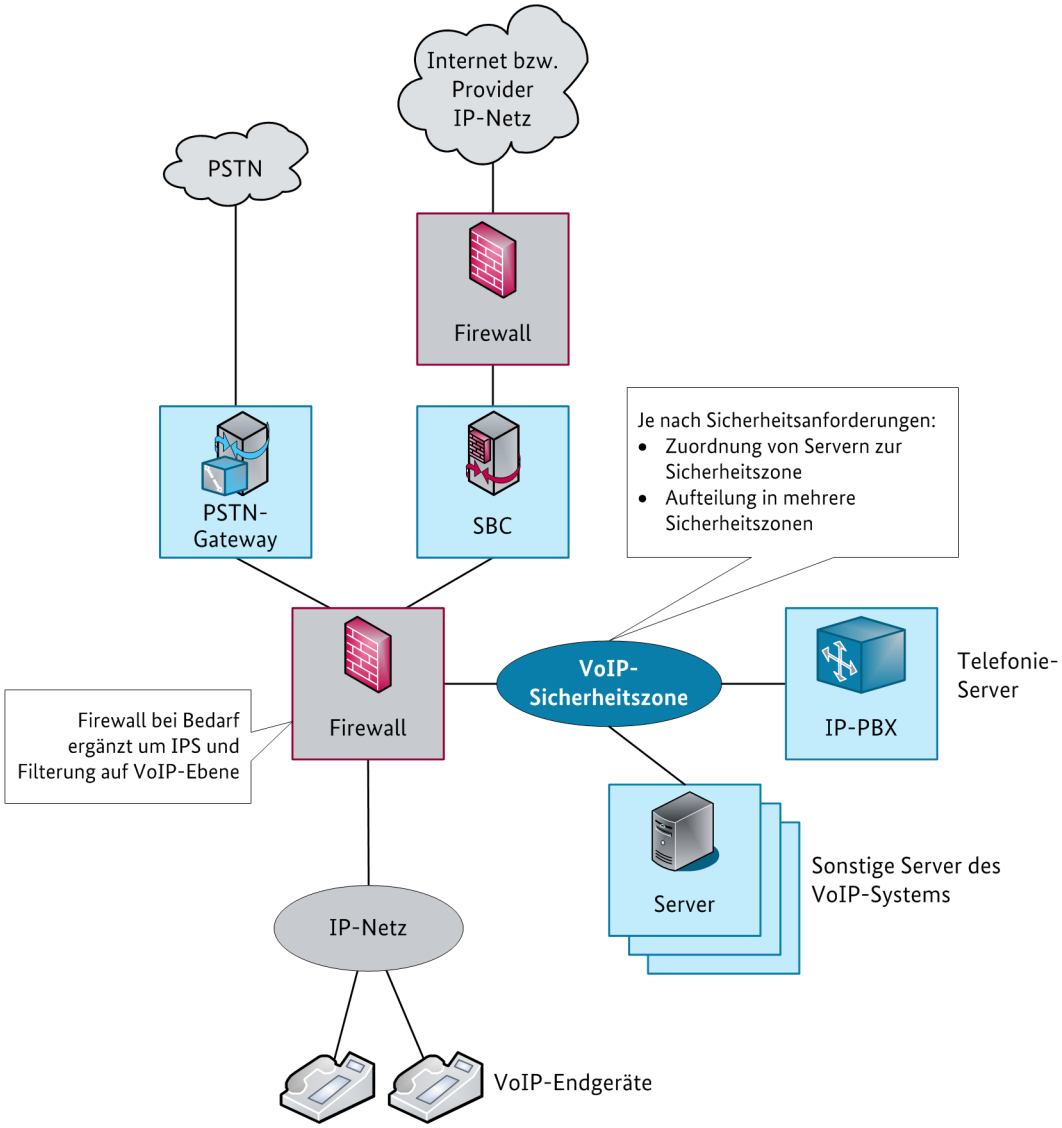


Abbildung 24: Sicherheitszone für zentrale VoIP-Komponenten

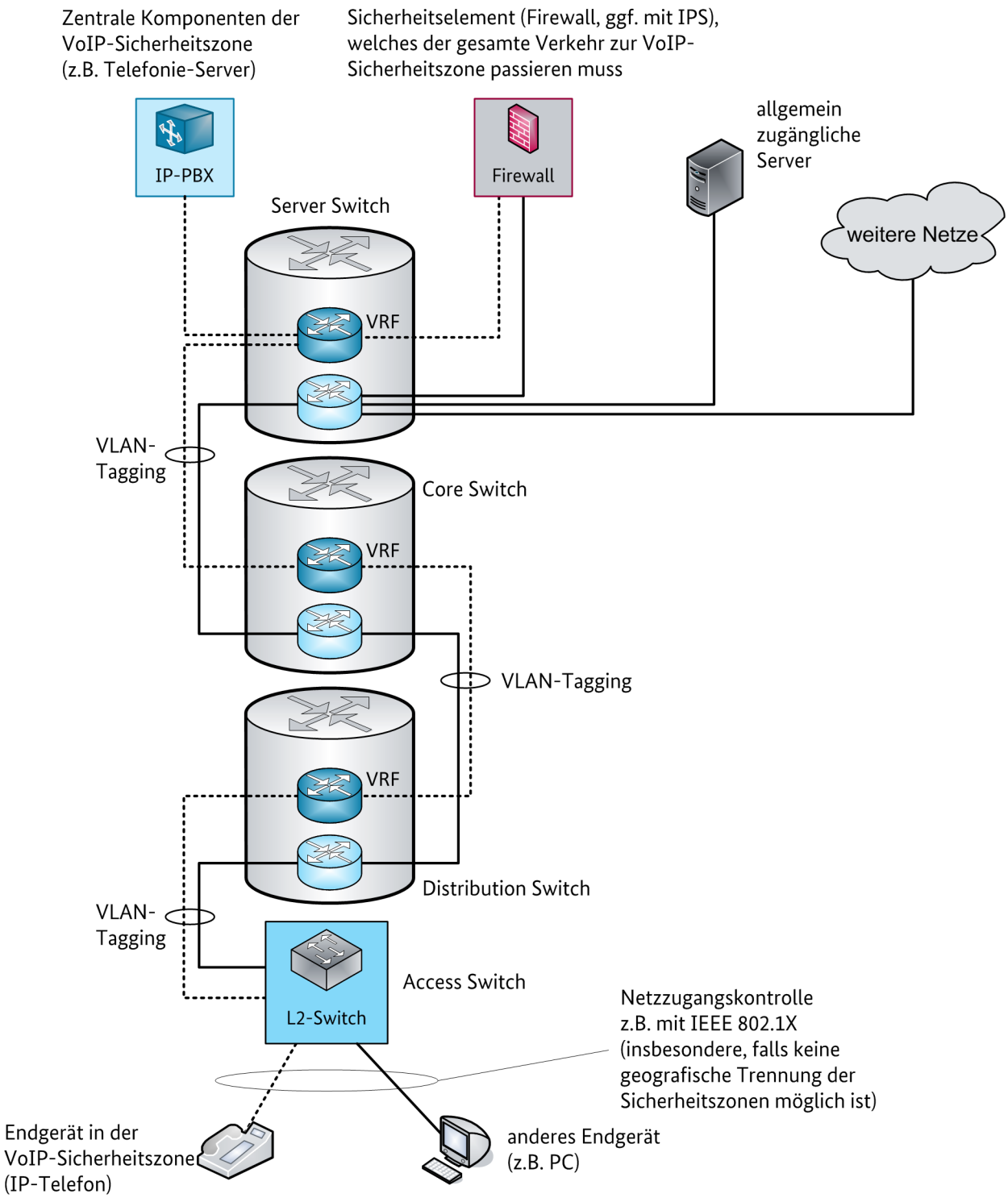


Abbildung 25: Beispiel für den Aufbau einer flächendeckenden VoIP-Sicherheitszone durch logische Netztrennung

M-TK-68 Netztrennung zwischen IP-PBX und Session Border Controller

In Anlehnung an die Maßnahme M-TK-67 „Netztrennung für VoIP“ kann der SBC in einem von der IP-PBX getrennten Netz, einer sogenannten DMZ, untergebracht werden, siehe Abbildung 26.

Über entsprechende Firewalls an den Netzübergängen kann die Kommunikation auf die verwendeten Protokolle zur Administration, Signalisierung und zur Übertragung der Medienströme beschränkt werden. Je nach Funktionsumfang des SBC erlaubt dieser z. B. eine Einschränkung des Portbereiches für RTP, welcher entsprechend auf der Firewall konfiguriert werden kann. Allgemein werden bei RTP für jeden Kommunikationskanal (z. B. Audio oder Video) zwei UDP-Ports (RTP und RTCP) verwendet, d. h. für 60 gleichzeitige Gespräche werden 120 UDP-Ports benötigt.

Tabelle 2 zeigt ein Beispiel-Regelwerk für einen dynamischen Paketfilter, der für die Netzarchitektur in Abbildung 26 zum Einsatz kommen könnte. Dies stellt nur einen Ausschnitt der erlaubten, relevanten Protokolle für die Signalisierung und den Austausch der Nutzdaten dar. Nicht betrachtet werden hierbei Regeln für Basisdienste wie DNS oder Network Time Protocol (NTP) sowie Protokolle für die Administration. Dabei wird angenommen, dass auf dem SBC ein Portbereich für RTP/RTCP von 16400 bis 16520 konfiguriert werden kann.

Falls das Betriebssystem des SBC entsprechend gehärtet und zusätzlich eine integrierte Firewall besitzt, kann der Einsatz eines solchen Produkts, d. h. Einsatz nur eines SBC und Verzicht auf eine DMZ für kleine Organisationen ausreichend sein.

Bei erhöhtem Schutzbedarf können Sicherheitsanforderungen bestehen, für welche die in Abbildung 26 dargestellte Firewall-Architektur nicht ausreicht. In diesem Fall ist eine mehrstufige Firewall-Architektur, wie in Abbildung 27 dargestellt, zu empfehlen.

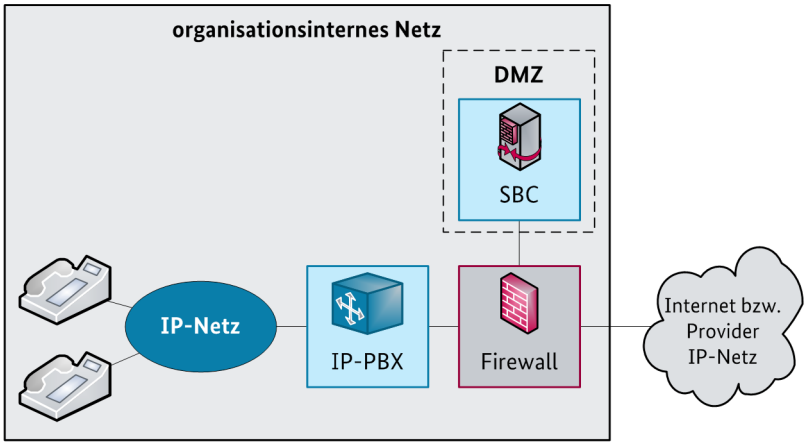


Abbildung 26: Netztrennung mit SBC bei normalem Schutzbedarf

Quelle	Ziel	Protokoll	Quell-Port(s)	Ziel-Port(s)	Bemerkung
Internet	SBC	TCP	> 1023	5061	SIP-TLS
Internet	SBC	UDP	> 1023	16400-16520	RTP
SBC	Internet	TCP	> 1023	5061	SIP-TLS
SBC	Internet	UDP	> 1023	> 1023	RTP
LAN	SBC	TCP	> 1023	5061	SIP-TLS
LAN	SBC	UDP	> 1023	16400-16520	RTP
SBC	LAN	TCP	> 1023	5061	SIP-TLS
SBC	LAN	UDP	> 1023	> 1023	RTP

Tabelle 2: Beispiel Firewall-Regeln für SBC in einer DMZ

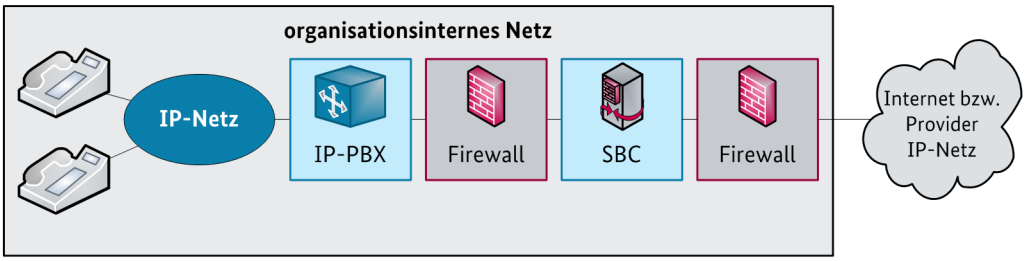


Abbildung 27: Mehrstufige Firewall-Architektur mit SBC bei erhöhtem Schutzbedarf

M-TK-69 Erkennung und Abwehr von DoS-Angriffen gegen VoIP und von SPIT durch IPS / IDS

DoS-Angriffe auf Ebene der VoIP-Signalisierung lassen sich in einem gewissen Umfang durch ein IPS oder durch ein Intrusion Detection System (IDS) erkennen und bei einem IPS auch blockieren. Solche IPS-Funktionen können auch in einer Firewall implementiert werden.

TDoS inkl. SIP Flooding kann bei signifikanten Abweichungen vom Normalverkehr durch statistische Methoden festgestellt werden. Für DoS-Angriffe, die speziell manipulierte Signalisierungsnachrichten verwenden, lassen sich grundsätzlich Signaturen entwickeln, welche ein IDS / IPS mit dem Netzverkehr vergleichen kann. Hierdurch können entsprechende auf die Signaturen passende Muster erkannt werden.

Außerdem sind Blacklists und Whitelists ein gängiges Abwehrinstrument, das in einem IPS realisiert werden kann. Hier wird zwar nicht unmittelbar der DoS-Angriff erkannt und abgewehrt, jedoch pauschal die Angriffsfläche reduziert. Weiterhin (ggf. in Kombination mit Blacklists und/oder Whitelists) kann ein IDS / IPS die Reputation der Quellen des Verkehrs bewerten und ein IPS könnte bei schlechter Reputation sogar eine Anfrage blockieren.

Mit ähnlichen Techniken kann auch gegen SPIT vorgegangen werden.

Hinweis: Angriffe wie DoS gegen VoIP und wie SPIT können durch Sicherheitsmaßnahmen nicht vollständig verhindert werden. Es bleibt vergleichbar zur Situation bei E-Mail ein Restrisiko, das gerade bei einem erhöhten Schutzbedarf für VoIP hinsichtlich der Verfügbarkeit genau bewertet werden muss.

M-TK-70 Angemessene Verfügbarkeit des LAN für die Verwendung von VoIP

Das LAN ist für die Verwendung von VoIP im Rahmen des Möglichen hochverfügbar auszulegen. Hierunter fallen die folgenden Einzelmaßnahmen:

- Vermeidung von sogenannten Single Points of Failure

  Aktive Komponenten sollten redundant ausgelegt werden, insbesondere ist diese Maßnahme für den Backbone vorzusehen.

- Strukturierte Kabelführung

  Zur Kabelführung gelten die allgemeinen in Maßnahme M-TK-227 „Sichere Kabelführung“ beschriebenen Einzelmaßnahmen.

- Wegeredundanz

  Durch die redundante Auslegung der Kabelstrecken zwischen wichtigen Netzwerk-Komponenten kann im Falle eines Ausfalls eines Kabels auf die redundante Strecke ausgewichen werden.

- Modulredundanz

  Module wie beispielsweise Netzteile von aktiven Komponenten sollten im Sinne der Notfallvorsorge redundant ausgelegt werden. Hierdurch werden längere Ausfallzeiten verhindert.

- Permanent-Überwachung

  Alle aktiven Netzwerk-Komponenten sollten in ein zentrales Netz- und System-management integriert werden, um eine permanente Überwachung sicherzustellen. Das System sollte zusätzlich über eine Alarmierungsfunktion verfügen, welches bei der Unter- bzw. Überschreitung von definierten Schwellwerten festgelegte Aktionen ausführt.

M-TK-71 Angemessene Verfügbarkeit der vom VoIP-System genutzten Netzdienste

Die vom VoIP-System genutzten Netzdienste wie z. B. DHCP, DNS und RADIUS[18] müssen entsprechend redundant ausgelegt werden. Des Weiteren ist eine geeignete Notfallvorsorge sicherzustellen (siehe Maßnahme M-TK-85 „Notfallvorsorge für das VoIP-System“). Unter diesen Punkt fällt beispielsweise, dass die Konfigurationen der Dienste regelmäßig gesichert werden, um in kurzer Zeit ein Ersatz-System bereitstellen zu können.

M-TK-72 Angemessene Verfügbarkeit der Stromversorgung für IP-Telefone

Die Stromversorgung von IP-Telefonen erfolgt heutzutage häufig über Power over Ethernet (PoE) nach IEEE 802.3af und IEEE 802.3at (siehe [IEEE 802.3-2012]). Dabei ist zu beachten, dass eine den Verfügbarkeitsanforderungen angemessene Stromversorgung durch die Switches sowie eine Notversorgung mit genügender Kapazität durch eine Unterbrechungsfreie Stromversorgung (USV) realisiert wird.

Bei der Planung der Stromversorgung muss auch eine spätere Erweiterung des VoIP-Systems berücksichtigt werden. Neben einer steigenden Anzahl von Endgeräten kann durch leistungsfähigere Endgeräte (z. B. mit größerem und höher auflösendem Farb-Display) ein höherer Strombedarf entstehen[19].

Werden IP-Telefone konventionell an das Stromnetz angeschlossen, muss eine genügende Anzahl von Steckdosen mit USV eingeplant werden.

18 RADIUS = Remote Authentication Dial In User Service

19 Für Geräte mit einer höheren Leistungsaufnahme (mehr als 12,95 Watt) ist der Standard IEEE 802.3at vorgesehen.

4.3.4 Netz- und Systemmanagement

M-TK-73 Sichere Administration des Telefonie-Servers

Administrationszugriffe auf Server des VoIP-Systems müssen durch Sicherheitsmechanismen angemessen geschützt werden. Hierzu sind die entsprechenden generellen Maßnahmen in Kapitel 10.2 und 10.3 umzusetzen. Dabei ist auch zu beachten, dass auf Telefonie-Servern personenbezogene Daten verarbeitet und gespeichert werden, die entsprechend vor einem unberechtigten Zugriff geschützt werden müssen.

Bei Telefonie-Servern ist allgemein das Sicherheitsziel Verfügbarkeit sehr hoch zu werten. Telefonie-Server müssen vor schadenstiftender Software geschützt werden (siehe M-TK-235 „Schutz vor schadenstiftender Software für die Server der TK-Lösung“). Dies gilt insbesondere bei Verwendung von Standard-Betriebssystemen. Sicherheits-Patches und Patches zur Stabilisierung der Software sind gleich zu priorisieren. Generell sind geeignete Methoden für die Datensicherung und das Patch-Management der Telefonie-Server einzusetzen (siehe Maßnahmen M-TK-234 „Berücksichtigung der Server der TK-Lösung im Datensicherungskonzept der Organisation“ und M-TK-236 „Einbindung der Server der TK-Lösung in das Patch-Management der Organisation“). Dabei muss beachtet werden, dass für Telefonie-Server oft keine Wartungsfenster mit einer Komplettabschaltung der Server (und damit des Telefoniedienstes) zur Verfügung stehen. Changes und Wiederherstellungsmaßnahmen müssen während des Betriebs durchgeführt werden.

Hinweis: Bei der Verwaltung von Telefonie-Servern muss beachtet werden, dass die Systeme teilweise als Appliance bzw. als Bündel (engl. Bundle) aus Betriebssystem und Telefonie-Anwendung geliefert werden. In dieser Situation ist mit herstellerspezifischen Besonderheiten und Einschränkungen hinsichtlich der folgenden Punkte zu rechnen:

- Zugriffsmöglichkeiten auf die Systemkonfiguration
- Methode für die Datensicherung
- Installation von Patches und Virenschutz-Software

M-TK-74 Sichere Administration von PSTN-Gateways

Zur sicheren Administration eines PSTN-Gateway sollten die entsprechenden generellen Maßnahmen in Kapitel 10.2 und 10.3 umgesetzt werden.

Falls ein Router als PSTN-Gateway verwendet wird, sollte bei erhöhtem Schutzbedarf der administrative Zugriff nur nach einer zentralen Authentisierung (etwa über RADIUS) möglich sein.

Bei PSTN-Gateways ist wie bei Telefonie-Servern allgemein das Sicherheitsziel Verfügbarkeit sehr hoch zu werten. PSTN-Gateways müssen vor schadenstiftender Software geschützt werden (siehe Maßnahme M-TK-235 „Schutz vor schadenstiftender Software für die Server der TK-Lösung“). Dies gilt insbesondere bei Verwendung von Standard-Betriebssystemen. Sicherheits-Patches und Patches zur Stabilisierung der Software sind gleich zu priorisieren. Generell sind geeignete Methoden für die Datensicherung und das Patch-Management der PSTN-Gateways einzusetzen (siehe Maßnahmen M-TK-234 „Berücksichtigung der Server der TK-Lösung im Datensicherungskonzept der Organisation“ und M-TK-236 „Einbindung der Server der TK-Lösung in das Patch-Management der Organisation“). Dabei muss beachtet werden, dass für PSTN-Gateways oft keine Wartungsfenster mit einer Komplettabschaltung der Systeme (und damit des Telefoniedienstes) zur Verfügung stehen. Changes und Wiederherstellungsmaßnahmen müssen während des Betriebs durchgeführt werden.

Hinweis: Bei der Verwaltung von PSTN-Gateways muss beachtet werden, dass die Systeme oft als Appliance geliefert werden. In dieser Situation ist mit herstellerspezifischen Besonderheiten und Einschränkungen hinsichtlich der folgenden Punkte zu rechnen:

- Zugriffsmöglichkeiten auf die Systemkonfiguration
- Methode für die Datensicherung
- Installation von Patches und Virenschutz-Software

M-TK-75 Sichere Administration von Anwendungs- und Management-Servern

Für die sichere Administration von Anwendungs- und Management-Servern sind die entsprechenden generellen Maßnahmen in Kapitel 10.2 und 10.3 angemessen umzusetzen.

Bei Applikations-Servern mit VoIP-Mehrwertdiensten gilt meistens „Sicherheit vor Verfügbarkeit". Beispiel: Eine vorübergehend nicht verfügbare Voicemail-Funktionalität ist besser als ein nicht sicherer (kompromittierbarer) Voicemail-Dienst. Anwendungs- und Management-Server müssen vor schadenstiftender Software geschützt werden (siehe Maßnahme M-TK-235 „Schutz vor schadenstiftender Software für die Server der TK-Lösung"). Dies gilt insbesondere bei Verwendung von Standard-Betriebssystemen.

M-TK-76 Sichere Administration von Abrechnungs- und Gebührenerfassungssystemen

Viele Unternehmen oder Behörden, die VoIP verwenden, setzen spezielle Systeme zur Abrechnung und Gebührenerfassung für die anfallenden Telefonate ein. Die Administration von Abrechnungs- und Gebührenerfassungssystemen muss gemäß den entsprechenden generellen Maßnahmen in Kapitel 10.2 und 10.3 abgesichert werden.

Hier muss ergänzend berücksichtigt werden, dass personenbezogene Daten von diesen Systemen verarbeitet und gespeichert werden. Der Schutz dieser Daten muss bei der Absicherung der Zugangswege zu den Systemen besonders berücksichtigt werden. Dies beinhaltet die Kontrolle (und Einschränkung) des Zugangs zu diesen Daten sowie die Verschlüsselung dieser Daten beim Transport über das Datennetz und auf den jeweiligen Datenträgern. Neben der Vertraulichkeit muss die Integrität der Abrechnungsdaten besonders geschützt werden. Dies kann beispielsweise durch den Einsatz von Signaturverfahren erfolgen.

M-TK-77 Sichere Verwaltung von Teilnehmerprofilen

Die auf einem Telefonie-Server gespeicherten Teilnehmerprofile müssen auf einem geeigneten Backup-Server gesichert werden. Hierzu sollte die Maßnahme M-TK-234 „Berücksichtigung der Server der TK-Lösung im Datensicherungskonzept der Organisation" umgesetzt werden.

Da diese Teilnehmerprofile personenbezogene Daten enthalten können, ist bei der Speicherung der Daten auf eine entsprechende Absicherung zu achten. Dies beinhaltet die Kontrolle (und Einschränkung) des Zugangs zu diesen Daten sowie die Verschlüsselung dieser Daten beim Transport über das Datennetz und möglichst auf den jeweiligen Datenträgern.

M-TK-78 Sichere Administration von Endgeräten

Der administrative Zugriff (lokal und über das Netzwerk) auf Endgeräte muss durch eine angemessene Authentisierung abgesichert werden. Die Authentisierung muss mindestens über Nutzername und Passwort erfolgen, wobei eine entsprechende Passwortrichtlinie konsequent umzusetzen ist. Siehe Maßnahme M-TK-56 „Einschränkung des lokalen Zugriffs auf die Konfiguration des IP-Telefons" für die Absicherung des lokalen Zugriffs. Für die Administration eines Endgerätes über das Netzwerk dürfen ausschließlich sichere Protokolle wie Secure Shell Version 2 (SSHv2), HTTPS, Secure Copy (SCP) und Simple Network Management Protocol (SNMP) v3 verwendet werden. Nach einer bestimmten Zeit der Inaktivität sollten dabei Administrationssitzungen soweit möglich automatisch geschlossen werden.

M-TK-79 Sichere Administration von Netzkomponenten

Generell gelten für die sichere Administration von Netzkomponenten (Router und Switches) die Anforderungen der IT-Grundschutz-Kataloge[20]. Dabei sind im Wesentlichen die entsprechenden generellen Maßnahmen in Kapitel 10.2 und 10.3 sinngemäß auf Netzkomponenten bezogen umzusetzen. Weiterhin sind auch für Netzkomponenten geeignete Methoden für die Datensicherung und das Patch-Management einzusetzen (sinngemäße Anwendung der Maßnahmen M-TK-234 „Berücksichtigung der Server der TK-Lösung im Datensicherungskonzept der Organisation“ und M-TK-236 „Einbindung der Server der TK-Lösung in das Patch-Management der Organisation“).

M-TK-80 Überwachung der Komponenten des VoIP-Systems

Die Komponenten des VoIP-Systems, insbesondere Telefonie-Server und PSTN-Gateways, müssen kontinuierlich hinsichtlich ihrer Verfügbarkeit überwacht werden. Hierzu ist Maßnahme M-TK-238 „Überwachung der Komponenten des Telekommunikationssystems“ umzusetzen.

Bei einem erhöhten Schutzbedarf muss zusätzlich die Qualität der Übertragung der Medienströme, z. B. der Sprachübertragung, zentral überwacht werden. Dies beinhaltet insbesondere die Messung und Aufzeichnung von Delay und MOS-Wert[21]. Weiterhin sollten Statistiken bzgl. der Verteilung erfolgreicher und fehlgeschlagener (inklusive abgebrochener) Verbindungen erfasst werden.

Bei Überschreiten von für die Installation individuell festgelegten (und am Schutzbedarf orientierten) Schwellwerten muss ein Alarm ausgelöst werden.

M-TK-81 Datensicherung für die Elemente des VoIP-Systems

Die Datensicherung ist eine Kernanforderung für den sicheren Betrieb von IT-Systemen und deren Notfallvorsorge. Auf Basis von Maßnahme M 6.101 „Datensicherung bei VoIP“ des Bausteins B 4.7 „VoIP“ der BSI IT-Grundschutz-Kataloge und M-TK-234 „Berücksichtigung der Server der TK-Lösung im Datensicherungskonzept der Organisation“ werden folgende Punkte für einen erhöhten Schutzbedarf bei VoIP besonders hervorgehoben:

- Die Datensicherung muss alle Komponenten des VoIP-Systems, d. h. die Telefonie-Server und insbesondere die PSTN-Gateways, in die Datensicherung einbeziehen. PSTN-Gateways und Telefonie-Server unterliegen in Organisationen zum Teil verschiedenen Betriebsverantwortlichkeiten. Hier muss eine konsistente Datensicherung erreicht werden.
- Die einsetzbaren Datensicherungsmöglichkeiten und -werkzeuge weichen häufig von Standardlösungen zur Sicherung ab. Hier muss ein abgestimmtes Konzept zu Integration solcher Lösungen in die Datensicherung erstellt und umgesetzt werden.

Wesentlich ist, dass in jedem Fall mit Hilfe der getroffenen Vorkehrungen der aktuelle Zustand vor Eintreten eines Notfalls für alle Teilsysteme der VoIP-Lösung wiederhergestellt werden kann (siehe Maßnahme M-TK-85 „Notfallvorsorge für das VoIP-System“).

Folgende Maßnahmen sind bei der Nutzung eines IP-Anlagenanschlusses zusätzlich zu beachten:

M-TK-82 VoIP-Tauglichkeit der IP-Infrastruktur für einen IP-Anlagenanschluss

Für die Nutzung eines IP-Anlagenanschlusses ist darauf zu achten, dass die IP-Infrastruktur die Anforderungen an einen stabilen und verfügbaren Betrieb erfüllt. Dies betrifft primär die IP-Anbindung zum ITSP, wobei folgende Punkte beachtet werden müssen:

20 Siehe [BSI GSK-2013]: Baustein B 3.302 „Router und Switches“ und in diesem Baustein speziell die Maßnahme M 4.204 „Sichere Administration von Routern und Switches“.

21 MOS ist eine Abkürzung für Mean Opinion Score und spezifiziert eine Qualitätsskala von 0 bis 5 für die Beurteilung der Sprachqualität. Der MOS-Wert korreliert mit dem R-Faktor (Rating Factor), der die Sprachqualität von VoIP auf einer Skala von 0 bis 100 bewertet.

- Es muss ausreichend Bandbreite vorhanden sein. Neben der reinen Anzahl von Sprachkanälen müssen insbesondere Sprach-Codec und Overhead berücksichtigt werden.
- Die Verbindungsqualität muss für einen IP-Anlagenanschluss geeignet sein. Dies betrifft insbesondere die Parameter Paketverlust, Verzögerung und Jitter.

In diesem Zusammenhang ist auch die Maßnahme M-TK-83 „Überwachung der VoIP-Anbindung zum ITSP“ zu beachten. Neben der IP-Anbindung zum ITSP stützt sich der IP-Anlagenanschluss auf Basisdienste wie z. B. DNS oder NTP sowie auf Netzwerkinfrastrukturen im LAN. Alle betroffenen Komponenten und Dienste müssen für einen IP-Anlagenanschluss entsprechend berücksichtigt werden.

M-TK-83 Überwachung der VoIP-Anbindung zum ITSP

Die Netzelemente zur Anbindung an den ITSP (u. a. Router, Switches und SBC) müssen überwacht werden. Für die Überwachung der Router und Switches gelten die Festlegungen der IT-Grundschutz-Kataloge. Für die Überwachung des SBC ist außerdem M-TK-80 „Überwachung der Komponenten des VoIP-Systems“ anzuwenden, da über den SBC auch Medienströme geleitet werden.

Neben der Kontrolle von QoS-Parametern (z. B. der Wert des Parameters Type-of-Service (TOS) in einem IP-Paket) und QoS-Indikatoren (Verzögerung, Jitter und Paketverlust) muss die Einhaltung von Vereinbarungen hinsichtlich Bandbreite bzw. Bandbreiten-Reservierung (z. B. T.38/Fax-URIs) überwacht werden.

Bei entsprechend hohen Verfügbarkeitsanforderungen kann in Betracht gezogen werden, einen regelmäßigen, automatisierten Testanruf über die Infrastruktur des ITSP durchzuführen und Qualitätsindikatoren zu messen.

Weiterhin muss mit dem ITSP die Überwachung dessen Infrastruktur abgestimmt werden. Hier müssen zunächst Vorgaben an den ITSP hinsichtlich des gewünschten Umfangs der Überwachung sowie hinsichtlich der Meldepflichten bei Vorfällen formuliert und in das Vertragswerk mit dem ITSP eingebettet werden. Dabei ist insbesondere festzulegen, auf welche Informationen beim ITSP zugegriffen werden kann und welche Ereignistypen (Funktionsstörungen und Sicherheitsvorfälle) vom ITSP gemeldet werden müssen.

Diese Überwachung liefert eine wesentliche Grundlage, um bei Fehlern, Überschreitung von (Performance-)Schwellwerten einen (automatischen) Fallback auf eine alternative Anbindung (Internet- bzw. IP-Anlagenanschluss) einzuleiten.

M-TK-84 Sichere Administration des Session Border Controller

Die im Falle des erhöhten Schutzbedarfs zu treffenden Vorkehrungen sind von den Konfigurationsmöglichkeiten und angebotenen Schnittstellen des SBC abhängig. Da über einen SBC die gesamte externe Kommunikation eines IP-Telefonie-Systems läuft, ist zunächst der Zugriff auf den SBC stets geeignet abzusichern. Hierzu sind Maßnahme M-TK-233 „Physische Sicherheit der Server der Telekommunikationslösung“ und die für eine ISDN-basierte TK-Anlage in Kapitel 3.3 beschriebenen Maßnahmen M-TK-4 „Erhöhter Zutrittsschutz“ und M-TK-5 „Geeignete Aufstellung der TK-Anlage“ auf einen SBC sinngemäß übertragen umzusetzen.

Generell müssen nicht benötigte Schnittstellen und Protokolle deaktiviert werden (sinngemäße Anwendung von Maßnahme M-TK-229 „Härtung von Servern des Telekommunikationssystems“). Die Administration eines SBC darf nur über entsprechend gesicherte Protokolle erfolgen (siehe Maßnahmen M-TK-232 „Einschränkung und Kontrolle des Zugangs zu einem Server des Telekommunikationssystems“ und M-TK-237 „Sichere Konfiguration des Netzwerk-Management-Protokolls“) und die Berechtigungen für einen Zugang sind den Anforderungen entsprechend anzupassen (siehe Maßnahme M-TK-231 „Einschränkung und Kontrolle von Berechtigungen für die Administration eines Servers des Telekommunikationssystems“).

Nachfolgend werden Ansätze aufgeführt, wie einzelne Zugriffsmöglichkeiten zum SBC abgesichert werden können.

- Serielle Schnittstelle

  Die serielle Schnittstelle kann je nach System für die Erstinbetriebnahme und allgemein für Wartungsaufgaben und Recovery-Aktionen genutzt werden und erfordert einen physischen Zugriff auf den SBC. Für den hierzu genutzten Administrations-PC gelten die im Kapitel 3.3 zu ISDN-basierten TK-Anlagen genannten Maßnahmen M-TK-24 „Sichere Aufstellung von Administrationsendgeräten“, M-TK-25 „Sichere Konfiguration von Administrationsendgeräten“ und M-TK-26 „Regelungen für sichere TK-Administration“.

- Telnet, HTTP, FTP[22]

  Im Falle erhöhten Schutzbedarfs ist die Verwendung dieser Schnittstellen bedenklich, sofern die Kommunikationsmöglichkeiten mit Zugriff auf die entsprechenden Dienste nicht mit den Mitteln der Netztrennung ausschließlich auf Administrations-PCs beschränkt werden. Es sollte dann für diese Dienste eine verschlüsselte Variante verwendet werden oder eine Abschaltung erfolgen.

- Verschlüsselte Varianten sind in diesem Fall z. B. SSHv2 anstelle von Telnet, HTTPS anstelle von HTTP und FTPS[23] bzw. SCP/SFTP[24] anstelle von HTTP und FTP. Für die Verwendung der SSL/TLS-gesicherten Protokolle HTTPS und FTPS gelten die Hinweise aus Kapitel 13.3.3.

- SNMP

  Für den Zugriff via SNMP ist die Maßnahme M-TK-237 „Sichere Konfiguration des Netzwerk-Management-Protokolls“ umzusetzen.

Weiterhin sind für eine sichere Administration eines SBC die in M-TK-234 „Berücksichtigung der Server der TK-Lösung im Datensicherungskonzept der Organisation“ genannten Konzepte zur Datensicherung sowie Maßnahme M-TK-236 „Einbindung der Server der TK-Lösung in das Patch-Management der Organisation“ zu den Bereichen Software-Sicherheit und Patch-Management umzusetzen. Dabei muss beachtet werden, dass ein SBC typischerweise als Appliance geliefert wird. Daher muss mit herstellerspezifischen Besonderheiten und Einschränkungen hinsichtlich der folgenden Punkte gerechnet werden:

- Zugriffsmöglichkeiten auf die Systemkonfiguration
- Methode für die Datensicherung
- Installation von Patches

4.3.5 Übergreifende Aspekte

M-TK-85 Notfallvorsorge für das VoIP-System

Telefonie gehört in jeder Organisation zu den wichtigsten IT-Diensten. Ein vollständiger Ausfall ist nicht hinzunehmen. Dies wird bereits im Baustein B 4.7 „VoIP“ der BSI IT-Grundschutz-Kataloge in Maßnahme M 6.100 „Erstellung eines Notfallplans für den Ausfall von VoIP“ adressiert. Für den erhöhten Schutzbedarf werden für die Basistechnologie VoIP die folgenden Aspekte der Notfallvorsorge besonders betont:

- Mindestens das Absetzen von Notrufen muss jederzeit möglich sein.

22 FTP = File Transfer Protocol

23 FTPS = FTP over SSL

24 SCP/SFTP = Secure Copy Protocol / SSH File Transfer Protocol

- Bei schadenstiftenden Ereignissen, die im IT-Bereich zu Ausfällen mit Notfallausmaß führen können, müssen während der Notfallbehandlung Telefonate mit Externen geführt werden können, z. B. mit Support-Firmen.
- Die Erreichbarkeit für Kunden oder Partner per Telefon ist wichtig für die Akzeptanz der angebotenen Leistungen.

Die genannten Gründe bedingen einen erhöhten Schutzbedarf bzgl. Verfügbarkeit insbesondere für TK-Lösungen, die die Basistechnologie VoIP nutzen. Einer speziellen Notfallvorsorge für VoIP-Lösungen über Maßnahme M-TK-246 „Notfallvorsorge für alle Teilsysteme der TK-Lösung“ hinaus kommt daher eine besonders hohe Bedeutung zu und beinhaltet mindestens die folgenden Elemente:

- Planung und Durchführung von Maßnahmen zur Vorbereitung einer schnellen Wiederherstellung aller essenziellen bzw. möglichst aller VoIP-Systemkomponenten

  Alle Vorkehrungen zur schnellen umfassenden Systemwiederherstellung sind in regelmäßigen Abständen (z. B. einmal im Jahr) auf Funktionsfähigkeit zu prüfen; die Tests und Testergebnisse sind zu dokumentieren.
- Festlegung von Sofortmaßnahmen für typische Schadenssituationen, z. B.:
  - Zugangssperre zur Telefonie für die Mehrzahl der Endgeräte, um so die Nutzung der verbliebenen Anlagenkapazitäten auf essenzielle Arbeitsplätze zu konzentrieren.
  - Abkopplung eines stark gestörten VoIP-Systems vom produktiven Netz bei Virenbefall als erkannter Ursache
- Planung und Vorbereitung von Notbetriebsformen, z. B. Inbetriebnahme separater Anschlüsse an das PSTN, parallel zur VoIP-Systemlösung, zur Sicherstellung der Erreichbarkeit.
- Aktivierung von Mobiltelefonen als erweiterte Notbetriebsform zur Sicherstellung einer grundlegenden Betriebsfähigkeit der Organisation, z. B. eines Kontaktcenters
- Festlegen, Konfigurieren und Bereithalten von Hardware und Software als funktionsgleiche Ausweichlösung für alle essenziellen Komponenten der VoIP-Lösung
- Festlegungen zur Wiederanlaufreihenfolge der Komponenten einer VoIP-Lösung
  - Priorisierung der VoIP-Komponenten untereinander entsprechend ihrer Bedeutung für die Organisation
  - Priorisierung der VoIP-Komponenten im gesamten IT-Systemverbund
- Abschluss von speziellen Support-Verträgen inklusive Notfall-Konditionen für die essenziellen VoIP-Komponenten
  - „Express-Lieferung“ von Ersatz-Hardware für alle Kernsysteme oder
  - eigene Reserveteilhaltung für wichtige Komponenten der VoIP-Lösung mit Unterbringung möglichst getrennt von den durch sie zu ersetzenden produktiven Komponenten
  - Unterstützung durch einen externen 3rd-Level-Support
- Erstellung eines speziellen Notfallplans für VoIP-Systeme mit allen für die Notfall-behandlung zur VoIP-Lösung relevanten Festlegungen
- Durchführung von Notfallübungen regelmäßig einmal im Jahr

M-TK-86 Harmonisierung zwischen IT-Betrieb und VoIP-Anlagen-Betrieb

Es muss eine Harmonisierung zwischen IT-Betrieb und VoIP-Anlagen-Betrieb stattfinden. Optimale Voraussetzung hierfür ist eine Instanz, welche direkte Weisungsbefugnisse für beide Teilbereiche besitzt. Wenn der Betrieb der VoIP-Lösung und der IT getrennt sein sollte, muss

die Kooperation der Verantwortungsbereiche etabliert werden. Die Harmonisierung betrifft den kompletten Lebenszyklus der Installationen von der Planung bis zur Außerbetriebnahme:

- Schaffung abgestimmter Konzepte, insbesondere durch frühzeitige Einbindung der VoIP-Planer in Projekten mit Auswirkung auf Infrastruktur und Basisdienste (Berücksichtigung der Telefonie bei der Anforderungsdefinition)
- Notwendige Abstimmung bzgl. Change-Planung und Wartungsarbeiten
- Notwendige abgestimmte Zeitpunkte zur operativen Durchführung von Wartungsarbeiten und Changes (koordinierte Change-Implementierung)
- Notwendige Kommunikationsflüsse zwischen Betreibern von VoIP-Anlage und sonstiger IT im Störungsmanagement (engl. Incident Management), insbesondere abgestimmtes Verhalten bei Sicherheitsvorfällen

4.4 Zusammenfassung

Bei VoIP-basierten TK-Lösungen werden die Sprachdaten IP-basiert übertragen. Je nach Umfang der Infrastruktur sind durch das Sicherheitskonzept einer Organisation folgende Angriffsziele gezielt zu berücksichtigen:

- zentrale Server bzw. Appliances einer VoIP-Lösung, soweit diese Teil der internen Infrastruktur der Organisation sind
- interne Netzinfrastruktur zur Übertragung von VoIP-Datenpaketen
- Anschlusspunkte der internen VoIP-Infrastruktur an externe TK-Infrastrukturen (VoIP-Infrastruktur eines Providers, eigener PSTN-Anschluss der Organisation)
- interne Netzinfrastruktur, über die VoIP-Signalisierung und -Datenströme transportiert werden (LAN, WAN zur Kopplung von Standorten der Organisation)
- VoIP-Endgeräte und Gateways zur Anbindung von klassischen TK-Endgeräten an eine VoIP-Infrastruktur

Die Angriffsrisiken müssen in Abhängigkeit des Umfangs der auf VoIP-Basis realisierten Kommunikationsdienste (z. B. Telefonie, Fax, Lösung der Sprach-Mailbox) und des Schutzbedarfs der übertragenen Informationen bewertet und durch Sicherheitsmaßnahmen minimiert werden.

Aus Sicht der Zielumgebung sind dabei besonders zu beachten:

- eigene Verfügbarkeitsansprüche, ggf. auch einzuhaltende gesetzliche oder ähnliche Auflagen, bzgl. der Verfügbarkeit von Telefonielösungen für Notrufe und weitere Begleitung von Notfallsituationen
- ggf. erhöhte Wichtigkeit zur Nutzung von Telefonie oder weiterer VoIP-Dienste an bestimmten Arbeitsplätzen und damit an bestimmten Endgeräten
- Umfang der Speicherung personenbezogener Daten im Rahmen der Lösung zu internen Zwecken bzw. ggf. zur Erfüllung gesetzlicher oder ähnlicher Aufgaben und des geeignet sicheren Umfangs damit

Die Erarbeitung und Umsetzung einer VoIP-Sicherheitskonzeption umfasst neben den generell zu ergreifenden Maßnahmen (siehe Kapitel 10) die folgenden Aspekte.

Grundabsicherung der zentralen VoIP-Server-Systeme und -Appliances

Zentrale VoIP-relevante Installationen und deren Vernetzung sind mit Blick auf die notwendige Verfügbarkeit angemessen auszustatten und ausreichend redundant auszulegen.

Im Bereich zentraler Elemente der VoIP-Lösung ist für Server gezielt eine Grundhärtung vorzusehen. Gleiches gilt für beteiligte Appliances im Rahmen der produktspezifischen Möglichkeiten.

Nicht benötigte und nicht geeignet absicherbare Schnittstellen sollten gezielt vermieden bzw. deaktiviert werden. Dies gilt für Schnittstellen zur internen Kopplung ebenso wie für Übergänge zu öffentlichen TK-Netzen (PSTN) und IP-basierte Provider-Anbindungen für den IP-Anlagenanschluss.

Von einer VoIP-Lösung realisierte TK-Leistungsmerkmale, die nicht benötigt werden, sind durch gezielte Konfiguration grundsätzlich abzusichern bzw. zentral zu sperren.

Absicherung der VoIP-Kommunikation

Signalisierung und Sprachdatenübertragung sind bei VoIP möglichst konsequent auf allen Übertragungsstrecken zu verschlüsseln. Hierfür sind sichere Versionen der verwendeten Protokolle einzusetzen, z. B. Transport Layer Security (TLS) für die Signalisierung und Secure Real-Time Transport Protocol (SRTP). Alternativ kann der Schutz der Übertragung durch eine verschlüsselte VPN-Verbindung erfolgen.

Für die Netzkomponenten der für VoIP-Kommunikation verwendeten Netzbereiche ist im Rahmen der hier aufgeführten Maßnahmen verbindlich vorzusehen, dass diese dem Schutzbedarf der VoIP-Kommunikation entsprechend zu härten, zu konfigurieren und zu administrieren sind.

Soweit Server und Appliances einer VoIP-Infrastruktur miteinander kommunizieren müssen, ist diese Kommunikation angemessen gegen Manipulation oder Abhören durch einen Angreifer zu schützen. Soweit derartige Server durch eine (logische) Netztrennung einer gemeinsamen internen Sicherheitszone im Netz zugeordnet werden können, kann dies als risikoreduzierende Rahmenbedingung bei der Auslegung ergänzender Maßnahmen zur Absicherung der verwendeten Schnittstellen und Kommunikation berücksichtigt werden. Vergleichbares gilt auch für die Absicherung der Kommunikation zur eigentlichen VoIP-Nutzung, soweit VoIP-Endgeräte in eine gezielte Netztrennung einbezogen werden.

Für die Teile der zentralen VoIP-Infrastruktur, die der Außenanbindung und ihrer Absicherung dienen (z. B. Session Border Controller, SBC), kann je nach Schutzbedarf und den Möglichkeiten zur Härtung solcher Komponenten eine eigene Sicherheitszone (Demilitarized Zone, DMZ) als Zusatzmaßnahme erforderlich sein.

Sicherheitsmaßnahmen auf Ebene des Netzes

Soweit die oben beschriebene Verschlüsselung nicht nutzbar ist, muss mit dem Restrisiko gezielt umgegangen werden. Möglichkeiten sind dann ein Schutz der Datenströme zur (internen) VoIP-Nutzung über eine Netztrennung oder sogar der Verzicht auf VoIP-Nutzung bei besonders schützenswerter Kommunikation über nicht ausreichend sichere Strecken oder mit Kommunikationspartnern, deren Endgeräte die erforderliche Verschlüsselung nicht unterstützen.

Kabelbasierte Endgerätezugänge zur VoIP-Infrastruktur sind mit Mitteln der eingesetzten Netztechnik durch eine Netzzugangskontrolle (Network Access Control, NAC) gegen unbefugten Anschluss von Endgeräten jeglicher Art mindestens so zu schützen, wie in der Zielumgebung mit Anschlüssen zu Netzbereichen vergleichbaren Schutzbedarfs verfahren wird. Hierbei ist zu berücksichtigen, dass VoIP-Telefone je nach Modell einen kaskadierten Anschluss eines weiteren Endgerätes ermöglichen. Eine als Maßnahme beschlossene Netzzugangskontrolle darf hierdurch nicht umgangen werden können.

Absicherung der VoIP-Endgeräte und deren Nutzung

VoIP-Endgeräte müssen gezielt in angemessenem Umfang mit Sicherheitsfunktionalitäten ausgestattet sein, um Sicherheitsvorfälle zu erschweren bzw. zu vermeiden:

- Schnittstellen, die zu den vorgesehenen Formen einer VoIP-Nutzung nicht benötigt werden, sind zu deaktivieren, zu blockieren oder durch entsprechende Endgerätewahl wegzulassen.
- Auf Endgeräten mit Softphone-artiger VoIP-Clientlösung ist eine konsequente Härtung vorzunehmen. Der Zugriff zum Endgerät und zur darauf gespeicherten Konfiguration sowie die Nutzung von benötigten Daten, Diensten und Leistungsmerkmalen zu VoIP sind gezielt abzusichern.

  Bei erhöhtem Schutzbedarf ist das verbleibende Restrisiko einer Kompromittierung des Endgerätes mit einem „Lauschtrojaner“ gezielt zu prüfen und je nach Einschätzung ist für bestimmte Software-Ausstattungen solcher Geräte auf die VoIP-Client-Nutzung zu verzichten.

Insbesondere die Nutzung von VoIP über externe IP-basierte Infrastrukturen, vornehmlich Internet-telefonie, sollte auf gezielt gehärtete Endgeräte beschränkt werden.

- Ist für unterschiedliche VoIP-Nutzertypen ein unterschiedlicher Umfang an zu nutzenden VoIP-Leistungsmerkmalen und Diensten vorgesehen, so ist eine zentrale Konfiguration entsprechend unterschiedlicher Nutzerprofile ein geeigneter Ansatz. Der Zugang zum spezifischen Nutzerprofil wird dann an eine Authentisierung am Endgerät geknüpft. Ohne angemessene Authentisierung steht nur ein einfacher Standardumfang zur Verfügung.

  Eine Reduktion des Funktionsumfangs auf das absolut Nötige (im Sinne eines Minimalprofils) ist insbesondere bei VoIP-Endgeräten notwendig, die in schlecht zugangsgeschützten oder öffentlich zugänglichen Bereichen aufgestellt werden müssen.

  Bei Endgerätetypen, für die unterschiedliche Nutzerprofile bzw. ein ausreichend minimiertes Standardprofil nicht realisierbar ist (z. B. Fax), sollte ein festgelegter Grad an Zugangsschutz nicht unterschritten werden. In Räumlichkeiten, wo dieser nicht gewährleistet werden kann, ist auf die Aufstellung solcher Geräte zu verzichten.

  Bei dennoch an solchen Orten aufgestellten Multifunktionsgeräten müssen ohne geeigneten Zugangsschutz zu riskante Funktionalitäten vollständig unterbunden werden. Soweit dies anteilig über die zentrale VoIP-Infrastruktur zu realisieren ist, stellt dies eine Ergänzung der Grundabsicherung im Bereich zentraler VoIP-Systeme dar.
- Je nach VoIP-basierten Diensten, die von einem Endgerät aus genutzt werden können, kann eine gezielte Limitierung der zulässigen Kommunikationspartner zu diesem Endgerät eine zu erwägende Option sein.
- Für den Schutz der VoIP-Datenströme ist die Option einer Verschlüsselung von großer Bedeutung. Für den Anwender muss daher eine ausreichend intuitive und unmittelbare Anzeige des Gerätezustands im Rahmen eines Telefonats zur Verfügung stehen. Bei einem erhöhten Schutzbedarf ist die Warnung bei Nutzung unsicherer Merkmale wie z. B. unverschlüsselte Kommunikation mangels geeigneter Verschlüsselungsunterstützung beim Kommunikationspartner besonders wichtig.

Netz- und Systemmanagement

Die Administration von VoIP-Komponenten erfordert generell einen besonderen Schutz. Neben den Sicherheitsmaßnahmen, die auch für sonstige IT-Systeme gelten, ist für VoIP speziell zu beachten, dass bei der Überwachung die VoIP-Dienstgüte und insbesondere auch die Sprachqualität berücksichtigt werden.

Wartungsverträge und Notfallplanung für VoIP-relevante Systeme und Endgeräteeinbindung müssen dem Schutzbedarf entsprechend ausgelegt werden.

Übergreifende Aspekte

Basis einer ausreichend abgesicherten Kommunikation mittels VoIP ist eine Produktauswahl unter Berücksichtigung vorgesehener Sicherheitsmaßnahmen. Dies betrifft zunächst zentrale VoIP-Systeme und Netzkomponenten. Bei erhöhtem Schutzbedarf muss auf eine ausreichende Sicherheitsintelligenz der VoIP-Endgerätelösungen gezielt geachtet werden.

Wartungsverträge und Notfallplanung für VoIP-relevante Systeme und Endgeräteeinbindung müssen dem Schutzbedarf entsprechend ausgelegt werden.

Für Notfallsituationen sind Optionen bzgl. Notbetriebsformen gezielt zu prüfen. Entsprechende Ausstattung ist vorzuhalten, nach Möglichkeit betriebsbereit in die Infrastruktur zu integrieren. Die Aktivierung festgelegter Notbetriebsformen ist so vorzubereiten, dass alle besonders wichtigen Funktionalitäten der VoIP-Infrastruktur zügig durch die Notbetriebsform übernommen werden und festgelegten Endgeräten bzw. Arbeitsplätzen gezielt bereitgestellt werden können.

Abbildung 28 zeigt zusammenfassend die grundsätzliche Vorgehensweise bei der Absicherung von VoIP und macht deutlich, dass manche Maßnahmen nur dann ergriffen werden müssen, wenn andere Maßnahmen nicht ausreichend umgesetzt werden können.

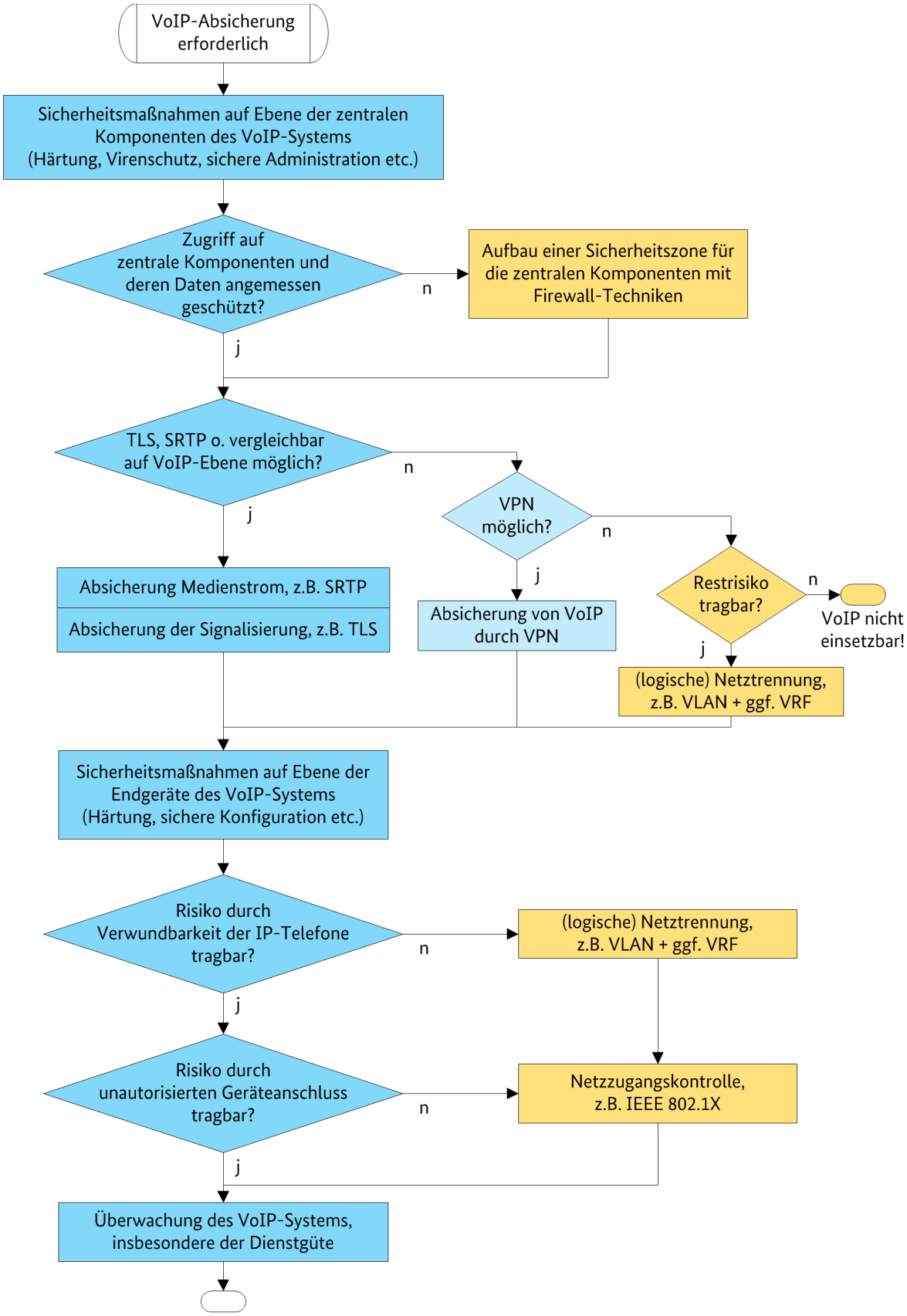


Abbildung 28: Grundsätzliche Vorgehensweise bei der Absicherung von VoIP

5 Hybrid-Anlagen

Hybrid-Anlagen stellen als Kombination von klassischer Telekommunikationstechnik und Voice over IP (VoIP) einen möglichen Migrationspfad zu VoIP dar, der jedoch auch mit spezifische Gefährdungen verbunden ist, die sich aus der Verbindung der verschiedenen Techniken ergeben. Die zu ergreifenden Sicherheitsmaßnahmen müssen diesen Aspekt besonders berücksichtigen.

5.1 Basiswissen

Der Begriff Hybrid-Anlagen bezeichnet TK-Anlagen, die durch folgende Eigenschaften ausgezeichnet sind (siehe Abbildung 29):

- Eine Hybrid-Anlage verfügt zumindest über einen PSTN- und optional über einen IP-Anlagen-Anschluss.
- Eine Hybrid-Anlage stellt sowohl Ports für den Anschluss herkömmlicher Endgeräte (analoge und digitale Endgeräte) als auch für den Anschluss von IP-Telefonen bereit.

Manche herkömmliche Telefonanlagen können auch mit VoIP-Modulen zu einer Hybrid-Anlage aufgerüstet werden.

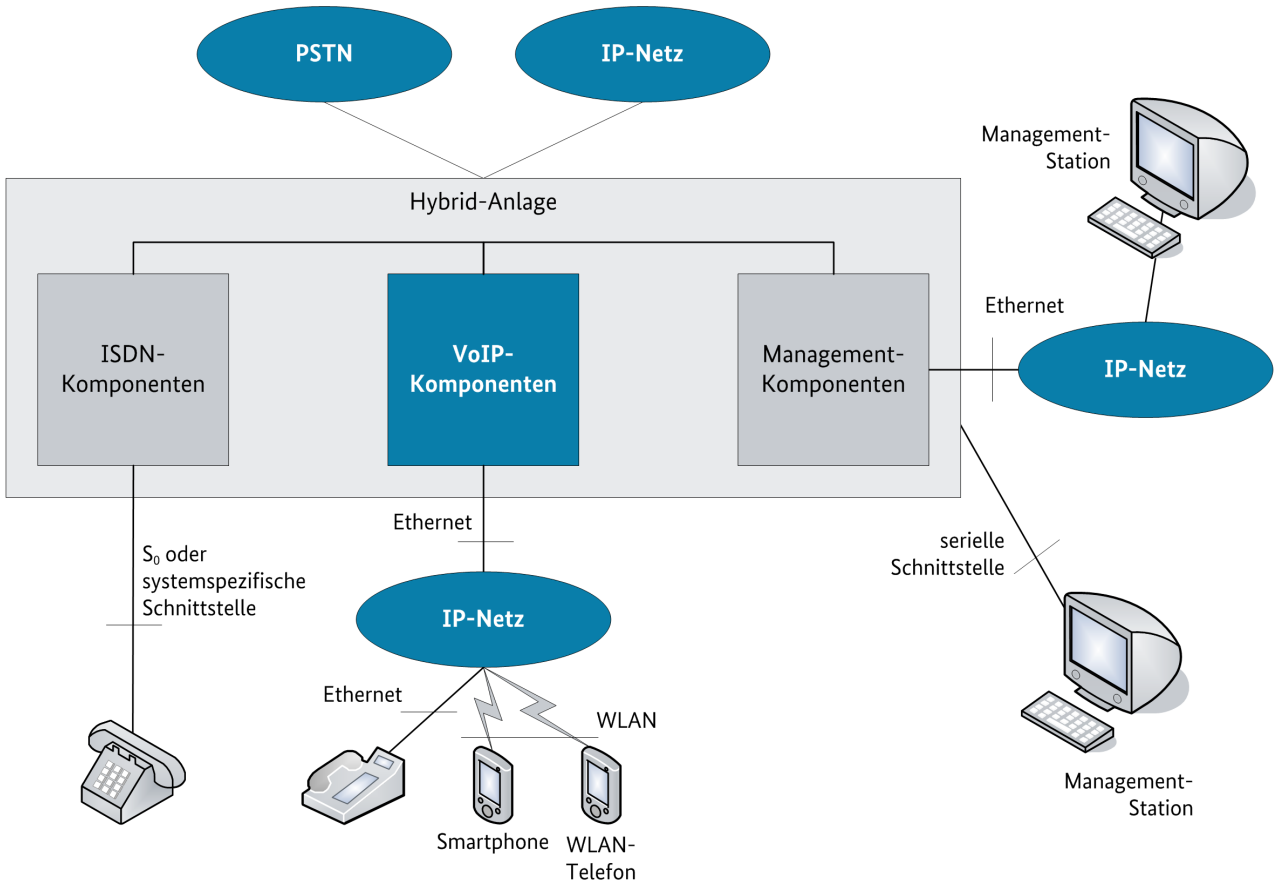


Abbildung 29: Hybrid-Anlage im Überblick

Seitens der Hersteller von Hybrid-Anlagen wird als Vorteil oft angebracht, dass Hybrid-Anlagen den schrittweisen Umstieg auf eine VoIP-Infrastruktur erlauben. Alle bestehenden Endgeräte, Applikations-Server und Leistungsmerkmale können zunächst weitergenutzt und sukzessive für die IP-Telefonie ausgetauscht bzw. umgestellt werden. Hier muss aber betont werden, dass sanfte Migrationspfade auch hin zu reinen VoIP-Systemen ohne die Verwendung von Hybrid-Anlagen möglich sind.

5.2 Gefährdungen

Die bereits festgestellten Gefährdungen für klassische TK-Anlagen basierend auf Integrated Services Digital Network (ISDN) und für VoIP-Systeme gelten auch für Hybrid-Anlagen. Es besteht weiterhin die Möglichkeit, dass eine Gefährdung, die beispielsweise auf VoIP-Komponenten einwirkt, einen Seiteneffekt auf eine ISDN-Komponente des Hybrid-Systems hat, wie in Abbildung 30 illustriert. In diesem Sinne kann sich die Gefährdungslage sogar derart kumulieren, dass in Summe die Gefährdungen durch die Integration von Systemen größer werden als für die Einzelsysteme allein. Diese Seiteneffekte sind meist implementierungsabhängig und müssen ggf. im Einzelfall betrachtet werden.

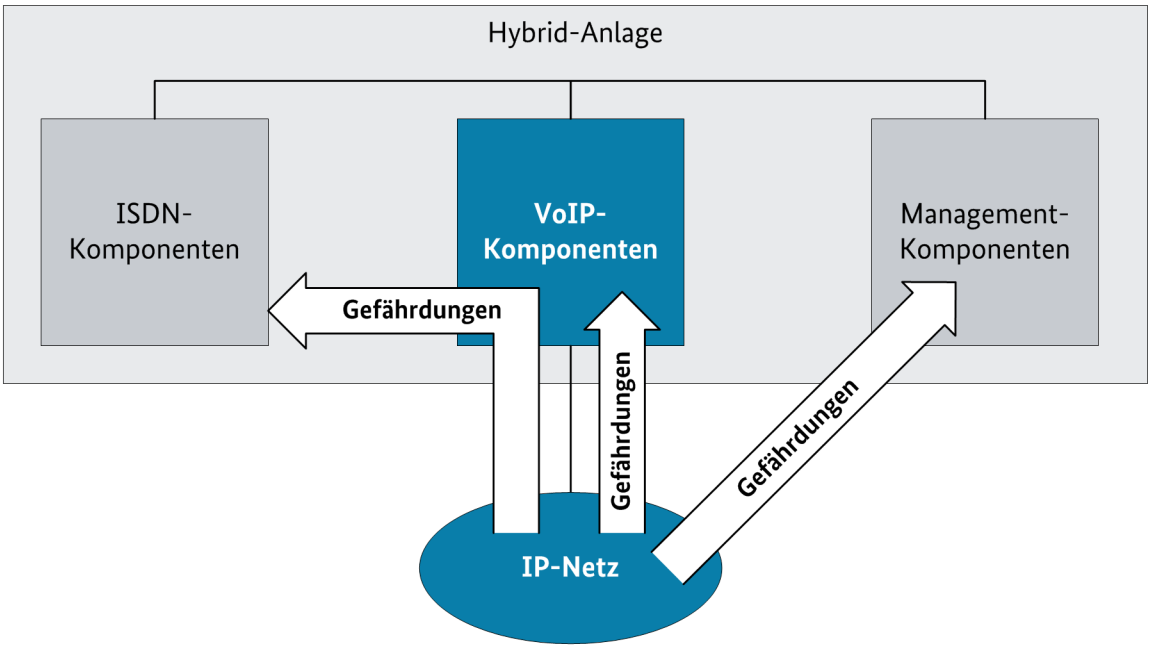


Abbildung 30: Kumulationseffekt durch zusätzliche Komponenten und Schnittstellen (vereinfacht)

5.2.1 Höhere Gewalt

Für Hybrid-Anlagen gelten die entsprechenden Gefährdungen für die Basistechnologien „Klassische Telekommunikationstechnik“ (siehe Kapitel 3.2.1) und „Voice over IP“ (siehe Kapitel 4.2.1).

5.2.2 Organisatorische Mängel

Folgende bereits für ISDN-basierte TK-Anlagen und für VoIP-Systeme betrachtete Gefährdungen sind hervorzuheben, da sie durch das Zusammenwirken beider Systeme eine besondere Ausprägung erfahren.

G-TK-39 Unzureichende oder fehlende Kompetenzen für Planung und Betrieb einer Hybrid-Anlage

Für Planung und Betrieb einer Hybrid-Anlage ist eine Kompetenz sowohl für den Bereich der klassischen ISDN-basierte TK-Anlage als auch für den Bereich VoIP erforderlich.

Kompetenzmängel in einem der beiden Bereiche können für das Gesamtsystem erhebliche Auswirkungen haben.

Es ist wichtig zu verstehen, dass in einer Hybrid-Anlage sehr heterogene Techniken integriert werden. Beide Bereiche haben beispielsweise eine eigene Terminologie, die für den Betrieb einer Hybrid-Anlage und für die Kommunikation zwischen dem beteiligten Personal beherrscht werden muss. Missverständnisse aus mangelndem (gegenseitigem) Verständnis sind eine nicht zu unterschätzende Gefahrenquelle.

G-TK-40 Unzureichende organisatorische Struktur für den Betrieb einer Hybrid-Anlage

Die Technologiebereiche ISDN und VoIP werden manchmal von unterschiedlichen Gruppen einer Linienorganisation betreut. Die Folge kann durchaus sein, dass verschiedene Gruppen eine Hybrid-Anlage gemeinsam administrieren. Dies erfordert eine gruppenübergreifende reibungslose Abstimmung. Dabei besteht grundsätzlich die Gefahr, dass diese Abstimmung nur unzureichend in der Organisation umgesetzt wird. Dies kann beispielsweise zur Folge haben, dass Informationen verloren gehen und Meldewege nicht oder nur unzureichend funktionieren.

G-TK-41 Unzureichende oder fehlende Konzepte, Regelungen und Prozesse für das Management einer Hybrid-Anlage

Konzepte, Regelungen und Prozesse für eine ISDN-basierte TK-Anlage müssen für den Einsatz einer Hybrid-Anlage entsprechend um VoIP-bezogene Elemente erweitert werden. Eine Gefährdung besteht darin, dass sich diese Erweiterung als unzureichend erweist. Kritisch sind dabei diejenigen Elemente, die einen übergreifenden Bezug zu beiden Systemen (ISDN und VoIP) haben, z. B. der Austausch eines ISDN-Telefons gegen ein IP-Telefon.

G-TK-42 Unzureichend abgestimmte Konfigurationen und Sicherheitseinstellungen für ISDN und VoIP

Für den ISDN- und VoIP-Bereich werden technologie- und produktbedingt unterschiedliche Konfigurationen und Sicherheitseinstellungen vorgenommen, die geeignet abzustimmen sind, damit ein einheitliches Sicherheitsniveau sichergestellt wird. Dies beinhaltet sowohl die Einstellungen am Endgerät und die zugehörigen Festlegungen der Nutzerrechte als auch die Parameter für den administrativen Zugang. Werden diese Einstellungen nicht geeignet abgestimmt, kann es vorkommen, dass in einem Bereich (z. B. auf der VoIP-Seite) ein zu geringes Sicherheitsniveau besteht.

5.2.3 Menschliche Fehlhandlungen

Generell gilt, dass mit der Komplexität eines Systems auch das Risiko einer menschlichen Fehlhandlung steigt. Dies gilt auch für die Integration einer ISDN-basierten TK-Anlage und eines VoIP-Systems in einer Hybrid-Anlage.

5.2.4 Technisches Versagen

Es gelten die bereits für die Basistechnologien „Klassische Telekommunikationstechnik“ (siehe Kapitel 3.2.4) und „Voice over IP“ (siehe Kapitel 4.2.4) genannten Gefährdungen. Durch die Integration dieser heterogenen Komponenten in das Gesamtsystem einer Hybrid-Anlage entsteht allerdings auch für den Bereich „Technisches Versagen“ eine besondere Bedrohungslage.

G-TK-43 Gesamtverfügbarkeit bei Störung einer Komponente

Eine Störung bzw. ein Ausfall einer VoIP-Komponente kann sich – je nach internem Aufbau der Hybrid-Anlage – in der Anlage fortpflanzen und ggf. auch ISDN-Komponenten in ihrer Funktion beeinflussen. Die Ursache kann beispielsweise in einem Hardware- oder Software-Fehler bei der Integration der VoIP-Komponenten liegen.

Grundsätzlich kann auch ein Ausfall der ISDN-Komponente die VoIP-Komponente beeinflussen, jedoch ist diese Gefährdung aufgrund der Stabilität der ISDN-basierten TK-Anlagen von geringer Relevanz.

G-TK-44 Fehlende oder unzureichende Integration der Management-Komponenten

Hybrid-Anlagen sind manchmal nicht aus einem Guss, d. h. es werden Komponenten unterschiedlicher Hersteller bzw. Produkte in ein Gesamtsystem integriert. Dabei kann es vorkommen, dass die Management-Komponenten des ISDN-Teils und des VoIP-Teils der Hybrid-Anlage nicht oder nur unzureichend zusammenpassen. Im Extremfall gibt es unterschiedliche oder nur unvollständig integrierte Benutzerschnittstellen, die ein einheitliches Management der Hybrid-Anlage erschweren oder sogar unmöglich machen. Dies erhöht generell das Risiko eines Bedienfehlers und erschwert die Abstimmung von Konfigurationen und Sicherheitseinstellungen zwischen den Teilsystemen ISDN und VoIP.

5.2.5 Vorsätzliche Handlungen

Im Bereich der vorsätzlichen Handlungen besteht die wesentliche Gefährdung darin, dass Angriffe eine technologieübergreifende Wirkung entfalten können. Die Gefährdungslage konzentriert sich dabei auf die VoIP-Komponente einer Hybrid-Anlage, da hier die größte Angriffsfläche besteht und auf eine Vielzahl bereits bekannter Angriffsmethoden zurückgegriffen werden kann.

G-TK-45 Übergreifende Wirkung eines Angriffs auf eine VoIP-Komponente

Ein Angriff aus einem IP-Netz (z. B. dem LAN) auf eine VoIP-Komponente einer Hybrid-Anlage kann sich – je nach internem Aufbau der Hybrid-Anlage – in der Anlage fortpflanzen und ggf. funktionieren in Folge sogar ISDN-Komponenten nicht mehr korrekt. Beispielsweise könnte ein Angriff vom Typ Denial of Service aus dem LAN heraus in einer zentralen Steuerungskomponente der Anlage eine Überlastsituation erzeugen, die dazu führt, dass auch ein Ruf von einem lokal angeschlossenen ISDN-Telefon abgewiesen wird. Außerdem kann dabei ein unberechtigter Zugriff auf Informationen und Sprachdaten der ISDN-Seite von der IP-Seite aus erfolgen.

5.3 Sicherheitsmaßnahmen

Hybrid-Systeme bieten die Möglichkeit, klassische Telefonie-Endgeräte (analog oder digital) direkt an die Anlage anzuschließen und zusätzlich im Bereich der Endgeräte und Leistungsmerkmale die VoIP-Technologie zu nutzen. Entsprechend addieren sich aber auch die Gefährdungen der beiden in einem solchen System vereinten Anlagentypen „ISDN-basierte TK-Anlage“ und „VoIP-System“.

Entsprechend sollten insbesondere die für ISDN-basierte TK-Anlagen spezifizierten Maßnahmen konsequent umgesetzt werden. Bei diesen Maßnahmen wurden im Falle einer ISDN-basierten TK-Anlage gewisse Abstriche zugelassen, sofern die Anlage noch nicht über neueste Möglichkeiten der Verwaltung von port- bzw. nutzerbezogenen Sicherheitsfestlegungen verfügt. Erweist sich für eine solche, bereits viele Jahre eingesetzte Anlage das erreichbare Sicherheitsniveau nicht mehr als dem Schutzbedarf angemessen, so muss dies zum Anlass genommen werden, eine Neubeschaffung zu forcieren.

Im Falle einer Hybrid-Anlage sieht dies anders aus: Einerseits ist es hier aus betriebswirtschaftlichen Erwägungen oft nicht sinnvoll, mit einer kurzfristigen Ersatzbeschaffung zu reagieren. Die Anlage befindet sich womöglich noch in der frühen Phase ihres Amortisationszeitraums. Andererseits sollte, angesichts der VoIP-Unterstützung, die Anlagen-Software so aktuell sein, dass den Forderungen der formulierten Maßnahmen mit den Mitteln der Anlage entsprochen werden kann. Ein Fehlen von Konfigurationsmöglichkeiten auf vorhandenen, älteren Telefonen kann hier als Argument nicht gelten gelassen werden. Es ist bei der Beschaffung der Hybrid-Anlage darauf zu achten, dass das notwendige Sicherheitsniveau erreicht werden kann.

Im Falle erhöhten Schutzbedarfs für die Telefonie ist insofern insbesondere von Hybrid-Lösungen abzuraten, bei denen eine ältere ISDN-basierte TK-Anlage durch VoIP-Module zur Anbindung von VoIP-Endgeräten aufgerüstet wird, ohne die notwendigen Funktionalitäten zur Umsetzung der VoIP-Maßnahmen aufzuweisen.

Spezielle Maßnahmen nur für Hybrid-Anlagen fallen aus Sicherheitsgesichtspunkten nicht an. Vielmehr gilt es, entsprechend den genutzten Funktionalitäten zur Anbindung von analogen und digitalen Endgeräten alle relevanten Maßnahmen der Basistechnologien „Klassische Telekommunikationstechnik“ (siehe Kapitel 3.3) und „Voice over IP“ (siehe Kapitel 4.3) zu berücksichtigen. Maßstab für den Umsetzungsgrad ist der zu erfüllende Schutzbedarf.

In diesem Sinne für Hybrid-Anlagen in jedem Fall zu berücksichtigende Maßnahmen der beiden zugrunde liegenden Basistechnologien werden im Folgenden gelistet. Der Maßnahmenkatalog zur Absicherung von Nutzung und Betrieb von Hybrid-Systemen ist in die folgenden Blöcke aufgeteilt:

- Zentrale Anlage, Server und Anwendungen, siehe Kapitel 5.3.1
- Endgeräte, siehe Kapitel 5.3.2
- Netzwerk, siehe Kapitel 5.3.3
- Netz- und Systemmanagement, siehe Kapitel 5.3.4
- Übergreifende Aspekte, die allgemein für Hybrid-Systeme gelten, siehe Kapitel 5.3.5

5.3.1 Zentrale Anlage, Server und Anwendungen

Gerade in den Bereichen zentrale Anlage, Server und Anwendungen schlägt sich die Möglichkeit zum gemischten Einsatz der klassischen Technik und des VoIP-Ansatzes im Umfang der zu treffenden Maßnahmen nieder. Im Falle des erhöhten Schutzbedarfs ist zu beachten, dass das erreichte Sicherheitsniveau durch diejenige Technologie bestimmt wird, für die der Schutz schwächer ausfällt: Es ist wenig sinnvoll, für den VoIP-basierten Anlagenteil eine maximale Maßnahmenkombination zu ergreifen, wenn andererseits der einer klassischen TK-Anlage vergleichbare Teil nur auf durchschnittlichem Niveau abgesichert wird. Anders herum ist eine hinsichtlich ISDN-Telefonie wohlgeschützte Anlage in nicht hinnehmbarer Weise verwundbar, sofern nicht hinsichtlich der IP-Telefonie bzw. der Management-Schnittstelle(n) durch gezielte Maßnahmenwahl ein vergleichbares Schutzniveau erreicht wird.

Entsprechend ist aus den Basistechnologien „Klassische Telekommunikationstechnik“ (siehe Kapitel 3.3.1) und „Voice over IP“ (siehe Kapitel 4.3.1) gezielt eine dem Schutzbedarf geeignete Umsetzung der hier genannten Maßnahmen erforderlich. Dabei kann es erforderlich sein, die Maßnahmen an die spezifischen Eigenschaften der eingesetzten Hybrid-Lösung anzupassen.

5.3.2 Endgeräte

Für Endgeräte in Hybrid-Anlagen gelten die Maßnahmen zu den Basistechnologien „Klassische Telekommunikationstechnik“ (siehe Kapitel 3.3.2) und „Voice over IP“ (siehe Kapitel 4.3.2), es sind allerdings ggf. Maßnahmenanpassungen für eine Hybrid-Lösung sinnvoll, da sich verschiedene Aspekte aus der Vermischung zweier Technologien im Endgerätebereich ergeben können.

Beispielsweise ist hinsichtlich der Einsatzdauer von Endgerätetypen mindestens im Falle erhöhten Schutzbedarfs gezielt zu prüfen, wie lange Endgeräte im Sinne klassischer TK-Technik noch eingesetzt werden sollen bzw. können (typische Lebensdauer). Während organisatorisch angelegte Maßnahmen (vor allem physischer Zugangsschutz zu Endgeräten) für jeden Endgerätetyp und jede Endgeräteausprägung sinnvoll sind und somit auch bei Technologiewechsel Bestand haben, gilt dies für technische Maßnahmen vielfach nicht. Entsprechend ist schon aus Wirtschaftlichkeitsüberlegungen zu prüfen, wie lange ein bestimmter Endgerätetyp, für den besondere Schutzmaßnahmen zu ergreifen wären, in der Zielumgebung noch Verwendung finden wird. Beispiele sind:

- Fallen bei erhöhtem Schutzbedarf für Vertraulichkeit der Telefonate je nach Technologie unterschiedliche technische (Beschaffungs-) Maßnahmen an, so kann es sinnvoll sein, für die Arbeitsplätze mit solchem Schutzbedarf von vorneherein auf VoIP-Telefone zu setzen: Es fallen nur Kosten für die VoIP-spezifischen Schutzmaßnahmen in den Bereichen Beschaffung und Aufbau der Betriebskompetenz an, die auf lange Sicht ohnehin notwendig würden.
- Oft ist für bestimmte Einsatzbereiche (z. B. Sekretariate) absehbar, dass auch bei längerfristigem Wechsel zu einem zentralen VoIP-Kernsystem klassische Faxgeräte ohne VoIP-Fähigkeit verwendet werden sollen. Hier erfüllt die Einführung spezieller technischer Sicherheitsmaßnahmen für solche Geräte sofort die Anforderungen eines strategischen Investitionsschutzes.

5.3.3 Netzwerk

Im Bereich des Netzwerks gelten für Hybrid-Anlagen uneingeschränkt und ohne spezifische Ergänzungen die Maßnahmen für die Basistechnologien „Klassische Telekommunikationstechnik“ (siehe Kapitel 3.3.3) und „Voice over IP“ (siehe Kapitel 4.3.3), da auf Ebene des Netzwerks systembedingt eine klare Trennung vorliegt.

5.3.4 Netz- und Systemmanagement

Hinsichtlich Netz- und Systemmanagement addieren sich im Falle einer Hybrid-Anlage die für ISDN-basierte TK-Anlagen und VoIP-Systeme zu diesem Themenkomplex detailliert beschriebenen Maßnahmen. Auch bei Maßnahmen, die inhaltlich zunächst überschneidend sind, ist je nach Ausprägung der Hybrid-Anlage zumindest zu prüfen, inwieweit technologiespezifische Details zu beachten sind.

Hier ist beispielsweise M-TK-30 „Abschluss eines Support-Vertrags inklusive externer Beratungskompetenz“ zu nennen. Dabei ist im Falle einer Hybrid-Anlage durch entsprechende Vertragsgestaltung/Auswahl des Vertragspartners dafür Sorge zu tragen, dass das Support-Unternehmen ausreichende Kompetenz nicht nur für die klassische Telefonie, sondern auch für VoIP besitzt. Anbieter von Hybrid-Anlagen entstammen historisch oft dem Markt der klassischen Telefonie. Nötigenfalls muss der Vertragspartner durch einen geeigneten Subunternehmer nachweislich sicherstellen, dass eine angemessene VoIP-Kompetenz gegeben ist.

5.3.5 Übergreifende Aspekte

Im Bereich der übergreifenden Aspekte gelten für Hybrid-Anlagen die Maßnahmen für die Basistechnologie „Voice over IP“ (siehe Kapitel 4.3.5) uneingeschränkt und ohne spezifische Ergänzungen.

5.4 Zusammenfassung

Hybrid-Anlagen bieten die Möglichkeit zur Kombination von klassischen TK-Endgeräten und VoIP-Endgeräten in einer Anlage. Für eine Hybrid-Anlage gelten mindestens die Gefährdungen für ISDN-basierte TK-Anlagen und VoIP-Systeme.

Weiterhin können sich die Gefährdungen für die Einzelsysteme so kumulieren, dass die Gefährdungslage für das Gesamtsystem deutlich höher ist, als diese jeweils für die Einzelsysteme ist.

Die Sicherheitskonzeption muss daher, neben den Maßnahmen für die klassische Telekommunikation (siehe Kapitel 3.3) und VoIP (siehe Kapitel 4.3), Maßnahmen gegen Gefährdungen, welche durch die Kombination dieser Techniken und die daraus resultierende heterogene Anlage entstehen, besonders berücksichtigen.

Die Erarbeitung und Umsetzung der Sicherheitskonzeption umfasst die folgenden Aspekte:

Absicherung der zentralen Anlage

Die Anlage ist gezielt zu härten und gegen unbefugte Nutzung zu sichern. Hierzu sind die Maßnahmen der Basistechnologien „Klassische Telekommunikationstechnik“ (siehe Kapitel 3) und „Voice over IP“ (siehe Kapitel 4) zu beachten. Im Falle des erhöhten Schutzbedarfs wird das erreichte Sicherheitsniveau der Hybrid-Anlage von der Technologie bestimmt, für welche der Schutz schwächer ausfällt. Es müssen daher die Maßnahmen für die Komponenten so ergriffen werden, dass für beide Technologien ein vergleichbarer Schutz erreicht wird.

Absicherung der an der Anlage zusammenlaufenden Netzinfrastrukturen

Die Absicherung erfolgt separat für die beiden Anschlusstypen „klassische TK-Basistechnologie“ bzw. „VoIP-Infrastrukturanschluss“, da systembedingt eine klare Trennung vorliegt. Bei Überschneidungen der Maßnahmen ist zu prüfen, ob bei der Umsetzung technologiespezifische Details zu beachten sind.

Absicherung der Kommunikation zur Administration und zum Management der Anlage

Je nach Nutzungsform sind die Ausführungen für die administrative Kommunikation zu klassischen TK-Anlagen bzw. VoIP-Anlagen entsprechend dem für die Hybrid-Anlage festgestellten Schutzbedarf zu berücksichtigen. Dabei ist die Absicherung der Zugänge für Administration und Management besonders kritisch, da über diese Zugänge prinzipiell sowohl der leitungsvermittelete Teil der TK-Anlage, als auch der VoIP-Part kompromittiert werden können.

Sicherheitsmaßnahmen im Bereich Endgeräte und Endgerätenutzung

Sicherheitsmaßnahmen ergeben sich aus der je Endgerät genutzten Basistechnik (klassische, leitungsvermittelnde TK-Technik bzw. VoIP) und dem Schutzbedarf.

Bei der Neubeschaffung von TK-Endgeräten nach Einführung einer Hybrid-Anlage ist auf geeignete Konfigurationsmöglichkeiten der Endgeräte zu achten. Die Konfiguration der Hybrid-Anlage muss gemäß den formulierten Maßnahmen konfiguriert werden und bei Übernahme von klassischen TK-Endgeräten der zuvor genutzten Anlage müssen die Endgeräte die geforderten Konfigurationen zulassen. Anderenfalls ist die Möglichkeit zur Ablösung durch VoIP-Endgeräte zu prüfen.

Übergreifende Maßnahmen

Beim Übergang von klassischer TK-Technologie auf vermehrte VoIP-Nutzung darf auch vorübergehend kein Qualitätsabfall bei Betriebsqualität, Anwender-Support oder kompetentem Umgang mit Sicherheitsrisiken eintreten. Wurden diese Bereiche bisher von unterschiedlichen Personen oder Gruppen betrieben, ist daher auf eine genaue Abstimmung zu achten.

6 Unified Communications and Collaboration

In Organisationen werden im Umfeld von TK-Anlagen eine Vielzahl von Applikationen und Diensten eingesetzt. Der Begriff Unified Communications (UC) bezeichnet die Zusammenführung dieser Kommunikationskanäle und Applikationen auf einer einheitlichen Infrastruktur mit einer einheitlichen Nutzeroberfläche. Diese Integration wurde mit der Konvergenz der Sprach- und Datennetze auf IP-Basis möglich. UC vereint somit viele teils historisch gewachsene Lösungsanteile in einer hochintegrierten Systemlandschaft eines oder mehrerer Hersteller. Aufgrund der Konvergenz der zentralen Plattformen kann vielfach nicht mehr zwischen einer auf Voice over IP (VoIP) basierenden Telefonanlage und einer UC-Lösung unterschieden werden, da Sprach- und Multimediadienste von demselben System erbracht werden.

UC adressiert vorwiegend die Bereiche der Echtzeitkommunikation und des Messaging. Um die interne und externe Zusammenarbeit zu optimieren, werden diese Kommunikationskanäle verstärkt in Intranet-Plattformen, Kollaborationsportale, Dokumentenmanagementsysteme und Social Business Software integriert. Diese Integration von Kommunikations- und Kollaborationswerkzeugen wird unter dem Begriff Unified Communications and Collaboration (UCC) zusammengefasst. Im Fokus dieser Richtlinie stehen nicht die Plattformen für Zusammenarbeit als solche, sondern die Integration von Kommunikations-kanälen in diese Systeme und die dafür notwendigen Schnittstellen. Im Folgenden wird nicht zwischen UC- und UCC-Lösungen unterschieden, da eine scharfe Abgrenzung der beiden Begrifflichkeiten, z. B. über den Grad der Integration des konkreten Systems, im Sinne der Technischen Leitlinie nicht zielführend ist. Daher wird in diesem Dokument einheitlich der Begriff UCC verwendet.

UCC bietet vielfältige Möglichkeiten zur Kommunikation – aber auch zum potenziellen Missbrauch.

Durch die tiefe Integration von UCC-Diensten in andere IT-Anwendungen ergibt sich ein großes Potenzial, um die Kommunikation des Anwenders zu vereinfachen und ihn von unnötigen Arbeitsschritten zu entlasten. Zudem erlauben Dienste wie Präsenz die Steuerung der Erreichbarkeit durch den Anwender. Somit ergibt sich eine Chance, den Anwender von der täglich wachsenden Kommunikationsflut zu entlasten und ihm ein effektives Werkzeug für die Steuerung und Organisation seiner Arbeit an die Hand zu geben. Aus der engen Verzahnung mit Anwendungen und der automatisierten Informationsbereitstellung (z. B. automatisierte Präsenzzustände) ergeben sich jedoch auch Gefährdungen für die Privatsphäre des Einzelnen. Auch der verbreitete Einsatz von Videotechniken wie Desktop-Video wirft Datenschutzbedenken auf. Es muss daher bereits im Planungsstadium ein besonderes Augenmerk auf Datenschutz-Aspekte gelegt werden.

6.1 Basiswissen

UCC bezeichnet als Oberbegriff eine konvergente Plattform mit einer Vielzahl von Diensten. Der Funktionsumfang einer konkreten Lösung bestimmt sich dabei aus dem Dienstportfolio des oder der Hersteller und dem Bedarf der jeweiligen Organisation. UCC umfasst im Wesentlichen die folgenden Dienste und Aspekte:

- Telefonie
- Präsenzdienste
- Instant Messaging
- Unified Messaging
- Audiokonferenzen
- Desktop-Video und Integration von Videokonferenzräumen
- Webkonferenzen, Desktop- und Application-Sharing

- Mobilintegration
- Computer Telephony Integration und Anwendungsintegration
- Integration von Kommunikationskanälen in Web-basierte Applikationen
- Integration von Verzeichnisdiensten und Datenbanken
- Integration Sozialer Netzwerke

Abbildung 31 illustriert die Systemlandschaft einer typischen UCC-Lösung sowie die gängigen Integrationspunkte und Schnittstellen. Im Mittelpunkt steht die Systemlandschaft am Zentralstandort der Organisation (z. B. Rechenzentrum). Ein zentraler UCC-Server realisiert Registrierung und Routing der Signalisierung des Session Initiation Protocol (SIP). Eine IP-PBX[25], welche separat zum UCC-Server realisiert sein kann, übernimmt das Routing der Telefonie-Signalisierung und stellt Telefonteilnehmern Telefonie-Leistungsmerkmale bereit. Um diese beiden zentralen Serverrollen gruppieren sich die UCC-Dienste Chat-Server (für Gruppen-Chat), Webkonferenz-Server, Präsenz-Server und eine Video-Bridge zur Bereitstellung von Desktop-Videokonferenzen. Die Video-Bridge kann optional über eine Kopplung zu einer Video Multipoint Control Unit (MCU) verfügen, die als Gateway für die Durchführung von Videokonferenzen mit internen und externen Videokonferenzsystemen dient. Ein Server zur Computer Telephony Integration (CTI) realisiert CTI-Dienste, Schnittstellen zur Anwendungs-Integration und steuert die Routing-Instanzen (IP-PBX und UCC-Server). Er verfügt optional über Schnittstellen zu Datenbank-Servern oder Applikations-Servern. Eine Audio-Bridge stellt Ressourcen für die Durchführung von Audiokonferenzen bereit. Ein Unified-Messaging-Server, der einen Groupware-Server als Back-End verwendet, ist via SIP-Trunk an die UCC-Lösung angebunden. Der Präsenz-Server bezieht Präsenzinformationen einzelner Anwender wahlweise vom Groupware-Client oder vom Groupware-Server. Zusätzlich werden weitere Informationen aus dem zentralen UCC-Routing (z. B. Belegtstatus) bezogen. Ein Directory-Server dient zur Bereitstellung von Nutzerkonten und Kontaktdaten.

Zur Anbindung externer und mobiler Teilnehmer sowie zur Bereitstellung eines WebRTC[26]-Gateways zur Einbindung in Webangebote wird ein Front-End-Server in der Web-DMZ betrieben, der an das zentrale UCC-System gekoppelt ist. In der Web-DMZ ist zudem ein Web-Server zur Bereitstellung von WebRTC-Angeboten bereitgestellt. Aus Komplexitätsgründen wurden hier keine weiteren Netzzonen bzw. Sicherheitszonen (außer der Web-DMZ) abgebildet. Für die Einbindung von Filialstandorten und zur Anbindung an das öffentliche Festnetz werden Voice Gateways bereitgestellt. Zur Zonierung zwischen Außenstellen und zentralem Standort bzw. den Übergängen in das öffentliche Festnetz können hier Security Appliances (z. B. Firewalls, Intrusion Prevention Systems, Intrusion Detection Systems oder Session Border Controller) zum Einsatz kommen.

Auf Seiten der Außenstelle sind als exemplarische Teilnehmer ein UCC-Client, ein Telefonendgerät und ein Videoraumsystem abgebildet, welche sich via WAN an der zentralen UCC-Lösung registrieren. Das lokale Voice Gateway kann zur Abbildung von überlebensfähiger Telefonie an das Public Switched Telephone Network (PSTN) angebunden sein (optional). Auf der Teilnehmerseite des Zentralstandorts sind exemplarisch ein UCC-Client, ein Telefon und ein Videokonferenzraumsystem mit ihren jeweiligen Verbindungen zu UCC-Diensten abgebildet.

Des Weiteren spielen für den Betrieb einer UCC-Lösung die folgenden Aspekte eine wichtige Rolle:

- Standortübergreifende Kommunikation
- UCC über Vertrauensgrenzen hinweg
- Virtualisierung von UCC-Servern und -Clients
- WebRTC

Im Folgenden werden die in Abbildung 31 dargestellten und in der Praxis häufig vorzufindenden Unified-Communications-Dienste sowie die von ihnen verwendeten Protokolle und Schnittstellen beschrieben.

25 IP-PBX = Internet Protocol - Private Branch eXchange

26 WebRTC = Web Real-Time Communication

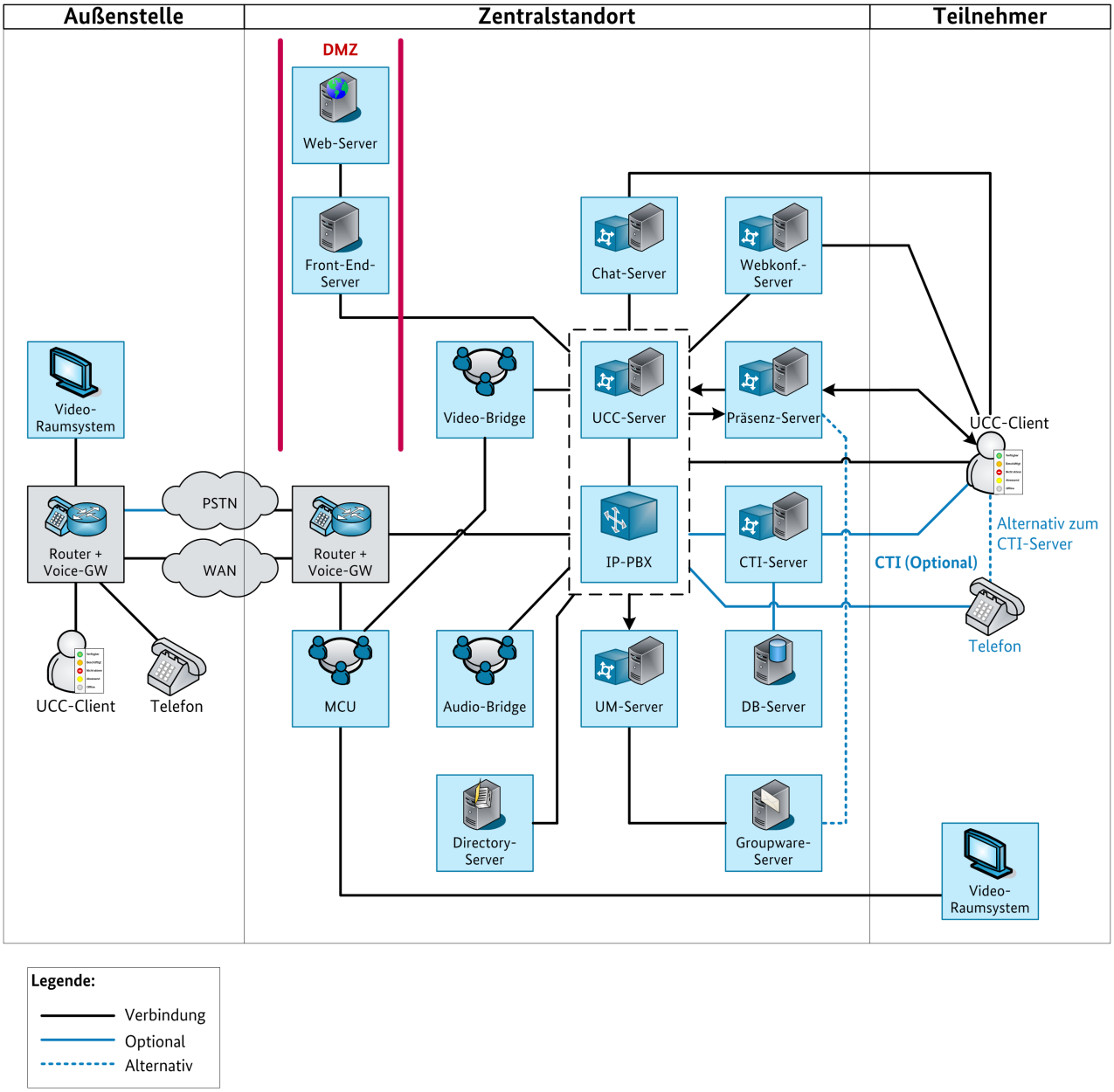


Abbildung 31: UCC – Systeme und Integrationspunkte

6.1.1 Telefonie

Der Telefonie-Dienst wird von einer VoIP-basierten TK-Anlage gemäß Kapitel 4 erbracht. Die zugehörigen Eigenschaften, Gefährdungen und Maßnahmen werden hier nicht separat beschrieben.

6.1.2 Präsenzdienste

Bei Präsenzinformationen handelt es sich um Informationen zur Gesprächsbereitschaft und zu den verfügbaren Kommunikationskanälen sowie zu deren grafischer Darstellung. Präsenzinformationen signalisieren die Möglichkeit und Bereitschaft der Nutzer eines Präsenzsystems zur Kommunikation. Das Präsenzsystem kann hierzu viele verschiedene Informationen aggregieren und (teil-)automatisiert in den

Präsenzstatus der Anwender einfließen lassen. Zum Beispiel kann der Präsenzstatus während eines Gesprächs automatisch gesetzt werden, wenn ein Teilnehmer mit der UCC-Lösung telefoniert oder an einer Webkonferenz teilnimmt. Auch Ortsinformationen und Statusmeldungen des Anwenders können je nach Implementierung in den Präsenzstatus einfließen.

Nutzen von Präsenzinformationen

Präsenzinformationen wurden ursprünglich im Kontext von Instant Messaging, d. h. Systemen zum Austausch von kurzen Textnachrichten in Quasi-Echtzeit, eingesetzt, haben mittlerweile aber auch für organisationsinterne UCC-Lösungen an Bedeutung gewonnen. Der Nutzen eines Präsenzdienstes liegt in zwei wesentlichen Funktionen:

- Durch die Sichtbarkeit der Bereitschaft und Fähigkeit eines Anwenders zur Kommunikation kann ein potenzieller Kommunikationspartner entscheiden, ob eine Kontaktaufnahme zum gegenwärtigen Zeitpunkt sinnvoll ist und anhand welchen Mediums dies idealerweise erfolgen sollte.
- Die Informationen des Präsenzdienstes können für automatisierte Routing-Entscheidungen des UCC-Systems herangezogen werden. So werden beispielsweise Anrufe nicht zu einem Teilnehmer durchgestellt, der sich im Status „Bitte nicht stören“ befindet. Stattdessen kann eine Vertreterregelung greifen und der Anruf direkt zum Stellvertreter umgeleitet werden. Für diese zweite Funktionalität ist eine Sichtbarkeit der Präsenzinformation für andere Anwender nicht zwingend notwendig.

Bereitstellung von Präsenzinformationen

Die Präsenzinformation wird bei den meisten Systemen zentral durch einen Präsenzdienst bereitgestellt und verwaltet. Der Client eines Nutzers sendet die manuell oder automatisch ermittelte Verfügbarkeit des Nutzers an den Präsenzdienst, wo sie anderen Nutzern bzw. Clients zur Verfügung gestellt wird. Informationen zum Nutzerstatus können jedoch auch aus anderen Quellen stammen. In der Praxis werten Präsenzdienste üblicherweise den Kalender eines Nutzers, die IP-Adresse des Clients, die Aktivität des Anwenders am Endgerät sowie die Nutzung der verschiedenen Kommunikationskanäle der UCC-Lösung aus.

Erhebung von Präsenzinformationen

Die Erhebung der Informationen findet je nach Szenario und Lösung Client-seitig oder Server-seitig statt. So kann die Kalenderinformation beispielsweise Client-seitig aus dem lokalen Groupware-Client oder Server-seitig mittels eines Groupware-Connectors ausgelesen werden. Die Umsetzung entsprechender Abfragen ist produktabhängig; mögliche Varianten reichen von einfachen Datenbankabfragen über proprietäre Protokolle bis hin zu standardisierten Mechanismen. Im Fall der Einbindung des Gesprächsstatus einer Telefonanlage können neben herstellerspezifischen Ansätzen u. a. die Protokolle Computer Supported Telecommunications Application (CSTA, siehe Kapitel 13.2.2.1) oder auch Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIP/SIMPLE) bzw. eXtensible Messaging and Presence Protocol (XMPP) eingesetzt werden. Eine detaillierte Beschreibung der beiden Protokolle ist Kapitel 13.2.1 zu entnehmen.

Protokolle

SIP/SIMPLE und XMPP dienen der Kommunikation zwischen Präsenzdienst und Clients. Die ersten Präsenzdienste und Instant-Messaging-Dienste waren auf Privatkonsumenten ausgerichtet und verwendeten proprietäre Protokolle. Mittlerweile setzten sich insbesondere im Unternehmensbereich jedoch zunehmend Systeme auf Basis der beiden zuvor genannten Standards durch. SIP/SIMPLE ist eine Erweiterung des weit verbreiteten VoIP-Signalisierungsprotokolls SIP und bietet unter anderem folgende Funktionen:

- Registrierung für Präsenzinformationen und Benachrichtigung, wenn sich der Status eines Nutzers ändert
- Senden und Empfangen von kurzen Textnachrichten
- Management von Sitzungen, in denen Nachrichten in Echtzeit ausgetauscht werden (sogenannte Chats)

XMPP bietet im Kern dieselbe Funktionalität, ist jedoch nicht an SIP gebunden. Beide Protokolle bieten einen Ereignismechanismus, der für die Signalisierung von Statuswechseln des Anwenders (z. B. Telefoniestatus und Kalenderstatus) an den Präsenzdienst geeignet ist. Diese Protokolle werden nicht nur für den Austausch von Präsenzinformationen zwischen Präsenzdienst und Client, sondern auch für den Abgleich von Zustandsinformationen zwischen Präsenzdienst und externen Quellen (z. B. der Telefonanlage) eingesetzt.

Absicherung von Präsenzdiensten

Werden diese Schnittstellen nicht abgesichert, können die über den Präsenzdienst erhobenen und aggregierten Information abgehört und manipuliert werden.

Sowohl SIP/SIMPLE als auch XMPP bieten jedoch die Möglichkeit eine Authentisierung per Transport Layer Security (TLS) durchzuführen und den Nachrichtentransport zu verschlüsseln. Es stellt sich außerdem die Frage, ob jeder authentisierte Benutzer Zugriff auf alle organisationsintern verfügbaren Präsenzinformationen haben darf. Um die Sichtbarkeit von Präsenzinformationen individuell für Teilnehmer oder gruppenweise einzuschränken, erlauben einige Präsenzdienste die Einschränkung auf Basis von detaillierten Regelwerken. Um dies zuverlässig umzusetzen, ist eine Authentisierung der Dienstnutzung, beispielsweise per TLS, eine zwingende Voraussetzung. Die Einschränkung der Sichtbarkeit von Präsenzinformationen muss insbesondere im Zusammenhang mit der Möglichkeit zur Leistungsüberwachung von Mitarbeitern diskutiert werden.

Organisationsübergreifende Präsenzdienste

Neben der organisationsinternen Nutzung von Präsenzdiensten spielt die organisationsübergreifende Kommunikation von Präsenzinformationen eine immer größere Rolle. Somit sollen Mitarbeiter externer Partnerorganisationen oder auch Kunden in die Lage versetzt werden, an der verbesserten Erreichbarkeit durch Präsenzdienste zu partizipieren. Hierzu kann eine Kopplung zweier Präsenzdienste, beispielsweise zweier organisationsinterner UCC-Lösungen oder einer UCC-Lösung und eines öffentlichen Sozialen Netzwerks, vorgenommen werden. Eine solche Kopplung wird im Allgemeinen als Föderation (engl. Federation) bezeichnet. Eine kontrollierte Kopplung findet in der Regel auf Basis eines Gateways und unter Verwendung eines Standardprotokolls wie XMPP oder SIP/SIMPLE statt. Auch hierbei spielt die Authentisierung, Verschlüsselung und Filterung von Informationen auf Basis von Berechtigungskonzepten eine wichtige Rolle.

6.1.3 Instant Messaging und Gruppen-Chat

Instant Messaging (IM) bezeichnet den spontanen, einfachen Versand von Kurznachrichten zwischen zwei oder mehr Kommunikationspartnern. Die Nachrichtenübermittlung findet dabei in Quasi-Echtzeit statt, weshalb die Konversationsform IM nicht mehr eindeutig der asynchronen Kommunikation zuzuordnen ist. Sie weist vielmehr Ähnlichkeiten zur Echtzeitkommunikation wie z. B. Telefonie oder Desktop-Video auf. Neben der Punkt-zu-Punkt-Kommunikation zwischen zwei Gesprächspartnern bilden Instant Messaging Produkte heute oft auch die Kommunikation zwischen mehreren Gesprächspartnern ab. Diese Funktion wird als Gruppen-Chat bezeichnet.

Der Vorteil von Instant Messaging und Gruppen-Chat liegt in seiner unkomplizierten Form und der Möglichkeit zur Ad-hoc-Nutzung. Im Gegensatz zur Kommunikation per E-Mail, welche die formalen Züge einer Briefkommunikation fortführt, wird Instant Messaging als schnelles, einfaches und dialog-orientiertes Kommunikationsmedium eingesetzt. Die Anwendungsfälle reichen von der einfachen Anbahnung einer nachfolgenden Echtzeitkommunikation bis hin zur fortlaufenden Diskussion von Themen im Stile eines Diskussionsboards. Insbesondere in zeitkritischen Anwendungsszenarien, wo es dennoch auf die Präzision der übermittelten Informationen ankommt, wird Instant Messaging häufig eingesetzt. Ein Beispiel ist der Informationsaustausch zwischen Börsen-Händlern. So kann z. B. ein Uniform Resource Locator (URL) einfacher, schneller und zuverlässiger via Instant Messaging übermittelt werden als per Sprachkommunikation.

Anwendungsbereiche von Instant Messaging

Instant Messaging gewinnt auch in der organisationsübergreifenden Kommunikation an Bedeutung. Über Föderationen mit externen oder öffentlichen Plattformen wird die Kommunikation mit Partnerorganisationen und Kunden ermöglicht. Die Anwendungsfelder reichen von der Nutzung als Kundenkanal bis hin zum Wissensmanagement zwischen Abteilungen verschiedener Organisationen.

Die Anwendungsfälle von IM sind mit denen von Telefongesprächen vergleichbar. Es muss also davon ausgegangen werden, dass über ein Instant-Messaging-System – neben vielen nicht klassifizierten Informationen – auch schützenswerte und klassifizierte Informationen ausgetauscht werden. Somit muss diese Kommunikation vor nicht-autorisiertem Zugriff geschützt werden.

Absicherung von Instant Messaging

Wie auch Präsenzinformationen hat Instant Messaging seinen Ursprung in öffentlichen Plattformen für die private Kommunikation. Die Übermittlung von kurzen Sprachnachrichten erfolgt ebenfalls vorwiegend über die Protokolle SIP/SIMPLE und XMPP (siehe Kapitel 13.2.1). Eine Teilnehmer-Authentisierung und Inhaltsverschlüsselung ist somit beispielsweise über TLS möglich.

Die Verbreitung von Hyperlinks via Instant Messaging stellt ebenfalls eine Gefährdung für die Informationssicherheit dar, da sich URLs von bösartigen Web-Angeboten über den Kanal Instant Messaging massenhaft verbreiten können. Dies gilt insbesondere bei Föderation des IM-Dienstes mit externen oder sogar öffentlichen IM-Plattformen. Einige IM-Lösungen bieten daher die Möglichkeit, die Übermittlung von Hyperlinks vollständig zu deaktivieren oder zumindest das Öffnen des Hyperlinks per Click im IM-Client zu unterbinden.

Archivierungspflichten

Beim Einsatz von Instant Messaging ist zu beachten, dass für dieses Medium gegebenenfalls dieselben Aufbewahrungs- und Archivierungspflichten einzuhalten sind wie für die E-Mail-Kommunikation oder sogar die Sprachkommunikation (z. B. im Finanz- und Versicherungsumfeld). Dies ist häufig aus juristischen oder regulatorischen Gründen notwendig. So muss z. B. im Umfeld von Handelsarbeitsplätzen eine Protokollierung von handelsbezogener Kommunikation stattfinden. Dies gilt für die Schriftkommunikation ebenso wie für die Sprachkommunikation.

Die Aufzeichnung und Archivierung von IM-Inhalten kann somit ein wichtiger Bestandteil eines IM-Systems sein und findet sich aus diesem Grund in zahlreichen Produkten wieder. Jedoch kann die Funktion durchaus auch missbräuchlich eingesetzt werden, weshalb eine Deaktivierung bei Nichtverwenden oder aber eine Aufklärung aller Anwender über die Möglichkeit der Aufzeichnung erfolgen muss.

6.1.4 Unified Messaging

Unified Messaging (UM) integriert verschiedene Nachrichtenformate in einem einheitlichen System. Die Anwender entnehmen ihre Nachrichten (z. B. E-Mail, Fax, SMS und Sprachnachrichten) einer einzigen Datenbank bzw. können über eine einzige Nutzerschnittstelle Nachrichten unterschiedlichen Formats versenden. Viele UM-Systeme bieten zudem die Möglichkeit, auf diesen konsolidierten Nachrichteneingang über verschiedene Kanäle zugreifen zu können, z. B. über einen E-Mail-Client, eine Web-Oberfläche oder per Telefon.

Durch die Integration verschiedener Medientypen in einem einheitlichem Nachrichteneingang und dem Versand derselbigen über eine einheitliche Nutzerschnittstelle ergibt sich Optimierungspotenzial für den Zugriff und die Verarbeitung dieser Nachrichtenformate. So lassen sich beispielsweise physische Fax-Geräte und somit die hierfür meist notwendigen analogen a/b-Schnittstellen einsparen, indem diese durch die UM-Integration in das persönliche E-Mail-Postfach obsolet werden. Zudem wird ein zeitnaher, nahezu geräteunabhängiger Zugriff, z. B. vom mobilen Endgerät aus auf alle entgangenen Nachrichten ermöglicht. Das Ablegen von Nachrichten in elektronischen Posteingängen bietet zudem einen Schutz vor dem absichtlichen oder unabsichtlichen Zugriff auf Fax-Nachrichten, wie er an einem nicht zusätzlich

gesicherten physischen Fax-Gerät jederzeit stattfinden kann. Dies setzt allerdings einen entsprechenden Zugriffsschutz (Authentisierung und Autorisierung) für den elektronischen Nachrichteneingang voraus.

Es muss betont werden, dass keine allgemein akzeptierte Definition des Funktionsumfangs von Unified Messaging existiert. So vertreiben einige Hersteller reine Sprachnachrichtensysteme unter dem Begriff Unified Messaging, während Produkte anderer Hersteller nur den Empfang von Faxnachrichten im E-Mail-Postfach der Benutzer unterstützen. Im Folgenden wird der Begriff Unified Messaging entsprechend der einleitenden Beschreibung sehr weit gefasst, um alle sicherheitsrelevanten Aspekte von UCC zu erfassen.

Schnittstellen von UM-Systemen

UM-Produkte mit einem umfassenden Funktionsspektrum benötigen naturgemäß eine Vielzahl von Schnittstellen für Benutzer sowie unterschiedliche Dienste und Anwendungen. Im Mittelpunkt stehen dabei die Schnittstellen zu TK- und E-Mail-Systemen. Hinzu kommen noch Schnittstellen zur Kopplung mit anderen Kommunikationssystemen, Administrationsschnittstellen, Benutzerschnittstellen, Anbindungen an Verzeichnisdienste sowie Schnittstellen zu Geschäftsapplikationen.

Für die Integration von UM-System und klassischem oder VoIP-basiertem Telekommunikationssystem werden (zumindest aus logischer Sicht) zwei Schnittstellen benötigt. Über eine Medienschnittstelle werden von der TK-Anlage kommende Anrufe an das Speichersystem übergeben. Umgekehrt werden bei telefonischen Abfragen die Nachrichten über die Sprachschnittstelle ausgegeben. Die zweite Schnittstelle wird für Signalisierungsdaten benötigt. Über die Signalisierungsschnittstelle wird dem Client oder Endgerät beispielsweise signalisiert, dass neue Nachrichten vorliegen.

Kopplung mit klassischen TK-Anlagen und VoIP-Systemen

Die Kopplung mit klassischen TK-Anlagen (siehe Kapitel 3) erfolgt in der Regel über eine in den UM-Server eingebaute Schnittstellen-Karte. Über diese Karte werden die Sprachdaten verarbeitet und bei einigen Produkten durch speziell kodierte Tonfolgen auch die Signalisierungsdaten. Mittlerweile nur noch selten gebräuchlich ist die Abbildung der Signalisierungsschnittstelle durch ein serielles Verbindungskabel zwischen UM-Server und TK-Anlage oder durch andere dedizierte und proprietäre Verbindungen. Bei VoIP-basierten Anlagen erfolgt die Anbindung typischerweise durch ein VoIP-Protokoll (z. B. SIP oder H.323, siehe Kapitel 4 sowie Kapitel 13.1.1), wobei diese Protokolle sowohl für den Sprach- als auch den Signalisierungskanal verwendet werden und somit keine dedizierten Verbindungskabel erforderlich sind.

Im Prinzip verhält sich der UM-Server aus Sicht der TK-Anlage zunächst wie ein Endgerät. Die Gefährdungssituation bezüglich der Sprachschnittstelle entspricht damit jener der Endgeräte einer entsprechenden TK-Anlage. Ein weiteres Gefährdungspotenzial ergibt sich aus der Signalisierungs-schnittstelle.

Integration in E-Mail-Systeme

Bei der Integration in E-Mail-Systeme muss zwischen zwei Szenarien unterschieden werden. Beim sogenannten True Unified Messaging werden alle eingegangenen Nachrichten durch den UM-Server im E-Mail-Postfach eines Benutzers, d. h. auf dem E-Mail-Server, abgelegt. Für die Auslieferung der Nachrichten kann z. B. das Simple Mail Transfer Protocol (SMTP) eingesetzt werden; weit verbreitet ist jedoch auch der Einsatz des proprietären Protokolls Messaging Application Programming Interface Remote Procedure Call (MAPI-RPC). Bei UM-Systemen, die kein True Unified Messaging unterstützen, werden die eingegangenen Nachrichten von einem separaten E-Mail-Server auf dem UM-Server bereitgestellt. Die Nutzer müssen daher ihre E-Mail-Clients so einrichten, dass ihre Nachrichten von diesem Server abgeholt werden, z. B. per Post Office Protocol Version 3 (POP3) oder Internet Message Access Protocol Version 4 (IMAP4).

Zusätzlich oder als Alternative zur Integration in E-Mail-Systeme bieten viele UM-Dienste eine Web-Schnittstelle, um Benutzern Zugriff auf ihre Nachrichten zu ermöglichen bzw. um Nachrichten zu versenden.

Kopplung von Unified-Messaging-Systemen

Zur Verbindung von UM- bzw. Sprachspeichersystemen untereinander, z. B. während Migrationsphasen, existieren zwei Protokolle. Audio Messaging Interchange Specification (AMIS) ist ein Protokoll zur Kopplung älterer Sprachspeichersysteme über eine analoge Telefonleitung. Voice Profile for Internet Mail (VPIM) wird von neueren digitalen Systemen eingesetzt und verwendet SMTP zur Auslieferung von Sprach- und Faxnachrichten.

Es sollte beachtet werden, dass ein spezifisches UM-System noch eine Reihe weiterer Schnittstellen bieten kann, die hier nicht aufgeführt wurden. Beispiele hierfür sind Anbindungen an sogenannten SMS Large Accounts zur massenhaften Versendung von Kurznachrichten und die Anbindung an Verzeichnisdienste und Fax-Server. Es ist daher im Einzelfall mit dem Hersteller eines Systems zu klären, welche Schnittstellen vorhanden sind, welche für den Betrieb unter den gegebenen Anforderungen benötigt werden und welche gegebenenfalls deaktiviert werden können.

6.1.5 Audiokonferenzen und Konferenzsysteme

Bei Audiokonferenzen handelt es sich im Allgemeinen um eine Echtzeit-Sprachkommunikation mit mehreren Teilnehmern gleichzeitig. Hierzu wählen sich die Teilnehmer per Telefon oder Softphone in eine sogenannte Konferenzbrücke ein, die alle Sprachkanäle zusammenführt. Die Konferenzbrücke dient hierbei als zentrale Einheit für Empfang, Transcoding und Versand aller Audiodatenströme. Sie mischt die verschiedenen Sprachkanäle zu einem gemeinsamen Audiosignal, welches an alle Teilnehmer versendet wird. Solche Konferenzbrücken bieten meist eine große Zahl virtueller Räume, um zeitgleich mehrere Konferenzen zu ermöglichen. Sie sind zumeist ein Bestandteil der TK-Anlage bzw. direkt über dedizierte Sprachkanäle mit dieser gekoppelt. Audiokonferenzen sind eine wesentliche Grundlage aller Echtzeit-Konferenzdienste wie z. B. Desktop-Video und Webkonferenzen. Je nach Systemarchitektur existieren dedizierte Audiokonferenzbrücken für jeden Konferenztyp (Audio, Video, Web) oder eine einheitliche Konferenzbrücke, auf der flexibel die gewünschten Medientypen für eine Konferenz gewählt werden können.

Unabhängig vom Typ des Konferenzsystems dient die Kopplung an eine Telefonanlage der Anbindung von Telefonteilnehmern. Aus technischer Perspektive ist das Konferenzsystem damit ein Endgerät der TK-Anlage und unterliegt der gleichen Gefährdungssituation bezüglich der Sprachschnittstelle. Für eine detailliertere Betrachtung dieser Schnittstelle wird auf Kapitel 3 und 4 verwiesen. Als Ergänzung oder auch alternativ zur Anbindung an eine TK-Anlage können Konferenzsysteme auch über eine direkte Verbindung zum PSTN verfügen.

Neben der organisationsinternen Bereitstellung von Konferenzsystemen ist auch die Bereitstellung eines Konferenzsystems durch einen Service Provider oder einen Cloud Service Provider (CSP) üblich. Hierbei wird ein Konferenzdienst oder ein dediziertes Konferenzsystem bedarfsgerecht bei einem Dienstleister eingekauft und durch diesen betrieben. Die Einwahl erfolgt via Telefon über öffentliche Einwahlrufnummern oder via Softphone bzw. UCC-Client über VoIP. Die Steuerung und Verwaltung der Konferenzräume erfolgt in der Regel über eine Web-Anwendung. Die Spezifika von gehosteten oder Cloud-basierten Konferenzsystemen werden in Kapitel 8.2 betrachtet. Sowohl für interne als auch externe Konferenzsysteme bietet sich der Einsatz von Buchungsportalen an. Diese ermöglichen die Erstellung von virtuellen Konferenzräumen und die Reservierung von Konferenzressourcen. Die Eigenschaften von Einheiten zur Ressourcenreservierung, die damit verbundenen Gefährdungen und Sicherheitsmaßnahmen können Kapitel 7.1 entnommen werden.

Topologie von Konferenzsystemen

Eine grundsätzliche, in der Architektur von Konferenzsystemen begründete Problematik besteht in der Verschlüsselung der Medienströme. Bei rein IP-basierten Konferenzen kann eine Verschlüsselung der Medienströme zwischen Teilnehmer und Konferenzbrücke durchgeführt werden, sofern die verwendete Konferenzbrücke dies unterstützt. Um die Medienströme mischen zu können, muss dabei die Verschlüsselung jedes Medienstroms an der Konferenzbrücke terminiert werden. Damit liegen alle Sprachinformationen an der Konferenzbrücke unverschlüsselt vor. Die Konferenzbrücke muss somit eine

Vertrauensstellung inne haben und entsprechend abgesichert werden. Theoretisch könnte auch eine Ende-zu-Ende-Verschlüsselung zwischen jedem einzelnen Konferenzteilnehmer erzielt werden. Hierzu müsste keine zentrale Konferenzbrücke, sondern eine vollvermaschte Topologie (engl. Full Mesh) mit direkten Medienströmen zwischen jedem einzelnen Teilnehmer implementiert werden. Dies ist allerdings aus Netzlast-, Leistungs- und Qualitätsgründen für größere Teilnehmerzahlen nicht praktikabel. Die verschiedenen Konferenztopologien und die zugehörigen Medienströme sind Abbildung 32 zu entnehmen.

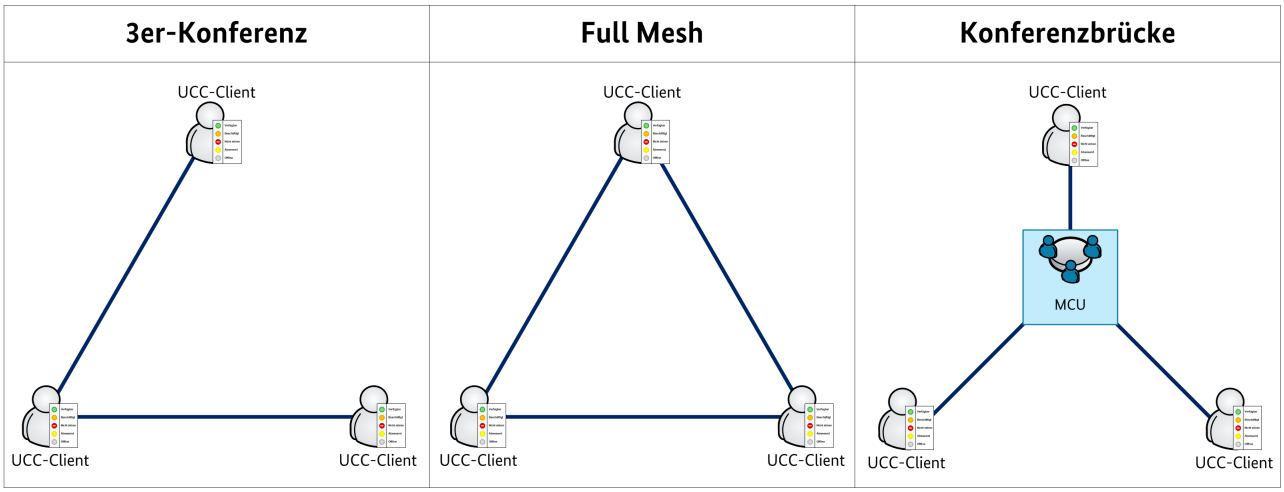


Abbildung 32: Konferenztopologien - Endgeräte-basierte Konferenz (3er-Konferenz, Full Mesh, Konferenzbrücke)

Schnittstellen für Integration und Management

Neben der Schnittstelle zur TK-Anlage bzw. dem VoIP-Kommunikationssystem verfügen Konferenzsysteme meist über eine Anbindung an einen Verzeichnisdienst, z. B. um Teilnehmer anhand ihres Namens anzuwählen. Weiterhin bieten Konferenzsysteme in der Regel zumindest Web-basierte Management-Schnittstellen sowie die Nutzung von Secure Shell (SSH) oder Simple Network Management Protocol (SNMP), um eine abgesetzte Wartung und Überwachung durchzuführen. Wie bei anderen UCC-Diensten gilt auch hier, dass für ein konkretes Produkt die Zahl, die konkrete Ausprägung und die Absicherung der Schnittstellen eines Konferenzsystems geklärt werden sollte.

6.1.6 Desktop-Video und Integration von Videokonferenzräumen

Desktop-Video bezeichnet die Nutzung von Videokommunikation an einem persönlichen Endgerät wie z. B. dem Desktop-PC. Anstelle eines dedizierten Videokonferenzendgerätes wird ein separater oder in die UCC-Lösung integrierter Video-Client verwendet, um die Videobilder und Sprache des Teilnehmers aufzunehmen und zu übermitteln sowie das empfangene Video- und Audiosignal wiederzugeben. Zur Aufnahme des Videobildes wird eine integrierte oder extern anzuschließende, meist via Universal Serial Bus (USB), Kamera verwendet. Als Ein- und Ausgabegerät für Audio dienen entweder integrierte Mikrofone und Lautsprecher oder ein externes Audiogerät, z. B. ein Headset. Das Transcoding der aufzunehmenden und zu empfangenden Mediendaten wird vollständig mit Hilfe von Software realisiert.

In den Anfängen galten Desktop-Videolösungen wegen der geringeren Qualität der Ein- und Ausgabegeräte und begrenzten Leistungsfähigkeit der Software-basierten Transcodierung im Vergleich zu dedizierten Videokonferenzsystemen als qualitativ minderwertig. Heute schließt sich diese qualitative Lücke zusehends und Desktop-Video nimmt einen immer höheren Stellenwert in der Kommunikation ein. Der Mehrwert im Vergleich zur reinen Audiokommunikation ergibt sich hierbei aus dem zusätzlichen Informationsgehalt des Videobildes und der damit deutlich persönlicheren Kommunikation.

Punkt-zu-Punkt- und Mehrpunkt-Video

Desktop-Video kann für die Punkt-zu-Punkt-Kommunikation, aber auch als Mehrpunkt-Konferenz genutzt werden. Auch hier werden Konferenzbrücken eingesetzt, falls mehr als zwei Endsysteme an einer Konferenz beteiligt sind. In diesem Zusammenhang werden die Brücken häufig auch Multipoint Control Unit (MCU) genannt. Während Desktop-Videolösungen ursprünglich einen eigenständigen Bereich unter den Videolösungen darstellten, wachsen diese Systeme im Zuge von UCC zusehends mit den dedizierten Videokonferenzsystemen zusammen. Hierfür findet eine Integration der Systeme statt, sodass sowohl dedizierte Videoraumsysteme als auch Desktop-Video-Clients gleichzeitig an einer Konferenz teilnehmen können. Entweder wird dies über eine gemeinsame MCU oder über die Kopplung der Lösungen mittels Video-Gateway realisiert.

Protokolle für Desktop-Video

Im Falle von Konferenzen auf Basis von Desktop-Video gelten dieselben Anforderungen wie auch für Konferenzbrückensysteme im Allgemeinen. Desktop-Video basiert im Wesentlichen auf denselben Technologien wie dedizierte IP-basierte Videokonferenzsysteme. Für die Übertragung von Medienströmen wird das Real-Time Protocol (RTP) verwendet. Für die Signalisierung setzen die meisten Systeme auf SIP. H.323 wird ebenfalls noch eingesetzt, befindet sich jedoch im Rückgang. Des Weiteren sind teils noch proprietäre Übertragungsprotokolle im Einsatz. Das Transcoding basiert in der Regel auf denselben Codecs, die auch im Zusammenhang mit dedizierten Videokonferenzlösungen eingesetzt werden. Für die Gefährdungslage und entsprechende Sicherheitsmaßnahmen ergeben sich somit zunächst dieselben Grundlagen wie für dedizierte Videokonferenzsysteme (siehe Kapitel 7.1). Durch den Einsatz von Video am Desktop ergeben sich zusätzliche Gefährdungen, denen durch geeignete Maßnahmen begegnet werden muss, um die Gefährdung der Informationssicherheit der Organisation sowie der Persönlichkeitsrechte der Mitarbeiter zu minimieren.

6.1.7 Webkonferenzen, Desktop und Application Sharing

Webkonferenzen sind ein Werkzeug zur Verbesserung der ortsunabhängigen Zusammenarbeit an Dokumenten und Applikationen. Die Anwendungsfälle reichen von der Durchführung einer Präsentation oder Produktdemonstration über die gemeinsame Arbeit an Dokumenten bis hin zum Einsatz als Instrument zur Fernwartung oder als Schulungsplattform. So sollen überflüssige Reisetätigkeiten, beispielsweise bei räumlich weit verteilten Projektteams, vermieden und die Effizienz der Zusammenarbeit erhöht werden.

Bei Webkonferenzen können alle Teilnehmer in einem Fenster auf ihrem Bildschirm das Geschehen auf dem Desktop (Desktop Sharing) oder in der freigegebenen Applikation (Application Sharing) eines dedizierten Teilnehmers verfolgen. Dieser Teilnehmer gibt die Inhalte als Moderator anderen Teilnehmern frei. Im Laufe einer Webkonferenz kann diese Moderatorrolle zwischen den Teilnehmern (und ihren Endgeräten) gewechselt werden. Weitere typische Funktionen von Webkonferenzen sind:

- Präsentationsmodus
- Virtuelles Whiteboard
- Dokumentenablage
- Gruppen-Chat und privater Chat
- Umfrage- und Abstimmungsfunktion
- Video (Moderator bzw. Sprecher)
- Videokonferenz (Bild aller Teilnehmer, sogenannte Continuous Presence)

Die notwendige Sprachübertragung erfolgt entweder über eine separate Audiobrücke oder bei voll-integrierten IP-basierten Konferenzen alternativ auch über eine eingebaute Brücke des UCC-Systems. Gleiches gilt für einen eventuell genutzten Bildkanal. Die bei Webkonferenzen übermittelten Video-, Audio- und Chat-Inhalte müssen gegebenenfalls aus juristischen oder regulatorischen Gründen

aufgezeichnet werden. Dabei ist zu beachten, dass eine Aufzeichnung alle genutzten Medienkanäle (synchron) umfassen muss, um sinnvoll den Kommunikationsfluss einer Webkonferenz nachvollziehen zu können. Dies wird von den meisten Webkonferenzsystemen unterstützt. Es muss im Sicherheitskonzept berücksichtigt werden, ob die Aufzeichnung Client-seitig oder Server-seitig vorgenommen wird. Sowohl Server-seitig aufgenommene Webkonferenzen als auch durch die Teilnehmer bereitgestellte Dokumente oder Präsentationen können in Webkonferenzlösungen zum Download bereitgestellt werden. Hierbei ist zu beachten, dass dieser Verbreitungsweg für Dokumente und Daten im Sicherheitskonzept berücksichtigt oder deaktiviert werden muss.

Für Webkonferenzen gelten darüber hinaus dieselben Eigenschaften, Gefährdungen und Maßnahmen wie für allgemeine Konferenzsysteme.

6.1.8 Mobilintegration

Ein wesentlicher Bestandteil von UCC-Systemen ist die Integration mobiler Endgeräte. Die Einbindung von mobilen Endgeräten als virtuelle Nebenstellen der klassischen TK-Anlage bzw. des VoIP-Systems ist hierbei ein wichtiger Aspekt. Das Ziel einer solchen Integration ist die bessere Einbindung mobiler Mitarbeiter sowie die Vereinfachung der Kontaktaufnahme und die Verbesserung ihrer Erreichbarkeit. Ein Ansatz hierzu ist die Implementierung von Single Number Reach (SNR), das eine Erreichbarkeit des mobilen Endgerätes unter einer einheitlichen (Festnetz-)Rufnummer sicherstellt. Damit dieser Ansatz konsistent umgesetzt werden kann, ist es zudem notwendig, dass die einheitliche Rufnummer auch bei Anrufen vom mobilen Endgerät ausgehend signalisiert wird (Single Number Present, SNP). Ansonsten würden Kommunikationspartner die mobile Rufnummer präsentiert bekommen und diese bei Rückrufen verwenden, was die Vorteile von Single Number Reach aufheben würde. Der gleichzeitige Einsatz beider Leistungsmerkmale wird auch als One Number Service (ONS) bezeichnet und ist ein wichtiger Bestandteil von UCC-Lösungen, kann jedoch auch auf Basis separater Produkte im Zusammenspiel mit einer klassischen TK-Anlage oder einer VoIP-Lösung dediziert realisiert werden (Fixed Mobile Convergence). Aufgrund der eigenständigen Verfügbarkeit und der Wichtigkeit der Mobilintegration wird die Einbindung mobiler Endgeräte separat in Kapitel 9 behandelt.

6.1.9 Computer Telephony Integration und Anwendungsintegration

Computer Telephony Integration (CTI) bezeichnet die Kombination der Steuerung eines Telefons und eines PCs. Dies umfasst insbesondere den automatischen Aufbau, die Annahme und Beendigung von Telefongesprächen, den Aufbau von Telefonkonferenzen, Anrufjournale, Telefonbuchdienste sowie die Weitervermittlung von Gesprächen.

Es wird zwischen Einzelplatzlösungen (First Party Call Control) und Mehrplatzlösungen (Third Party Call Control) unterschieden. Bei Einzelplatzlösungen ist das Telefon entweder im Computer integriert oder direkt mit diesem verbunden. In diesem Fall kann eine CTI-Applikation lediglich das mit dem Computer verbundene Telefon steuern. Bei Mehrplatzlösungen ist in der Regel ein sogenannter CTI-Server zwischen dem Computernetzwerk und dem Telefonnetz beziehungsweise der Telefonanlage geschaltet. Dies erlaubt zusätzlich zur Kontrolle des eigenen Telefons grundsätzlich auch die Steuerung anderer Endgeräte der Gruppe.

Protokolle und Architektur

CTI und die Integration von Anwendungen erfordert die Kopplung mit der klassischen TK-Anlage oder dem VoIP-System. Hierfür wurden in der Vergangenheit eine Reihe von Protokollen und Application Programming Interfaces (APIs) entwickelt. Hierunter fallen unter anderem das Protokoll Computer Supported Telecommunications Applications (CSTA) sowie die weit verbreiteten APIs Telephony Application Programming Interface (TAPI), Telephony Server API (TSAPI) und Java Telephony API (JTAPI). In modernen UCC-Lösungen werden zunehmend SIP-basierte CSTA-Varianten und Remote Procedure Calls über Webservices via Hypertext Transfer Protocol (HTTP) bzw. der TLS/SSL-gesicherten Entsprechung HTTP Secure (HTTPS) genutzt. Einen Überblick über die für CTI und Anwendungsintegration relevanten Protokolle bietet Kapitel 13.2.2.

Neben der herkömmlichen Integration von Telekommunikation in Arbeitsplatzanwendungen via CTI hat mit dem Entstehen von UCC die Client-seitige Integration in Anwendungen unter Verwendung des UCC-Clients und teils proprietärer Applikationsschnittstellen zugenommen. Ein Beispiel hierfür ist die Anzeige des Präsenzstatus im E-Mail-Client und die direkte Kontaktaufnahme über einen frei wählbaren, von der UCC-Lösung bereitgestellten Kommunikationsweg. Durch eine solche Integration in wichtige Geschäftsanwendungen lässt sich der mit der Kommunikation verbundene Aufwand reduzieren und kommunikationsoptimierte Geschäftsprozesse gestalten (Communications Enabled Business Processes, CEBP).

Viele UCC-Systeme bilden somit eine Brücke zwischen der Kommunikations- und der IT-Landschaft einer Organisation. Ein solches Brückenszenario zeigt Abbildung 33 am Beispiel CTI. Der CTI-Server bildet hier die Brücke zwischen TK- und IT-Systemen, in der Abbildung exemplarisch als Datenbank-Server und CTI-Client dargestellt. Unterschiede bestehen hauptsächlich in der Anzahl und Art der Schnittstellen zu verschiedenen TK- und IT-Systemen sowie in der Natur der zwischen den Systemen ausgetauschten Informationen.

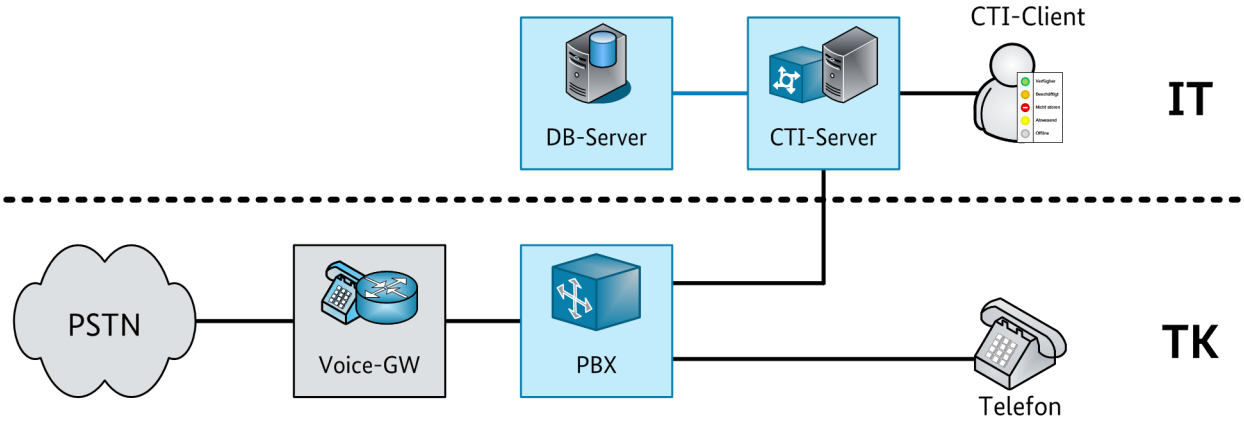


Abbildung 33: Brückenszenario CTI im UCC-Kontext

Die möglichen Wechselwirkungen zwischen den integrierten Systemen sind vielfältig. Eine Gefährdungsanalyse für die Anwendungsintegration muss insbesondere das Zusammenspiel mit unterschiedlich gearteten TK-Anlagen und VoIP-Systemen berücksichtigen.

6.1.10 Integration von Web-basierten Applikationen

Bei der Bereitstellung von Unternehmensanwendungen kommen vermehrt Webtechnologien zum Einsatz. In diesen werden häufig Kontaktinformationen aufgeführt bzw. verarbeitet. Die damit verbundene Vereinfachung der Kontaktaufnahme ist insbesondere in Hinblick auf die Optimierung von Geschäftsprozessen zielführend. Zudem ist, je nach Anwendungsszenario, die Speicherung von Metadaten zur Kommunikation in einer Webapplikation notwendig. Dies ist zum Beispiel bei Web-basierten Customer-Relationship-Management-Systemen (CRM) erforderlich, um die Kommunikationsbeziehungen eines Vertriebsmitarbeiters für die spätere Analyse der Vertriebsaktivitäten zu dokumentieren.

Um generische Webapplikationen zu integrieren, sind somit zwei Mechanismen notwendig. Zum einen muss eine Auflösung von angezeigten Kontaktnamen oder Kontaktdaten (z. B. Telefonnummer, E-Mail-Adresse) stattfinden. Hierzu eignen sich entweder spezielle Programmcodes, welche direkt via Webservice auf die UCC-Lösung und angeschlossene Kontaktverzeichnisse zugreifen und die in die Webapplikation durch den Entwickler integriert werden müssen. Alternativ können Browser Plug-ins zum Einsatz kommen, welche im Zusammenspiel mit einem UCC-Client diese Namensauflösung und eine Kontaktaufnahme per Click realisieren. Zum anderen ist die Speicherung von kommunikationsbezogenen Metainformationen in der Applikation wichtig für die Geschäftsprozessoptimierung. Hierzu bieten viele Webapplikationen APIs bzw. Webservices an, die ein Systemintegrator zur Anschaltung des entsprechenden UCC-Systems nutzen kann. Der Zugriff erfolgt meist über HTTP bzw. HTTPS.

Beiden Integrationswegen ist gemeinsam, dass die verwendeten Schnittstellen potenziell Zugriff auf schützenswerte Organisationsdaten oder personenbezogene Daten erlauben können. Zudem ist ein Missbrauch von Webservices zur Erlangung von weitergehenden Zugriffsrechten oder zur Durchführung von Denial-of-Service-Attacken (DoS) möglich. Die Schnittstellen zur Integration in Web-basierte Applikationen müssen daher durch entsprechende Sicherheitsmechanismen abgesichert werden.

6.1.11 Integration von Verzeichnisdiensten und Datenbanken

Um eine Namensauflösung für interne und externe Kontakte zu realisieren und somit die Zuordnung von Kommunikationsverläufen zu Personen zu vereinfachen, ist es notwendig ein entsprechendes Kontaktverzeichnis zu führen. Im klassischen TK-Umfeld werden hierfür meist Elektronische Telefonbücher (ETB) geführt, welche die Zuordnung interner Teilnehmer zu Nebenstellen realisieren. Nachteilig ist hierbei, dass meist nur interne Kontakte abgebildet werden und eine redundante Pflege von Kontaktinformationen in einem weiteren Verzeichnis notwendig ist. Daher setzt sich zunehmend die Integration existierender Verzeichnisdienste und Datenbanken durch, wodurch eine mehrfache Pflege von Kontaktinformationen vermieden werden kann.

Die Integration von Verzeichnisdiensten findet in den meisten Fällen über das weitgehend standardisierte Protokoll Lightweight Directory Access Protocol (LDAP, siehe [IETF RFC4511-2006]) statt. Auch ein Zugriff über proprietäre Mechanismen, z. B. Microsoft Active Directory (MS AD), ist üblich. Während Verzeichnisdienste vorrangig für die Pflege interner Kontakte eingesetzt werden, werden externe Kontakte oft in separaten Datenbanken, z. B. einem CRM-System, gepflegt. Diese Systeme können entweder ebenfalls über eine LDAP-Schnittstelle oder alternativ über eine Datenbankschnittstelle wie Open DataBase Connectivity (ODBC) bzw. Structured Query Language (SQL) integriert werden.

Verzeichnisdienste werden zudem häufig für die Pflege und den automatisierten Import von Benutzerkonten sowie die automatisierte Provisionierung neu angelegter Nebenstellen genutzt. In diesem Fall wird meist eine Nutzerauthentisierung im Zusammenspiel mit dem Organisationsverzeichnis per Single Sign-On implementiert, um Mehrfachauthentisierungen des Anwenders zu vermeiden. In diesem Fall spielt der Zugriff auf Verzeichnisdienste eine zentrale Rolle im Sicherheitskonzept einer UCC-Lösung. Durch die Integration von Verzeichnis und Datenbank kann zudem ein unautorisierter Zugriff oder eine Kompromittierung von schützenswerten Daten erfolgen. Die Integration von Verzeichnisdiensten und Datenbanken muss daher sorgfältig abgesichert werden.

6.1.12 Integration Sozialer Netzwerke und Sozialer Medien

Die Begrifflichkeiten Soziale Netzwerke und Soziale Medien (engl. Social Networks and Social Media) umfassen insbesondere Web-Plattformen zur Vernetzung von Anwendern und zur Kommunikation zwischen Anwendern sowie zur Bereitstellung von nutzererzeugten Inhalten. In Sozialen Netzwerken werden insbesondere persönliche Informationen und Kontaktinformationen als Grundlage der sozialen Vernetzung gepflegt. Die Integration Sozialer Netzwerke ist Bestandteil aktueller UCC-Plattformen. Es sind viele Arten und Anwendungsfälle für eine Integration von Sozialen Netzwerken denkbar. Soziale Netzwerke dienen unter anderem als:

- Datenquelle für externe und interne Kontaktinformationen
- Kommunikationskanal mit externen Teilnehmern
- Datenbasis zur Optimierung des Kundenkontakts im Kontaktcenter

Ebenso vielfältig wie die Integrationsmöglichkeiten und sinnvollen Anwendungsfälle sind auch die Bedrohungen für die Informationssicherheit. Die Schnittstellen zwischen UCC-System und öffentlichem Sozialen Netzwerk sind mögliche Angriffsvektoren auf die organisationsinternen Infrastrukturen. Zudem besteht die Gefahr, dass Informationen aus der Organisation durch Fehlbedienung oder technische Isolationsfehler in die öffentlichen Netzwerke abfließen. Kapitel 8.1 beschreibt die Integrationsmöglichkeiten Sozialer Netzwerke und Medien, die hiervon ausgehenden Gefährdungen und die zu treffenden Sicherheitsmaßnahmen.

6.1.13 Standortübergreifende Kommunikation

Die standortübergreifende Kommunikation auf Basis von UCC-Systemen entspricht weitestgehend der in Kapitel 4.1.7 beschriebenen standortübergreifenden Kommunikation für Voice-over-IP-basierte Systeme (siehe Kapitel 4). Im Wesentlichen sind

- die Vernetzung verschiedener UCC-Systeme an separaten Standorten,
- die Anbindung entfernter Standorte und Außenstellen sowie
- die Anbindung von Telearbeitsplätzen

auf Basis von IP-Vernetzung zu unterscheiden. Wesentliche Unterschiede ergeben sich insbesondere aufgrund der erforderlichen Datenraten (insbesondere für Video) und der im UCC-Umfeld zusätzlich eingesetzten Protokolle.

Signalisierung

Die Signalisierung basiert vorrangig auf SIP und die Übertragung von Echtzeitmedienströmen auf RTP. Außerdem werden Instant Messaging und Präsenzdienste auf Basis von SIP/SIMPLE oder XMPP sowie HTTP-basierte Applikationsprotokolle über Standortgrenzen hinweg eingesetzt. Zur Vernetzung von UCC-Systemen über Standortgrenzen hinaus werden hierbei SIP-Trunks bzw. XMPP-Föderationen genutzt.

Anbindung der Teilnehmer

Die Anbindung von Teilnehmern an entfernten Standorten findet entweder direkt – unter Verwendung der zugrunde liegenden IP-Netze – durch Registrierung der Teilnehmer am zentralen UCC-System oder unter Verwendung eines Gateways mit „Überlebensfähigkeit“ (engl. Survivability) statt. Im zweiten Fall beherbergt das Gateway rudimentäre UCC-Funktionen und optional eine eigene Anbindung an das öffentliche Festnetz. So kann bei Ausfall der WAN-Strecke zum zentralen UCC-System zumindest die interne Kommunikation und ggf. die Sprachkommunikation in das öffentliche Festnetz aufrecht erhalten werden. Es ist dabei zu beachten, dass diese Gateways im Notbetrieb in der Regel nur eine deutlich eingeschränkte Funktionalität zur Verfügung stellen (meist nur Basismerkmale für Telefonie). Alternativ sind Lösungen verfügbar, die erweiterte UCC-Funktionen im Notfallbetrieb durch einen abgesetzten UCC-Server am entfernten Standort, der in das Management der zentralen Lösung integriert ist, bereitstellen.

Telearbeitsplätze

Die Anbindung von Anwendern an Telearbeitsplätzen findet direkt an die zentrale UCC-Lösung oder über einen Session Border Controller (SBC) bzw. einen UCC-Proxy-Server in einer Demilitarisierten Zone statt. Bei der Verwendung des Internets muss die Anbindung von Telearbeitsplätzen entsprechend gesichert werden. Dies kann alternativ auf Basis eines Virtual Private Network (VPN) oder durch eine dienstbezogene Verschlüsselung mittels Transport Layer Security (TLS) und Secure Real-Time Transport Protocol (SRTP) vorgenommen werden.

Bei der Kommunikation über Standortgrenzen kann auch eine Überschreitung von Vertrauensgrenzen erfolgen. Dies macht den Einsatz von Sicherheits-Gateways (z. B. Firewalls, Intrusion Prevention Systems, Data Loss Prevention Systems oder Session Border Controller) erforderlich. Kapitel 6.1.14 beschreibt den Einsatz von UCC über Vertrauensgrenzen hinweg.

6.1.14 UCC über Vertrauensgrenzen hinweg

Neben der organisationsinternen Kommunikation bedient UCC auch die organisationsübergreifende Kommunikation. Die Kommunikation zwischen Partnerorganisationen (Business-to-Business, B2B) sowie Organisation und Einzelperson (Business-to-Customer, B2C) wird zunehmend durch UCC-Lösungen adressiert. Hierbei findet eine Kommunikation über Vertrauensgrenzen statt, deren Vertraulichkeit und Integrität durch eine Absicherung der Netzübergänge, Übertragungswege und Inhalte geschützt werden muss. Aber auch innerhalb von Organisationen werden Vertrauensgrenzen überschritten, wenn z. B. ein

Dienstleister UCC-Dienste zentral für verschiedene Mandanten innerhalb der eigenen Organisation bereitstellt.

Bei der Überschreitung von Vertrauensgrenzen ist der Einsatz von Sicherheits-Gateways notwendig. Ihre Eigenschaften entsprechen im Wesentlichen den Beschreibungen im Kapitel Voice over IP (siehe Kapitel 4.1.8).

Die verwendeten Sicherheits-Gateways müssen die selektive Öffnung einzelner Ports für RTP-basierte Medienströme, die dynamische Überbrückung von Network Address Translation (NAT) mittels der Methodik Interactive Connectivity Establishment (ICE) bzw. der hierdurch genutzten Verfahren wie Traversal Using Relays around NAT (TURN) oder Session Traversal Utilities for NAT (STUN) und den Umgang mit SIP-basierter Signalisierung beherrschen. Bei Funktionalitäten zur Angriffserkennung via SIP müssen Protokollerweiterungen wie SIP/SIMPLE für Instant Messaging und Präsenz ebenfalls berücksichtigt werden. Eine Unterstützung von H.323 kann je nach Szenario zusätzlich notwendig sein.

Neben der Signalisierung und den Medienströmen von Echtzeitkommunikation können weitere UCC-Protokolle die Vertrauensgrenzen passieren. In diesem Fall müssen die eingesetzten Sicherheits-Gateways in der Lage sein, mit Protokollen wie XMPP, HTTP-basierten Applikationsprotokollen oder proprietären Protokollvarianten umzugehen. Dies ist in der Regel bei modernen UCC-fähigen Firewalls und bei spezialisierten SBCs der Fall.

6.1.15 Virtualisierung von UCC-Servern und UCC-Clients

Die oben beschriebenen Dienste werden in der Regel auf Basis von Standard-Servern oder vom Hersteller auf Basis von Standard-Hardware erstellten Appliances bereitgestellt. Wie auch VoIP-basierte Kommunikationssysteme werden UCC-Systeme heute vermehrt auf virtualisierten Serverinstanzen bereitgestellt. Hierdurch lässt sich die Ausnutzung der Server-Hardware optimieren, die Skalierbarkeit der Gesamtsysteme erhöhen und Betriebs- und Wartungsprozesse der Installationen verbessern. Die Server-Virtualisierung hat jedoch auch Auswirkungen auf die Informationssicherheit. Die physischen Grenzen bei der Datenhaltung werden aufgehoben und eine Trennung einzelner Server-Instanzen wird nur noch durch die Virtualisierungsschicht realisiert. Diese muss daher ein geeignetes Sicherheitsniveau aufweisen und es müssen Maßnahmen zum Schutz der virtualisierten Server-Instanzen getroffen werden.

Die Desktop-Virtualisierung ermöglicht zudem die zentrale Bereitstellung virtueller Desktop-Umgebungen. Diese werden in einer virtuellen Desktop-Infrastruktur (Virtual Desktop Infrastructure, VDI) zentral ausgeführt und bereitgestellt. Die Arbeitsplatz-Terminals (Thin Client) verfügen über ein minimales Betriebssystem, welches ausschließlich der Ausführung einer Client-Software zum Zugriff auf den virtualisierten Desktop über das Netzwerk dient. Die grundlegende Funktionsweise einer VDI wird in Kapitel 4.1.9 erläutert.

Für UCC-Dienste ergeben sich im Zusammenhang mit der Virtualisierung von Desktops ebenfalls Probleme bei der Echtzeitkommunikation. Diese Problematik besteht bei UCC jedoch nicht nur für Audio-Datenströme, sondern auch für die deutlich Bandbreiten-intensivere Videoübertragung. Um das Hairpinning-Problem zu vermeiden, bieten sich auch hier die in Kapitel 4.1.9 erläuterten Maßnahmen zur Medienstromauskopplung am Client an. Da die Codierung von Videodatenströmen in der Regel deutlich rechenintensiver ist als die Codierung von Audioströmen und die Thin Clients nicht die erforderliche Rechenleistung bereitstellen können, wird hier in der Praxis teilweise auf spezielle Zusatz-Hardware (z. B. Kameras mit eingebautem Co-Prozessor für Videokodierung) zurückgegriffen. Empfangene Videobilder müssen wiederum dekodiert und in die Darstellung der VDI-Sitzung am Thin Client eingeblendet werden. Die hierfür auf dem Thin Client benötigte Applikationslogik führt grundsätzlich zu denselben Gefährdungen wie eine Applikationslogik zur Verarbeitung von VoIP-Datenströmen. Es gelten somit die diesbezüglichen Gefährdungen und Maßnahmen der Basistechnologie Voice over IP (siehe Kapitel 4).

6.1.16 WebRTC

Ein wichtiger Treiber für die Kommunikation über die Grenzen der Organisation hinweg ist Web Real-Time Communication (WebRTC). Bei WebRTC handelt es sich um ein offengelegtes API, welches die einfache Programmierung von Anwendungen zur Echtzeitkommunikation im Browser ermöglichen soll. Die Initiative geht ursprünglich auf den US-Software-Hersteller Google Inc. zurück. Seine Standardisierung wird von der WebRTC Working Group des World Wide Web Consortium (W3C) vorangetrieben. Der Vorteil von WebRTC liegt darin, dass außer dem WebRTC-fähigen Browser kein lokaler UCC-Client und auch keine zusätzliche Software, z. B. Browser Plug-in, auf dem Endgerät benötigt wird. Hierdurch wird die tiefe Einbindung von UCC-Funktionen in webbasierte Applikationen und eine einfachere Erstellung webbasierter, plattformunabhängiger Clients möglich. WebRTC kann in Zukunft ein wichtiges Element sein, um Desktop-Umgebungen nicht mehr in Form von VDI-Lösungen, sondern auf Basis von Web-Technologien zentral bereitzustellen.

WebRTC wird zunehmend durch den Markt angenommen und durch Hersteller adaptiert. Einige Hersteller streben hingegen die Durchsetzung eigener Gegenentwürfe zu WebRTC an, welche im Kern aber dieselben Eigenschaften und Funktionalitäten bieten. Bei WebRTC werden Medienströme grundsätzlich RTP-basiert übertragen. Hierbei kann optional eine SRTP-basierte Medienstromverschlüsselung zum Einsatz kommen. Die Wahl des verwendeten Signalisierungsprotokolls obliegt jedoch dem Anwendungsprogrammierer. Prinzipiell kann auch hier eine standardbasierte Signalisierung wie SIP zum Einsatz kommen. Es können aber auch proprietäre Mechanismen über die WebRTC-Schnittstellen implementiert werden. Hierbei können z. B. Java WebSockets Verwendung finden.

Abbildung 34 zeigt eine grundlegende WebRTC-Architektur mit Anbindung an eine native SIP-Infrastruktur auf. Die Client-Anwendung wird in einem WebRTC-fähigen Browser als JavaScript-Anwendung ausgeführt. Diese verbindet sich per WebSocket mit einem Web-Server, der die Applikationslogik bereitstellt und die WebSocket-Signalisierung terminiert. Ein WebRTC-SIP-Gateway übersetzt die WebSocket-Signalisierung in standardisiertes SIP und leitet diese zum SIP-Proxy weiter. An diesem ist der Gesprächspartner mit einem SIP-Endgerät angemeldet. Das Gateway kann auf derselben Server-Instanz wie der Web-Server oder aber auf einer separaten Server-Instanz installiert sein. Nachdem die Kommunikation per SIP etabliert wurde, wird der Medienstrom direkt zwischen dem Browser und dem SIP-Endgerät des Gesprächspartners per SRTP aufgebaut. Alternativ kann dieser Medienstrom über das WebRTC-SIP-Gateway geführt werden, um zwischen zwei unterschiedlichen Audio- oder Video-Codecs zu transkodieren. Dies ist in der Abbildung durch gestrichelte Linien angedeutet. Das Gateway nimmt dann zusätzlich die Rolle eines Media-Gateway ein.

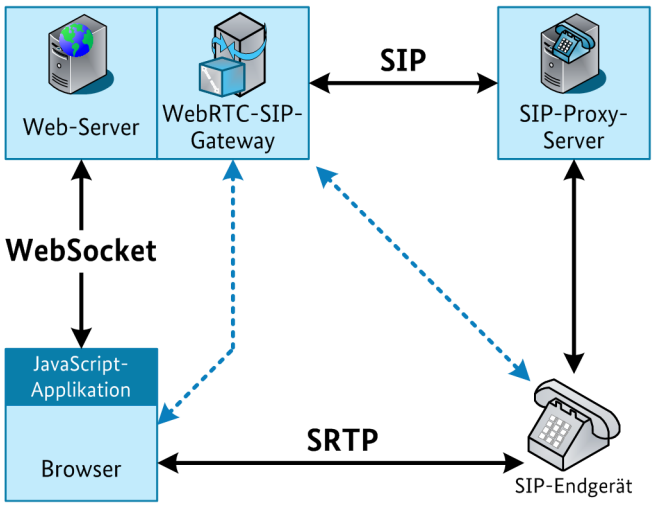


Abbildung 34: Basis-Architektur WebRTC

Die Sicherstellung von vertraulicher Kommunikation durch den Einsatz von TLS-Verschlüsselung für die Signalisierung obliegt somit dem Anwendungsprogrammierer. Bei der Anbindung WebRTC-basierter Clients und Applikationen ist auf deren korrekte und sichere Implementierung zu achten. Zudem sind die Koppelelemente an die UCC-Infrastruktur, z. B. Gateways, so zu gestalten, dass die UCC-Infrastruktur vor fehlerhaften und unsicheren WebRTC-Implementierungen geschützt wird.

6.2 Gefährdungen

Dieser Abschnitt analysiert die Gefährdungslage für UCC-Systeme, die den Gefährdungen der Tele- und Datenkommunikation ausgeliefert sind. Zudem können auch Gefährdungen zwischen Tele- und Datenkommunikation überspringen.

Durch den Einsatz von UCC in der Organisation ergeben sich einige übergreifende Gefährdungen. So handelt es sich bei UCC um relativ neue Medien, die den meisten Anwendern allenfalls aus dem privaten Umfeld bekannt sind. Durch den ungeübten oder aus privater Gewohnheit nachlässigen Umgang mit diesen Medien ergibt sich eine erhöhte Gefährdungslage für die Informationssicherheit. Über die vielfältigen Kommunikationskanäle und die tiefe Integration in Applikationen können versehentlich Daten abfließen oder bei unzureichenden Sicherheitsmaßnahmen der Datenverkehr auf dem Übertragungsweg mitgelesen werden. Im Folgenden wird die Gefährdungslage für UCC-Systeme detailliert dargestellt.

Es ist zu beachten, dass viele Gefährdungen für VoIP-Systeme analog auch für UCC-Systeme gelten. Diese werden im Folgenden entsprechend referenziert und sind sinngemäß auf den Anwendungsfall eines UCC-Systems zu übertragen.

6.2.1 Höhere Gewalt

Auf UCC-Installationen treffen wie für alle IT-Lösungen allgemein die Gefährdungen durch höhere Gewalt zu, die in den IT-Grundschutz-Katalogen genannt sind.

Zudem ergeben sich bei Einsatz einer UCC-Lösung die folgenden identischen Gefährdungen der höheren Gewalt, die für die Basistechnologie VoIP genannt sind:

G-TK-18 „Ausfall der mitgenutzten IP-Infrastruktur“

G-TK-19 „Ausfall eines für VoIP mitgenutzten Weitverkehrsnetzes“

6.2.2 Organisatorische Mängel

Organisatorische Mängel treffen UCC-Systeme grundsätzlich genauso wie beliebige andere IT-Systeme. Mit der Einführung von UCC-Systemen müssen bestehende Entscheidungen und Konzepte für eine durch UCC mitgenutzte IT gezielt überprüft werden. Gefährdungen durch organisatorische Mängel ergeben sich insbesondere

- bei einer unzureichender Schutzbedarfsfeststellung,
- bei fehlenden oder fehlerhaften zentralen Elementen in Sicherheitskonzepten und
- fehlenden oder fehlerhaften organisatorischen Regelungen im Bereich Technikbetrieb.

Besonders zu beachten sind zudem

- die erhöhte Gesamtwirkung einer Gefährdung durch die Server-seitige Integration verschiedener IT-, TK- und UCC-Systeme sowie
- die erhöhte Gesamtwirkung einer Gefährdung durch Nutzung gemeinsamer Endgeräte mit anderen Anwendungsformen, vor allem zur Datenverarbeitung.

Gefährdungen, die sich auf bestimmte Betriebssysteme, Verzeichnisdienste, Clients usw. beziehen, können ebenfalls Auswirkungen auf TK-nahe Systeme haben. Für jedes spezifische System müssen die relevanten Gefährdungen daher in jedem Fall auch berücksichtigt werden.

G-TK-46 Unzureichende oder fehlende Kompetenzen für Planung und Betrieb eines UCC-Systems

Für die Planung und den Betrieb eines UCC-Systems und dessen Kopplung mit der ISDN-basierten TK-Anlage oder dem VoIP-System sowie mit Fachapplikationen (d. h. durch die Fachbereiche direkt betreuten Applikationen) ist Kompetenz sowohl für den Bereich des UCC-Systems als auch für die gekoppelten Systeme erforderlich. Kompetenzmängel in einem der drei Bereiche können für das Gesamtsystem erhebliche Auswirkungen haben.

Dieser Gefährdung kommt eine besonders große Bedeutung zu, wenn Planung und Betrieb der Teilsysteme von verschiedenen Personengruppen durchgeführt werden. Dies ist insbesondere dann der Fall, wenn UCC-System, TK-Anlage und Fachapplikation unterschiedlichen organisatorischen Einheiten zugeordnet sind. Als Beispiel sind hier CRM-Systeme zu nennen, die in der Regel im Zuständigkeitsbereich der Fachapplikationsbetreuung liegen. Missverständnisse aus mangelndem (gegenseitigem) Verständnis sind hier eine nicht zu unterschätzende Gefahrenquelle.

G-TK-47 Unzureichende Organisation des Betriebs eines UCC-Systems

Für den Betrieb eines UCC-Systems müssen häufig neben den UCC-spezifischen Schnittstellen auch andere Schnittstellen, z. B. zu Datenbanksystemen oder Verzeichnisdiensten, berücksichtigt werden. Der Betrieb des UCC-Systems, der IP-Infrastruktur und der Server für solche Fachanwendungen kann von unterschiedlichen Gruppen durchgeführt werden. Eine fehlende oder unzureichende Abstimmung der beteiligten Gruppen kann beispielsweise dazu führen, dass sich über eine CTI-Applikation eine Gefährdung auf das UCC-System bzw. allgemein auf Telekommunikationsdienste fortpflanzt. Als besonders kritisch sind in allen Integrationsszenarien Versionswechsel eines Teilsystems zu bewerten. Hier kann unter ungünstigen Bedingungen die Verfügbarkeit des Gesamtsystems bedroht sein.

G-TK-48 Ungeordnete Nutzung der Kommunikationsmöglichkeiten

UCC-Systeme integrieren die Möglichkeiten zur Sprachkommunikation mit weiteren Kommunikationswegen. Als wichtige Beispiele sind hier Unified-Messaging-Systeme und Instant Messaging zu nennen. Die ungeordnete Nutzung von E-Mail, Unified Messaging und Instant Messaging kann dazu führen, dass sensitive Daten Unbefugten zur Kenntnis gelangen oder das gewünschte Ziel nicht rechtzeitig erreichen. Zum Beispiel ist es durch eine Fehlbedienung möglich, dass ein vertrauliches Fax über den Messaging-Client per E-Mail an die falsche Person weitergeleitet wird. Diese Gefährdung ist grundsätzlich bekannt, überträgt sich jedoch beim Einsatz von UM und IM auch auf andere Nachrichtentypen wie z. B. SMS, Fax, Instant Messaging und Kurznachrichten in Sozialen Netzwerken. Hier besteht ein erhöhtes Gefährdungspotenzial, da die Hürden zum Wechsel des Kommunikationskanals durch UCC abgebaut werden.

Diese Gefährdung kann sowohl von den Benutzern selbst ausgehen als auch vom Gesamtsystem. Durch Fehlkonfiguration oder Malware (in den IT-Grundschutz-Katalogen auch Schadcode genannte) ist es z. B. möglich, dass via IM oder UM unbemerkt Nachrichten verbreitet werden und somit ein Schaden verursacht wird.

G-TK-49 Unzureichende oder fehlende Konzepte, Regelungen und Prozesse für das Management eines UCC-Systems

Konzepte, Regelungen und Prozesse, die eine TK-Anlage oder ein VoIP-System betreffen, müssen für UCC-Systeme entsprechend erweitert werden. Eine Gefährdung besteht darin, dass sich diese Erweiterung als unzureichend erweist. Kritisch sind dabei diejenigen Elemente, die einen übergreifenden Bezug zwischen Kommunikationssystemen und Applikationen haben, z. B. die Änderung des Rufnummernplans.

G-TK-50 Nicht abgestimmte Konfigurationen und Sicherheitseinstellungen

Technologie- und produktbedingt werden für den Kommunikations- und den Applikationsbereich unterschiedliche Konfigurationen und Sicherheitseinstellungen vorgenommen, die geeignet abzustimmen sind, damit ein einheitliches Sicherheitsniveau gewährleistet ist. Dies beinhaltet sowohl die Einstellungen für einfache Nutzer als auch die Parameter für den administrativen Zugang. Werden diese Einstellungen nicht geeignet abgestimmt, kann es vorkommen, dass in einem Bereich (z. B. auf Seite der Applikation) ein zu geringes Sicherheitsniveau besteht.

6.2.3 Menschliche Fehlhandlungen

Durch die Kopplung von UCC-Lösungen mit Applikationen steigt die Komplexität des Gesamtsystems. Damit wächst zum einen das Risiko einer menschlichen Fehlhandlung, da z. B. die Konsequenzen einer Handlung auf andere Teilsysteme mangels geeigneter Schulung nicht bedacht werden. Zum anderen wachsen auch die potenziellen Auswirkungen auf das Gesamtsystem, da durch die Integration Wechselwirkungen und Abhängigkeiten zwischen den Teilsystemen entstehen.

Damit gelten – sofern technisch anwendbar – grundsätzlich die im Gefährdungskatalog G 3 „Menschliche Fehlhandlungen“ der BSI IT-Grundschutz-Kataloge (siehe [BSI GSK-2013]) aufgeführten Gefährdungen. Es gelten insbesondere die folgenden Gefährdungen:

- G 3.3 „Nichtbeachtung von Sicherheitsmaßnahmen“
- G 3.7 „Ausfall der TK-Anlage durch Fehlbedienung“

Die Auswirkungen der jeweiligen Gefährdungen können jedoch systemübergreifend sein und auf diese Weise erheblich größere Schäden verursachen. Durch das Zusammenspiel verschiedener Dienste können sich Gefährdungen kumulieren. Somit entsteht ein höheres Gefährdungspotenzial als die reine Summe der jeweiligen Gefährdungen.

Ein durch die Fehlbedienung einer Fachapplikation bedingter Ausfall kann z. B. dazu führen, dass das UCC-System nicht mehr korrekt funktioniert. Umgekehrt ist es möglich, dass die Fehlkonfiguration eines UCC-Dienstes gekoppelte TK-Anlagen oder VoIP-Systeme (und damit alle hiervon abhängigen Applikationen) außer Betrieb setzt.

G-TK-51 Zustellung von UM-Nachrichten an falsches Postfach durch Fehlkonfiguration

Bei Fehlkonfiguration eines UM-Systems kann eine versehentliche Zustellung von eingehenden Nachrichten an ein falsches Postfach, z. B. eines nicht berechtigten Dritten, erfolgen. Umgekehrt kann durch fehlkonfigurierte Rufvermittlung und mangelhafte Authentisierungsmechanismen ein unautorisierter Zugriff auf andere UM-Postfächer erfolgen.

G-TK-52 Versehentliche Preisgabe von Informationen durch Verwendung von Video am Desktop

Durch die Verwendung von Desktop-Video und Webkonferenzen mit integrierter Videoübertragung können versehentlich Informationen preisgegeben werden, welche sich im Blickwinkel der für die Videoübertragung verwendeten Kamera befinden. Hierzu zählen insbesondere Informationen, welche sich auf Anzeigen im Hintergrund des Videoteilnehmers (auf Wandtafeln, Whiteboards, Flipcharts etc.) befinden. Zudem kann versehentlich der Aufenthaltsort des Kommunikationspartners enthüllt werden, der ggf. als schützenswert einzustufen ist. Die Gefahr der versehentlichen Preisgabe von Informationen besteht insbesondere bei einer ungeeigneten Wahl des Kamera-Blickwinkels.

G-TK-53 Unbeabsichtigte Preisgabe vertraulicher Informationen durch Application Sharing und Desktop Sharing

Durch die Freigabe von Applikationen oder der Desktop-Ansicht im Rahmen einer Webkonferenz (Application Sharing bzw. Desktop Sharing) können unbeabsichtigt

vertrauliche Informationen preisgegeben werden. Dies kann durch die versehentliche Freigabe der falschen Applikation geschehen. Die Freigabe des gesamten Desktops ist zudem kritisch, da hierauf abgelegte Informationen (z. B. Verknüpfungen, Dateinamen, Dokumente), Statusmeldungen und Benachrichtigungsfenster sowie Inhalte von im Hintergrund geöffneten Applikationen versehentlich preisgegeben werden können. Es kann zudem vorkommen, dass der Freigebende vergisst, die Freigabe im Anschluss wieder aufzuheben, sodass alle Applikationsinhalte während der Konferenz weiterhin eingesehen werden können.

G-TK-54 Fehlkonfiguration von Mehrfachsignalisierung und Weiterleitungen

Bei Verwendung eines One Number Service (ONS), der simultanen Gesprächssignalisierung auf mehreren Endgeräten (Simultaneous Ringing) und der individuellen Konfiguration von Rufweiterleitungen besteht die Gefahr der Fehlkonfiguration von Mehrfachsignalisierungs- und Weiterleitungszielen. Dies gilt insbesondere, wenn der Teilnehmer diese individuell konfigurieren kann. So können, ggf. vom Anwender unbemerkt, Anrufe mit vertraulichem Inhalt an nicht autorisierte Personen weitergeleitet werden.

G-TK-55 Zugriff auf Applikationen oder andere Ressourcen durch Freigabe der Steuerung

Innerhalb von Webkonferenzen kann die Steuerung der freigegebenen Applikationen oder des freigegebenen Desktops an den entfernten Kommunikationspartner übergeben werden. Die Aktionen des Kommunikationspartners werden dann mit den Rechten des Anwenders ausgeführt, welcher die Steuerung freigegeben hat. Hierdurch kann der Kommunikationspartner unbefugten Zugriff auf vertrauliche Informationen erhalten.

6.2.4 Technisches Versagen

Für UCC-Systeme und integrierte Applikationen gelten prinzipiell alle in den IT-Grundschutz-Katalogen genannten Gefährdungen, wie Stromausfall, Datenbankausfall und mangelnde Verschlüsselung, sofern diese für ein konkretes System technisch relevant sind. Aufgrund der Vielfalt UCC-naher Dienste und Applikationen sowie deren unterschiedlichen technischen Ausführungen werden an dieser Stelle keine weiteren applikationsspezifischen Gefährdungen – wie etwa „Ausfall des Web-Conferencing-Servers“ – genannt.

Durch die Integration mehrerer heterogener Komponenten in das Gesamtsystem entsteht allerdings auch für den Bereich „Technisches Versagen“ eine besondere Bedrohungslage.

G-TK-56 Verlust der Verfügbarkeit bei Störung anderer Systemkomponenten

Die Störung bzw. der Ausfall einer integrierten Applikation bzw. des UCC-Systems selbst kann sich – je nach Aufbau des Gesamtsystems und der Ausprägung der Teilsysteme – im Gesamtsystem fortpflanzen. Naturgemäß hat der Ausfall von UCC-Systemen die größten Auswirkungen auf das Gesamtsystem, da die meisten Applikationen auf deren Dienste zurückgreifen. Der Ausfall eines UCC-Systems führt z. B. nicht nur dazu, dass keine Telefongespräche mehr geführt werden können, sondern beeinträchtigt möglicherweise auch die Funktion integrierter Videokonferenzsysteme oder Kontaktcenter-Anwendungen. Es ist jedoch auch denkbar, dass die Störung einer integrierten Applikation oder eines integrierten Kommunikationssystems sich auf die UCC-Lösung und weitere davon abhängige Systeme überträgt. Die Ursache kann beispielsweise in einem Hardware- oder Software-Fehler bei der Integration von webbasierten Applikationen liegen.

G-TK-57 Fehlfunktion von Mehrfachsignalisierung und Weiterleitungen

Bei Verwendung eines One Number Services, der simultanen Gesprächssignalisierung auf mehreren Endgeräten (Simultaneous Ringing) und der Nutzung individueller Rufweiterleitungen besteht die Gefahr einer Fehlfunktion des Dienstes. So können ggf. vom Anwender unbemerkt Anrufe mit vertraulichem Inhalt an nicht berechtigte Personen weitergeleitet werden.

6.2.5 Vorsätzliche Handlungen

Im Bereich der vorsätzlichen Handlungen besteht die wesentliche Gefährdung darin, dass Angriffe eine applikationsübergreifende Wirkung entfalten können. Die Gefährdungslage konzentriert sich dabei auf die IP-basierten Komponenten eines Gesamtsystems, da sich hier die größte Angriffsfläche bietet und auf eine Vielzahl bereits bekannter Angriffsmethoden zurückgegriffen werden kann. Dennoch kann nicht ausgeschlossen werden, dass Angriffe auch über andere Kommunikationswege wie z. B. Fax oder SMS erfolgen, wenn das Gesamtsystem diese Möglichkeiten bietet.

G-TK-58 Übergreifende Wirkung eines Angriffs auf ein UCC-System

Ein Angriff auf ein UCC-System kann sich – je nach Art der Anbindung an andere Systeme, z. B. an eine TK-Anlage, ein VoIP-System oder eine Fachapplikation – im Gesamtsystem fortpflanzen. Beispielsweise könnte ein UCC-System aufgrund einer Überlastung durch eingehende Verbindungsanfragen überlastet werden und somit die Fähigkeit zum Call Routing beeinträchtigt werden. Dies kann Auswirkungen auf einen integrierten Web-konferenz-Dienst haben, der dann für die Teilnehmer nicht mehr erreichbar ist.

G-TK-59 Unbefugte oder missbräuchliche Nutzung eines UCC-Systems

Die unbefugte oder missbräuchliche Nutzung eines UCC-Systems kann in Abhängigkeit von der Art der Dienste und integrierten Applikationen zu unterschiedlichen Gefährdungen führen. Beispielsweise kann die unbefugte Nutzung eines UM-Systems zum Versenden von Fax- und SMS-Nachrichten einen finanziellen Schaden verursachen.

Eine weitere Bedrohung, die im Zusammenhang mit UCC-Systemen von Bedeutung ist, ist das Vortäuschen einer scheinbar vertrauenswürdigen Identität. Die unbefugte Nutzung eines UCC-Systems erlaubt es, einen Angriff auf vielen Kanälen, beispielsweise E-Mail, Fax, Instant Messaging, VoIP oder Mobilkommunikation, durchzuführen.

G-TK-60 Vertraulichkeitsverlust von in UCC-Systemen und integrierten Applikationen gespeicherten Daten

Viele UCC-Systeme und integrierte Applikationen arbeiten mit personenbezogenen Daten und reichen diese unter Umständen an andere Anwendungen weiter. Besonders hervorzuheben sind UM- und Präsenz-Dienste, bei denen die Auswirkungen eines Vertraulichkeitsverlustes aufgrund der zentralen Sammlung von Informationen und der einfachen Weiterverbreitung unterschiedlicher Nachrichtentypen gravierend sein können.

G-TK-61 Angriff auf die Trunk-Verbindungen zwischen UCC-Diensten

Zwischen einzelnen UCC-Diensten bzw. UCC-Systemen ist häufig eine Verbindung in Form eines Trunks erforderlich. So wird z. B. ein UM-System mittels SIP-Trunk an ein VoIP-basiertes Kommunikationssystem angebunden. Diese Server-zu-Server-Verbindung kann durch einen Angreifer abgehört oder manipuliert werden. Selbiges gilt für die Anbindung von Webkonferenzsystemen oder für die Föderation von IM-Diensten. Die Vertraulichkeit und Integrität der übermittelten Informationen ist somit gefährdet.

G-TK-62 Verlust der Vertraulichkeit durch Kompromittierung des UCC-Clients

Aus dem Einsatz von UCC an einem Desktop-PC, Notebook oder mobilen Endgerät ergeben sich zusätzliche Gefährdungen. So werden als UCC-Endgeräte Systeme mit Standard-Betriebssystemen eingesetzt, die aufgrund ihres hohen Verbreitungsgrades stärker für Malware-Bedrohungen exponiert sind als beispielsweise dedizierte Videosysteme oder Tischtelefone mit einem niedrigeren Verbreitungsgrad. Hierdurch entsteht eine generelle Gefährdungslage für die Vertraulichkeit der Kommunikation, der durch Absicherung des verwendeten Clients begegnet werden muss. Generell gelten hier die allgemeinen Gefährdungen für Clients (siehe [BSI GSK-2013]).

G-TK-63 Leistungsüberwachung und Profilbildung durch Präsenzdienste

Präsenzdienste aggregieren eine Vielzahl von nutzer- und anwendungsbezogenen Informationen, z. B. Aktivitäten, Kalender- und Ortsinformationen. Somit ist es bei unbefugtem Zugriff möglich, die Aktivitäten eines Anwenders und seinen Aufenthaltsort nahezu lückenlos zu verfolgen. Somit lassen sich anwenderbezogene Profile erstellen. Diese eignen sich einerseits zur Leistungsüberwachung durch Vorgesetzte in der Organisation, andererseits zur Unterstützung weiterer illegaler Aktivitäten, z. B. die Vorbereitung eines Einbruchs oder Überfalls anhand der Kenntnis des Aufenthaltsortes der Zielperson. Zudem lassen sich z. B. aus Anrufinformationen Erkenntnisse über die Kommunikationsbeziehungen und somit der geschäftlichen oder privaten Verknüpfungen des Anwenders gewinnen. Die Anwendungsfälle reichen von zielgerichteter Werbung bis hin zur Wirtschaftsspionage.

G-TK-64 Abfluss von Informationen via Instant Messaging

Durch den einfach zu bedienenden Kommunikationskanal Instant Messaging und die aus dem privaten Umfeld geprägten Nutzungsgewohnheiten besteht die Gefahr, dass Informationen versehentlich an einen Angreifer übermittelt werden. Verschärft wird diese Problematik durch die häufig integrierte Funktionalität für Peer-to-Peer-Datenübertragungen. Diese Gefahr besteht insbesondere, wenn eine Kopplung des IM-Dienstes per Föderation mit anderen Organisationen, öffentlichen IM-Diensten oder Sozialen Netzwerken implementiert wurde. Durch eine geeignete Namenswahl kann ein Angreifer seine Identität verschleiern und den Eindruck eines organisationsinternen, d. h. berechtigten Anwenders erzeugen.

G-TK-65 Verbreitung von Malware, bösartiger Hyperlinks und Spam via Instant Messaging

Über IM-Dienste lassen sich bösartige Hyperlinks verbreiten. Zudem ermöglicht die häufig vorhandene integrierte Funktion für Peer-to-Peer-Dateiübertragung die einfache Verbreitung von Malware-infizierten Dateien. Durch die scheinbar geschlossene Kommunikationsplattform wird ein Vertrauensstatus zum Kommunikationspartner suggeriert, welcher insbesondere bei großen Installationen und bei der Kopplung mit anderen, eventuell öffentlichen IM-Diensten nicht gegeben ist. Die Unmittelbarkeit der Kommunikation via Instant Messaging verleitet den uninformierten Anwender hierbei zu einem ungerechtfertigten Vertrauen in via IM verbreitete Inhalte und teilweise reflexartigem Klick auf empfangene Hyperlinks und Dateien. Zudem können infizierte UCC-Clients den IM-Kanal zur Weiterverbreitung von Malware nutzen und somit kann IM gleichzeitig als Einfallstor und als Verbreitungsweg in der Organisation dienen. Zusätzlich eignet sich IM als Verbreitungsweg für lästige Werbung (Spam over Instant Messaging, SPIM).

G-TK-66 Ausspähen von IM-Konversationen

Falls ein IM-System Mehrpunkt-Konferenzen (Multiparty Chat) unterstützt, könnte eine IM-Unterhaltung durch einen unbefugten Teilnehmer an der Konferenz ausgespäht werden. Dies ist insbesondere der Fall, wenn keine Teilnehmerliste vorhanden ist, die Aufschluss über die Anwesenheit eines möglichen Angreifers gibt.

G-TK-67 Ungesicherte Aufzeichnung bzw. Protokollierung von Kommunikation

Sowohl Webkonferenzen als auch UM- und IM-Systeme bieten die Möglichkeit, eine Server- oder Client-seitige Aufzeichnung der kommunizierten Inhalte vorzunehmen. Wird diese ungeschützt abgelegt und nicht ausreichend gegen Zugriffe Unbefugter abgesichert, ist ein nachträgliches Ausspähen von Unterhaltungen und ein Informationsabfluss möglich.

G-TK-68 Unberechtigter Zugriff auf Postfächer eines UM- oder Voicemail-Systems

Findet keine ausreichende Authentisierung des Teilnehmers bei Zugriff auf das UM-Postfach statt, ist ein unberechtigter Zugriff auf alle im Postfach enthaltenen Informationen möglich. Als Angriffsvektoren eignen sich das E-Mail-Postfach sowie die Fernabfrage von Postfachinformationen mittels Sprachkommunikation über einen Zugriffsassistenten (Auto Attendant).

G-TK-69 Denial-of-Service auf UM-Postfächer

Durch den massenhaften Versand großer Dateianhänge an ein UM-Postfach kann ein Überlauf des Postfaches provoziert werden und der Anwender vom Empfang weiterer Nachrichten abgeschnitten werden. Die grundlegende Gefährdung ist identisch mit der eines E-Mail-Postfaches (siehe [BSI GSK-2013]).

G-TK-70 Denial-of-Service-Attacken auf UCC-Dienste

Auf UCC-Dienste können auf vielfältige Art und Weise Denial-of-Service-Attacken (DoS-Attacken) durchgeführt werden. Hierfür sind besonders Routing-Instanzen (z. B. Call-Server, UCC-Server), Media-Server (z. B. Konferenzressourcen) und Komponenten an Netzübergängen (z. B. Gateways, Session Border Controller, Firewalls) anfällig (siehe Abbildung 35). Es besteht die Gefahr, dass eine Überlastung der jeweiligen Komponente durch eine übermäßige Anzahl an Verbindungsanfragen entsteht. Zudem können Limitierungen der maximalen Sitzungsanzahl ausgenutzt werden, um durch eine Vielzahl gefälschter und abgebrochener Verbindungsanfragen den Aufbau weiterer Sitzungen durch legitimierte Teilnehmer zu unterbinden. Durch den Aufbau einer Vielzahl von Medienströmen können gering dimensionierte Netzressourcen (z. B. WAN-Anbindungen) überlastet werden und der Aufbau weiterer Sitzungen verhindert werden. Durch die Ausnutzung von Infrastrukturen ohne intelligente Steuerung der Medienstrom-Anzahl auf schmalbandigen Verbindungen (Call Admission Control, CAC) ist sogar der Abbruch existierender Sitzungen möglich.

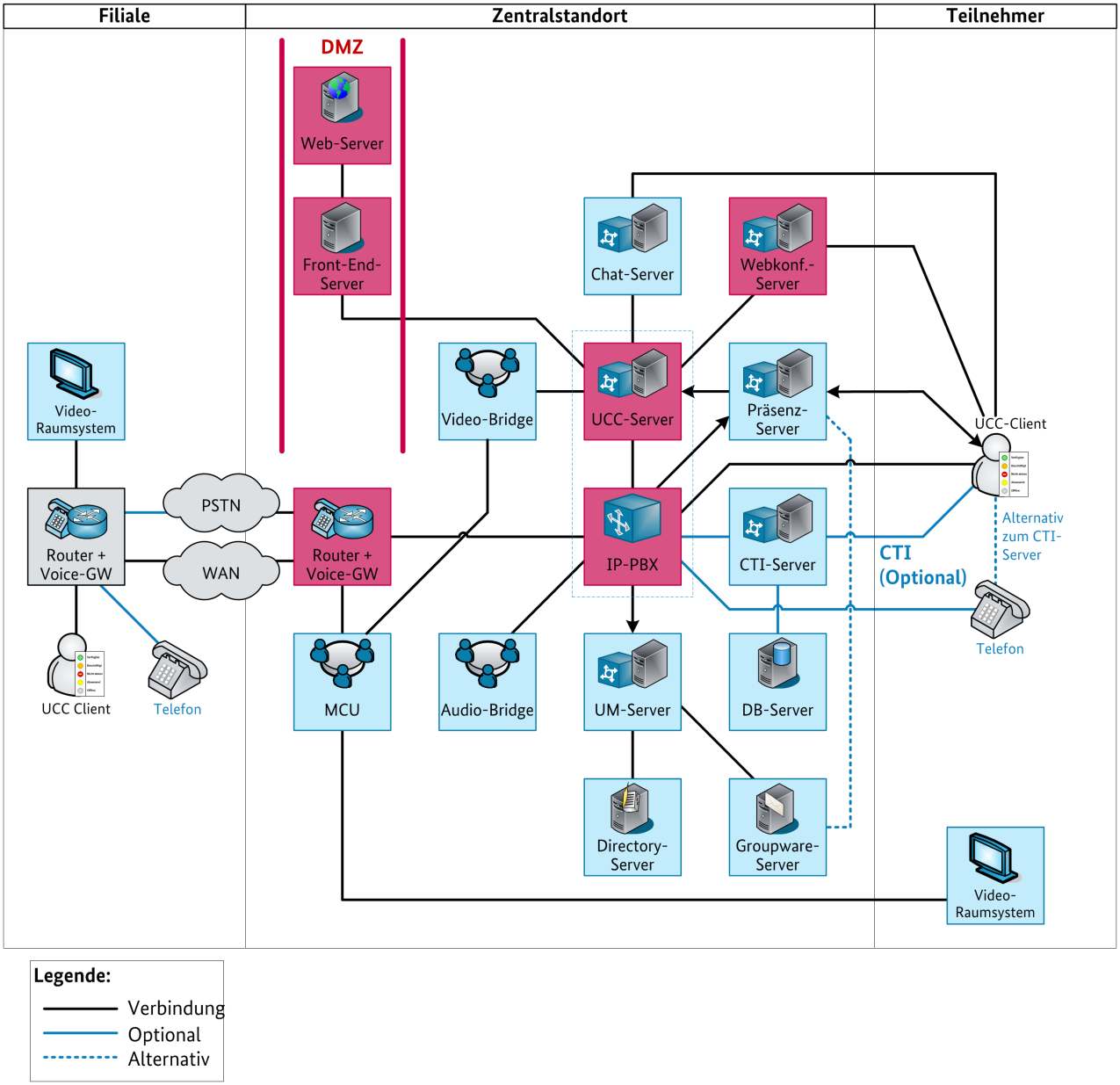


Abbildung 35: Primäre Angriffsziele (rot unterlegt) für DoS-Attacken in einer UCC-Infrastruktur

G-TK-71 Versenden gefälschter Faxe im Namen Dritter

Der Zugriff auf das Unified-Messaging-Dienstkonto eines Dritten kann zum Versenden gefälschter Faxsendungen verwendet werden. Hierdurch droht ein finanzieller Schaden (Gebührenbetrug) und ein Identitätsdiebstahl des Dritten. Durch den Identitätsdiebstahl kann gegebenenfalls die Ausführung nicht autorisierter Handlungen veranlasst werden. Generell gelten für den Faxversand via UM zudem die Gefährdungen für den Faxversand im Allgemeinen. Hierzu sei auf die Gefährdungen für den Faxversand der BSI IT-Grundschutz-Kataloge verwiesen (siehe [BSI GSK-2013]):

- G 5.7 „Abhören von Leitungen“
- G 5.30 „Unbefugte Nutzung eines Faxgerätes oder eines Fax-Servers“
- G 5.31 „Unbefugtes Lesen von Faxsendungen“

- G 5.32 „Auswertung von Restinformationen in Faxgeräten und Fax-Servern“
- G 5.33 „Vortäuschen eines falschen Absenders bei Faxsendungen“
- G 5.34 „Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes“
- G 5.35 „Überlastung durch Faxsendungen“

G-TK-72 Ausspähen von Anwendern und Räumen mittels UCC-Client und Desktop-Video

Durch die zunehmende Verfügbarkeit von Videodiensten an beliebigen, auch mobilen Clients steigt das Risiko einer Überwachung von Räumen und Personen durch integrierte Kameras und Mikrofone. Ein Angreifer kann bei Kompromittierung des Clients oder der genutzten Signalisierungsdienste Kamera und Mikrofon eines UCC-fähigen Endgerätes aktivieren und somit eine Überwachung des Anwenders oder des Raums durchführen. Dies kann vom Anwender unbemerkt geschehen. So kann z. B. ein stiller Anruf eines angegriffenen Tischtelefons, Konferenztelefons oder UCC-Clients durch den Angreifer ausgelöst werden, wenn der CTI-Dienst entsprechend kompromittiert wurde.

G-TK-73 Leistungsüberwachung durch Zugriff auf Videokamera

Durch den unbefugten Zugriff aus der Ferne auf Videokameras am PC-Arbeitsplatz oder mobilen Endgerät, welche für Desktop-Video und Webkonferenzen verwendet werden, kann eine Leistungsüberwachung des Kommunikationspartners erfolgen. Der unerlaubte Zugriff auf die Kameraressourcen des Arbeitsplatzendgerätes kann aus der Ferne durch den unbemerkten Verbindungsaufbau (z. B. durch automatische Rufannahme) oder durch die Fernsteuerung des Endgerätes (z. B. per Malware) erfolgen. Dies gilt zudem auch für weitere Personen im Hintergrund des Kamerabildes, welche auf diese Weise unbemerkt in ihrer Arbeit überwacht werden. Aus Gründen der Privatsphäre und des Arbeitnehmerschutzes sollte dies unbedingt vermieden werden.

G-TK-74 Abfluss von Daten und Informationen via Webkonferenz durch Screenshots oder Copy&Paste

Informationen, welche in Webkonferenzen anderen Kommunikationspartnern freigegeben werden, können durch diese per Screenshot oder – im Fall von Application Sharing und Desktop Sharing – per Copy&Paste abgegriffen werden. Hiervor schützt auch eine Deaktivierung der Aufzeichnungsfunktion des Webkonferenzsystems nicht.

G-TK-75 Vertraulichkeitsverlust durch Kompromittierung von Konferenzbrücken

Bei der Implementierung von Audio-, Video- und Webkonferenzen wird in der Regel auf eine sternförmige Topologie mit einer Konferenzbrücke als zentralem Knoten zurückgegriffen. Hier laufen Kommunikationsinhalte wie z. B. Echtzeitmediendaten, Kurznachrichten und Whiteboard-Inhalte zusammen, um gemischt und an die Teilnehmer verteilt zu werden. Damit dies durch die Konferenzbrücke geleistet werden kann, müssen die Kommunikationsinhalte unverschlüsselt vorliegen. Eine Ende-zu-Ende-Verschlüsselung ist somit nicht mehr möglich. Die Verschlüsselung der Mediendaten wird an der Konferenzbrücke terminiert. Wird nun die Konferenzbrücke kompromittiert (z. B. durch Malware), können Kommunikationsinhalte an dieser Stelle abgehört werden.

G-TK-76 Vertraulichkeitsverlust durch Malware auf Endgeräten mit Softphone oder UCC-Client

Bei Verwendung von Softphones und UCC-Clients besteht die Gefahr eines Vertraulichkeitsverlustes durch Malware. Die Malware kann durch einen Angreifer dazu genutzt werden, sensible Kommunikation noch vor Verschlüsselung bzw. nach Entschlüsselung direkt auf dem Endgerät abzuhören. Zudem kann Malware bewirken, dass anstelle eines einfachen Anrufs unbemerkt eine Dreierkonferenz aufgebaut wird. Hierüber kann der Angreifer unbemerkt die Kommunikation in Echtzeit abhören. Dies gilt gleichermaßen für PC-Endgeräte und mobile Endgeräte, sinngemäß aber ebenfalls für VoIP-Tischtelefone und Video-Terminals. Zu Gefährdungen und Maßnahmen bzgl. PCs und mobilen Endgeräten sei auf Kapitel 9 verwiesen (siehe [BSI GSK-2013]).

G-TK-77 Manipulation von Mehrfachsignalisierung und Weiterleitungen

Bei Verwendung eines One Number Service, der simultanen Gesprächssignalisierung auf mehreren Endgeräten (Simultaneous Ringing) und der Nutzung individueller Rufweiterleitungen besteht die Gefahr, dass die Konfiguration dieser Dienste durch einen Angreifer manipuliert wird. So können, ggf. vom Anwender unbemerkt, Anrufe mit vertraulichem Inhalt an einen Angreifer weitergeleitet werden.

6.3 Sicherheitsmaßnahmen

Im Folgenden werden die Sicherheitsmaßnahmen, die für UCC-Dienste empfohlen werden, beschrieben. Als Grundlage sind alle Sicherheitsmaßnahmen für VoIP-Systeme anzuwenden (siehe Kapitel 4.3), sofern VoIP Basis der betrachteten UCC-Lösung ist. Zudem gelten im Zusammenhang mit Desktop-Video und Webkonferenzen mit Videounterstützung sinngemäß die Maßnahmen zu Videokonferenzen (siehe Kapitel 7.1.3).

Die beschriebenen Ansätze greifen zum Teil auch für andere vernetzte IT-Systeme bzw. auch bei normalem Schutzbedarf. Je nach Szenario und insbesondere für erhöhten Schutzbedarf kommt es darauf an, aus dieser Gesamtheit der Maßnahmen jeweils angemessene Pakete zu bilden.

Der Maßnahmenkatalog zur Absicherung der Nutzung und des Betriebs von UCC-Diensten ist in die folgenden Blöcke aufgeteilt:

- Server und Anwendungen, siehe Kapitel 6.3.1
- Endgeräte und Clients, siehe Kapitel 6.3.2
- Netzwerk, siehe Kapitel 6.3.3
- Netz- und Systemmanagement, siehe Kapitel 6.3.4
- Übergreifende Aspekte, siehe Kapitel 6.3.5

Grundsätzlich wird die Umsetzung der generell zu ergreifenden Maßnahmen (siehe Kapitel 10) vorausgesetzt.

6.3.1 Server und Anwendungen

Es gelten sinngemäß die für die Basistechnologie Voice over IP aufgeführten Maßnahmen bzgl. Server und zentraler Komponenten (siehe Kapitel 4.3.1). Ergänzende Maßnahmen werden im Folgenden dargestellt.

M-TK-87 Absicherung der E-Mail-Kommunikation eines UCC-Systems

Der Austausch von E-Mails zwischen UCC-Systemen und E-Mail-Clients oder anderen Diensten unterliegt den gängigen Gefährdungen der E-Mail-Kommunikation. Im Bereich der UCC-Systeme sind vor allem Unified-Messaging-Server bzw. Fax- und Voicemail-Server betroffen. Abhängig davon, ob es sich um ein True-Unified-Messaging-System mit vereinheitlichtem Posteingang auf dem E-Mail-Server handelt, sind unterschiedliche Schnittstellen zu schützen:

- Im Falle von True Unified Messaging (TUM) ist die Verbindung zwischen E-Mail- und UM-Server zu schützen, welche zum Nachrichtenaustausch benötigt wird und in der Regel auf SMTP oder MAPI-RPC basiert. Bei einer direkten Verbindung der beiden Systeme (z. B. über ein einzelnes Netzwerkkabel) ist diese Verbindung meist nicht schutzbedürftig. Anders stellt sich die Situation bei räumlicher Entfernung, eventuell sogar über die Grenzen des Standortnetzwerks hinaus, oder bei erhöhtem Schutzbedarf dar. Bei der Kommunikation per SMTP kann auf SSL bzw. TLS zur Authentisierung und Verschlüsselung zurückgegriffen werden (siehe auch Kapitel 13.3.3). Bei MAPI-RPC muss man sich auf proprietäre Mechanismen zur Absicherung verlassen.

- Im Falle, dass UM-Server und E-Mail-Server dem Anwender separate Postfächer zur Verfügung stellen, muss der E-Mail-Client Verbindungen zu beiden Servern aufbauen. Wie die Verbindung zwischen Client und E-Mail-Server wird auch für die Verbindung von Client und UM-Server auf gängige Mail-Protokolle zurückgegriffen. Dies sind in der Hauptsache SMTP, POP3 und IMAP. Diese Protokolle sehen ursprünglich nur eine Übertragung der Authentisierungsdaten im Klartext vor. Nachträglich wurden für diese Protokolle Hash-Verfahren für die Authentisierung spezifiziert, welche in der Praxis jedoch nur eine geringe Relevanz besitzen. Effektiver ist die Absicherung der kompletten Datenübertragung mittels SSL bzw. TLS. Dieses Verfahren ist für alle drei Protokolle spezifiziert (siehe auch Kapitel 13.3.3).
- Die Übertragung von Sprachnachrichten zwischen verschiedenen UM-Systemen kann mittels Voice Profile for Internet Mail (VPIM) erfolgen. Dieses Protokoll basiert auf dem Simple Mail Transfer Protocol (SMTP), das mittels SSL/TLS gesichert werden kann. Zudem kann eine Inhaltsverschlüsselung von VPIM-Nachrichten mittels S/MIME erfolgen.
- Zusätzlich zur gesicherten Übertragung zwischen UM- bzw. Fax-Server und E-Mail-Server bzw. E-Mail-Client kann die Integrität der übermittelten Dokumente abgesichert werden. Hierzu eignet sich beispielsweise die Verwendung von signierten Portable Document Files (PDF) anstelle von Tagged Image File Format (TIFF) oder anderer Bildformate. Ein solcher Integritätsschutz geht in der Regel mit einer hohen Systemkomplexität einher und bringt bei ordnungsgemäß authentisierter und verschlüsselter Client-Server-Kommunikation in aller Regel keinen Mehrwert. Diese Option sollte nur in Betracht gezogen werden, wenn den verwendeten Methoden zum Schutz der E-Mail-Kommunikation nicht vertraut werden kann.

Die grundsätzliche Absicherung von E-Mail-Kommunikation ist bereits in den IT-Grundschutz-Katalogen beschrieben. Anwendung finden insbesondere die Maßnahmen:

- M 5.56 „Sicherer Betrieb eines Mailservers“
- M 5.57 „Sichere Konfiguration der Mail-Clients“
- M 5.108 „Kryptographische Absicherung von E-Mail“
- M 5.109 „Einsatz eines E-Mail-Scanners auf dem Mail-Server“

Diese Maßnahmen sind nicht nur auf UM-Systeme sondern auch auf andere UCC-Applikationen mit E-Mail-Schnittstellen anzuwenden.

M-TK-88 Absicherung des Sprachkanals zwischen TK-Anlage bzw. VoIP-Kommunikationssystem und UCC-Systemen

Sprachverbindungen sind bei UCC-Systemen, sei es im Rahmen von Audio-, Video- und Webkonferenzen oder auch der Mobil-Integration, naturgemäß von großer Bedeutung. Sowohl die Sprach- als auch die Signalisierungsdaten können sensible Inhalte haben und dementsprechend schützenswert sein.

Für die genutzten Übertragungswege muss geprüft werden, ob zusätzliche Schutzmaßnahmen ergriffen werden müssen. Besteht ein erhöhter Schutzbedarf oder sind Strecken in unsicheren Netzen zu überbrücken, ist ein Schutz der Verbindungen notwendig. Die Art der Schutzmechanismen unterscheidet sich je nach zugrunde liegender Technik.

- Bei analoger oder digitaler Telefonie kann bei erhöhtem Schutzbedarf auf den Einsatz von Kryptoboxen zurückgegriffen werden (siehe auch M-TK-19 „Geschützte Übertragung von Sprachdaten“).

- Bei IP-basierter Übertragung steht SRTP als verschlüsselte Variante des RTP zur Übertragung von Sprachdaten zur Verfügung (siehe M-TK-31 „Durchgängige Verschlüsselung des Medienstroms“). Alternativ können VPN-Techniken unter Verwendung von IP Security (IPsec) oder TLS/SSL genutzt werden (siehe Kapitel 13.2).
- Zur Sicherung der Signalisierung per SIP kann auf TLS zurückgegriffen werden (siehe auch Kapitel 13.3.3).

Im Kontext IP-basierter Sprachübertragung sind insbesondere die folgenden Maßnahmen zu beachten:

- M-TK-31 „Durchgängige Verschlüsselung des Medienstroms“
- M-TK-32 „Durchgängige Verschlüsselung der Signalisierung“
- M-TK-34 „Authentisierung zwischen Endgeräten und Servern des VoIP-Systems“
- M-TK-35 „Authentisierung zwischen Servern“

M-TK-89 Absicherung von CTI-Verbindungen und Schnittstellen zur Anwendungsintegration

Bei CTI wird zwischen Einzelplatz- und Mehrplatzlösungen unterschieden. Während die direkte Verbindung zwischen Telefon und Rechner bei Einzelplatzlösungen in der Regel aufgrund der räumlichen Nähe und der proprietären, vom restlichen Netzwerk unabhängigen Anbindung keines zusätzlichen Schutzes bedarf, besteht bei Mehrplatzlösungen eine Verbindung zwischen jedem Endgerät und einem zentralen CTI-Server, der für die Steuerung der Endgeräte verantwortlich ist. Diese Verbindung wird oft auf Basis von CSTA realisiert. CSTA kann sowohl über ISDN- als auch über TCP/IP-basierte Verbindungen transportiert werden. Je nach Anbindung des Endgerätes finden verschiedene Verfahren Anwendung:

- Bei einer ISDN-Anbindung sollten Kryptoboxen eingesetzt werden (siehe auch M-TK-19 „Geschützte Übertragung von Sprachdaten“).
- IP-basiertes CSTA sollte durch Verwendung von TLS oder IPsec gesichert werden (siehe auch Kapitel 13.3).

Neben CSTA finden im Bereich der CTI-Applikationen auch viele proprietäre Protokolle Verwendung, deren Umsetzungsdetails durch vom Hersteller angebotene Treiber für TAPI-, JTAPI- und TSAPI-Schnittstellen sowie Webschnittstellen verborgen bleiben. Der Hersteller sollte in diesen Fällen zur grundsätzlichen Möglichkeit einer Authentisierung und Verschlüsselung sowie zur konkreten Konfiguration einer sicheren Verbindung befragt werden. Im Zweifel sollte auch hier die Möglichkeit in Betracht gezogen werden, den gesamten Datenverkehrs zwischen Endgerät oder UCC-Client-Software und UCC-Infrastruktur über ein geeignet gesichertes VPN zu tunneln (siehe auch Kapitel 13.3).

M-TK-90 Absicherung der Kommunikation zwischen UCC-System und weiteren IT-Systemen

Die Kommunikation zwischen UCC-System und weiteren IT-Systemen, z. B. Geschäftsanwendungen bzw. Verwaltungsverfahren, findet auf Basis von unterschiedlichsten Protokollen statt. Neben proprietären Schnittstellen und einer Vielzahl von Protokollen für Remote Procedure Calls (RPCs) kommen auch Standardprotokolle wie etwa HTTP zum Einsatz. Mit der zunehmenden Verbreitung von serviceorientierten Architekturen (SOA) und Web Services halten weitere Protokolle Einzug in die IT-Systeme. Als Beispiele seien hier die XML-basierten Mechanismen zum Prozedur-Fernaufruf Simple Object Access Protocol (SOAP) sowie XML Remote Procedure Call (XML-RPC) genannt. Darüber hinaus bieten weit verbreitete, herstellerabhängige Programmierschnittstellen mit ihren intern verwendeten RPC-Protokollen weitere Angriffsflächen. Hier muss im Einzelnen geprüft werden, wie in der konkreten Implementierung mit den für die Protokolle spezifizierten Sicherheitsmechanismen umgegangen worden ist.

Eine pauschale Antwort, wie die Kommunikation zwischen UCC- und Geschäftsapplikationen abzusichern ist, kann also nicht gegeben werden. Erste Maßnahme sollte es daher sein, die

verwendeten Protokolle durch Nachfrage bei den Herstellern zu ermitteln und sie auf verfügbare Sicherheitsmechanismen zu prüfen. Außerdem kann man in Betracht ziehen, bei erhöhtem Schutzbedarf eigene Schwachstellen-Analysen durchzuführen bzw. deren Durchführung zu beauftragen. Da Sicherheitsmechanismen bei weitem nicht für alle Protokolle zur Verfügung stehen, kann bei erhöhtem Schutzbedarf ein Tunnel, z. B. auf Basis von IPsec, die einfachste und umfassendste Lösung sein (siehe auch Kapitel 13.3). Bei erhöhtem Schutzbedarf sollte jedoch im Zweifel auch in Betracht gezogen werden, von einer Integration von UCC- und IT-Anwendungen Abstand zu nehmen (siehe auch M-TK-228 „Produktauswahl von TK-Lösungen unter Berücksichtigung von Sicherheitsaspekten“).

M-TK-91 Absicherung der Kommunikation zwischen UCC-System und Datenbank

Oftmals ist der Zugriff von UCC-Diensten auf Datenbanken notwendig, sei es um Abfragen und Manipulationen am Organisationsverzeichnis durchzuführen (z. B. mittels Lightweight Directory Access Protocol, LDAP) oder um Datenbestände wie Kundendaten oder die Lagerhaltung in die UCC-Lösung einzubeziehen. Wichtig ist die umsichtige Vergabe von Zugriffsrechten auf Datenbanken und Verzeichnisse. Dem UCC-System sollten nur solche Zugriffsrechte erteilt werden, die für eine sinnvolle Nutzung notwendig sind. Darüber hinaus sollte der entstehende Datenverkehr bei einem erhöhten Schutzbedarf durch Verschlüsselung gesichert werden.

LDAP sieht zunächst keinerlei Verschlüsselungsmechanismen vor und überträgt auch Authentisierungsdaten im Klartext. Die Verwendung von TLS zur Verschlüsselung der gesamten Kommunikation ist allerdings im aktuellen Standard LDAPv3 spezifiziert und bei einer Nutzung dringend anzuraten. Alternativ können zur Absicherung der Kommunikation VPN-Techniken angewandt werden.

Datenbankzugriffe unterliegen ähnlichen Gefährdungen wie Verzeichniszugriffe mittels LDAP. Die Kommunikation zwischen z. B. einem ODBC-Treiber und der Datenbank über ein Netzwerk findet oft anhand proprietärer Protokolle statt, oft sogar im Klartext. Bei erhöhtem Schutzbedarf sollte die Verbindung mittels IPsec oder TLS abgesichert werden (siehe auch Kapitel 13.3).

M-TK-92 Schutz vor unberechtigtem Zugriff auf Datenbanksysteme

Datenbanksysteme, deren Datenbestände durch das UCC-System verwaltet (z. B. Call Records) werden oder durch Kopplung mit dem UCC-System in diesem genutzt werden (z. B. CRM-System), können sensible Informationen (z. B. personenbezogene Daten) enthalten. In diesem Fall muss ein wirksamer Zugriffsschutz implementiert werden.

Eine grundlegende Maßnahme ist die Implementierung eines Rechtesystems zum Schutz vor unberechtigtem Zugriff. Eine weiterführende Schutzmaßnahme bei erhöhtem Schutzbedarf ist die Verschlüsselung der Datenbestände. Idealerweise werden hier sensible Datenbank-Inhalte bereits bei Ablage in das Datenbanksystem transparent verschlüsselt. Alternativ kann auch der gesamte Datenbankinhalt verschlüsselt werden. Falls diese Varianten technisch oder wirtschaftlich nicht tragfähig sind, kann alternativ das Speicher-Back-End zur dauerhaften Speicherung der Datenbankinhalte und von Datenbank-Backups auf Datei- bzw. Datenträgerebene verschlüsselt werden.

M-TK-93 Absicherung der Kommunikation eines Präsenzsystems

Präsenzinformationen sind, auch wenn Privatanwender oft sorglos mit ihnen umgehen, gerade im Geschäftsumfeld sensible Informationen. Neben der Verfügbarkeit eines Anwenders geben sie eventuell Informationen über den aktuellen Aufenthaltsort und die jeweilige Betätigung preis. Daher ist es unumgänglich, auch Präsenz- und Instant Messaging-Systeme durch Verschlüsselung und Authentisierung zu sichern. Ein probates Mittel ist hier der Einsatz von TLS zwischen Client und Präsenz-Server (siehe auch Kapitel 13.3). Dieses Verfahren wird zumindest auch von den beiden wichtigsten Protokollstandards XMPP und SIP/SIMPLE vorgesehen.

Auch eine Verschlüsselung und Authentisierung der Kommunikation von Servern bzw. Gateways untereinander kann mittels TLS vorgenommen werden. Alternativ hierzu kann eine ungesicherte Verbindung zwischen Infrastruktursystemen durch einen IPsec-Tunnel abgesichert werden.

Bei der Anbindung (Föderation) eines externen Systems (z. B. Partnerorganisation oder öffentlicher Präsenzdienst) muss die Vertrauenswürdigkeit und das Schutzniveau des föderierten Systems festgestellt werden. Kann ein hinreichender Schutz der Präsenzinformationen nicht sichergestellt werden, so sollte die Übermittlung von Präsenzinformationen vermieden werden. Es muss mindestens eine Möglichkeit zur Einschränkung der Weitergabe von Präsenzinformationen Einzelner bestehen. Auch an vertrauenswürdige föderierte Systeme übermittelte Präsenzinformationen müssen durch Authentisierung und Verschlüsselung geschützt werden. Falls dies nicht möglich ist, sollte bei erhöhtem Schutzbedarf die Weitergabe von Präsenzinformationen vollständig unterbunden werden.

M-TK-94 Vermeidung der Speicherung von Präsenzinformationen

Die durch das Präsenzsystem erfassten Anwesenheitszustände, Orts- und Statusinformationen sollten nicht an zentraler Stelle mitgeschnitten und gespeichert werden (engl. Logging). Dies ermöglicht andernfalls eine systematische Leistungsüberwachung aller oder einzelner Mitarbeiter. Zudem besteht die Gefahr, dass sensible Informationen zum Aufenthaltsort der Teilnehmer erhoben, analysiert und missbräuchlich eingesetzt werden. Neben der Leistungsüberwachung durch Mitarbeiter der Organisation besteht zudem die Gefahr, dass sich unberechtigte Dritte von außerhalb Zugriff auf die im Präsenzsystem gespeicherten Informationen verschaffen.

Falls eine Speicherung aufgrund besonderer Anwendungsfälle notwendig sein sollte bzw. systembedingt nicht vermieden werden kann, muss eine missbräuchliche Verwendung der Informationen unbedingt vermieden werden. Hierzu müssen

- das Präsenzsystem durch Härtung vor unerlaubtem Zugriff geschützt,
- das Präsenzsystem in einer gesicherten Netzzone positioniert,
- klare Regelungen zum Zugriff auf und Umgang mit Präsenzinformationen geschaffen,
- klare organisationsinterne Regelungen gegen Leistungsüberwachung getroffen,
- der Zugriff auf Präsenzinformationen durch Implementierung von Zugriffsrechten geschützt sowie
- der Zugriff auf Präsenzinformationen zur Leistungsüberwachung durch differenzierte Zugriffsrechte verhindert werden.

Falls diese Maßnahmen nicht wirksam umgesetzt werden können, ist ggf. auf einen Einsatz von Präsenzdiensten zu verzichten.

M-TK-95 Einschränkung der Sichtbarkeit von Präsenzinformationen

Auch wenn der unbefugte Zugriff durch Außenstehende auf Präsenzinformationen mithilfe von Verschlüsselung und Authentisierung unterbunden wird, ist innerhalb des authentisierten Nutzerstamms eine Einschränkung der grundlegenden Sichtbarkeit von Präsenzinformationen notwendig. Die Präsenzinformation eines Nutzers sollte daher vor Zugriff durch andere Nutzer des Präsenzsystems geschützt bleiben, sofern nicht eine individuelle Freigabe der Information erfolgt ist (Nutzer, die eine solche individuelle Freigabe erhalten haben, werden üblicherweise „Buddy“, englisch für Kumpel, genannt). Um dies zu ermöglichen, muss das verwendete Präsenzsystem über einen Mechanismus verfügen, der es den Administratoren oder besser noch den Nutzern erlaubt, die Sichtbarkeit von Präsenzinformationen einzuschränken.

Auch aus Datenschutzgründen muss es dem Benutzer möglich sein, die Sichtbarkeit der eigenen Präsenzinformationen nach außen zu steuern.

M-TK-96 Differenzierung der Sichtbarkeit von Präsenzinformationen

Auch wenn ein Nutzer den Personenkreis, der grundsätzlich Zugriff auf die eigene Präsenzinformation besitzt, definieren kann, ist eine weitere Differenzierung der bereitgestellten Informationen notwendig. So ist es für bestimmte Personen wie zum Beispiel Teamleiter hilfreich, die Verfügbarkeit, die private Telefonnummer oder auch den Aufenthaltsort der Mitarbeiter einsehen zu können. Jedoch sollten nicht alle Nutzer des Präsenzsystems auf solch detaillierte Informationen zugreifen können. Um eine differenzierte Freigabe von Informationen zu ermöglichen, muss das verwendete Präsenzsystem über eine Rechtehierarchie verfügen, die es den Administratoren oder besser noch den Nutzern erlaubt, die Sichtbarkeit von Präsenzinformationen pro Benutzer oder Benutzergruppe einzuschränken.

M-TK-97 Verhindern der Verbreitung von Malware und bösartigen Hyperlinks per Instant Messaging

Mit Instant Messaging besteht ein weiterer Verbreitungsweg für schadenstiftende Software und bösartige Hyperlinks. Dies gilt auch für den Peer-to-Peer-Dateitransfer, der Bestandteil vieler Instant-Messaging-Clients ist. Durch die Übertragung von (eingebetteten) Bilddateien besteht zudem die Möglichkeit der Verbreitung von Malware. Daher ist der Einsatz eines Virenscanners zu empfehlen, der auch die Kommunikation über Instant Messaging berücksichtigt. Dieser sollte die über Instant-Messaging-Clients versendeten Dateien Client-seitig auf Malware untersuchen. Idealerweise überprüft ein solches Produkt auch empfangene Hyperlinks und Bilder auf Bösartigkeit bzw. eingebettete Malware.

Bei einer dezentralen Untersuchung am Client sollte idealerweise mindestens das Management dieser Komponenten sowie die Definition der Filterregeln zentral erfolgen können, um den Management-Aufwand zu minimieren und die Konsistenz sicherzustellen. Zudem sollte die Lösung optimalerweise ein Bestandteil des allgemeinen Malware-Schutzes am Client sein. Somit wird die Unterstützung der eingesetzten UCC-Lösung ein relevantes Auswahlkriterium für den Malware-Schutz.

Wenn die Systemarchitektur dies erlaubt, könnte alternativ auch eine Filterung auf Malware und schadenstiftende Hyperlinks an zentraler Stelle, z. B. an einem zentralen XMPP-Gateway, stattfinden. Hierzu müsste allerdings der Peer-to-Peer-Datenverkehr wie z. B. Dateitransfer immer über zentrale Gateways ausgeliefert werden. Dies wird nicht von allen Lösungen unterstützt und muss ggf. bei der Dimensionierung der Systeme und der Planung von Netzressourcen berücksichtigt werden. Zudem muss die eingesetzte Verschlüsselung durch das Gateway bzw. der zentrale Malware-Schutz im Sinne eines freundlichen Man-in-the-Middle aufgebrochen werden. Hierbei ist zu beachten, dass das Gateway bzw. der zentrale Malware-Schutz eine besondere Vertrauensstellung einnimmt und dessen Integrität sichergestellt werden muss. Dies bedarf einer grundlegenden Härtung und ggf. einer Positionierung dieser Systeme in einer geschützten Netzzone.

Falls diese Maßnahmen mit der gewählten UCC-Lösung nicht umzusetzen sein sollten, muss eine Deaktivierung des Peer-to-Peer-Dateitransfers, der Übertragung von Hyperlinks und der Übertragung von Bilddateien in Betracht gezogen werden.

M-TK-98 Vermeidung von Spam over Instant Messaging

Spam over Instant Messaging **(SPIM) bezeichnet die Verbreitung von unerwünschter Werbung (Spam) über Kurznachrichten. SPIM ist vor allem zu erwarten, wenn eine Verbindung zwischen** der organisationsinternen IM-Lösung und einem öffentlichen IM-Dienst besteht. Eine solche Föderation zweier IM-Dienste eignet sich dann zum Versand von SPIM, wenn ein massenhafter Versand an „erratene“ Adressen unbekannter Adressaten möglich ist. Um dies zu vermeiden, kann der Empfang von Nachrichten auf bekannte Absender eingeschränkt werden. Hierfür bieten einige Lösungen auf den zentralen IM-Servern eine automatische Filterung von Kommunikation anhand der eigenen Kontaktliste. Alternativ könnte SPIM aus externen Quellen auch am zentralen Übergang der Föderation durch eine Security Appliance herausgefiltert werden, wie dies auch in Maßnahme M-TK-69 „Erkennung

und Abwehr von DoS-Angriffen gegen VoIP und von SPIT durch IPS / IDS“ zur Vermeidung von Spam over Internet Telephony (SPIT) beschrieben wird. Bei der organisationsinternen Kommunikation via IM stellt SPIM in aller Regel keine Gefährdung dar.

M-TK-99 Verhinderung des Datenabflusses durch Data Loss Prevention

Sowohl über Instant Messaging als auch über die häufig in IM-Clients integrierte Funktion zum Peer-to-Peer-Dateitransfer können sensible Informationen an Dritte abfließen. Zur Verhinderung eines Datenabflusses kann ein System für Data Loss Prevention (DLP, auch Data Leak / Leakage Prevention genannt) eingesetzt werden.

DLP-Systeme prüfen, klassifizieren und autorisieren Transaktionen zur Datenübertragung und -verarbeitung. Beispiele hierfür sind das Kopieren von Daten auf einen Wechseldatenträger oder die Übermittlung einer Datei als E-Mail-Anhang an einen externen Empfänger. Hierfür müssen zunächst die Transaktion und die betroffenen Daten festgestellt werden. Dann wird die Klassifizierung der Daten auf Basis von statischen Dateiattributen oder mithilfe dynamischer Erkennungsalgorithmen bestimmt. Im Anschluss wird die Legitimität einer Transaktion, z. B. anhand der Berechtigungsstufe von Sender und Empfänger bei einem Sendevorgang, überprüft und hieraus Aktionen abgeleitet. Das Aktionsspektrum reicht vom Zulassen oder Verhindern der Transaktion bis hin zur Information einer zentralen Stelle (z. B. des IT-Sicherheitsbeauftragten) über kritische Vorgänge.

Um DLP im Kontext von UCC sinnvoll einsetzen zu können, muss das DLP-System in der Lage sein, alle Datei-Transaktionen über das UCC-System zu erkennen und zu klassifizieren. Bei DLP-Systemen unterscheidet man grundsätzlich zwei unterschiedliche Ansätze (siehe Abbildung 36):

- Netzwerk-basierte DLP erkennt und verhindert Transaktionen an einem zentralen Netzknotenpunkt.
- Host-basierte DLP erkennt und verhindert Transaktionen am Server bzw. Client.

Darüber hinaus sind Kombinationen der beiden Ansätze möglich.

Netzwerk-basierte DLP-Systeme können überall dort zum Einsatz kommen, wo eine zentrale Kontrolle der Datenströme möglich ist. Im Falle von UCC-Systemen ist dies in der Regel für den Dateiaustausch über Webkonferenz-Systeme und Peer-to-Peer-Dateiübertragung zu externen Teilnehmern der Fall. Hierbei muss die verschlüsselte Kommunikation zur Untersuchung durch das DLP-System im Sinne eines freundlichen Man-in-the-Middle aufgebrochen werden. Das DLP-System muss daher gehärtet und in einer gesicherten Netzzone positioniert werden. Dieser Ansatz eignet sich besonders, wenn nur die organisations- bzw. systemübergreifende Kommunikation mittels DLP gesichert werden soll.

Host-basierte DLP-Systeme eignen sich für die Überwachung sowohl organisationsinterner als auch organisationübergreifender Kommunikation und insbesondere für die Peer-to-Peer-Dateiübertragung. Damit Host-basiertes DLP wirksam eingesetzt werden kann, muss die Vertrauenswürdigkeit und Integrität der jeweiligen Hosts gewährleistet sein, da ansonsten die auf dem Host installierten DLP-Agenten kompromittiert werden könnten (Lying-Endpoint-Problem). Der Einsatz von Host-basiertem DLP ist insbesondere dann sinnvoll, wenn Peer-to-Peer-Kommunikation kontrolliert und deren Ende-zu-Ende-Verschlüsselung nicht aufgebrochen werden soll. Sie eignet sich besonders für die Kontrolle des organisationsinternen Dateitransfers. Die organisationsinterne Verwendung von DLP ist nur dann zielführend, wenn Dateien und Daten unterschiedlicher Klassifizierungen zwischen Anwendern mit unterschiedlichen Berechtigungsstufen ausgetauscht werden sollen.

Falls der Schutzbedarf den Einsatz von DLP innerhalb der UCC-Lösung sinnvoll erscheinen lässt, wird dies aller Wahrscheinlichkeit nach auch für weitere IT-Dienste, wenn nicht für die gesamte IT-Infrastruktur gelten. Bei einem isolierten Einsatz allein für UCC-Systeme wird der Nutzen des Systems in Frage gestellt. Die Einführung eines DLP-Systems ist in aller Regel mit erheblichen Aufwendungen und Auswirkungen auf die Prozesse einer Organisation

verbunden, da jedes Dokument und jedes Datum einer Klassifizierung unterworfen werden muss. Die isolierte Betrachtung ist also insbesondere in Hinblick auf das Kosten-Nutzen-Verhältnis nicht zu empfehlen.

Der Einsatz von DLP-Systemen muss zudem unter Wirtschaftlichkeitsaspekten sinnvoll abgewogen werden. Hierbei stehen die direkten und indirekten Kosten des Systems dem Mehrwert einer Dateitransfer-Funktion gegenüber. Falls auf Funktionen zum Dateitransfer verzichtet werden kann, kann deren schlichte Deaktivierung die Mehrkosten für ein UCC-fähiges DLP-System überflüssig machen. Hier ist eine Einzelfall-Abwägung empfehlenswert.

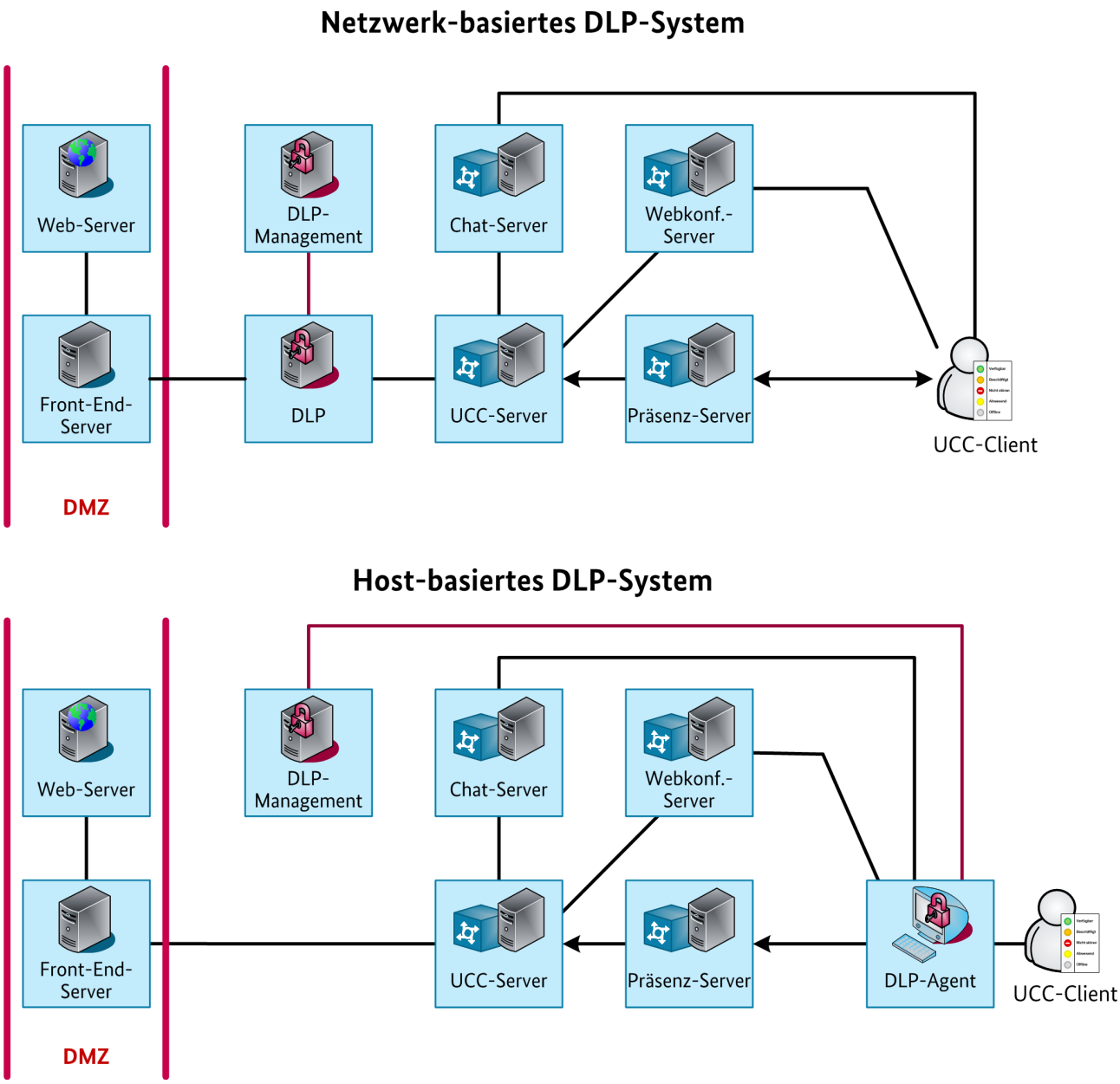


Abbildung 36: Host-basiertes versus Netzwerk-basiertes DLP-System im UCC-Kontext

M-TK-100 Sicherung von Konferenzräumen

Von UCC-Systemen bereitgestellte virtuelle Konferenzräume (Audio, Video, Web und Chat) müssen vor unberechtigtem Zugriff und der unbemerkten Anwesenheit von Angreifern geschützt werden.

Während im Bereich der Chat- und Webkonferenzen in der Regel eine Teilnehmerauthentisierung anhand von Nutzername und Passwort durchgeführt wird, wird bei Audio- und Videokonferenzen häufig eine Authentisierung auf Basis einer PIN durchgeführt. Dies gilt auch für die Telefoneinwahl in eine Webkonferenz über das öffentliche Festnetz. Zu beachten ist hierbei, dass die PIN häufig nicht personenbezogen ist, sondern für alle Nutzer eines Konferenzraumes identisch ist. Dies kann sogar soweit gehen, dass die PIN nicht nur für eine anberaumte Konferenz gilt, sondern zeitlich unbestimmt für den Konferenzraum. Um den Beitritt nicht gewünschter Teilnehmer zu verhindern oder zumindest zu erschweren, können Konferenzsysteme auf folgende Weise gesichert werden:

- Vergabe von persönlichen PINs für jeden Teilnehmer und individuellen Konferenz-PINs
- Schließung des Konferenzraums durch den Moderator, sobald alle gewünschten Teilnehmer beigetreten sind
- Beitritt in eine Konferenz nur durch Hinzuschalten eines Teilnehmers durch den Moderator

Denkbar ist auch eine Authentisierung des verwendeten Endgerätes per Zertifikat oder die Eingabe von Nutzername und Passwort. Das erste Verfahren ist nur in rein IP-basierten Systemen möglich. Das zweite Verfahren erfordert eine alphanumerische Tastatur am Endgerät.

Es muss zudem verhindert werden, dass an Gesprächen und Konferenzen unbemerkt Dritte teilnehmen. Hierbei ist, neben dem Schutz durch Verschlüsselung und Authentisierung, besonders wichtig, dass die Teilnehmer einer Konferenz über die Teilnahme Dritter informiert werden. Dies kann im Fall von Audio-, Video- und Webkonferenzen z. B. über ein akustisches Aufmerksamkeitssignal oder die Nennung des Namens des neuen Teilnehmers erfolgen. Zudem ermöglichen UCC-Clients und Web-Clients zur Konferenzsteuerung das Einblenden einer Teilnehmerliste. Diese sollte sich im Regelfall zur Kontrolle auf unbemerkte und unbefugte Teilnehmer im Vordergrund des Bildschirms befinden und sollte nicht dauerhaft ausgeblendet werden. Zudem muss mindestens durch den Moderator die Teilnehmerliste kontrolliert und die Teilnahme anonymer Teilnehmer unterbunden werden.

Generell sollten Konferenzräume jedweder Art vor unbefugter Nutzung geschützt werden. Die Prüfung der Zugangsberechtigung ist jedoch bei der Absicherung von Audiokonferenzräumen, z. B. durch PINs, von besonderer Bedeutung, da die im Raum befindlichen Teilnehmer nicht immer ermittelt werden können. Es müssen daher Maßnahmen zum Umgang mit PINs implementiert werden, u. a. Regelung zur Weitergabe von PINs und Festlegung einer minimalen PIN-Komplexität. Zu beachten ist jedoch, dass eine PIN häufig für einen bestimmten Raum gilt und damit allen Teilnehmern bekannt sein muss. Eine Authentisierung der einzelnen Teilnehmer findet in diesem Fall nicht statt, d. h. jeder, der die PIN kennt, kann sich in den Konferenzraum einwählen. In diesem Zusammenhang ist die Meldefunktion vieler Audiokonferenzsysteme sehr hilfreich, da sie den Eintritt bzw. das Austreten einzelner Teilnehmer akustisch meldet. Zudem besteht bei einigen Systemen die Möglichkeit, dass dem Moderator auf einer Webseite alle Teilnehmer angezeigt werden und einzelne Teilnehmer entfernt werden können. Die PIN zur Absicherung eines Konferenzraumes sollte zudem regelmäßig geändert werden, um die dauerhafte Kompromittierung einzelner Räume zu vermeiden.

M-TK-101 Sicherer Umgang mit Gesprächs- und Konferenzaufzeichnungen

Die Aufzeichnung von Gesprächen bzw. Konferenzen muss den teilnehmenden Parteien im Vorfeld bekannt gegeben werden. Hierzu ist eine Vorabinformation in Form einer Ansage (Audio-/Video-/Webkonferenz) bzw. einer eingeblendeten Benachrichtigung (Video-/Webkonferenz) sinnvoll. Zudem sollte bei Aktivierung bzw. Deaktivierung der Aufzeichnung ein im Vorfeld bekannt gegebener Aufmerksamkeitston ausgelöst werden. Die Aufzeichnung von Gesprächen und Konferenzen kann am Client oder am Konferenz-Server stattfinden. Wenn Gespräche mit sensiblen Inhalten aufgezeichnet werden sollen, müssen am

Client erstellte Aufzeichnungen in das Konzept zur sicheren Datenhaltung integriert und gegebenenfalls durch Maßnahmen zur Data Loss Prevention erfasst werden. Wenn sich dies als nicht praktikabel erweisen sollte, ist die Client-seitige Aufzeichnungsfunktion zu deaktivieren. Server-seitig erstellte und gespeicherte Aufnahmen sind ebenfalls vor unbefugtem Zugriff zu schützen. Der Zugriff muss durch ein Berechtigungssystem abgesichert werden. Je nach Sensibilität der aufgezeichneten Informationen kann ein zusätzlicher Schutz im Sinne eines Vier-Augen-Prinzips implementiert werden. Kann ein wirksamer Zugriffsschutz nicht sichergestellt werden, so ist auf eine Bereitstellung der Aufzeichnungen über das Netzwerk zu verzichten.

M-TK-102 Absicherung des telefonischen Zugriffs auf UCC-Anwendungen durch eine PIN

Falls aus technischen Gründen keine Authentisierung auf Basis von Zertifikaten oder Nutzerdaten realisierbar ist, muss jede sensible UCC-Anwendung zumindest durch eine PIN geschützt werden. Zu diesen Applikationen zählen zum Beispiel Unified-Messaging-Server mit telefonischem Zugriff auf den Posteingang, Webkonferenzen oder Audiokonferenzsysteme.

Da eine PIN im Gegensatz zu Passwörtern nur aus Zahlen und nicht aus alphanumerischen Zeichen besteht, ist es nicht möglich, den Grad der Komplexität durch das Hinzufügen von Buchstaben und Sonderzeichen zu erhöhen. Einzige Möglichkeit ist der Einsatz einer längeren PIN. Als absolutes Minimum gelten 4-stellige PINs, eine Länge von 6 oder mehr Stellen ist aber dringend empfehlenswert (siehe BSI IT-Grundschutz-Kataloge, M 2.11 „Regelungen des Passwortgebrauchs“). Des Weiteren sind triviale PINs wie z. B. ‚0000’, ‚4321’ oder simple Muster auf dem numerischen Tastaturblock zu vermeiden.

Um die fehlende Komplexität gegenüber alphanumerischen Passwörtern auszugleichen, ist es sinnvoll, bei wiederholter falscher Eingabe der PIN den Zugriff auf den UCC-Dienst zumindest temporär zu sperren.

Alternativ kann der Zugriff auch über temporäre Passwörter oder PINs, z. B. Transaktionsnummern (TAN) für mobile Endgeräte (mobile TAN oder auch mTAN), abgesichert werden. Dies kann auch zum Aufbau einer Zweifaktor-Authentisierung genutzt werden.

M-TK-103 Einschränkung der Zugriffsrechte

UCC-Dienste verbinden in vielen Fällen unterschiedliche Anwendungsdomänen wie z. B. Telefoniedienste mit Kundendatenbanken oder betriebswirtschaftlicher Software. Als konkretes Beispiel sei die Kopplung eines VoIP-Kommunikationssystems mit einem CRM-System über einen CTI-Server genannt. Diese Brückenfunktion kann das Sicherheitsniveau des VoIP-Systems, der Anwendung sowie darüber hinausgehend auch anderer IT-Systeme herabsetzen.

Abhängig vom geforderten Schutzbedarf sind daher die Zugriffsrechte der beteiligten Dienst- und Nutzerkonten geeignet einzuschränken, um einen unerlaubten bzw. unvorhergesehenen Durchgriff auf Informationen zu vermeiden. Die spezifischen Maßnahmen hängen dabei vom betrachteten Dienst bzw. auch vom Produkt ab. Folgende Aspekte sind bei erhöhtem Schutzbedarf zu beachten:

- Wenn Zugriffsrechte auf Basis von Benutzerkonten definiert werden, so ist die Verwendung eines zentralen oder zumindest synchronisierten Benutzerverzeichnisses einer getrennten Rechteverwaltung für unterschiedliche Anwendungsdomänen vorzuziehen. Auf diese Weise kann eine unkoordinierte bzw. unkontrollierte Rechtevergabe vermieden werden.
- Benötigen die betrachteten UCC-Dienste spezielle Dienstkonten, so sind deren Zugriffsrechte soweit einzuschränken, dass ausschließlich die für die Ausführung des Dienstes notwendigen Rechte zur Verfügung stehen. Auf diese Weise kann der Schaden, der durch eine unberechtigte Nutzung eines Dienstkontos (z. B. durch Malware) entstehen kann, minimiert werden.

M-TK-104 Einschränkung von Weiterleitungszielen und gleichzeitiger Rufsignalisierung

Das Weiterleiten von Anrufen und die gleichzeitige Rufsignalisierung auf mehreren Endgeräten spielt in der Anwendungspraxis eine große Rolle. Jedoch besteht die Gefahr, dass durch unbedachtes Weiterleiten eines Rufes bzw. durch Fehlkonfiguration eines Weiterleitungsziels Dritte Kenntnis von vertraulichen Vorgängen erlangen. Daher sollten Weiterleitungen und gleichzeitige Rufsignalisierungen nur an vertrauenswürdige Nebenstellen erfolgen.

Da durch die gleichzeitige Signalisierung von Rufen, insbesondere im Zusammenhang mit der Integration mobiler Endgeräte, ein erheblicher Praxisnutzen entsteht, sollte diese Möglichkeit nicht generell deaktiviert werden. Vielmehr ist die Einschränkung der Konfigurationsmöglichkeiten des Anwenders zielführend. Die Auswahl des Weiterleitungsziels durch den Anwender wird auf eine Liste vertrauenswürdiger Ziele begrenzt. Hierzu zählen z. B. das persönliche mobile Endgerät sowie die interne Durchwahl eines Stellvertreters. So kann eine bewusste oder unbewusste Fehlkonfiguration durch den Anwender vermieden werden.

Falls die eingesetzte Lösung die Einschränkung auf vertrauenswürdige Weiterleitungsziele nicht unterstützt, sollte bei erhöhtem Schutzbedarf auf den Einsatz von Rufweiterleitungen und One Number Service bzw. Single Number Reach verzichtet werden.

M-TK-105 Deaktivierung der CTI-Funktion für Konferenztelefone

Durch CTI ist eine unbemerkte Fernsteuerung von Telefonendgeräten und ein stiller Anruf eines Endgerätes bei einem Angreifer möglich. Um die Auswirkung einer solchen Attacke zu minimieren, sollten bei Einsatz von CTI die in Konferenzräumen eingesetzten Endgeräte (z. B. Konferenzspinnen) grundsätzlich von der Fernsteuerung per CTI ausgenommen werden.

6.3.2 Endgeräte und Clients

Es gelten sinngemäß die im Kapitel VoIP aufgeführten Maßnahmen bzgl. der Endgeräte (siehe Kapitel 4.3.2). Ergänzende Maßnahmen werden im Folgenden dargestellt.

M-TK-106 Absicherung von UCC-Systemen auf Ebene der Endgeräte

Viele UCC-Dienste basieren darauf, dass sie Dienste, die typischerweise über einen PC oder über eine spezielle Hardware bedient werden, auch sprachgesteuert über das Telefon anbieten. Als Beispiel sei hier der Zugriff auf das E-Mail-Postfach per Telefon genannt. Umgekehrt lässt sich auf viele Dienste, die üblicherweise über das Telefon bzw. die TK-Anlage genutzt werden, auch per PC zugreifen. Anrufjournale und die Web-basierte Konfiguration von Telefonen sind Beispiele für solche Dienste. Eine dritte Kategorie wiederum verwendet die Browser-Funktion moderner Telefone, um beliebige Dienste (z. B. Zeiterfassung, Lagerverwaltung) bereitzustellen.

Die Tatsache, dass solche Dienste auf mehreren Wegen erreicht und gesteuert werden können, hat für die Benutzer praktische Vorteile, stellt jedoch auch eine Gefährdung eines UCC- und IT-Systems dar. Ein Dienst kann nur so sicher sein wie der am schwächsten geschützte Zugang.

Für den erhöhten Schutzbedarf muss daher jedes Endgerät geeignet gesichert sein, um eine unbefugte Nutzung von UCC-Diensten zu vermeiden. Für PC-Applikationen gelten hier die Empfehlungen der IT-Grundschutz-Kataloge. Der Zugang zu Telefonen und anderen Endgeräten mit eingeschränkten Eingabemöglichkeiten und Rechenleistungen sollte zumindest über einen mehrstelligen Zahlencode abgesichert sein. Ein auf diese Weise gesichertes Endgerät sollte nach mehrfacher Falscheingabe des Codes ohne administrativen Eingriff nicht mehr zu verwenden sein. Sicherere Authentisierungsmechanismen wie Smartcards sind zu bevorzugen.

M-TK-107 Möglichkeit zur individuellen Einstellung des Präsenzstatus bei Endgeräten

Die eingesetzten UCC-Clients müssen die Möglichkeit bieten, die Regeln zum automatisierten Setzen des Präsenzstatus, z. B. durch Auslesen von Kalenderinformationen oder Überprüfung der Nutzeraktivität am Endgerät, durch das individuelle Setzen des Präsenzstatus außer Kraft zu setzen. Hierdurch kann nicht nur die individuelle Erreichbarkeit durch den Einzelnen gesteuert, sondern auch einer Leistungsüberwachung durch den missbräuchlichen Zugriff auf (gespeicherte) Präsenzinformationen individuell gegengesteuert werden.

M-TK-108 Ständiges Einblenden der Teilnehmerliste auf den Endgeräten

Der eingesetzte UCC-Client sollte für alle angebotenen Kommunikationsmedien über eine dauerhaft sichtbare und übersichtliche Darstellung der aktuellen Kommunikationspartner (Teilnehmerliste) verfügen. Dies gilt insbesondere für Konferenzen (IM, Audio/Video, Web) aber auch für Zwiegespräche und Konferenzen, die aus Zwiegesprächen aufgebaut werden. Durch die ständige Anzeige der Teilnehmerliste kann die Teilnahme nicht berechtigter Personen an einem Gespräch erkannt und verhindert werden. Die UCC-Lösung sollte diese Funktion mindestens für alle Konferenzmedien unterstützen. Falls das ständige Einblenden der Teilnehmerliste nicht ohnehin die Standardeinstellung darstellt, sollte sie durch den Administrator aktiviert werden.

M-TK-109 Verwenden von Kameras mit geeigneter Brennweite

Um das Risiko für das versehentliche Enthüllen von vertraulichen Informationen zu minimieren, sollten für Video- und Webkonferenzen am Desktop ausschließlich Endgeräte zum Einsatz kommen, die über eine Kamera mit geeigneter Brennweite verfügen. Diese sollte so gewählt sein, dass der Teilnehmer optimal erfasst wird. Zudem sollten keine Endgeräte mit Weitwinkel-Funktion verwendet werden. Falls eine Anpassung der Bildausschnittes auf den Kommunikationsteilnehmer auf Software-Basis möglich ist, hilft dies zusätzlich bei der Vermeidung der versehentlichen Preisgabe von Informationen.

M-TK-110 Signalisierung der Kameraaktivität und Verwendung von Kameraabdeckungen

Damit eine Leistungsüberwachung oder das Ausspähen von Teilnehmern und Räumlichkeiten per Desktop-Video erkannt werden kann, empfiehlt sich der Einsatz von Endgeräten mit optischer Signalisierung der Kameraaktivität. Hierzu ist an vielen Endgeräten eine LED angebracht, welche bei Betrieb der Kamera aktiviert wird. Eine solche Anzeige stellt jedoch den Kamerastatus nicht mit absoluter Verlässlichkeit dar, da prinzipiell eine Deaktivierung der Warn-LED durch einen Angreifer denkbar ist.

Existiert keine Warn-LED am Endgerät, so stellt eine Kameraabdeckung (z. B. Schutzkappe) einen verlässlichen und einfach zu realisierenden Schutz dar. Hierbei ist die Praktikabilität eines Abdeckungsmechanismus unbedingt zu beachten. Klebesiegel für den einmaligen Gebrauch eignen sich beispielsweise nur für die dauerhafte Abdeckung einer Kamera. Sie sind in Verbindung mit dem häufigen Gebrauch von Desktop-Video nicht praktikabel. Die letzte Option ist die Hardware-seitige Deaktivierung von Kameras durch Zerstörung oder Ausbau. Sie setzt einen vollständigen Verzicht auf Videofunktionalität voraus.

M-TK-111 Richtliniengesteuerte Aktivierung/Deaktivierung von Kamera und Mikrofon

Falls der Einsatz von Desktop-Video auf ein klares Umgebungsszenario eingegrenzt werden kann (z. B. nur im eigenen Büro, nur in einem dedizierten Videokonferenzraum, nur außerhalb eines sicherheitskritischen Bereiches), könnten eingebaute Kameras und Mikrofone von transportablen und mobilen Endgeräten in Abhängigkeit vom Ort aktiviert bzw. deaktiviert werden. Hierzu ist die Formulierung ortsabhängiger Richtlinien sowie deren Umsetzung auf Basis von aktuellen Ortsinformationen notwendig. Die Feststellung des Aufenthaltsortes kann hierbei auf gemessenen Koordinaten (z. B. Global Positioning System, GPS) oder auf Netzwerkinformationen (IP-Adresse, Service Set Identifier (SSID) etc.) basieren. Eine Umsetzung solcher Richtlinien ausschließlich für ein UCC-Szenario ist nach heutigem Stand nicht machbar, da hierfür derzeit keine Funktionen in Standardprodukten enthalten

sind. Eine Umsetzung im Rahmen von weiter gefassten ortsabhängigen Richtlinien ist hingegen auch heute schon denkbar.

M-TK-112 Geeignete Standortwahl und Umgebungsgestaltung bei Einsatz von Desktop-Video

Bei der Verwendung von Desktop-Video und Webkonferenzen mit Videoübertragung muss auf eine geeignete Standortwahl geachtet werden, um die Gefährdung durch einen versehentlichen Abfluss von Informationen und die Möglichkeit der unbemerkten Leistungsüberwachung zu minimieren.

Die Positionierung des Endgerätes und der Kamera sollte dabei so erfolgen, dass der Blickwinkel der Kamera nicht versehentlich sensible Informationen oder unbeteiligte Dritte umfasst. Folgende Eckpunkte sollten beachtet werden:

- Keine Erfassung von Informationen im Hintergrund (z. B. Whiteboard, Monitor, Pinnwand)
- Keine Erfassung von Durchgangswegen
- Keine Erfassung von Arbeitsplätzen unbeteiligter Dritter

Falls der Aufenthaltsort als sensible Information einzustufen ist, sollten auch keine Fensterflächen im Hintergrund erfasst werden. Falls diese Punkte nicht nur durch geschickte Positionierung des Endgerätes bzw. der Kamera zu erzielen ist (z. B. im Großraumbüro), kann auf Trennwände oder Raumteiler zurückgegriffen werden. Führt auch das nicht zum gewünschten Ergebnis, sollte auf einen Einsatz von Desktop-Video am betreffenden Arbeitsplatz verzichtet werden. Alternativ kann, insbesondere bei vertraulichen Gesprächsinhalten in Großraumumgebungen, die Verwendung von Desktop-Video auf dedizierte Videoarbeitsräume oder Stillarbeitsräume (Think Tank) beschränkt werden.

6.3.3 Netzwerk

Es gelten sinngemäß die im Kapitel Voice over IP aufgeführten Maßnahmen bzgl. des Netzwerkes (siehe Kapitel 4.3.3). Ergänzende Maßnahmen werden im Folgenden dargestellt.

M-TK-113 Netztrennung zwischen UCC-Systemen und weiteren IT-Systemen

Durch die Konvergenz von Sprach- und Datennetz auf Basis des Internet Protocol (IP) wird die Nutzung einer gemeinsamen Netzinfrastruktur möglich. Für den Zugriff auf Sprachanwendungen und IT-Systeme kann eine Trennung der Zugriffsnetze unter gewissen Rahmenbedingungen aufrecht erhalten werden (siehe Kapitel 4.3.3). UCC-Clients werden jedoch auf Endgeräten für die Datenverarbeitung betrieben. Da diese Endgeräte in der Praxis nicht gleichzeitig zwei unterschiedlichen Zugriffsnetzen zugeordnet werden können und dies zudem einen Kurzschluss in der Sicherheitsarchitektur darstellen würde, kann eine Trennung der Zugriffsnetze bei der Nutzung von UCC-Diensten nicht sinnvoll aufrecht erhalten werden. Dies gilt sinngemäß auch beim Einsatz von Softphones bei reinen Telefonielösungen. Unterliegen Daten und Kommunikationsinhalte unterschiedlichen Schutzniveaus, so ist gegebenenfalls auf den Einsatz von UCC-Clients und Softphones zu verzichten. Es gilt sinngemäß die Vorgehensweise gemäß den Maßnahmen für die Basistechnologie Voice over IP (siehe Kapitel 4.3.3).

Die Server-Systeme einer UCC-Installation können bei Bedarf generell in separaten Sicherheitszonen platziert werden (siehe Maßnahme M-TK-67 „Netztrennung für VoIP“ und für den netztechnischen Aufbau von Sicherheitszonen Kapitel 13.3.1). Dies kann beispielsweise erforderlich sein, falls auf Ebene der UCC-Server für einen erhöhten Schutzbedarf keine angemessene Absicherung möglich ist oder falls das für die UCC-Server erzielbare Schutzniveau nicht den Anforderungen an allgemeine IT-Systeme genügt und diese daher von anderen IT-Systemen separiert werden müssen. Es ist zu beachten, dass UCC-Systeme eine Vielzahl von Integrationspunkten und Schnittstellen zu anderen IT-Systemen aufweisen. Eine Separierung in unterschiedliche Sicherheitszonen kann daher zu erheblichen administrativen und betrieblichen Aufwendungen führen (siehe Abbildung 37).

Der Zugang zu diesen Sicherheitszonen sollte durch eine Firewall kontrolliert werden. Je nach geforderter Verfügbarkeit muss die Firewall redundant ausgelegt werden. Weiterhin muss die geforderte Leistung bei der Dimensionierung des Systems berücksichtigt werden. In Abhängigkeit von der Gefährdungslage ist der zusätzliche Einsatz eines Intrusion Prevention System (IPS) zu empfehlen. Das IPS kann dabei eine Komponente der Firewall oder eine separate Appliance sein.

Da manche Protokolle (z. B. Distributed Component Object Model, DCOM) dynamisch die für die Kommunikation verwendeten TCP- bzw. UDP-Ports aushandeln, kann eine Firewall basierend auf einem dynamischen Paketfilter diese Protokolle ggf. nicht geeignet filtern und es müssten große Port-Bereiche permanent freigeschaltet werden. In diesem Fall sollte eine Firewall mit entsprechender Applikationsintelligenz eingesetzt werden, die in der Lage ist, die Anwendungsprotokolle zu analysieren und Ports dynamisch freizuschalten und bei Beendigung der Kommunikation wieder zu schließen.

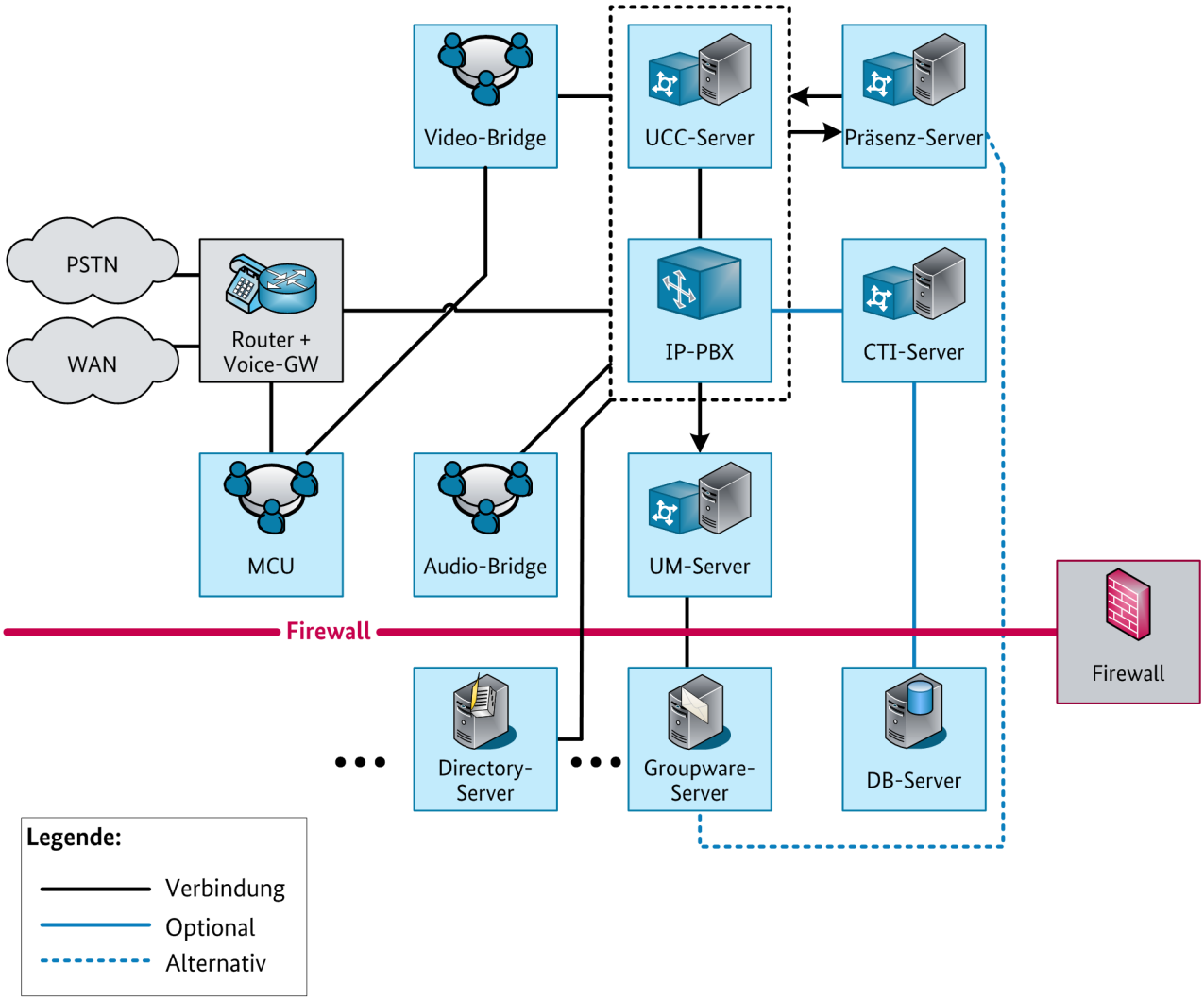


Abbildung 37: Separierung von UCC-System und sonstigen IT-Systemen in zwei Sicherheitszonen

6.3.4 Netz- und Systemmanagement

Es gelten sinngemäß die im Kapitel Voice over IP aufgeführten Maßnahmen bzgl. Netz- und Systemmanagement (siehe Abschnitt 4.3.4). Ergänzende Maßnahmen werden im Folgenden dargestellt.

M-TK-114 Sichere Administration der Server für UCC-Systeme

Die Administration von Servern für UCC-Systeme muss durch Sicherheitsmechanismen angemessen geschützt werden. Hierzu sind die entsprechenden generellen Maßnahmen in Kapitel 10.2 und 10.3 umzusetzen.

Für die sichere Administration von Anwendungs- und Management-Servern sind ebenfalls die entsprechenden generellen Maßnahmen in Kapitel 10.2 und 10.3 angemessen anzuwenden.

Für Applikations-Server mit VoIP-Diensten gilt meistens „Sicherheit vor Verfügbarkeit". Beispiel: Eine vorübergehend nicht verfügbare Voicemail-Funktionalität ist oft besser als ein nicht sicherer (kompromittierbarer) Voicemail-Dienst. Anwendungs- und Management-Server müssen vor schadenstiftender Software geschützt werden (siehe Maßnahme M-TK-235 „Schutz vor schadenstiftender Software für die Server der TK-Lösung"). Dies gilt insbesondere bei Verwendung von Standard-Betriebssystemen.

M-TK-115 Absicherung der Management-Schnittstellen eines UCC-Systems

Um die Management-Schnittstelle von UCC-Systemen vor Manipulation und Ausspähen zu schützen, müssen eine Reihe von Maßnahmen ergriffen werden. Oftmals wird die administrative Bedienoberfläche einer Appliance als Web-Interface realisiert. Da unverschlüsselte HTTP-Verbindungen keinerlei Schutz bieten, ist hier unbedingt auf HTTPS zurückzugreifen. HTTPS bietet mittels SSL/TLS eine Verschlüsselung und Authentisierung der zu übertragenden Daten (siehe auch Kapitel 13.3.3). Nicht geeignet gesicherte Management-Schnittstellen sind unbedingt zu deaktivieren.

Eine zweite wichtige Management-Schnittstelle ist SNMP, welches die Fernwartung von Netzinfrastruktur und Server-Applikationen ermöglicht. Hier ist die allgemeine Maßnahme M-TK-237 „Sichere Konfiguration des Netzwerk-Management-Protokolls" umzusetzen.

6.3.5 Übergreifende Aspekte

Es gelten sinngemäß die im Kapitel Voice over IP aufgeführten Maßnahmen bzgl. übergreifender Aspekte (siehe Abschnitt 4.3.5). Ergänzende Maßnahmen werden im Folgenden dargestellt.

M-TK-116 Koordination der Planung und Administration von UCC-Diensten

Um die möglichen Sicherheitsrisiken eines integrierten UCC-Systems zu erkennen, ist eine Übersicht über das Gesamtsystem erforderlich. Insbesondere bei UCC umfasst das Gesamtsystem eine Vielzahl unterschiedlicher Teilsysteme und verschiedenartige Integrationspunkte. Die Risiken können nicht allein aufgrund der isolierten Betrachtung von Teilsystemen abgeschätzt werden; sie sind sozusagen mehr bzw. größer als die Summe der Einzelrisiken.

Vor diesem Hintergrund ist es erforderlich, sowohl die Planung als auch den Betrieb der Teilsysteme zu koordinieren. Die an diesen Prozessen beteiligten Personen und Organisationseinheiten müssen mittels geeigneter Maßnahmen über alle sicherheitsrelevanten Vorgänge informiert werden. Hierzu sind u. a. Vorgänge der folgenden Art zu zählen:

- Aufspielen von Patches bzw. Updates auf ein Teilsystem
- Einführung neuer Benutzergruppen
- Änderungen der Rechte von Benutzergruppen
- Änderungen der Zusammensetzung von Benutzergruppen

- Aktivierung neuer Funktionen des UCC-Systems oder der Applikationen
- Konfigurationsänderungen, die über eine einfache Benutzerverwaltung hinausgehen

6.4 Zusammenfassung

UCC bezeichnet die Zusammenführung von verschiedenen Kommunikations- und Kollaborationswerkzeugen in einer einheitlichen Infrastruktur. UCC-Gesamtlösungen können somit viele verschiedene Anwendungen und Dienste zur Vereinfachung der Zusammenarbeit beinhalten.

Zur Nutzung dieser Dienste ist die Integration verschiedener Kommunikationskanäle in das UCC-System notwendig. Aus der Komplexität des Systems und den vielfältigen Kommunikationsmöglichkeiten ergeben sich eine hohe Anzahl von Angriffspunkten. Diese lassen sich wie folgt systematisieren:

- zentrale Systeme (Server, TK-Systeme im engeren Sinne) und Anwendungen, die Teile der Gesamtlösung bilden
- Schnittstellen und Kommunikation, über die diese Lösungselemente miteinander kombiniert werden
- Endgeräte mit Zugriff auf UCC-Dienste sowie die von und zu diesen Geräten erfolgende Kommunikation

Die Bewertung der Angriffsrisiken und die Auswahl der zur Entschärfung der Risiken notwendigen Sicherheitsmaßnahmen sind abhängig von

- Gefährdungspotenzial und Schutzbedarf der einzelnen Komponenten sowie der UCC-Gesamtlösung als Ganzes,
- den verwendeten Schnittstellen, Protokollen und Kommunikationsmöglichkeiten zwischen den Teillösungen der UCC-Gesamtlösung sowie
- den von der UCC-Gesamtlösung verwendeten und gespeicherten Daten und Informationen.

Besonders zu beachten sind dabei je nach Zielumgebung und konkretem Lösungsumfang:

- mögliche Wechselwirkungen der verschiedenen Lösungselemente aufeinander und die damit verbundenen Möglichkeiten zu übergreifenden Sicherheitsvorfällen, vor allem bei der Integration von internen und externen Dienstangeboten in einer UCC-Gesamtlösung
- einzuhaltende Sicherheitsanforderungen für die Nutzung personenbezogener Daten, insbesondere im Hinblick auf den Austausch von personenbezogenen Daten zwischen verschiedenen Komponenten der UCC-Gesamtlösung
- die hohe Anzahl an Zugriffsmöglichkeiten auf die UCC-Gesamtlösung durch Nutzung verschiedener Endgeräte und Kommunikationsmöglichkeiten
- Alternativen zu klassischen Maßnahmen wie Netztrennung über Sicherheits-Gateways mit reiner Paketfilterintelligenz, da diese mit der Notwendigkeit zu übergreifender Kommunikation in einem Zielkonflikt stehen

Die Erarbeitung und Umsetzung einer Sicherheitskonzeption für UCC-Systeme umfasst die im Folgenden aufgeführten Aspekte. Diese werden ergänzt durch die generell zu ergreifenden Maßnahmen (siehe Kapitel 10) und durch die für die Basistechnologie VoIP (siehe Kapitel 4.3) spezifizierten Maßnahmen für die entsprechenden Teilkomponenten. Bei allen zu ergreifenden Sicherheitsmaßnahmen sind bei UCC-Systemen übergreifende Aspekte, insbesondere bezüglich der vorhandenen Datenflüsse und Zugriffsmöglichkeiten, angemessen zu berücksichtigen.

Absicherung der zentralen Komponenten

Um Angriffe auf die zentralen Komponenten des UCC Systems und Angriffe auf das Gesamtsystem über zentrale Komponenten zu vermeiden, sind die zentralen Komponenten dem Schutzbedarf entsprechend angemessen zu härten. Es ist außerdem darauf zu achten, dass diese mit einem ausreichenden Virenschutz ausgestattet sind und die Administration nur über abgesicherte Verbindungen erfolgt. Können die

zentralen Komponenten nicht ausreichend abgesichert werden, ist für diese der Aufbau einer Sicherheitszone zu erwägen.

Soll ein UCC-System in ein vorhandenes TK-System integriert werden oder sollen vorhandene Anwendungen und Dienste in einem UCC-System zusammengeführt werden, so ist darauf zu achten, dass die zentralen Komponenten des UCC-Systems so ausgewählt werden, dass sie zur vorhandenen Produktlandschaft möglichst kompatibel sind. Dies beinhaltet insbesondere Schnittstellen, genutzte Protokolle und Management-Optionen.

Zentrale Komponenten und deren Vernetzung sind mit Blick auf notwendige Verfügbarkeit der einzelnen UCC-Komponenten angemessen auszustatten und ausreichend redundant auszulegen. Weiterhin sind bestehende Wartungsverträge und Notfalllösungen für Teillösungen zu prüfen und bei Bedarf an die Anforderungen des Gesamtsystems anzupassen.

Absicherung des Sprachkanals zur TK-Anlage

Bei der Absicherung des Sprachkanals zur TK-Anlage ist zu beachten, dass sowohl die über den Sprachkanal übertragenen Sprachdaten als auch die Signalisierungsdaten schützenswerte Informationen enthalten können. Der Sprachkanal muss daher angemessen abgesichert werden.

Führen die Übertragungswege zur TK-Anlage über unsichere Netze oder ist ein zusätzlicher Schutz notwendig, so sind weitere Maßnahmen zu ergreifen, welche abhängig von der verwendeten Technik zu wählen sind. Bei Nutzung von Telefonieverbindungen ist eine weitere Absicherung beispielsweise über Kryptoboxen möglich und bei IP-basierter Übertragung die Verschlüsselung mittels SSL bzw. TLS.

Absicherung der Kommunikation mit weiteren IT-Systemen

Bei der Kommunikation zwischen dem UCC-System und weiteren IT-Systemen werden verschiedene, d. h. vom IT-System abhängige, Protokolle verwendet. Die unterschiedlichen Protokolle können unterschiedlich geschützt werden.

Zum Schutz der Kommunikation ist es daher wichtig zu wissen, über welche Protokolle das UCC-System mit anderen IT-Systemen kommuniziert. Die Maßnahmen, welche zum Schutz der Kommunikation zwischen diesen Systemen sinnvoll sind, müssen dann abhängig von den verwendeten Protokollen im Einzelfall gewählt werden.

Absicherung der Kommunikation mit der Datenbank

Für verschiedene Komponenten des UCC-Systems ist die Kommunikation mit einer Datenbank des UCC-Systems notwendig. Der Zugriff auf Datenbestände in der Datenbank sollte allerdings nur für die Komponenten erlaubt werden, für die diese Kommunikation notwendig ist. Weiterhin sollte der Zugriff nur auf die für die jeweilige Komponente notwendigen Datensätze freigegeben sein. Eine solche Regelung kann beispielsweise über ein Rechtesystem implementiert werden. Beim Zugriff auf sensible Daten sollte die Kommunikation außerdem verschlüsselt erfolgen.

Einschränkung der Zugriffsrechte

In vielen Fällen gibt es für UCC-Dienste Nutzerkonten, über welche ein Dienst auf die für ihn notwendigen Ressourcen zugreifen kann. Die für ein solches Konto erteilten Zugriffsrechte sind soweit einzuschränken, dass ausschließlich die für den Dienst notwendigen Rechte zur Verfügung stehen.

Beim Einsatz von Endgeräten ist der Zugriff der Endgräte auf die Teillösungen des UCC-Systems zu beschränken, welche für den Nutzer des Endgerätes notwendig sind. Der Zugriff auf nicht benötigte Anwendungen, Dienste und Daten ist zu unterbinden. Weiterhin müssen Endgeräte mit Zugriff auf UCC-Lösungen geeignet gesichert sein, um einen unbefugten Zugriff auf das UCC-System zu vermeiden. Neben den für die Basistechnologie VoIP (siehe Kapitel 4.3.2) aufgeführten Maßnahmen sind für Endgeräte mit Zugriff auf das UCC-System daher die folgenden Maßnahmen umzusetzen:

- Schnittstellen, die für die vorgesehene UCC-Nutzung eines Endgerätes bzw. dessen Nutzers nicht benötigt werden, sind zu deaktivieren, zu blockieren oder durch entsprechende Endgeräteausstattung wegzulassen.

- Der Zugriff auf ein Endgerät sowie auf darauf installierte UCC-Client-Lösungen ist gezielt abzusichern. Dies schließt je nach Endgeräteausstattung eine manuelle Deaktivierbarkeit von Ein-/Ausgabeschnittstellen wie beispielsweise Kamera und Mikrofon ein.
- Personenbezogene Daten, welche dem UCC-System mitgeteilt werden (wie zum Beispiel der Präsenzstatus des Nutzers) sollten am Endgerät gezielt festlegbar sein. Ihre Erzeugung und Übermittlung sollte gezielt blockierbar und über Verschlüsselung absicherbar sein.
- Der Anwender sollte Einstellungen zur Kommunikationsabsicherung und Übermittlung personenbezogener Daten einfach einsehen und - falls erwünscht - intuitiv ändern können.

Schutz vor unberechtigtem Zugriff auf Datenbanksysteme der Dienst- und Nutzerkonten

Daten der Dienst- und Nutzerkonten, welche das UCC-System nutzt oder diesem zur Verfügung gestellt werden, sind häufig in Datenbanken gespeichert. Da diese Datenbänke somit sensible Daten enthalten, ist ein angemessener Zugriffsschutz zu implementieren.

Eine Maßnahme gegen unberechtigten Zugriff ist beispielsweise die Einrichtung eines Rechtesystems für den Zugriff auf die Datenbank. Zusätzlich ist bei erhöhtem Schutzbedarf auch die Verschlüsselung der Daten auf der Datenbank zu erwägen.

Schutz vor Abfluss klassifizierter Daten

Um zu verhindern, dass vertrauliche Information an unberechtigte Dritte abfließen können, müssen Regelungen für den Umgang mit diesen Daten innerhalb der UCC-Lösung getroffen werden. Vor allem wenn im Rahmen von UCC-Teillösungen personenbezogene oder andere besonders vertraulich zu behandelnde Daten verwendet werden, ist gezielt zu prüfen und festzulegen,

- in welchem Umfang eine Speicherung solcher Daten notwendig bzw. zulässig ist und
- ob ein Austausch bzw. eine gemeinsame Nutzung solcher Daten zwischen verschiedenen Teillösungen einer UCC-Architektur erfolgen darf.

Bei diesen Entscheidungen sind die Risiken zu berücksichtigen, die für die Organisation durch ungewollten Informationsabfluss entstehen können.

Abhängig von diesen Entscheidungen sind ggf.

- die Datenspeicherung auf einzelnen Servern der UCC-Lösung gezielt zu unterbinden,
- die Möglichkeiten eines Systems, mit anderen Systemen besonders schützenswerte Daten auszutauschen bzw. Dienste mit solchen Daten gemeinsam zu nutzen, gezielt zu limitieren und
- die Möglichkeiten für Anwender, auf besonders schützenswerte Daten zuzugreifen und den zugehörigen Datenaustausch zu initiieren, über Nutzerprofile geeignet zu konfigurieren.

Weiterhin kann der Datenabfluss auch durch den Einsatz von Systemen für Data Loss Prevention (DLP) verhindert werden.

Absicherung der einzelnen UCC-Dienste

Die Grundabsicherung der UCC-Gesamtlösung baut auf den Sicherheitsmaßnahmen für integrierte Anwendungen und Dienste auf. Dies bedeutet, dass die Sicherheitsmaßnahmen, welche zum Schutz der Teillösungen bei Einzelnutzung notwendig sind, auch für das Gesamtsystem erfüllt sein müssen.

Die dazu notwendigen Maßnahmen sind abhängig von den eingesetzten Anwendungen und Diensten. Die Durchführung dieser Maßnahmen erfolgt bei erhöhtem Schutzbedarf gemäß den anwendbaren Bausteinen der BSI IT-Grundschutz-Kataloge sowie gemäß den Empfehlungen für die entsprechenden Teillösungen, die im vorliegenden Dokument spezifiziert sind. Dies beinhaltet insbesondere die für die Basistechnologie VoIP (siehe Kapitel 4.3) aufgeführten Maßnahmen.

Aufbauend auf den Maßnahmen für die eingesetzten Dienste und Anwendungen ist eine Absicherung der durch die Kombination der Technologien entstehenden zusätzlichen Gefährdungen notwendig.

Abbildung 38 und Abbildung 39 zeigen zusammenfassend die grundsätzliche Vorgehensweise bei der Absicherung von UCC und machen deutlich, dass manche Maßnahmen nur dann ergriffen werden müssen, wenn andere Maßnahmen nicht ausreichend umgesetzt werden können.

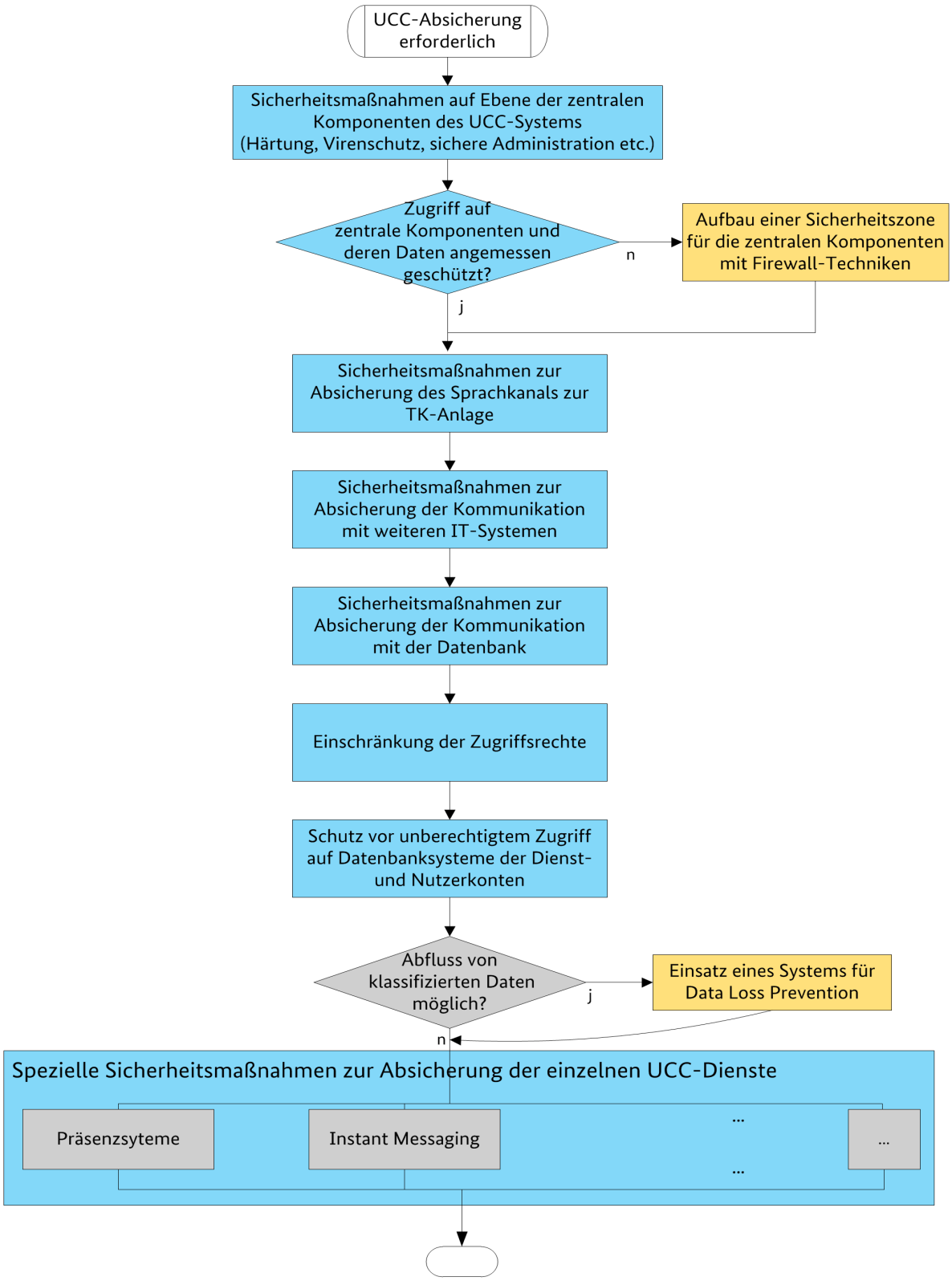


Abbildung 38: Grundsätzliche Vorgehensweise bei der Absicherung von UCC

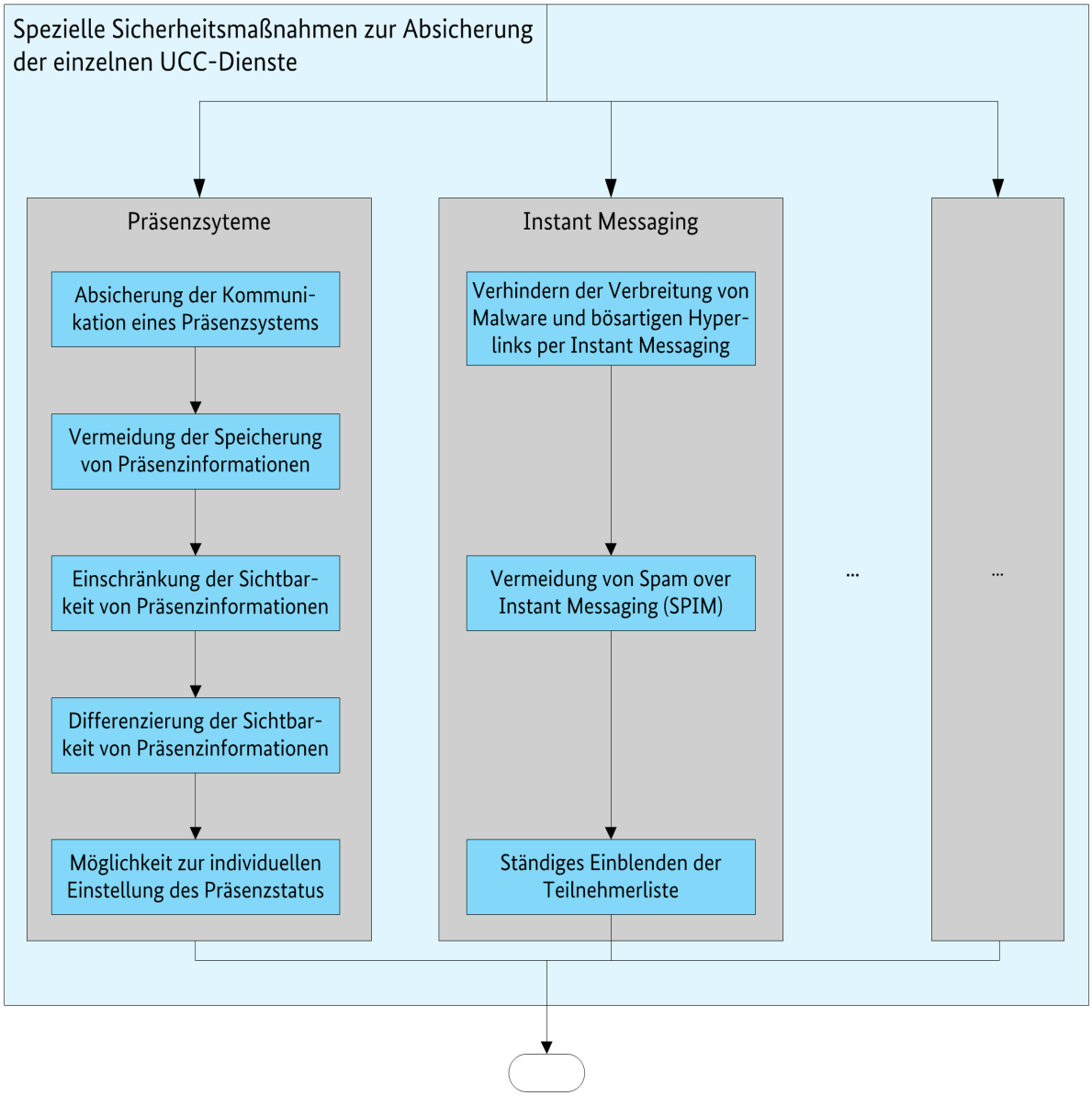


Abbildung 39: Beispielhafte Vorgehensweise bei der Absicherung von UCC-Anwendungen

7 Spezielle TK-Systeme

Mit den in den Kapiteln 3 und 4 betrachteten Basistechnologien der ISDN-basierten TK-Anlagen (klassische Telekommunikationstechnik) und der VoIP-basierten TK-Anlagen sind für verschiedene spezielle Anwendungsbereiche entsprechende TK-Systeme entwickelt worden. Für folgende spezielle TK-Systeme werden in diesem Kapitel Sicherheitsbetrachtungen durchgeführt:

Die Abbildung verdeutlicht die im Text zuvor beschriebenen grundsätzlichen Schritte und zur Absicherung von UCC-Anwendungen (Beispiel) in Form eines Flussdiagramms.

- Videokonferenz (Kapitel 7.1)
- Kontaktcenter (Kapitel 7.2)
- Händlersysteme (Kapitel 7.3)
- Alarmierungssysteme (Kapitel 7.4)

Darüber hinaus wird für alle speziellen TK-Systeme die Umsetzung der generell zu ergreifenden Maßnahmen (siehe Kapitel 10) vorausgesetzt.

7.1 Videokonferenz

Mit der Verfügbarkeit leistungsfähiger Internet- und WAN-Verbindungen haben sich Videokonferenzsysteme stark verbreitet und als Standardkomponente einer IT-Infrastruktur etabliert.

Für den TK-Bereich Videokonferenz gelten dabei weitgehend die Gefährdungen und Sicherheitsmaßnahmen der Basistechnologien klassische Telekommunikationstechnik (siehe Kapitel 3), Voice over IP (siehe Kapitel 4) und Unified Communications and Collaborations (siehe Kapitel 6). Zudem sind die generell zu ergreifenden Maßnahmen aus Kapitel 10 anzuwenden. Diese Sicherheitsmaßnahmen müssen jedoch wie in diesem Kapitel beschrieben ggf. an die spezifischen Komponenten für Videokonferenzen und den sich daraus ergebenden Gefährdungen angepasst werden.

7.1.1 Basiswissen

Die Technik der Videokonferenz ermöglicht die Echtzeitübertragung von Bild- und Ton-Daten der teilnehmenden Endgeräte. Die Übertragung der Bilder und des Tones erfolgen über kurze Strecken innerhalb eines Gebäudes genauso wie über tausende Kilometer Entfernung.

Videokonferenzen werden in unterschiedlichsten Organisationen branchenübergreifend eingesetzt. Der zunehmende Kostendruck und die damit verbundene erforderliche Steigerung der Effizienz haben zu einer weiten Verbreitung von Systemen und Lösungen für Videokonferenzen geführt.

Beispiele für den Einsatz von Videokonferenzen sind:

- Arbeitstreffen über verteilte Standorte
- Einbindung von Heimarbeitsplätzen
- Steuerung des Außendienstes
- Schulungen
- Projekttreffen mit Kunden und Lieferanten

Hierdurch sind die folgenden effizienzsteigernden Vorteile verbunden:

- weniger Reisezeit

- reduzierte Reisekosten
- optimierte Ressourcennutzung
- verbesserte Zusammenarbeit virtueller Teams
- standortunabhängige Zusammenarbeit

Videokonferenzen können mit Hilfe unterschiedlicher Netztechniken realisiert werden. Die ersten Systeme für Videokonferenzen nutzten Integrated Services Digital Network (ISDN). In der Weiterentwicklung erfolgte der Einsatz über IP-Netze mittels H.323 oder Session Initiation Protocol (SIP) für die Signalisierung sowie mittels Real-Time Protocol (RTP) für die Übertragung der Mediendaten.

Systeme, die ISDN nutzen, sind bei den meisten Organisationen noch im Einsatz, werden jedoch bei einer neuen Beschaffung nicht mehr berücksichtigt. ISDN bietet normalerweise deutlich geringere Bandbreiten und damit weniger Übertragungsqualität als IP-basierte Systeme. Daher ersetzen Videokonferenzsysteme auf Basis des Internet Protocol (IP) unter Nutzung der Protokolle und Standards innerhalb H.323 und SIP immer mehr die ISDN-basierten Systeme. IP-basierte Videokonferenzsysteme bilden daher den Schwerpunkt der folgenden Betrachtungen.

7.1.1.1 Überblick Komponenten einer Videokonferenzlösung

Eine Videokonferenzlösung besteht aus unterschiedlichen Komponenten, insbesondere:

- Video-Terminals
- Gateways
- Mehrpunkt-Videokonferenzbrücke
- Registrierungseinheit
- Ressourcenmanagement

Der direkte Kontakt der Teilnehmer erfolgt über die Video-Terminals, die die Anfangs- und Endpunkte der Bild- und Tonübertragung darstellen. Video-Terminals können dedizierte Video-Endgeräte (Raumsysteme, Desktop-Systeme), Standard-PC-Systeme, Tablets oder sogar Smartphones sein.

Ein Videokonferenz-Gateway realisiert bei Videokonferenzen den Übergang in andere Zonen und Netze. Ein solches Gateway wird beispielsweise bei einer Verbindung vom IP-Netz zum Telefonnetz in beide Richtungen benötigt. Dabei erfolgt eine Protokollumsetzung von ISDN auf IP und umgekehrt.

Eine Mehrpunkt-Videokonferenzbrücke wird dann benötigt, wenn mehr als zwei Teilnehmer beziehungsweise Video-Terminals an einer Videokonferenz teilnehmen sollen. Die Mehrpunkt-Videokonferenzbrücke wird auch Multipoint Control Unit (MCU) genannt.

Die Registrierungseinheit übernimmt die Funktionen der Zugangskontrolle der Video-Terminals, der Auflösung der Adressen und das Leiten der Signalisierung. Die Registrierungseinheit ist bei SIP und H.323 unterschiedlich aufgebaut. Bei SIP werden die Rollen durch Proxy-Server, Redirect-Server und Registrar umgesetzt. Bei H.323 erfolgt dies durch den Gatekeeper.

Das Ressourcenmanagement beinhaltet die Verwaltung von Konferenzräumen und anderen Ressourcen, inklusive der Reservierung von Nutzer-Zuordnung. Dies beinhaltet auch die Verwaltung von PINs oder Passwörtern für den Zugang zu einer Videokonferenz. Dabei sind typischerweise auch Schnittstellen zu einer Groupware erforderlich (z. B. für die Einladungen zu einer Videokonferenz in Verbindung mit der Buchung der zugehörigen Ressourcen). Das Ressourcenmanagement ist als herstellerspezifische Software ein optionaler Bestandteil einer Videokonferenzlösung.

Die oben genannten Komponenten stehen nicht immer als eigenständige Einheiten in einer Videokonferenzlösung zur Verfügung. In der Regel werden Komponenten wie Gatekeeper und MCU in einer Einheit zusammengefasst. Die Aufgabe der Komponenten innerhalb der Videokonferenzlösung bleibt damit jedoch unverändert.

Abbildung 40 stellt die Komponenten einer Videokonferenzlösung dar. Zentraler Punkt ist das IP-Netz, mit dem die Komponenten verbunden sind. Die internen Video-Terminals sind an die MCU via IP angebunden. Die Verbindungen zum klassischen Telefonnetz (Public Switched Telephone Network, PSTN) realisiert ein ISDN-Gateway und zu externen IP-Teilnehmern ein Videokonferenz-Gateway, die beide via IP mit der MCU verbunden sind. Das Videokonferenz-Gateway befindet sich üblicherweise innerhalb einer demilitarisierten Zone (Demilitarized Zone, DMZ) und realisiert neben Network Address Translation (NAT) auch Proxy-Funktionen für Signalisierung und Medienstrom. Das Videokonferenz-Gateway ist meist eine proprietäre Komponente des Herstellers der Videokonferenzlösung, die entsprechenden Funktionen können jedoch grundsätzlich auch durch einen Session Border Controller (SBC) realisiert werden.

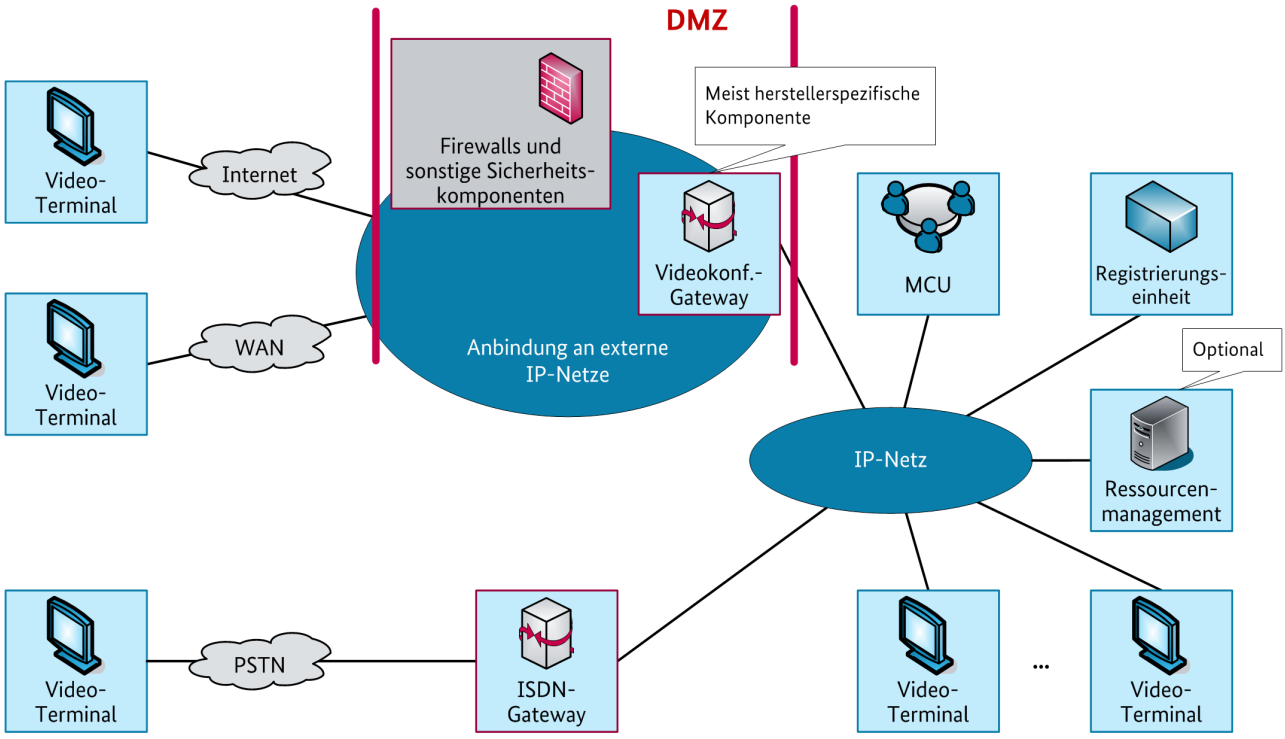


Abbildung 40: Überblick Komponenten Videokonferenzlösung

Der Austausch der Bild- und Tondaten zwischen den Komponenten erfolgt über die zwei Ebenen Signalisierung und Übertragung der Mediendaten. Bei allen drei Standards - ISDN, H.323 und SIP - wird zuerst über die Signalisierung die Verbindung ausgehandelt und aufgebaut. Erst danach erfolgt die Übertragung der Mediendaten. Die Standards unterscheiden sich im Detail bei der Signalisierung und der Medienübertragung in den genutzten Protokollen und Codecs.

7.1.1.2 Anwendungsfälle für Videokonferenz

Die Anwendungsfälle für Videokonferenz ergeben sich aus den Verbindungen von zwei oder mehr Teilnehmern innerhalb einer Videokonferenz. Zudem ist zu unterscheiden, ob einer oder mehrere Teilnehmer sich außerhalb des eigenen und gesicherten Netzes befinden. Verbindungen von zwei Teilnehmern werden Punkt-zu-Punkt-Video und von mehr als zwei Teilnehmern Mehrpunkt-Video genannt. Bei einer zusätzlichen Unterscheidung für interne und externe Teilnehmer beziehungsweise der Möglichkeit externe Teilnehmer einzubeziehen, ergeben sich insgesamt vier Anwendungsfälle:

- Punkt-zu-Punkt-Video interner Teilnehmer
- Punkt-zu-Punkt-Video interner und externer Teilnehmer
- Mehrpunkt-Video interner Teilnehmer
- Mehrpunkt-Video interner und externer Teilnehmer

Bei einer Punkt-zu-Punkt-Videokonferenz verbinden sich die Video-Terminals direkt miteinander. Auf Basis der Netzinfrastruktur erfolgt der Verbindungsaufbau und Austausch der Mediendaten direkt zwischen den Video-Terminals.

Für eine Mehrpunkt-Videokonferenz benötigt man eine MCU, eine Registrierungseinheit und Video-Terminals. Der Verbindungsaufbau erfolgt über die Registrierungseinheit. Der Austausch der Mediendaten erfolgt zentral über die MCU.

Immer wenn ein externes Video-Terminal an der Videokonferenz teilnehmen soll, egal ob Punkt-zu-Punkt-Video oder Mehrpunkt-Video, wird bei IP ein Videokonferenz-Gateway und bei ISDN ein ISDN-Gateway benötigt.

7.1.1.3 Übertragung von Signalisierungsdaten

Bei der Übertragung der Daten zur Signalisierung werden unterschiedliche Protokolle eingesetzt. Zu nennen sind hier insbesondere:

- SIP, siehe 13.1.1.1
- H.323, siehe 13.1.1.2
- Digital Subscriber System No. 1 (DSS1) im ISDN

7.1.1.4 Übertragung der Nutzdaten

Videokonferenzsysteme auf Basis von IP nutzen analog zu VoIP-Systemen das Real-Time Transport Protocol (RTP) für die Übertragung der Nutzdaten, das verbindungslos über das User Datagram Protocol (UDP) übertragen wird (siehe Kapitel 13.1.2) und daher von Paketverlusten und Schwankungen in Delay und effektiv verfügbarer Bandbreite geprägt ist.

Im Gegensatz hierzu kann ISDN Daten mit festen Bandbreiten übertragen. Ein digitaler B-Kanal, der zur Übertragung der Nutzdaten dient, bietet je Kanal eine Bandbreite von 64 kbit/s. Der von der International Telecommunication Union (ITU) definierte Standard H.320 gibt die Rahmenspezifikation für schmalbandige Videokommunikation vor. H.320 umfasst entsprechende Spezifikationen für die Kommunikation von Audio, Video, Daten und Signalisierung sowie für die Steuerung. H.320 basiert auf einer Leitungsvermittlung (circuit-switched), im Gegensatz zu paketvermittelnden Protokollen (packet-switched) wie TCP/IP im Internet. Die Audio-Signale und die Video-Signale der Konferenzteilnehmer werden zum Senden digitalisiert und auf die verfügbare Bandbreite (*n* mal 64 kbit/s) durch sogenannte Codecs (engl. Coder/Decoder, deutsch Kodierer/Dekodierer) verlustbehaftet komprimiert. H.320 definiert für die Übertragung von Audio-Daten die Protokolle G.711, G.722 sowie G.728 und für die Übertragung von Video-Daten die Protokolle H.261, H.263 und H.264. Die Datenübertragung erfolgt über die Standards T.120 und H.239.

7.1.1.5 Sicherheitsmechanismen in Videokonferenzen

Dedizierte Sicherheitsmechanismen für die Absicherung der Übertragung bei Videokonferenzen sind nicht spezifiziert. Stattdessen werden die für die Basistechnologien zur Verfügung stehenden Mechanismen verwendet:

- Sicherer Medientransport
  - Zum sicheren Medientransport (z. B. Sprache oder Video) wird vor allem das Secure Real-Time Transport Protocol (SRTP, siehe Kapitel 13.1.3.1) eingesetzt. Es kommen aber auch andere Verfahren wie IPsec (IP Security, siehe Kapitel 13.1.3.2) und allgemein VPN-Techniken in Frage.
  - Eine Verschlüsselung der Nutzdaten erfolgt bei ISDN-basierten Videokonferenzsystemen im Gegensatz zu IP-basierten nicht in der Basisausstattung. Eine Verschlüsselung durch einen zusätzlichen Einsatz von speziellen ISDN-Verschlüsselungssystemen an jedem Kommunikations-endpunkt ist jedoch möglich.

- Sichere Signalisierung
  - Videokonferenzsitzungen werden über Signalisierungsprotokolle auf- und abgebaut sowie gesteuert. Die Absicherung dieser Protokolle erfolgt bei Videokonferenzen meist auf der Transportschicht über Transport Layer Security (TLS, siehe Kapitel 13.1.3.3) oder auf der Vermittlungsschicht über IPsec. Im Detail unterscheiden sich die verschiedenen Signalisierungsprotokolle (SIP und H.323) hinsichtlich ihrer Absicherung, siehe Kapitel 13.1.3.4 und 13.1.3.5.
  - Beim Einsatz von ISDN-Videokonferenzsystemen und DSS1 erfolgt keine Verschlüsselung der Signalisierung.

7.1.2 Gefährdungen

Im Folgenden werden die spezifischen Gefährdungen für Videokonferenzlösungen analysiert.

7.1.2.1 Höhere Gewalt

Für Videokonferenzlösungen gelten die entsprechenden Gefährdungen, die für die Basistechnologien „Klassische Telekommunikationstechnik“ (Kapitel 3.2.1) und „Voice over IP“ (Kapitel 3.2.1) spezifiziert sind.

7.1.2.2 Organisatorische Mängel

Die Gefährdungen durch organisatorische Mängel, die bereits für die Basistechnologien „Klassische Telekommunikationstechnik“ (Kapitel 3.2.1) und insbesondere „Voice over IP“ (Kapitel 3.2.1) genannt wurden, lassen sich unmittelbar auf Videokonferenzen übertragen, wie die folgenden Punkte zeigen.

G-TK-78 Unzureichende Regelungen für den Einsatz von Videokonferenzen

Für den Einsatz von Videokonferenz sind Regelungen zu treffen und einzuhalten, die der Bedeutung der Sicherheit für ein Unternehmen bzw. eine Behörde gerecht werden.

Zur Erreichung der Ziele Verfügbarkeit, Vertraulichkeit und Integrität müssen Regelungen für Videokonferenzen konsequent umgesetzt werden.

Ein Beispiel zu Regelungsaspekten und Gefährdungen bei Videokonferenzlösungen ist der Einsatz von Messtechnik im Umfeld von Netzwerk-Bereichen, die durch Videokonferenzen mitgenutzt werden. Hier ist es möglich, mit Hilfe von Analysator-Software, wie sie zur Diagnose in Netzwerken (LAN und WAN) eingesetzt wird, den Inhalt der Videokonferenz aufzuzeichnen und nachträglich wiederzugeben. Der Einsatz solcher Diagnosetechnik muss so geregelt sein, dass keine Verletzung von Datenschutz- und Persönlichkeitsrechten des Anwenders droht.

G-TK-79 Unzureichende Planung von Videokonferenzsystemen

Der störungsfreie Betrieb von Videokonferenzsystemen stellt hohe Anforderungen in Bezug auf Bandbreiten, Delay und Jitter an das LAN, die Netzübergänge und die Netzanbindungen. Netze, in denen Datendienste ohne Störungen funktionieren, sind nicht automatisch auch für Echtzeitanwendungen wie Videokonferenz geeignet.

Videokonferenzen stellen die konstante und verlustfreie Datenübertragung als Hauptanforderung an Netze. Für Netze, in denen Videokonferenz genutzt werden soll, muss die Übertragung von Videokonferenzdaten in der Planung berücksichtigt werden.

G-TK-80 Unzureichende Harmonisierung zwischen IT-, TK-Anlagen- und Videokonferenz-Betrieb

Wenn der Betrieb der Videokonferenzlösung und der IT-Betrieb getrennt sind, muss die Kooperation dieser beiden Verantwortungsbereiche etabliert werden. Dies betrifft den kompletten Lebenszyklus der Installationen von der Planung bis zur Außerbetriebnahme.

Wird bei solchen Punkten nicht in abgestimmter Weise verfahren, so ist mindestens die Verfügbarkeit der Videokonferenz stark gefährdet.

G-TK-81 Unzureichende Verwaltung und Kontrolle von Zugangs- und Zugriffsmöglichkeiten auf Video-Terminals

Durch die Möglichkeit zum Abrufen von Kontaktinformationen auf Video-Terminals werden diese Geräte relevant für den Datenschutz.

Bei frei zugänglichen Video-Terminals besteht die Gefahr, dass über das gewünschte Dienstspektrum hinaus Funktionen am Gerät genutzt werden können. Außerdem besteht auf Video-Terminals typischerweise die Möglichkeit, lokal am Gerät Konfigurationsänderungen vorzunehmen. Diese sind ab Werk durch Default-Kennwörter bzw. -PINs geschützt. Werden diese nicht vor Freigabe für den Anwender abgeändert, drohen Manipulationen.

G-TK-82 Kein ordnungsgemäßer Benutzerwechsel für Video-Terminals

Video-Terminals werden in der Regel ohne personenbezogene Nutzerprofile betrieben. Damit besteht für einen nachfolgenden Nutzer die Möglichkeit, über ungelöschte Anruflisten Informationen über zuletzt vom Vorgänger genutzte Verbindungen zu erlangen. Dies kann z. B. zur Verletzung des Datenschutzes führen.

G-TK-83 Mangelhafte Behandlung der Archivierung von Videokonferenzen

Eine Datenarchivierung kann bei Videokonferenzlösungen primär in folgenden Bereichen anfallen:

- Archivierung von Verbindungsdaten und Abrechnungen
- Archivierung von Protokollen der Videokonferenzen in Form von Multimedia-Dateien

Werden diese Archivierungsformen nicht ausreichend geregelt und berücksichtigt, so drohen einerseits Verletzungen der Vertraulichkeit oder des Datenschutzes. Weiterhin sind Verletzungen von Aufbewahrungspflichten möglich, etwa durch ungeeignete Lösungen, die nicht für die Archivierung von speziellen Multimedia-Dateien, insbesondere mit großem Datenvolumen, ausgelegt sind.

7.1.2.3 Menschliche Fehlhandlungen

Menschliche Fehlhandlungen kommen bei jeglicher Form von IT-Lösungen vor, so auch für Videokonferenzlösungen. Dabei sind Fehlhandlungen der Videokonferenznutzer ebenso zu berücksichtigen wie solche des IT-Personals.

G-TK-84 Unzureichende Prüfung der Identität von Kommunikationspartnern

Die Identität des Kommunikationspartners wird aus Gründen der Höflichkeit oft nicht hinterfragt.

Diese Bedrohung wird durch die Anzeige des Anrufers begünstigt, da die Anzeige der vermeintlichen richtigen Adressierung den Benutzer in Sicherheit wiegt. Dabei kann der Anrufer lediglich ein unbeaufsichtigtes Video-Terminal unbefugt verwenden oder die Rufnummer vortäuschen.

Diese Gefährdung besteht zwar grundsätzlich auch für Videokonferenzsysteme, ist aber hier geringer ausgeprägt als bei einer reinen Telefonielösung.

G-TK-85 Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten der Videokonferenzbenutzer

Derart verursachte Vertraulichkeits- oder Integritätsverluste können vor allem bei Mehrwert-Funktionalitäten von Videokonferenzlösungen auftreten, z. B. durch die Zugänglichkeit von Kontaktinformationen für Dritte aufgrund schlecht oder gar nicht geschützter Speicherung auf allgemein zugänglichen Videokonferenzsystemen.

G-TK-86 Konfigurationsfehler und Bedienungsfehler bei Videokonferenzlösungen

Konfigurationsfehler an MCUs, Gateways und ähnlichen zentralen Komponenten können zu Fehlfunktionen, Vertraulichkeitsverlusten, Nicht-Verfügbarkeit von Leistungsmerkmalen oder Absturz zentraler Komponenten und damit zu einer Nicht-Verfügbarkeit des Videokonferenzdienstes als Ganzes führen.

Dies lässt sich ausweiten auf Komponenten der IP-Infrastruktur, soweit sie auch für die Videokonferenz genutzt werden, aber in ihrer Konfiguration nicht bzw. nicht vollständig auf die Anforderungen der Videokommunikation umgestellt wurden.

Eine Gefährdung durch Konfigurations- und Bedienfehler besteht auch im Bereich der Video-Terminals durch die automatische Annahme von externen Anrufen.

Im Zusammenhang mit der automatischen Annahme von externen Anrufen können ungewollt aktive Verbindungen mit dem Videokonferenzsystem hergestellt werden. Dabei ist es beispielsweise grundsätzlich möglich, den Sichtbereich der Videokamera auszuspähen und den Audiobereich des Mikrofons abzuhören.

G-TK-87 Fehlerhafte Administration von Zugangs- und Zugriffsrechten zu Videokonferenz-Installationen

Diese Gefährdung ist für Videokonferenzen relevant im Zusammenhang mit folgenden Punkten:

- Zugang zu Videokonferenz-Mehrwertfunktionen und zugehörigen Datenbeständen
- Konfigurationsmöglichkeiten des Nutzers für die Videokonferenz-Nutzungsumgebung (z. B. administrative Bereiche, PIN-Code): Bei Änderung durch unbefugte Dritte können sicherheitsrelevante Einstellungen verändert werden.

7.1.2.4 Technisches Versagen

Die Gefährdungen der Katalogisierung „Technisches Versagen“ des Kapitels 3.2.4 für klassische Telekommunikationstechnik und Kapitel 4.2.4 für Voice over IP (VoIP) treffen auch für Videokonferenzen grundlegend zu, soweit die durch eine Gefährdung bedrohte Technik eingesetzt wird:

- Netzwerk-Technik (LAN, WAN, gegebenenfalls auch Wireless LAN)
- im Rahmen einer konkreten Videokonferenzlösung eingesetzten Betriebssystem(e) und Hardware
- Endgeräte-Betriebssysteme, soweit die Endgeräte als Video-Terminals eingesetzt werden

  Hierzu gehören auch Clients für Unified Communications and Collaboration (UCC-Clients).

7.1.2.5 Vorsätzliche Handlungen

Zudem ergeben sich bei Einsatz einer ISDN-basierten Videokonferenzlösung die folgenden, identischen Gefährdungen der höheren Gewalt wie bei klassischer Telekommunikationstechnik.

G-TK-13 „Abhören von Räumen“

G-TK-14 „Missbrauch von Wartungszugängen“

Beim Einsatz einer IP-basierten Videokonferenzlösung bestehen die folgenden, identischen Gefährdungen der vorsätzlichen Handlungen wie bei VoIP.

G-TK-35 „Denial-of-Service-Angriffe auf VoIP“

G-TK-36 „Abhören der VoIP-Kommunikation durch Schwachstellen in Netzwerkprotokollen“

G-TK-37 „Missbräuchlicher Zugriff auf VoIP-Geräte“

7.1.3 Sicherheitsmaßnahmen

Dieses Kapitel beschreibt Maßnahmen zur Absicherung von Videokonferenzlösungen unter besonderer Berücksichtigung eines erhöhten Schutzbedarfs.

Grundlage der Absicherung von Videokonferenzsystemen ist dabei die bedarfsorientierte und für Videokonferenzen lösungsabhängige Anwendung der Sicherheitsmaßnahmen für die Basistechnologien „Klassische Telekommunikationstechnik“ (siehe Kapitel 3.3) und „Voice over IP“ (siehe Kapitel 4.3). Im Folgenden wird diese Anpassung der Maßnahmen dargestellt und um spezifische Maßnahmen für Videokonferenzen ergänzt.

Der Maßnahmenkatalog zur Absicherung von Nutzung und Betrieb von Videokonferenzlösungen ist in die folgenden Blöcke aufgeteilt:

- Zentrale Systeme, Server und Anwendungen, siehe Kapitel 7.1.3.1
- Video-Terminals, siehe Kapitel 7.1.3.2
- Netzwerk, siehe Kapitel 7.1.3.3
- Netz- und Systemmanagement, siehe Kapitel 7.1.3.4

7.1.3.1 Zentrale Systeme, Server und Anwendungen

M-TK-117 Absicherung der zentralen Komponenten des Videokonferenzsystems

Für das ISDN-Gateway ist als grundlegende Härtungsmaßnahme M-TK-1 „Sperrung nicht benötigter oder sicherheitskritischer Leistungsmerkmale“ anzuwenden.

Für alle zentralen Komponenten des Videokonferenzsystems, die über das IP-Netz der Organisation oder über externe IP-Netze erreichbar sind (ISDN-Gateway, Videokonferenz-Gateway, MCU, Registrierungseinheit und Ressourcenmanagement), müssen die Maßnahmen M-TK-229 „Härtung von Servern des Telekommunikationssystems“ bis einschließlich M-TK-233 „Physische Sicherheit der Server der Telekommunikationslösung“ umgesetzt werden.

Die Notwendigkeit und Art der Anwendung von Maßnahme M-TK-234 „Berücksichtigung der Server der TK-Lösung im Datensicherungskonzept der Organisation“ muss je nach Anforderungen an die Verfügbarkeit entschieden werden.

Für zentrale Komponenten, die auf einem Standardbetriebssystem (z. B. Linux oder Microsoft Windows) laufen, sind Maßnahmen M-TK-235 „Schutz vor schadenstiftender Software für die Server der TK-Lösung“ und M-TK-236 „Einbindung der Server der TK-Lösung in das Patch-Management der Organisation“ umzusetzen.

M-TK-118 Durchgängige Verschlüsselung eines mit IP übertragenen Video-Medienstroms

Für den erhöhten Schutzbedarf muss ein mit IP übertragener Medienstrom durchgängig zwischen den IP-Kommunikationspartnern verschlüsselt werden. Hierzu ist Maßnahme M-TK-31 „Durchgängige Verschlüsselung des Medienstroms“ aus Kapitel 4 „Voice over IP“ für das Videokonferenzsystem umzusetzen.

Hinweis: Während die Übertragung des Medienstroms innerhalb einer Videokonferenzanlage (z. B. zwischen Video-Terminals und MCU) und zwischen einheitlichen Anlagen an verschiedenen Standorten einer Organisation mit den in Maßnahme M-TK-31 „Durchgängige Verschlüsselung des Medienstroms“ geforderten Mitteln für viele Produkte abgesichert werden kann, ist bei der Anlagen-übergreifenden Kommunikation insbesondere zwischen unterschiedlichen Organisationen mit erheblichen Problemen zu rechnen. Der Grund besteht darin, dass für die verfügbaren Videokonferenzlösungen in der Praxis etablierte Standards für die Verschlüsselung in einer heterogenen Anlagenumgebung fehlen. Daher verhindern in dieser Situation oft entweder Inkompatibilitäten eine Verschlüsselung oder aufwendige

Abstimmungen zwischen den Organisationen und manuelle Einstellungen an den Anlagen sind erforderlich.

M-TK-119 Durchgängige Verschlüsselung einer IP-basierten Video-Signalisierung

Für den erhöhten Schutzbedarf muss eine Video-Signalisierung, die über IP übertragen wird, durchgängig zwischen Video-Terminal bzw. einem Gateway und zentralen Systemen wie MCU und Registrierungseinheit verschlüsselt werden. Hierzu ist Maßnahme M-TK-32 „Durchgängige Verschlüsselung der Signalisierung“ aus Kapitel 4 „Voice over IP“ für das Videokonferenzsystem umzusetzen.

Falls die Maßnahmen

M-TK-117 „Absicherung der zentralen Komponenten des Videokonferenzsystems“,

M-TK-118 „Durchgängige Verschlüsselung eines mit IP übertragenen Video-Medienstroms“ und

M-TK-119 „Durchgängige Verschlüsselung einer IP-basierten Video-Signalisierung“

nicht akzeptabel umgesetzt werden können, müssen auf Ebene des Netzes Ausgleichsmaßnahmen ergriffen werden (siehe Kapitel 7.1.3.3).

M-TK-120 Authentisierung zwischen Video-Terminals und zentralen Video-Systemen

Für den erhöhten Schutzbedarf muss zwischen den Video-Terminals und den zentralen Video-Systemen, mit denen das Video-Terminal kommuniziert, eine Authentisierung erfolgen. Dabei sollte nach Möglichkeit eine gegenseitige Authentisierung stattfinden. Empfohlen wird der Einsatz von Mutual TLS (MTLS) unter Beachtung der Hinweise für den Einsatz von TLS in Kapitel 13.3.3.

M-TK-121 Sicheres Ressourcenmanagement für Videokonferenzen

Der Zugang zu Videokonferenzräumen muss gemäß Maßnahme M-TK-100 „Sicherung von Konferenzräumen“ abgesichert werden.

Teilnehmerdaten und andere kritische Videokonferenzdaten (z. B. Diensteprofile, nutzerspezifische Einstellungen sowie PINs zur Freischaltung von Diensten und zum Zugang zu Konferenzräumen) müssen sicher gespeichert werden. Die Berechtigungen für den Zugriff auf diese Daten müssen so eingestellt sein, dass nur die notwendigen Zugriffe für autorisierte Teilnehmer gestattet sind. Die Protokolle für den Zugang auf Telefoniedaten im Verzeichnisdienst müssen hinsichtlich Vertraulichkeit und Integrität abgesichert sein. PINs und sonstige Daten mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit und Integrität müssen dabei verschlüsselt hinterlegt werden.

Diese Forderung gilt auch für die Verwaltung von Videokonferenz-bezogenen Daten in einer Groupware oder in einem Verzeichnisdienst.

7.1.3.2 Video-Terminals

M-TK-122 Einschränkung des lokalen Zugriffs auf die Konfiguration des Video-Terminals

Das Video-Terminal stellt meist einen Zugang über Bedientasten am Gerät oder über eine Fernbedienung bereit, über die verschiedene Einstellungen vorgenommen und geändert werden können.

Dabei müssen grundsätzlich zwei Einstellbereiche unterschieden werden:

- Im ersten Bereich der Einstellungen kann der Benutzer z. B. Displayauflösungen oder Videosignalausgänge einstellen und den Kontrast des Displays ändern. Dieser Bereich sollte grundsätzlich bei jedem Video-Terminal freigegeben sein (Bedienzugang für den Anwender).
- In einem weiteren Bereich besteht Zugang zu den Netzwerk- und Administrations-einstellungen des Video-Terminals.

Nach einer Prozedur zum Entsperren der Einstellungen können diese auch geändert werden (lokaler Administrationszugang zum Video-Terminal). So könnte z. B. die IP-Adresse geändert werden. Der Zugriff auf diesen Bereich muss eingeschränkt werden.

Die vom Hersteller voreingestellte PIN für administrative Zugriffe bzw. ein voreingestelltes Kennwort (typisch sind leicht zu erratende PINs wie 0000 oder der Herstellername als Default-Kennwort) muss geändert werden. Die Komplexität von PIN oder Kennwort muss dabei möglichst hoch gewählt und wenn möglich durch das System geprüft werden.

M-TK-123 Automatische Annahme eines Video-Anrufs deaktivieren

Video-Terminals bieten in der Regel die Möglichkeit der automatischen Annahme eines Video-Anrufs. Damit ist es möglich, zu jeder Zeit einen Anruf auf eine bekannte Adresse eines Video-Terminals zu initiieren und über die automatische Annahme des Video-Anrufs, sowohl Bild als auch Ton zu aktivieren. Funktionen zur automatischen Annahme eines Video-Anrufs müssen im Video-Terminal deaktiviert werden. In keinem Fall darf es möglich sein, dass eine automatische Aktivierung eines Video-Terminals von außerhalb des Videokonferenzraumes erfolgen kann.

- Dass ein Video-Terminal in Betrieb ist, muss deutlich sichtbar sein, d. h. ein Video-Terminal muss eine sichtbare Aktiv-Leuchte besitzen.
- Zudem muss bei Inaktivität des Video-Terminals die Kamera automatisch so aus dem Raumsichtfeld gedreht werden, dass kein auswertbares Signal übertragen werden kann und die Tonübertragung deaktiviert wird. Hierdurch ist den Nutzern eines Raumes mit Videokonferenzlösung sofort sichtbar, ob ein Video-Terminal aktiv oder inaktiv ist.

M-TK-124 Deaktivierung / Ausschaltung des Video-Terminals

Video-Terminals bieten die Möglichkeit, das Gerät auszuschalten und damit zu deaktivieren. Hierbei ist darauf zu achten, nicht nur in den Stand-By-Modus zu wechseln, sondern das Video-Terminal vollständig auszuschalten. Bei Unsicherheit des zu erkennenden Betriebszustands sollte das Video-Terminal vom Netz getrennt werden.

M-TK-125 Anzeige der aktuellen Teilnehmer und Benachrichtigung bei neu eintretenden Teilnehmern einer Videokonferenz

Innerhalb der Anzeige des Video-Terminals sollten die teilnehmenden Video-Terminals angezeigt werden.

Treten neue Teilnehmer der Videokonferenz bei, so ist der Vorgang allen bereits in der Videokonferenz befindlichen Teilnehmern anzuzeigen.

7.1.3.3 Netzwerk

Beim Einsatz einer IP-basierten Videokonferenzlösung bestehen die identischen Sicherheitsmaßnahmen für das zugrunde liegende Netzwerk, die für VoIP in Kapitel 4.3.3 spezifiziert sind. Dabei wird insbesondere darauf hingewiesen, dass hier Maßnahmen genannt werden, die auch als Ausgleichsmaßnahmen in Betracht zu ziehen sind, falls Maßnahmen auf Ebene der zentralen Komponenten des Videokonferenzsystems nicht geeignet umgesetzt werden können:

- Falls die Maßnahme M-TK-117 „Absicherung der zentralen Komponenten des Videokonferenzsystems“ nicht umfänglich umgesetzt werden kann, müssen zumindest die betroffenen (ggf. alle) zentralen Komponenten einer Sicherheitszone gemäß Maßnahme M-TK-67 „Netztrennung für VoIP“ zugeordnet werden.

- Können die Maßnahmen M-TK-118 „Durchgängige Verschlüsselung eines mit IP übertragenen Video-Medienstroms“ und M-TK-119 „Durchgängige Verschlüsselung einer IP-basierten Video-Signalisierung“ nicht zufriedenstellend umgesetzt werden, ist Maßnahme M-TK-66 „VPN zur Kommunikation über eingeschränkt vertrauenswürdige Netze“ sinngemäß auf das Videokonferenzsystem anzuwenden. Für Bereiche, in denen auch dies nicht angemessen anwendbar ist, muss Maßnahme M-TK-67 „Netztrennung für VoIP“ auf das Videokonferenzsystem übertragen werden.

Für Videokonferenzen über ISDN ist bei erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit Maßnahme M-TK-22 „Gesicherte Übertragung der Sprachdaten zwischen Partnerstandorten durch Leitungsverschlüsselung“ in Betracht zu ziehen.

7.1.3.4 Netz- und Systemmanagement

Beim Einsatz einer Videokonferenzlösung sind die generellen Sicherheitsmaßnahmen für den Server-Betrieb sowie das Netz- und Systemmanagement, wie in Kapitel 10.2 und Kapitel 10.3 dargestellt, für alle zentralen Server-Komponenten der Videokonferenzlösung möglichst umzusetzen.

Dabei ist jedoch zu beachten, dass für Videokonferenzsysteme im Vergleich zur Telefonie oft geringere Verfügbarkeitsanforderungen bestehen. Dies zeigt sich insbesondere in der Überwachung der Systemverfügbarkeit eines Videokonferenzsystems, welche durch eine System-Monitoring-Plattform oder durch Monitoring-Funktionen des Netz- und Systemmanagements realisiert werden kann. Sofern die Anforderungen an die Verfügbarkeit es gestatten, kann ggf. sogar auf eine ständige Verfügbarkeits-überwachung verzichtet werden.

7.1.3.5 Übergreifende Aspekte

Die Maßnahme M-TK-86 „Harmonisierung zwischen IT-Betrieb und VoIP-Anlagen-Betrieb“ muss auf das Videokonferenzsystem ausgedehnt bzw. übertragen werden.

7.1.4 Zusammenfassung

Videokonferenzsysteme haben sich in letzter Zeit als Standardkomponente in vielen IT-Strukturen etabliert. Sie können zur Effizienzsteigerung beitragen, da hierdurch beispielsweise Reisen zur standortübergreifenden Zusammenarbeit häufig vermieden werden können.

Abhängig von der dem Videokonferenzsystem zugrunde liegenden Technologie unterliegen Videokonferenzsysteme den Gefährdungen und Maßnahmen von klassischer Telekommunikationstechnik (siehe Kapitel 3), Voice over IP (siehe Kapitel 4) und Unified Communications and Collaborations (siehe Kapitel 6).

Bei der Planung von Sicherheitsmaßnahmen müssen insbesondere folgende Angriffspunkte berücksichtigt werden, welche sich aus den Gefährdungen für die zugrunde liegenden Technologien ergeben:

- zentrale Systeme der Videokonferenzanlage
- Schnittstellen zur Anbindung an Netzinfrastrukturen, insbesondere Gateways und Konferenzbrücken
- Endgeräte, d. h. Video-Terminals, welche an der Videokonferenz teilnehmen

Die Angriffsrisiken sind entsprechend den bereitgestellten Nutzungsmöglichkeiten, den Verfügbarkeits-anforderungen und der geforderten Vertraulichkeit der über Videokonferenzen ausgetauschten Daten zu bewerten und müssen durch Sicherheitsmaßnahmen minimiert werden.

Besonders zu beachten sind dabei aus Sicht der Zielumgebung

- die Notwendigkeit auch externe Teilnehmer einzubinden,
- die konkret zu berücksichtigenden Verfügbarkeitsanforderungen sowie

- die zu berücksichtigende Notwendigkeit zu Mitschnitten von Videokonferenzen und deren Aufbewahrung.

Die Erarbeitung und Umsetzung einer Sicherheitskonzeption umfasst neben den generell zu ergreifenden Maßnahmen (siehe Kapitel 10) und den für die ggf. zugrunde liegenden Technologien klassische Telekommunikationstechnik (siehe Kapitel 3.3), Voice over IP (siehe Kapitel 4.3) und Unified Communications and Collaboration (siehe Kapitel 6.3) spezifizierten Maßnahmen die folgenden Aspekte:

Absicherung der zentralen Videokonferenzanlage

Zentrale Komponenten der Videokonferenzlösung müssen entsprechend dem Schutzbedarf für die eingesetzten Technologien gezielt gehärtet werden. Weiterhin ist, sofern erforderlich, ein angemessener Zugangsschutz zu Räumen mit Videokonferenzsystemen einzusetzen. Weiterhin sind die zugrunde liegenden Technologien entsprechend dem Schutzbedarf so einzurichten, dass ein sicherer Betrieb möglich ist.

Die Anlagenkomponenten müssen so konfiguriert werden, dass eine initiale Authentisierung und eine verschlüsselte Übertragung von Sprach- und Datenströmen möglich ist. Einzelheiten wie eingesetzte Protokolle sind in Abhängigkeit von den eingesetzten Schnittstellen und TK-Technologien abzusichern.

Absicherung von Video-Terminals

Video-Terminals müssen oft in Räumen aufgestellt werden, die wechselnden Personen zugänglich sind (Konferenzräume). Durch eine gezielte Konfiguration der Video-Terminals ist sicherzustellen, dass diese stets im gewünschten Zustand sind und nicht missbräuchlich von extern gesteuert werden können. Insbesondere Automatismen, die unbemerkte Statuswechsel ermöglichen, sind gezielt abzuschalten und der Status des Systems muss stets erkennbar sein. Es wird so vermieden, dass Kamera und Mikrofon unbemerkt zum unbefugten Ausspionieren von Gesprächen und Vorgängen im Konferenzraum verwendet werden können.

Weiterhin sind Videokonferenzsysteme gegen unbemerkte unbefugte Teilnahme eines Angreifers an einer Videokonferenz zu sichern. Beim Hinzukommen neuer Teilnehmer muss daher die Konferenzanlage an alle Teilnehmer eine Benachrichtigung übermitteln.

Sicherheitsbeiträge im internen Netz der Organisation

In manchen Fällen kann es vorkommen, dass die Maßnahmen zur Absicherung von zentralen Komponenten bzw. zur Verschlüsselung von Kommunikation nicht geeignet umgesetzt werden können. Hier sind dann Sicherheitsmaßnahmen im Netzbereich umzusetzen, um die notwendige Sicherheit zu garantieren.

Übergreifende Aspekte

Um das geforderte Sicherheitsniveau zu erreichen, ist ein abgestimmter Betrieb von Videokonferenzanlage und der zur Außenanbindung genutzten TK-Anlage notwendig.

7.2 Kontaktcenter

Kontaktcenter realisieren die massenhafte Kommunikation mit – meist externen – Kommunikationspartnern und bündeln diese Kommunikation in einer integrierten Lösung. Man unterscheidet Lösungen für die eingehende (engl. inbound) und die ausgehende (engl. outbound) Kommunikation. Systeme für Inbound-Kontaktcenter analysieren, klassifizieren und verteilen dabei die eingehenden Kontaktaufnahmen an die mit der Kommunikation betrauten Sacharbeitern (Agenten). Outbound-Lösungen automatisieren die Kontaktaufnahme mit externen Ansprechpartnern und optimieren diese im Sinne einer hohen Arbeitseffizienz der Agenten. Kontaktcenter besitzen in vielen Organisationen einen hohen Stellenwert, da sie oft mit der Abarbeitung von geschäftskritischen Prozessen betraut sind. Da in Kontaktcentern häufig personenbezogene oder anderweitig schützenswerte Daten verarbeitet werden, sollte diesen Systemen ein besonderes Augenmerk gelten. Der Schutzbedarf der Systeme leitet sich hierbei in erster Linie aus dem konkreten Anwendungsfall und dem Schutzbedarf der verarbeiteten Daten ab.

Die grundlegenden Eigenschaften von Lösungen für Kontaktcenter, die Gefährdungen in diesem Bereich sowie die zugehörigen Sicherheitsmaßnahmen und Sicherheitskonzepte zur Absicherung der Datenhaltung, der Integrationsschnittstellen und der eigentlichen Kommunikation werden im Folgenden beschrieben.

7.2.1 Basiswissen

7.2.1.1 Kommunikationskanäle und Medien

Inbound- und Outbound-Kontaktcenter bedienen heute eine Vielzahl von Kommunikationskanälen, über die ein Kontaktweg für Kunden oder Bürger bereitgestellt wird. Die wesentlichen, heute zu berücksichtigenden Kommunikationswege sind:

- Telefonie & VoIP
- Fax
- E-Mail
- Videokommunikation
- Instant Messaging
- Rückruf-Formulare im Web (Web Callback)
- Chat-Unterstützung beim Surfen (Webchat)
- Kommunikation via Soziale Netzwerke und Medien (SNM)

Die Basistechniken zur Bereitstellung der diversen Kommunikationskanäle entsprechen grundsätzlich den Beschreibungen in den zugehörigen Kapiteln dieser Technischen Leitlinie. Dies gilt insbesondere für Telefonie, Fax und VoIP (siehe Kapitel 3 und Kapitel 4), Instant Messaging bzw. Webchat und Video (siehe Kapitel 6 und Kapitel 7.1) sowie Kommunikation über Soziale Netzwerke und Medien (siehe Kapitel 8.1). Leistungsmerkmale wie Web Callback nutzen die bereits beschriebenen Kommunikationsmedien, werden jedoch über Systemschnittstellen in das automatisierte Routing der Kontaktcenter-Lösung integriert. Die sichere E-Mail-Kommunikation liegt außerhalb des Fokus dieser Technischen Leitlinie. Hierzu sei auf die relevanten Maßnahmen der IT-Grundschutz-Kataloge verwiesen, insbesondere:

- M 5.108 „Kryptographische Absicherung von Groupware bzw. E-Mail“
- M 5.109 "Einsatz eines E-Mail-Scanners auf dem Mailserver"
- M 5.116 "Integration eines E-Mail-Servers in ein Sicherheits-Gateway"

7.2.1.2 Systemarchitektur

Um die verschiedenen Kommunikationskanäle bereitzustellen, wird eine System-Schicht für Verarbeitung und Zustellung der Kommunikation an den Kommunikationspartner bzw. den Kontaktcenter-Agenten benötigt („Processing & Routing“). Die Kopplung mit Arbeitsplatzanwendungen und Datenbeständen der Organisation wird durch die System-Schicht „Applikationen“ realisiert. Die Überwachung und Einsatzplanung wird durch die Schicht „Monitoring & Management“ bereitgestellt. In diesen Schichten sind jeweils diverse Subsysteme angesiedelt. Abbildung 41 zeigt die grundlegende Struktur inklusive der Systemschichten am Beispiel eines Inbound-Kontaktcenters.

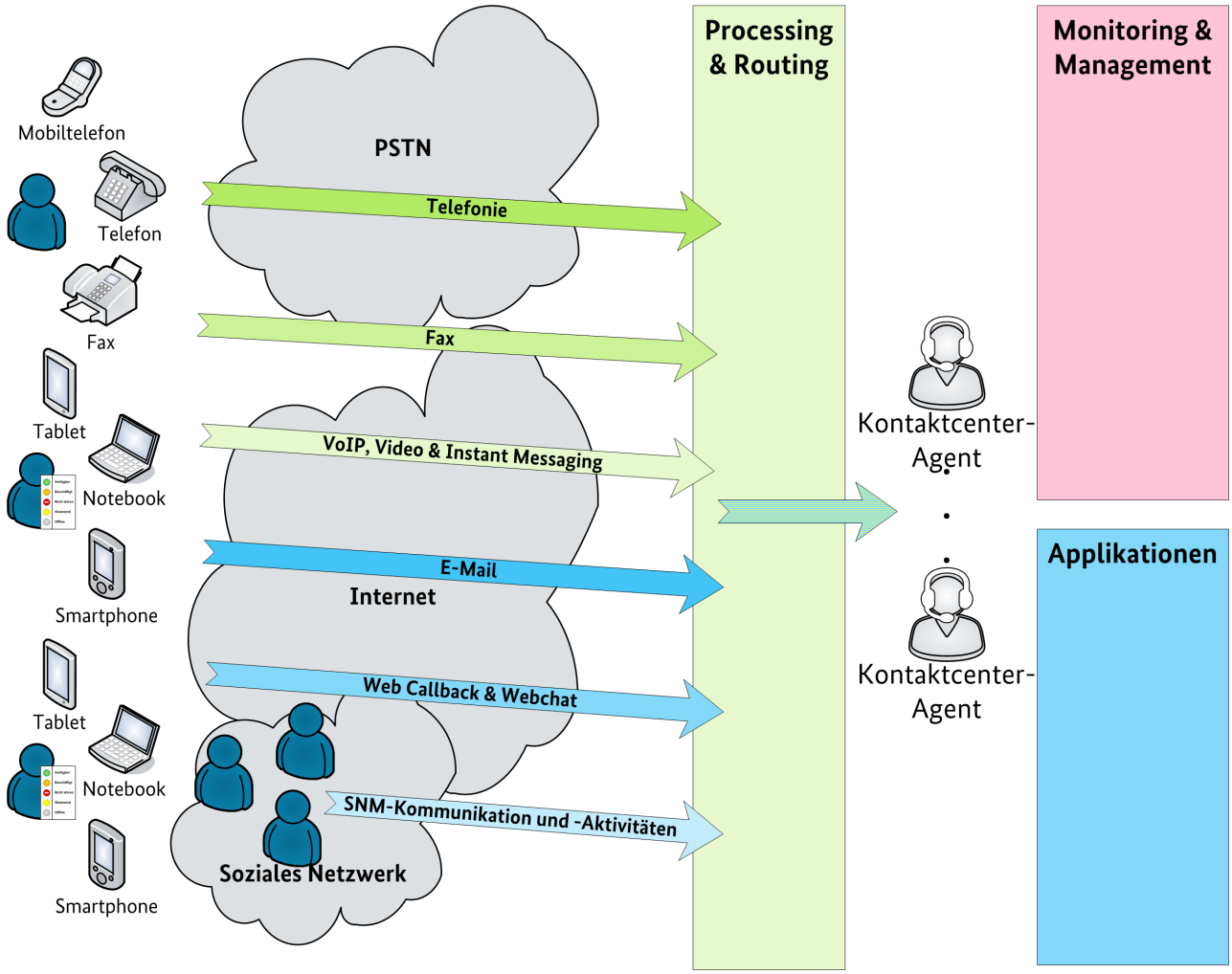


Abbildung 41: Prinzipdarstellung eines typischen Inbound-Kontaktcenter

Die grundlegende Struktur eines Outbound-Kontaktcenter ist identisch zu der eines Inbound-Kontaktcenters. Jedoch gestaltet sich der Layer „Processing & Routing“ unterschiedlich und ist in der Regel auf die Verarbeitung weniger Medien (oft nur Sprachkommunikation) beschränkt.

Die Systemschicht „Processing & Routing“ beinhaltet die herkömmlichen Routing-Systeme für Sprachkommunikation und Unified Communications and Collaboration. Zudem sind hier Systeme für die Außenanbindung (z. B. IP-ISDN-Gateway, SNM-Konnektor) angesiedelt. Weitere Instanzen terminieren und bedienen Kommunikationskanäle (Fax-Server, E-Mail-Server, Interactive Voice / Video Response (IVR) und Media-Server). Hier wird die Kommunikation entweder abschließend bearbeitet (z. B. IVR) oder für ein weiteres Routing vorgehalten (z. B. Fax-Server).

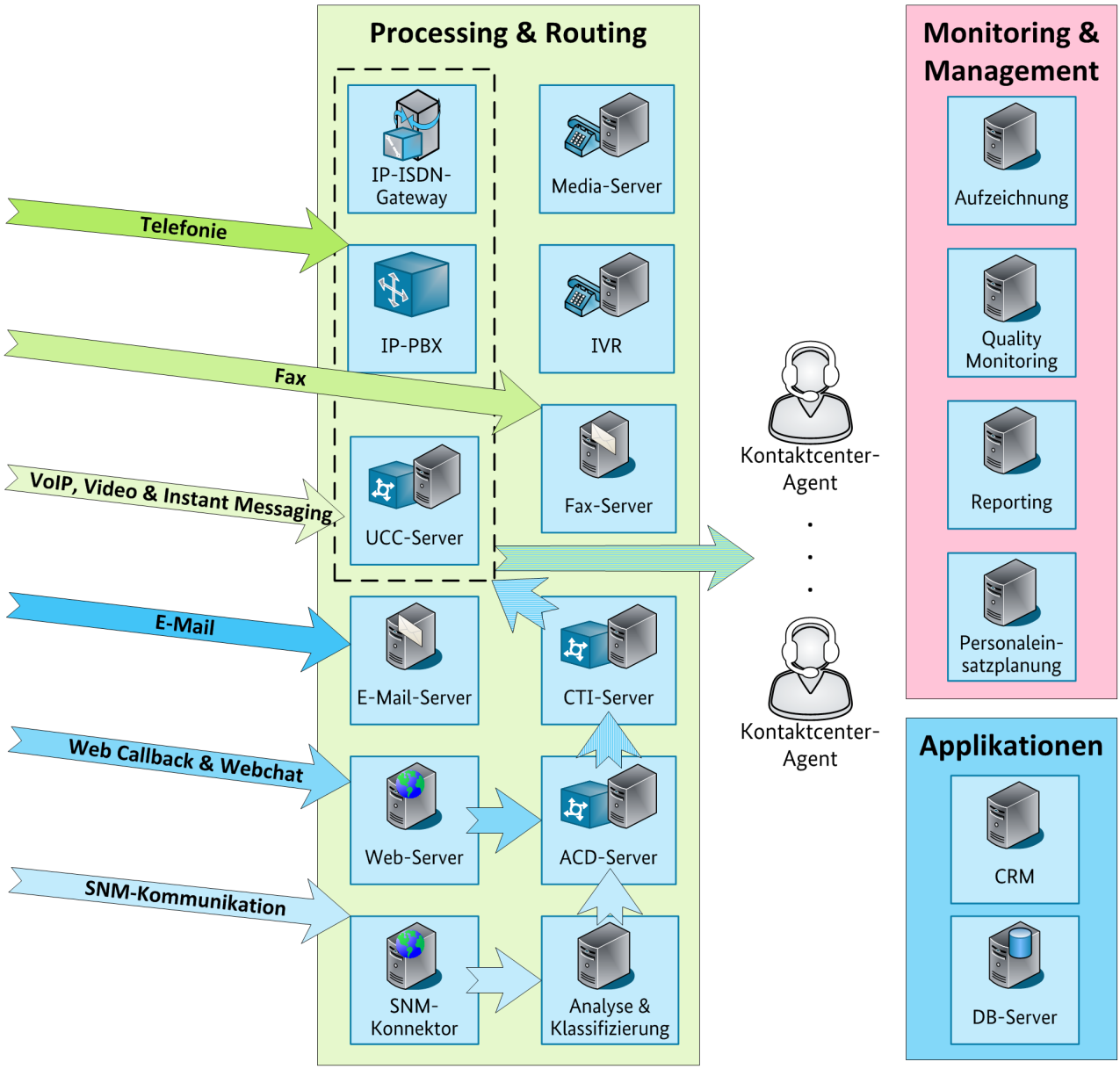


Abbildung 42: Detailansicht der Systemebene eines typischen Inbound-Kontaktcenter

Weitere Systeme dienen der Analyse und Klassifizierung von Kommunikation, der Anwendung von Algorithmen zur Verteilung von eingehenden Kommunikationsanfragen (Automatic Call Distribution, ACD) und der Steuerung und Integration der Kommunikationsinfrastruktur (CTI-Server). Ein Outbound-Kontaktcenter verfügt im Wesentlichen über dieselben Systeme im Layer „Processing & Routing“. Jedoch tritt ein sogenannter Dialer zur automatisierten Abarbeitung von Kontaktlisten (sogenannte Kampagnen) an die Stelle des ACD-Systems. Auch die Systeme zur Terminierung von Inbound-Kontakten (z. B. IVR, SNM-Konnektor) entfallen im Outbound-Kontaktcenter.

Die Applikationsschicht stellt die Einbindung in die Applikations- und Prozesslandschaft der Organisation sicher. Hier sind beispielsweise das Customer Relationship Management (CRM) oder Datensysteme enthalten. Der Bereich Monitoring & Management umfasst Systeme zur Personaleinsatzplanung, zur Qualitätsüberwachung und Berichtgenerierung sowie zur Aufzeichnung der abgewickelten Kommunikation. Die in den jeweiligen Schichten angesiedelten Systeme sind in Abbildung 42 dargestellt. Hier ist zudem anhand von Pfeilen das vereinfachte Zusammenspiel der Infrastruktur zum Routing von SNM-Kommunikation, Web Callback und Webchat dargestellt.

Viele der Systeme der Schicht Processing & Routing wurden bereits für die zugrunde liegenden Technologie beschrieben. Darüber hinaus sind die Systeme IVR, ACD und Dialer, Analyse & Klassifizierung und Computer Telephony Integration (CTI) von besonderem Interesse. Die Schicht Monitoring & Management ist insbesondere in Hinblick auf Aufzeichnung und Überwachung von Kommunikation zu berücksichtigen. Die Applikations-Schicht liegt, abgesehen von den zugehörigen Schnittstellen zur CTI-Kopplung, außerhalb des Fokus dieser Technischen Leitlinie.

7.2.1.3 Interactive Voice Response

Interactive Voice Response (IVR) bietet die Möglichkeit, teil- oder vollautomatisierte Sprachdialoge zu führen. Dies umfasst sowohl einfache Sprachmenüs, durch die per Tastendruck navigiert werden kann („*Für den Vertrieb drücken Sie bitte die '1', für Service die '2', ...*“), als auch Systeme, die einen natürlichsprachlichen Dialog zur Abfrage von Informationen (z. B. Fahrplanauskünften) erlauben. IVR-Applikationen dienen sowohl der fallabschließenden Kommunikation (z. B. Informationsabfrage) als auch der Vorqualifizierung eines Anrufs zur weiteren Bearbeitung durch menschliche Agenten.

Bei frühen IVR-Systemen wurde nicht klar zwischen Applikationen (d. h. den konkreten Dialogabläufen) und der ausführenden Plattform getrennt. Die möglichen Dialoge waren bei solchen Systemen praktisch vorgegeben und nur schwer zu ändern bzw. anzupassen. Im Laufe der Zeit entwickelten die Hersteller von IVR-Systemen verschiedene proprietäre Dialogbeschreibungssprachen, die es den Administratoren und Anwendern erlauben, eigene Sprachapplikationen zu entwickeln und anzupassen. Inzwischen existiert eine Reihe von Standards für Sprachen zur Beschreibung von Dialogabläufen. Einer der bekanntesten Standards ist die XML-basierte Empfehlung des World Wide Web Consortium (W3C) namens VoiceXML (Voice Extensible Markup Language). Mithilfe von VoiceXML können Sprachapplikationen in ähnlicher Weise entwickelt und bereitgestellt werden wie visuelle Applikationen mittels HTML.

Aus dieser Ähnlichkeit ergeben sich Gefährdungen analog zu Web-Applikationen. Zum einen kann ein Sprachdialogsystem Zugriff auf schützenswerte Daten geben. Zu solchen Applikationen zählen beispielsweise das Telefon-Banking, der Anrufbeantworter im Netz oder die Abfrage des E-Mail-Postfachs per Telefon. Somit muss der Zugriff auf die gesamte Applikation bzw. auf schützenswerte Punkte gesichert sein. Bei Web-Applikationen erfolgt die Authentisierung in der Regel durch Benutzername und Passwort, während bei IVR-Systemen meist eine Personal Identification Number (PIN) verwendet wird. Die Stimmbiometrie findet zunehmend Verbreitung zur Absicherung des Zugriffs auf schützenswerte Daten, weshalb im Kontaktcenter-Umfeld bereits vereinzelt Systeme zur Sprecher-Erkennung zum Einsatz kommen.

Neben der Kopplung mit der TK-Anlage über einen Sprachkanal, ist ein IVR-System häufig auch mit anderen IT-Komponenten der Applikationsschicht, z. B. mit Datenbanken, verbunden. Die spezifische IT-Komponente (und damit letztlich auch die spezifische Schnittstelle) hängt dabei von der implementierten IVR-Applikation ab. In der Regel werden für die Anbindung solcher externer Systeme jedoch die in Kapitel 13.2 vorgestellten Schnittstellen, wie LDAP (Lightweight Directory Access Protocol), ODBC (Open DataBase Connectivity) und SOAP sowie weitere RPC-Mechanismen, verwendet.

Schließlich verfügen IVR-Systeme auch über Administrations- und Konfigurationsschnittstellen. Das Spektrum reicht von dedizierten Applikationen zur Erzeugung neuer Applikationen, die über proprietäre Protokolle oder Dateiformate mit dem IVR-System kommunizieren, bis hin zu gewöhnlichen Web-basierten Management-Schnittstellen. Es gilt auch hier, dass mit dem Produkthersteller die konkrete Zahl und die Ausprägungen der Schnittstellen eines IVR-Systems geklärt werden sollten, um diese entsprechend abzusichern bzw. deaktivieren zu können.

7.2.1.4 Analyse und Klassifizierung, ACD und Dialer

Automatic Call Distribution (ACD) ist eine Kontaktcenter-spezifische Funktion, die eingehende Anrufe automatisch an eine definierte Menge von Mitarbeitern (sogenannte Kontaktcenter-Agenten) vermittelt. Ist kein freier Agent verfügbar, leitet das ACD-System den Anrufer automatisch an eine Warteschlange (engl. Queue) weiter. Diese Routing-Funktionalität ist ein wesentliches Kernelement des Inbound-Kontaktcenter.

Ursprünglich nur für die Verarbeitung von eingehenden Telefonanrufen gedacht, bieten moderne Kontaktcenter-Produkte auch das Inbound-Routing weiterer Kanäle wie z. B. E-Mail, Instant Messaging und Video. Je nach Medium werden hier verschiedene Warteschlangentypen implementiert. Während klassische Telefonanrufe in Wartefeldern unter Einspielung von Wartemusik (engl. Music-on-Hold) durch den Medien-Server realisiert werden, werden Nachrichtenformate wie Fax und E-Mail in Eingangspostfächern zur weiteren Bearbeitung vorgehalten und anschließend dem Agenten zur Bearbeitung zugestellt. Als Pendant zum Telefonwartefeld und zur klassischen IVR werden zukünftig Videowartefelder und interaktive Video-IVRs Einzug in das Kontaktcenter halten.

Das Ziel der Anrufverteilung über ACD ist die Effizienzsteigerung im Kontaktcenter bei gleichzeitiger Minimierung der Wartezeiten des Anrufers. Zudem soll die Zustellung an einen bearbeitenden Agenten derart gestaltet werden, dass die vom Kunden wahrgenommene Servicequalität steigt und die Rate der Anrufe, die mit dem Erstkontakt zur Kundenzufriedenheit behandelt wird (engl. First Call Resolution, FCR) maximiert wird. Hierzu werden Mechanismen zur Analyse und Klassifikation von Kommunikation eingesetzt. Bei eingehender Schriftkommunikation oder der Analyse von Inhalten aus Sozialen Netzwerken wird hierbei vermehrt auf semantische Inhaltsanalyse gesetzt. Diese Lösungen sind vermehrt lernfähig und müssen daher die erlernten Muster in einem Datenbank-Back-End speichern. Bei der Analyse eingehender Anrufe wird zumeist die Rufnummer berücksichtigt und ein Routing nach festgelegten Kriterien vorgenommen. Diese reichen vom Wohnort des Anrufers (Vorwahl), dem bevorzugten oder letzten Ansprechpartner (Agenten), über die Kontakthistorie mit dem Kunden bis hin zu offenen Vorgängen (z. B. Schaden am Kfz) und der automatischen Zuordnung zum entsprechenden Agententeam (Schadensregulierung Kfz). Es können auch die Fähigkeiten von Agenten (die sogenannten Skills) beim ACD-System hinterlegt werden, um eine Zuordnung des Anrufers zu einem qualifizierten Agenten vorzunehmen.

Hieraus ergibt sich, dass ACD-Systeme und Dienste zur Analyse und Klassifizierung über vielfältige Schnittstellen zu anderen IT-Systemen verfügen können. Typische Schnittstellen sind Datenbankanbindungen (u. a. ODBC und SOAP), die in Kapitel 13.2 vorgestellt werden.

Dialer veranlassen in Outbound-Kontaktcentern die Abarbeitung von Kampagnen, also die automatisierte Abarbeitung einer Aufgabenliste (z. B. den Anruf jeden Kontaktes einer Kundenliste zu Akquisitionszwecken). Diese Kampagnen werden in Form von Datensätzen für den Dialer und ggf. einer kampagnenspezifischen Anpassung der Agentenoberfläche programmiert. Diese Programmierung kann über Management-Oberflächen, die oft web-basiert bereitgestellt werden, durch Administrationspersonal vorgenommen werden. Zudem verfügen Dialer über Schnittstellen zur Eingabe der jeweiligen Adressdaten, also z. B. Schnittstellen zu Datenbanksystemen, Verzeichnisdiensten oder – zunehmend seltener – über Dateieingabe-Schnittstellen. Über eine CTI- oder Webservice-Schnittstelle steuert der Dialer zudem die Kommunikationslösung (siehe Kapitel 7.2.1.5). Diese Schnittstellen müssen bei einer Absicherung der Systeme entsprechend berücksichtigt werden.

7.2.1.5 Computer Telephony Integration und Applikationsanbindung

Computer Telephony Integration ermöglicht die Steuerung eines Telefons von einem PC aus. Die grundlegenden Eigenschaften dieser Schnittstelle werden im Kapitel 6.1.9 dargelegt. Im Kontaktcenter werden diese Schnittstellen jedoch auch von anderen Server-Systemen zur Steuerung des Routings und zum Abgriff relevanter Informationen verwendet.

So verwenden Dialer und ACD-Lösungen häufig die CTI-Schnittstellen eines Kommunikationssystems, um das Routing von Anrufen zu Agentenarbeitsplätzen und anderen Systemen, z. B. zu Wartefeldern und IVR, zu steuern.

Zur Integration in die Applikationsschicht eines Kontaktcenters werden ebenfalls CTI-Schnittstellen genutzt. Über eine Integration in das Customer Relationship Management wird Click-to-Call für Agenten und Supervisor realisiert. Diese manuelle Anrufsteuerung ist auch im hoch automatisierten Kontaktcenter notwendig, um Weitervermittlung und Rückfrage bei Dritten zu realisieren. Des Weiteren werden Verbindungsdaten zu Kommunikationsvorgängen (z. B. eingehender Anruf eines Kunden) im CRM-System dem jeweiligen Kunden-Datensatz zugeordnet.

Die eingesetzten Protokolle entsprechen im Wesentlichen denen, welche für klassische CTI-Anwendungen im Telefonie- bzw. UCC-Umfeld verwendet werden. Einen Überblick über diese Schnittstellen bietet Kapitel 13.2.2.

7.2.1.6 Monitoring und Management

Im Bereich Monitoring und Management kommen üblicherweise die folgenden Systeme zum Einsatz:

- Aufzeichnung (Recording)
- Qualitätsüberwachung (Quality Monitoring)
- Berichtserstellung (Reporting)
- Personaleinsatzplanung

Weitere Systeme in dieser Schicht können Management-Systeme z. B. für die Gestaltung von Abläufen in IVR oder für die Kampagnenplanung sein.

Insbesondere Systeme zur Aufzeichnung und Speicherung von Sprach- und Schriftkommunikation enthalten oft sensible und schützenswerte Inhalte. Diese sind jedoch oft aus rechtlichen Gründen oder zur Sicherstellung der Servicequalität zwingend erforderlich. Grundsätzlich ist zwischen zentraler und dezentraler Aufzeichnung zu unterscheiden. Eine zentrale Aufzeichnung erfordert die Umleitung des Medienstroms über das zentrale System. Aufgrund der Peer-to-Peer-Charakteristik von Voice over IP setzt sich hier jedoch zunehmend eine dezentrale Aufzeichnung durch, bei der von dezentralen Sensoren (z. B. IP-Tischtelefonen) die aufgezeichneten Medienströme an das zentrale Speichersystem geliefert werden. Eine dezentrale Speicherung der Medienströme auf dem Client oder Endgerät ist aufgrund der hohen Anforderungen an die Integrität der Aufzeichnungen im Kontaktcenter eher unüblich.

Systeme zur Qualitätsüberwachung ermöglichen neben der Überwachung von technischen Qualitätskriterien auch die stichprobenartige Kontrolle der durch die Agenten geführten Gespräche. Hierzu kann sich ein Supervisor still in das Gespräch eines Agenten zuschalten oder nachträglich ein aufgezeichnetes Gespräch kontrollieren. Quality-Monitoring-Systeme dienen in erster Linie der Qualitätsüberwachung in Echtzeit.

Reporting-Systeme dienen der Kontrolle der Auslastung, Leistungsfähigkeit und Effizienz eines Kontaktcenters. Es werden statistische Daten erhoben und für die regelmäßige Berichtserstellung aufbereitet. Reporting-Systeme dienen in erster Linie einer Bewertung a posteriori, z. B. als Grundlage für die zukünftige Personaleinsatzplanung (PEP). PEP selbst wird durch weitere Systeme realisiert, welche die Einteilung von personellen Ressourcen in Agentengruppen und eine Zuordnung zu bestimmten Aufgaben durchführen (z. B. Sachbearbeitung eingehender Produktanfragen, Mitarbeit in einer Outbound-Kampagne zur Neukundengewinnung). Die Personaleinsatzplanung wird durch die Verantwortlichen des Kontaktcenters vorgenommen (z. B. Schichtleiter, Leitung des Kontaktcenters). Die Tools zur Personaleinsatzplanung und weitere Management-Systeme im Kontaktcenter sind häufig webbasiert.

7.2.2 Gefährdungen

Kontaktcenter-Lösungen bilden in vielen Organisationen geschäftskritische Anwendungen und Prozesse ab. Ein Ausfall des Kontaktcenters kann für eine Organisation signifikante Einschnitte in das Tagesgeschäft bedeuten, die mit hohen finanziellen Verlusten oder einem Image-Schaden verbunden sein können. Ein Beispiel ist der Ausfall des Kontaktcenters einer Versicherung zur saisonbedingten Stoßzeit. Hierdurch ergibt sich für diese Fälle ein erhöhtes Risiko und dementsprechend höhere Anforderungen an Verfügbarkeit und Ausfallsicherheit.

Zudem sind Kontaktcenter häufig tief in die bestehende Kommunikations- und Applikationslandschaft integriert, da dies für eine Steigerung von Kommunikationseffizienz und Kundenzufriedenheit unerlässlich ist. Aus dieser Vielzahl von Integrationsschnittstellen ergibt sich eine erhöhte Gefährdung des Gesamtsystems, weshalb eine Absicherung dieser Schnittstellen nach Stand der Technik erfolgen muss.

Hinzu kommt, dass im Kontaktcenter häufig personenbezogene und andere sensible Daten in großem Umfang verarbeitet werden. Ein Beispiel ist die Aufnahme und Verarbeitung von Patientendaten im Kontaktcenter einer Krankenversicherung. Es besteht die Gefahr eines Vertraulichkeitsverlusts, was ein hohes Risiko für die Organisation oder den Kommunikationspartner (z. B. Kunden, Versicherter) der Organisation bedeuten kann.

In Kontaktcenter-Lösungen wird zunehmend eine Vielzahl von Kommunikationskanälen bedient. Diese Kommunikationskanäle sind einer Vielzahl von Gefährdungen ausgesetzt. Die Gefährdungen sind den zum jeweiligen Kommunikationskanal gehörigen Beschreibungen in dieser Technischen Leitlinie zu entnehmen. Hier sei insbesondere auf die Gefährdungen der Kapitel 3.2, 4.2, 6.2 und 8.1.2 verwiesen.

Die hierüber hinausgehenden Gefährdungen der Kontaktcenter-spezifischen Systeme sind im Folgenden aufgeführt.

7.2.2.1 Höhere Gewalt

Auf Kontaktcenter-Installationen treffen wie für alle IT-Lösungen allgemein die Gefährdungen durch höhere Gewalt zu, die in den IT-Grundschutz-Katalogen genannt sind. Es ist zudem zu beachten, dass aufgrund des hohen Stellenwertes des Kontaktcenters in der Organisation (z. B. für das Geschäftsmodell eines Versicherungsunternehmens) besondere Anforderungen an die Ausfallsicherheit eines Kontaktcenters bestehen können. Ist dies gemäß Schutzbedarfsanalyse der Fall, so ist der technischen Realisierung der Hochverfügbarkeit und der Überlebensfähigkeit des Kontaktcenters im Katastrophenfall besonderes Augenmerk zu schenken. Dies muss im Business Continuity Management (BCM) und im Risikomanagement Berücksichtigung finden.

7.2.2.2 Organisatorische Mängel

Organisatorische Mängel treffen Kontaktcenter-Systeme grundsätzlich genauso wie beliebige andere IT-Systeme. Mit der Einführung eines IT-gestützten Kontaktcenter-Systems müssen bestehende Entscheidungen und Konzepte für eine durch das Kontaktcenter mitgenutzte IT-Infrastruktur gezielt überprüft werden. Gefährdungen durch organisatorische Mängel ergeben sich insbesondere

- bei einer unzureichender Schutzbedarfsfeststellung,
- bei fehlenden oder fehlerhaften zentralen Elementen in Sicherheitskonzepten und
- bei fehlenden oder fehlerhaften organisatorischen Regelungen im Bereich Technikbetrieb.

Besonders zu beachten sind zudem

- die erhöhte Gesamtwirkung einer Gefährdung durch die Server-seitige Integration verschiedener IT-, TK- und Kontaktcenter-Systeme sowie
- das möglicherweise erhöhte Risiko aufgrund der großen Bedeutung des Kontaktcenters für kritische Geschäftsprozesse der Organisation.

7.2.2.3 Menschliche Fehlhandlungen

Durch die Kopplung von Kontaktcenter-Lösungen mit anderen Kommunikationssystemen und Applikationen steigt die Komplexität des Gesamtsystems. Damit wächst zum einen das Risiko einer menschlichen Fehlhandlung, da z. B. die Konsequenzen einer Handlung auf andere Teilsysteme mangels geeigneter Schulung nicht bedacht werden. Zum anderen wachsen auch die potenziellen Auswirkungen auf das Gesamtsystem, da durch die Integration Wechselwirkungen und Abhängigkeiten zwischen den Teilsystemen entstehen.

Damit gelten – sofern technisch anwendbar – grundsätzlich die im Gefährdungskatalog G.3 „Menschliche Fehlhandlungen“ der BSI IT-Grundschutz-Kataloge (siehe [BSI GSK-2013]) aufgeführten Gefährdungen. Es gelten insbesondere die folgenden Gefährdungen:

- G 3.3 „Nichtbeachtung von Sicherheitsmaßnahmen“
- G 3.7 „Ausfall der TK-Anlage durch Fehlbedienung“

Die Auswirkungen der jeweiligen Gefährdungen können jedoch systemübergreifend sein und auf diese Weise erheblich größere Schäden verursachen. Darüber hinaus können sich durch das Zusammenspiel verschiedener Dienste Gefährdungen kumulieren. Hierdurch entsteht ein höheres Gefährdungspotenzial als die Summe der jeweiligen Gefährdungen. Dies ist insbesondere zu beachten, wenn die allgemeine Kommunikationsinfrastruktur der Organisation für Kontaktcenter-Anwendungen mitgenutzt wird.

Spezifische Gefährdungen durch menschliche Fehlhandlungen sind:

G-TK-88 Fehlkonfiguration des IVR-Systems

Durch mangelhafte Authentisierung der Anwender am IVR-System oder eine fehlerhafte Integration und Zugriffssteuerung kann ein Angreifer Zugriff auf sensible Daten erlangen. Dies gilt insbesondere für den IVR-gestützten Zugriff auf Mehrwertdienste wie z. B. auf Mailboxen, Telefonbanking oder Patientendaten. Eine weitere mögliche Fehlerquelle sind die durch Administratoren der Organisation selbst erstellten IVR-Call-Flows.

G-TK-89 Fehlkonfiguration des Kommunikationsroutings

Durch eine versehentliche Fehlkonfiguration des Systemverbunds aus Analyse, Klassifizierung, ACD bzw. Dialer und Kommunikationslösung kann es zu falschem Routing ein- und ausgehender Kommunikation kommen. Bei Weiterleitung von Kommunikation an falsche, eventuell nicht autorisierte Adressaten kann es zu Vertraulichkeitsverlust, Produktivitätsverlust, wirtschaftlichen Einbußen und Reputationsverlust der Organisation kommen. Dem komplexen Zusammenspiel des Kommunikationsroutings im Kontaktcenter muss daher besonderes Augenmerk geschenkt werden.

7.2.2.4 Technisches Versagen

Für Kontaktcenter-Systeme und integrierte Applikationen gelten prinzipiell alle in den IT-Grundschutz-Katalogen genannten Gefährdungen wie Stromausfall, Datenbankausfall und mangelnde Verschlüsselung, sofern diese für ein konkretes System technisch relevant sind. Aufgrund der Vielfalt Kontaktcenter-naher Dienste und Applikationen sowie deren unterschiedlichen technischen Ausführungen werden an dieser Stelle keine weiteren Kontaktcenter-spezifischen Gefährdungen – wie etwa „Ausfall des ACD-Servers“ – genannt. Es gelten vielmehr sinngemäß die Gefährdungen für Unified Communications and Collaboration (siehe Kapitel 6.2.4).

7.2.2.5 Vorsätzliche Handlungen

Im Bereich der vorsätzlichen Handlungen besteht die wesentliche Gefährdung darin, dass Angriffe eine applikationsübergreifende Wirkung entfalten und im System verarbeitete, personenbezogene Daten betreffen können. Die Gefährdungslage konzentriert sich dabei auf die IP-basierten Komponenten eines Gesamtsystems, da sich hier die größte Angriffsfläche bietet und auf eine Vielzahl bereits bekannter Angriffsmethoden zurückgegriffen werden kann. Dennoch kann nicht ausgeschlossen werden, dass Angriffe auch über andere Kommunikationswege wie z. B. Fax, SMS oder ISDN erfolgen, wenn das Gesamtsystem diese Möglichkeiten bietet.

Im Kontaktcenter ist mit folgenden spezifischen Gefährdungen durch vorsätzliche Handlungen zu rechnen:

G-TK-90 Entwenden von sensiblen und personenbezogenen Daten

In vielen Kontaktcenter-Umgebungen wird eine massenhafte Verarbeitung sensibler und personenbezogener Daten durchgeführt. Aufgrund dieser Konzentration sensibler Daten sind Kontaktcenter-Umgebungen besonders anfällig für Angriffe auf die Vertraulichkeit dieser Daten. Die Angriffsvektoren reichen von den diversen Datenbankschnittstellen über die Kompromittierung von Systemen mit Anbindung an die betreffenden Datenbanken (z. B. IVR- oder ACD-Systeme) bis hin zum Client-seitigen Angriff. Hierbei ist zu beachten, dass neben einem Export der Daten aus der Client-Applikation auch das Erstellen von Bildschirmfotos (Screenshots) oder das Abfotografieren von Datensätzen möglich ist. Eine Automatisierung dieses Vorgangs, um mit hoher Geschwindigkeit Einzelabrufe von Datensätzen durchzuführen, diese zu erfassen und durch Texterkennung den Inhalt zu extrahieren, ist technisch problemlos realisierbar und erhöht das Schadenspotenzial erheblich. Ein solcher Angriff setzt lediglich einen entfernten Zugriff auf das Client-System voraus.

G-TK-91 Manipulation von Anrufverteilung oder Dialer

Durch die gezielte Manipulation der automatisierten Anrufverteilung bzw. der Dialer kann, wie auch bei unbeabsichtigter Fehlkonfiguration, ein Angreifer der Organisation erheblichen Schaden zufügen. Angriffspunkte für eine solche Manipulation sind die Systeme für Analyse und Klassifizierung, das ACD-System, der Dialer sowie die CTI-Schnittstelle. Auch die Routing-Konfiguration des Kommunikationssystems selbst sowie Editoren für eigendefinierte Routing-Regeln und die jeweiligen Quellsysteme für Routing-Entscheidungen können manipuliert werden. Das Spektrum der denkbaren Angriffsziele reicht von einer DoS-Attacke, über das Entwenden sensibler Informationen bis hin zu Gebührenbetrug durch die massenhafte Anwahl kostenpflichtiger Rufnummern.

G-TK-92 Attacken durch Missbrauch von Integration in öffentliche Webpräsenzen

Durch die Integration von Webschnittstellen in öffentlich zugängliche Webplattformen, z. B. ein Button zum Auslösen eines Rückrufs (Web Callback), können gezielte Attacken gegen ein Kontaktcenter geführt werden. So kann durch die automatisierte Platzierung von fingierten Rückrufanforderungen eine Überlastsituation mit eventuell gewichtigen wirtschaftlichen Folgen erzeugt werden. Zudem eröffnen öffentlich zugängliche Formulare zur Kontaktaufnahme Möglichkeiten des Gebührenbetrugs.

G-TK-93 Störung der Betriebsabläufe durch Manipulation von Management-Systemen

Durch Manipulationen an den diversen Management-Systemen können die Betriebsabläufe in einem Kontaktcenter erheblich gestört werden. Dies gilt z. B. für die Tools zur Personaleinsatzplanung. Durch Zugriff auf Systeme zur Qualitätsüberwachung ist zudem eine Behinderung des Geschäftsbetriebs durch Störung laufender Gespräche möglich.

7.2.3 Sicherheitsmaßnahmen

Im Folgenden werden die Maßnahmen zur Anwendung im Kontaktcenter beschrieben. Als Grundlage sind Sicherheitsmaßnahmen für VoIP-Systeme (siehe Kapitel 4.3) und – je nach Ausprägung des Kontaktcenters – für weitere Kommunikationskanäle anzuwenden (siehe Kapitel 3.3, 6.3 und 8.1.3). Zudem gelten im Zusammenhang mit Videounterstützung sinngemäß die Maßnahmen zu Videokonferenzen (siehe Kapitel 7.1.3).

Die beschriebenen Ansätze greifen zum Teil auch für andere vernetzte IT-Systeme bzw. auch bei normalem Schutzbedarf. Je nach Szenario und insbesondere für den erhöhten Schutzbedarf kommt es darauf an, aus dieser Gesamtheit der Maßnahmen jeweils angemessene Pakete zu bilden.

Der Maßnahmenkatalog zur Absicherung der Nutzung und des Betriebs von Kontaktcentern ist in die folgenden Blöcke aufgeteilt:

- Server und Anwendungen, siehe Kapitel 7.2.3.1
- Endgeräte und Clients, siehe Kapitel 7.2.3.2
- Netzwerk, siehe Kapitel 7.2.3.3
- Netz- und Systemmanagement, siehe Kapitel 7.2.3.4
- Übergreifende Aspekte, siehe Kapitel 7.2.3.5

7.2.3.1 Server und Anwendungen

Es gelten sinngemäß, je nach eingesetzten Kommunikationskanälen, die in den Kapiteln Voice over IP, Unified Communications and Collaboration sowie Soziale Netzwerke und Medien aufgeführten Maßnahmen bzgl. Server und zentraler Komponenten. Ergänzende Maßnahmen werden im Folgenden dargestellt.

M-TK-126 Authentisierung am IVR-System

Falls durch das IVR-System ein Zugriff auf Daten mit möglicherweise sensiblem Inhalt zugegriffen werden soll, so muss dieser Zugang mit einem dem Schutzbedarf angemessenen Verfahren zur Anrufer-Authentisierung abgesichert werden. Anwendungsbeispiele sind die telefonische Abfrage von Versicherungsdaten, das Telefon-Banking sowie eine Abfrage des persönlichen Unified-Messaging-Postfachs oder -Kalenders.

Die einfachste Authentisierungsmethode ist der Abgleich der Anruferkennung mit der bekannten Telefonnummer des IVR-Nutzers. Diese Methode ist z. B. beim Zugriff auf die persönliche Voicemail des Mobilfunkanbieters gebräuchlich. Da die Anruferkennung leicht manipuliert werden kann, bietet sie keinen nennenswerten Schutz. Lediglich in geschlossenen Systemen wie z. B. innerhalb des Mobilfunknetzes eines Anbieters, bei denen die Anruferidentität geprüft und zusätzliche Faktoren wie die International Mobile Subscriber Identity (IMSI) einbezogen werden können, bietet diese Methode einen Basisschutz. Als alleinige Maßnahme bei erhöhtem Schutzniveau ist sie vollkommen ungeeignet.

PIN-Abfragen sind heute noch immer die gebräuchlichste Authentisierungsmethode für IVR. Hierbei ist zu beachten, dass diese PINs nur eine geringe Komplexität (numerische PINs) aufweisen und in der Regel mit einer vier- bis sechsstelligen Kombination kein hohes Schutzniveau aufweisen. Diese Authentisierungsmethode ist daher nicht für Inhalte mit erhöhtem Schutzbedarf geeignet.

In organisationsinternen IP-basierten Systemen könnte zudem eine Authentisierung des Endgerätes bzw. Clients auf Basis von Zertifikaten erfolgen. Während eine Zertifikats-basierte Authentisierung an der Kommunikationsinfrastruktur gebräuchlich und für den erhöhten Schutzbedarf geeignet ist, ist die Authentisierung an einem Einzelsystem wie IVR in der Praxis nicht gebräuchlich.

Mit steigender Qualität von Spracherkennung und Analyse gewinnt zudem die sprachbasierte Anruferauthentisierung an Bedeutung. Diese Methode hat das Potenzial, eine zuverlässige Erkennung des Anrufers – und somit seiner Autorisierungsstufe – anhand der Stimmbiometrie zu gewährleisten. Die Tauglichkeit der eingesetzten Stimmbiometrie-Lösung sollte dabei unbedingt durch ein unabhängiges Gutachten oder eine Zertifizierung durch eine vertrauenswürdige Instanz nachgewiesen werden. Es ist zu beachten, dass das abgefragte Sprachmuster für den Angreifer nicht vorhersehbar sein darf. Ansonsten würde einem Angreifer eine einfache Sprachprobe des rechtmäßigen Besitzers zur Authentisierung am System genügen. Es empfiehlt sich daher eine Abfrage von zufällig gewählten Sätzen, Wort- oder Zahlenkombinationen. Eine so gestaltete Lösung bietet ein höheres Schutzniveau als eine einfach PIN-Abfrage.

Für einen Zugriff auf Daten mit erhöhtem Schutzbedarf kann eine Nutzerauthentisierung durch eine Kombination der vorgenannten Methoden im Sinne einer Zwei-Faktor-Authentisierung erfolgen.

M-TK-127 Qualitätssicherung der Routing-Regeln

Die Routing-Regeln von IP-basierten TK-Anlagen, UCC-Lösung und ACD-System sowie Call-Flows von IVRs sind verwundbar für Fehlkonfigurationen und Manipulation durch Angreifer. Um eine versehentliche Fehlkonfiguration und die daraus resultierende Betriebsbeeinträchtigung des Kontaktcenters zu vermeiden, sollten veränderte Routing-Regeln vor Einspielen in das System einer Qualitätssicherung durch sachkundiges, mit den eingesetzten Produkten vertrautes Personal erfolgen. Wenn möglich sollte hierzu die entsprechende Konfiguration in einer dem Produktivsystem nachempfundenen Testumgebung geprüft werden. Änderungen an Routing-Regeln sind zudem einem geordneten Change Management zu unterziehen, damit die Fehlkonfiguration vermieden bzw. rechtzeitig erkannt und revidiert werden kann.

7.2.3.2 Endgeräte und Clients

Es gelten sinngemäß, je nach eingesetzten Kommunikationskanälen, die in den Kapiteln Voice over IP, Unified Communications and Collaboration sowie Soziale Netzwerke und Medien aufgeführten Maßnahmen bzgl. der Endgeräte. Ergänzende Maßnahmen werden im Folgenden dargestellt.

M-TK-128 Data Loss Prevention am Agentenarbeitsplatz

Werden am Agentenarbeitsplatz sensible oder personenbezogene Daten verarbeitet, so muss der Agentenarbeitsplatz entsprechend abgesichert werden. Eine grundlegende Maßnahme ist es, dem Mitarbeiter (Agent) administrative Rechte zu entziehen. Des Weiteren sollte das Erstellen von Screenshots und die Verwendung von USB-Sticks (oder vergleichbaren Datenträgern) unterbunden werden. Je nach Schutzbedarf kann zudem ein Host-basiertes System für Data Loss Prevention ergänzend zum Einsatz kommen.

M-TK-129 Authentisierung des Zugriffs auf Kontaktcenter-Anwendungen

Der Zugriff auf Kontaktcenter-Systeme und -Anwendungen sollte durch eine Authentisierung nach Stand der Technik abgesichert werden. Diese ist durch eine Verschlüsselung der übertragenen Daten und Medienströme zu ergänzen. Dies gilt insbesondere für Agenten-arbeitsplätze, an denen sensible Daten verarbeitet werden. Ist dies nicht möglich, kann alternativ eine Abschottung des Netzes vor unbefugtem Zugriff erfolgen.

M-TK-130 Verhinderung des automatisierten Zugriffs auf Internet-Kontaktformulare

Um eine Störung der Betriebsabläufe oder sogar eine Denial-of-Service-Attacke über Webschnittstellen und Kontaktformulare zu vermeiden, sollte die automatisierte Kontaktaufnahme über Kontaktformulare und Web-Callback-Mechanismen unterbunden werden. Als Zugriffsschutz eignet sich z. B. die Abfrage eines nicht maschinenlesbaren Codes, der einen automatisierten, massenhaften Aufruf des Kontaktformulars durch einen Angreifer unterbindet.

7.2.3.3 Netzwerk

Es gelten sinngemäß, je nach eingesetzten Kommunikationskanälen, die in den Kapiteln Voice over IP, Unified Communications and Collaboration sowie Soziale Netzwerke und Medien aufgeführten Maßnahmen bzgl. des Netzwerkes. Ergänzende Maßnahmen werden im Folgenden dargestellt.

M-TK-131 Beschränkung des Netzzugriffs auf dedizierte Räumlichkeiten im Kontaktcenter

Um den Zugriff auf Kontaktcenter-Anwendungen und Management-Systeme abzusichern, kann der physische Zugriff auf das entsprechende Netzsegment auf dedizierte Räumlichkeiten im Kontaktcenter (z. B. den Arbeitsbereich der Agenten und Supervisor) beschränkt werden. Dies kann durch entsprechendes Patching der Netzwerkanschlüsse und sicherheitstechnische Separierung der betreffenden Netzzone (Sicherheitszone) erzielt werden. Diese Maßnahme ist dann zu treffen, wenn die Kontaktcenter-Systeme und -Anwendungen auf andere Weise (z. B. Authentisierung und Verschlüsselung) nicht hinreichend abgesichert werden können. Diese Maßnahme ist Grundlage für die Wirksamkeit einer Zugangsbeschränkung zu Kontaktcenter-Räumlichkeiten (siehe M-TK-136 „Zutrittsbeschränkung für Kontaktcenter-Räumlichkeiten“).

M-TK-132 Hochverfügbare Auslegung der Netzkomponenten und Systeme im Kontaktcenter

Die Netzkomponenten im Kontaktcenter sind Grundlage für die Funktionsfähigkeit der Gesamtlösung. Aufgrund der Kritikalität von Kontaktcenter-Anwendungen für das Kerngeschäft vieler Organisationen muss diese besonders gegen Ausfälle abgesichert werden. Die betroffenen Netzkomponenten sollten redundant ausgelegt und gegen äußere Einflüsse, z. B. gegen Stromausfälle, abgesichert werden. Bei der Planung der Maßnahmen zur Erhöhung der Überlebensfähigkeit des Kontaktcenters sind alle für die Funktionsfähigkeit des Kontaktcenters notwendigen Komponenten zu berücksichtigen. Hierzu zählen u. a. Agenten-PCs, IP-Telefone, Switches für Access-, Core- und Distribution-Ebene, Firewalls und andere Systeme zur Absicherung von Netzübergängen, Gateways sowie die wesentlichen Systeme für Routing und Processing. Werden Kontaktcenter-Funktionen an einem abgesetzten Standort genutzt, sind auch die Standort-Verbindungen entsprechend abzusichern. Aufgrund der Vielzahl der betroffenen Systeme kann eine Absicherung jeder einzelnen Komponente unwirtschaftlich sein. Das Designziel sollte daher sein, dass im Falle eines Ausfalls einzelner Komponenten die Leistungsfähigkeit des Kontaktcenters nicht beeinträchtigt wird. Im Falle eines großflächigen Ausfalls wie z. B. bei einem Stromausfall sollte eine genügend große Anzahl von Agentenarbeitsplätzen zur grundlegenden Bedienung der wichtigsten Prozesse weiterhin arbeitsfähig sein.

M-TK-133 Absicherung der Übergänge in öffentliche Netze

Um den direkten Zugriff auf Kontaktcenter-Systeme und die darin verarbeiteten, möglicherweise sensiblen Daten zu verhindern, müssen Netzübergänge nach Stand der Technik abgesichert werden. Um eine - wenn auch unwahrscheinliche - Attacke via ISDN zu verhindern, kann das IP-ISDN-Gateway in eine separate, durch eine Firewall abgetrennte Sicherheitszone verlagert werden. Aufgrund der ggf. komplexen Firewall-Konfiguration und eventueller Nebenwirkungen der Firewall-Regeln auf die Sicherheit weiterer Systeme ist eine Separierung dieser Sicherheitszone von der allgemeinen Internet-DMZ zu empfehlen.

Der Übergang in das Internet wird durch eine DMZ abgesichert. In dieser werden Proxy- und Gateway-Systeme aufgebaut, um den direkten Durchgriff auf interne Systeme zu verhindern und die eingehende Kommunikation zu filtern. Die grundsätzliche Vorgehensweise entspricht der Absicherung von VoIP- und UCC-Systemen. Eine Prinzipdarstellung der Absicherung eines Inbound-Kontaktcenters ist Abbildung 43 zu entnehmen.

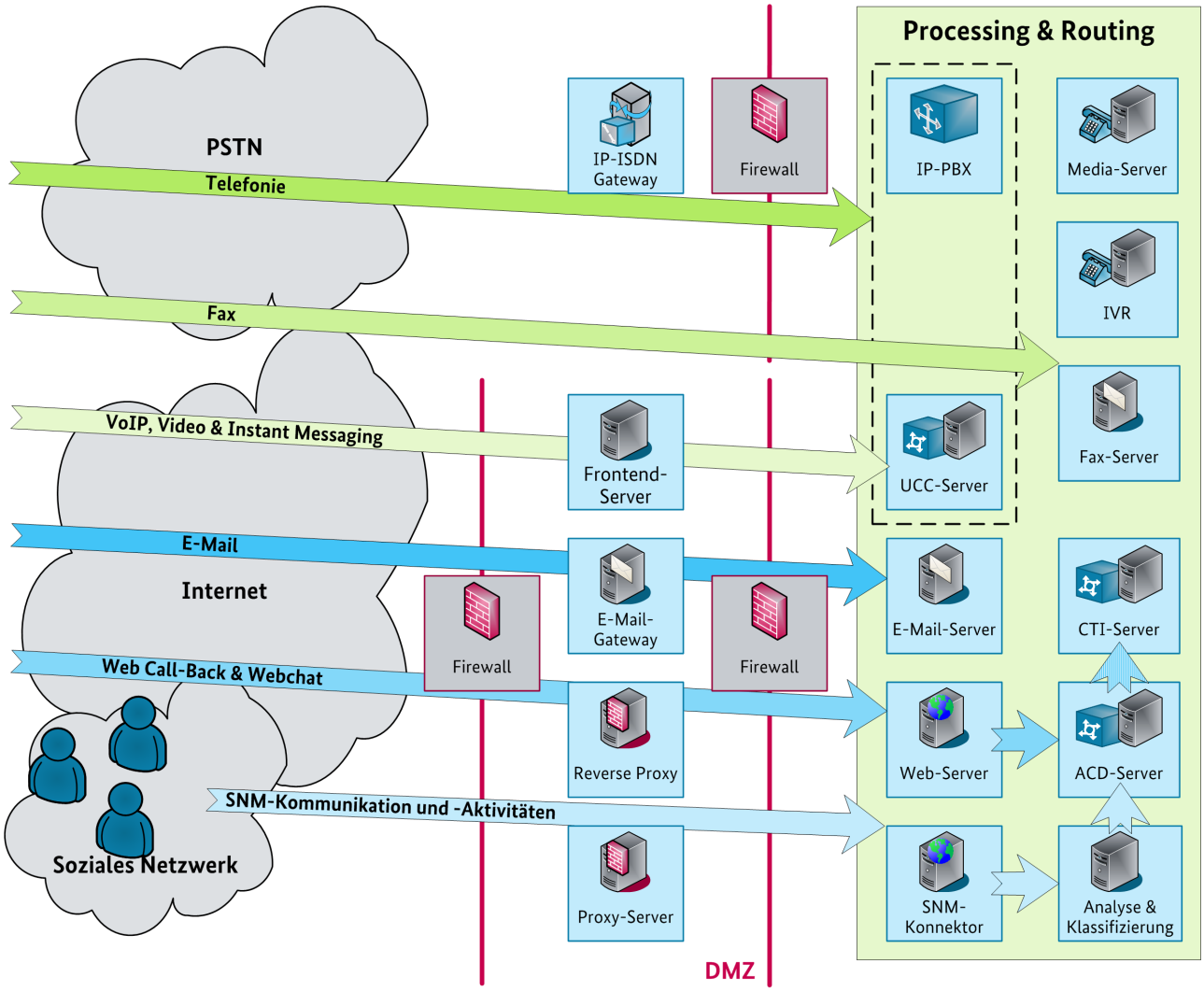


Abbildung 43: DMZ-Infrastruktur eines Inbound-Kontaktcenter

7.2.3.4 Netz- und Systemmanagement

Es gelten sinngemäß, je nach eingesetzten Kommunikationskanälen, die in den Kapiteln Voice over IP, Unified Communications and Collaboration sowie Soziale Netzwerke und Medien aufgeführten Maßnahmen bzgl. Netz- und Systemmanagement.

M-TK-134 Absicherung der Management-Schnittstellen

Durch den Eingriff in Management-Systeme können eine erhebliche Betriebsbeeinträchtigung, ein Abhören der internen Kommunikation und ein Vertraulichkeits- oder Integritätsverlust der in Kontaktcentern verarbeiteten, besonders sensiblen Daten verursacht werden. Management-Tools für die Gesamtumgebung (z. B. PEP, Quality Monitoring, Call-Flow-Editor) und Management-Schnittstellen von Routing-Systemen (z. B. ACD, Dialer oder IVR) sollten daher nach Stand der Technik abgesichert werden. Hierzu zählt die Zugriffseinschränkung auf bestimmte Nutzergruppen, die Authentisierung der Teilnehmer, die Verschlüsselung der Übertragung von Management-Daten sowie ggf. die Protokollierung von durchgeführten Änderungen.

7.2.3.5 Übergreifende Aspekte

Es gelten sinngemäß, je nach eingesetzten Kommunikationskanälen, die in den Kapiteln Voice over IP, Unified Communications and Collaboration sowie Soziale Netzwerke und Medien aufgeführten Maßnahmen bzgl. übergreifender Aspekte. Ergänzende Maßnahmen werden im Folgenden dargestellt.

M-TK-135 Schulung von Kontaktcenter-Administratoren und Schichtleitern/Supervisoren

Die mit der Konfiguration und dem Betrieb eines Kontaktcenter betrauten Administratoren sollten gemäß Maßnahme M-TK-249 „Schulung der Administratoren von TK-Lösungen“ einer umfassenden Schulung unterzogen werden. Ein besonderes Augenmerk sollte bei Kontaktcentern den Abhängigkeiten bei der Konfiguration von Routing-Regeln und Call Flows geschenkt werden, da diese erhebliche Auswirkungen auf die Leistungsfähigkeit und den reibungslosen Betrieb eines Kontaktcenters haben und sowohl von Administratoren als auch von Schichtleitern/Supervisoren durchgeführt werden. Die Administratorschulung für Kontaktcenter muss daher auf die Schichtleiter/Supervisoren und den Leiter des Kontaktcenter ausgeweitet werden.

M-TK-136 Zutrittsbeschränkung für Kontaktcenter-Räumlichkeiten

Kontaktcenter-Lösungen unterliegen bezüglich der Vertraulichkeit der Daten einem besonders hohen Schutzbedarf. Die zentralen Systeme und Anwendungen eines Kontaktcenters sollten gemäß Maßnahme M-TK-233 „Physische Sicherheit der Server der Telekommunikationslösung“ geschützt werden.

Darüber hinaus sind die Arbeitsplätze der Kontaktcenter-Mitarbeiter besonders zu schützen. Falls diese Arbeitsplätze nicht hinreichend durch technische Schutzmechanismen abgesichert werden können, so ist eine Zutrittsbeschränkung zu den Räumlichkeiten des Kontaktcenters (möglichst in Verbindung mit Maßnahme M-TK-131 „Beschränkung des Netzzugriffs auf dedizierte Räumlichkeiten im Kontaktcenter“) erforderlich. Dies gilt insbesondere dann, wenn große Mengen personenbezogener Daten oder anderer vertraulicher Informationen durch Zugriff auf ein System, z. B. einen Agentenarbeitsplatz, eingesehen werden könnten.

7.2.4 Zusammenfassung

Kontaktcenter bündeln die eingehende (engl. inbound) und ausgehende (engl. outbound) Kommunikation einer Organisation mit – meist externen – Kommunikationspartnern. Während früher über Kontaktcenter hauptsächlich Sprachkommunikation abgewickelt wurde, führen moderne Kontaktcenter-Lösungen eine Vielzahl von Kommunikationskanälen zusammen. Beispielsweise werden neben Telefonie oder VoIP auch Rückruf-Formulare im Web (Web Callback) oder Chat-Unterstützung beim Surfen (Webchat) genutzt.

Die über die verschiedenen Kanäle abgewickelte Kommunikation wird analysiert, klassifiziert und zugestellt („Processing & Routing“). Die Arbeit der Agenten wird durch eine tiefe Integration der Kommunikationskanäle in die Applikationswelt effizient gestaltet sowie durch Management-Werkzeuge überwacht und gesteuert. Aufgrund der Anzahl beteiligter Systeme und Schnittstellen zu weiteren IT-Systemen sowie der Vielzahl von Kommunikationskanälen ergibt sich eine hohe Systemkomplexität.

Die Angriffspunkte eines Kontaktcenters lassen sich wie folgt systematisieren:

- zentrale Systeme (Server, TK-Systeme im engeren Sinne) und Anwendungen, die Teile der Gesamtlösung bilden
- Schnittstellen und Kommunikation, über die diese Lösungselemente miteinander kombiniert werden
- Endgeräte und Clients mit Zugriff auf Kontaktcenter-Dienste sowie die Kommunikation von und zu diesen Geräten

Die Angriffsrisiken sind in Abhängigkeit der verwendeten Teillösungen, deren Schnittstellen und Protokollen sowie den von der Gesamtlösung verwendeten Kommunikationswegen und Daten zu bewerten und entsprechend zu minimieren. Weiterhin sind bei der Analyse der Angriffsrisiken

Anforderungen an die Hochverfügbarkeit des Systems und der bei Angriffen drohende ggf. hohe Schaden zu berücksichtigen.

Die Erarbeitung und Umsetzung einer Sicherheitskonzeption umfasst neben den generell zu ergreifenden Maßnahmen (siehe Kapitel 10) und den für die zugrunde liegenden Technologien klassische Telekommunikationstechnik (siehe Kapitel 3.3), VoIP (siehe Kapitel 4.3), UCC (siehe Kapitel 6.3) und Soziale Netzwerke und Medien (siehe Kapitel 8.1.3) spezifizierten Maßnahmen die folgenden Aspekte:

Grundabsicherung der zentralen Systeme zu Kontaktcenter-Teillösungen

Für die Systemlösungen der zusammengeführten Anwendungen und Dienste sowie für die zugehörigen Daten sind zunächst für sich genommen Sicherheitsmaßnahmen so zu planen, wie dies der Schutzbedarf bei Einzelnutzung dieser Anwendungen und Dienste notwendig macht. Die Umsetzung dieser Maßnahmen erfolgt wie in dieser Technischen Leitlinie jeweils in den Kapiteln zu den zugrunde liegenden (Tele-)Kommunikationstechnologien beschrieben.

Absicherung bzw. gezielte Beschränkung gespeicherter und ausgetauschter Daten

In einem Kontaktcenter wird häufig mit personenbezogenen, sensiblen Daten gearbeitet. Bei Übertragung oder Speicherung sind Daten daher zu verschlüsseln und es darf nur nach vorheriger Authentisierung von Agentenarbeitsplätzen auf sensible Daten zugegriffen werden. Als Maßnahme für Data Loss Prevention ist es weiterhin notwendig, die Verwendung von externen Speichergeräten an den Endgeräten zu unterbinden.

Absicherung der Kommunikation und des Kommunikationsroutings einer Kontaktcenter-Lösung

Um die Verfügbarkeit und Vertraulichkeit der Kommunikation über die Kontaktcenter-Lösung sicherzustellen, ist insbesondere die Absicherung der Kommunikation gemäß den für die genutzten Teilsysteme notwendigen Maßnahmen umzusetzen.

Zudem muss das Routing des Kontaktcenters vor Fehlfunktion und Manipulation geschützt werden, da ansonsten erhebliche Beeinträchtigungen von Verfügbarkeit und Vertraulichkeit nicht ausgeschlossen werden können. Kontaktcenter-Dienste, die den direkten oder indirekten Zugriff auf Datenbestände der Organisation ermöglichen oder das Potenzial haben, eine Überlast im Kontaktcenter zu verursachen, müssen vor einem missbräuchlichen Zugriff geschützt werden. Hierzu zählen beispielsweise die Authentisierung an kritischen IVR-Anwendungen oder die Verhinderung eines massenhaften Zugriffs auf webbasierte Kontaktformulare.

Übergreifende Aspekte

Implementierung und Betrieb einer Kontaktcenter-Lösung muss mit entsprechenden organisatorischen Maßnahmen gegen Fehlfunktion und Missbrauch abgesichert werden. Neben den für die Teilsysteme umzusetzenden Maßnahmen sind Know-how-Aufbau vor Planung, gezielte Produktauswahl sowie Sensibilisierungs- und Schulungsmaßnahmen für Administratoren, Supervisoren und Agenten notwendig.

7.3 Händlersysteme

Händlersysteme (auch Trading-Systeme) sind spezielle Telekommunikationssysteme zur Bereitstellung einer Vielzahl von verlässlichen Kommunikationskanälen an einem Arbeitsplatz, zwischen denen der Benutzer schnell hin und her wechseln kann. Der primäre Anwendungsfall ist die Kommunikation von Händlern (z. B. Börsenmakler, Energiehändler) mit anderen Händlern oder Organisationen. Über diese Händlersysteme wird die Kommunikation für teilweise sehr hohe Handelsvolumina abgewickelt. Daher ist die schnelle, effiziente und verlässliche Funktionsweise von Händlersystemen besonders wichtig. Die grundlegenden Eigenschaften von Händlersystemen sowie die zugehörigen Gefährdungen und Maßnahmen werden im Folgenden beschrieben.

7.3.1 Basiswissen

Bei Händlersystemen handelt es sich vorwiegend um Systeme zur Sprachkommunikation, die als Bestandteil einer bestehenden TK-Infrastruktur oder als eigenständiges System betrieben werden. Besonderes Merkmal von Händlersystemen sind die Vielzahl der Sprachkanäle, zwischen denen der Händler z. B. per Knopfdruck oder Klick wechseln kann. Hinter diesen Sprachkanälen verbergen sich Verbindungen zu einem oder mehreren Gesprächspartnern, die in einer Konferenzschaltung zusammengeschaltet sind. Diese Konferenzschaltungen werden entweder innerhalb der eigenen Organisation (zur internen Kommunikation zwischen Händlern) oder außerhalb der Organisation (z. B. zur Kommunikation mit einem Bankhaus oder der Börse) geschaltet.

Der schnelle Wechsel zwischen verschiedenen Sprachkanälen wurde in der Vergangenheit vielfach durch echte Standleitungen, heute vermehrt durch dauerhaft bestehende Wählverbindungen realisiert. Diese Wählverbindungen basieren auf klassischer Telekommunikationstechnik, VoIP oder auf UCC (siehe Kapitel 3, 4 und 6). Die verschiedenen Sprachkanäle werden vor Arbeitsbeginn des Händlers aufgebaut. Dieser bedient sie über ein spezielles Telefonendgerät (TDM- oder IP-basiert) oder eine spezielle Anwendungs-Software.

Zusätzlich zur Telefonie hat sich im Handelsumfeld die Benutzung von Instant Messaging zur Kommunikation zwischen Händlern (und ggf. weiteren, auch externen Kommunikationspartnern) etabliert. Auch E-Mail spielt in diesem Umfeld eine wichtige Rolle. Es ist zu berücksichtigen, dass durch die Händler häufig eigenmächtig auf öffentliche IM-Dienste (z. B. Yahoo Messenger) zurückgegriffen wird, da ein entsprechendes internes Alternativangebot fehlt.

An die Kommunikation im Handelsumfeld werden vielfältige Anforderungen bezüglich Rechtskonformität und Nachvollziehbarkeit gestellt. Diese Aspekte sollten, je nach Einsatzzweck des Händlersystems, durch juristische Beratung beleuchtet und in der Umsetzung entsprechend berücksichtigt werden. Eine besonders wichtige Anforderung, welche in vielen Fällen umgesetzt werden muss, ist die Aufzeichnung der internen und externen Kommunikation in revisionssicherer Art und Weise. Neben der Aufzeichnung von Sprachkommunikation muss auch die Schriftkommunikation entsprechend berücksichtigt werden. Die Verwendung von öffentlichen IM-Diensten stellt hierbei ein Problem dar, da diese nicht oder nur unter hohem Aufwand von der Protokollierung und Archivierung erfasst werden können. Insofern ist die Bereitstellung eines internen IM-Dienstes, der ggf. auch zur externen Kommunikation geeignet ist, sinnvoll.

Die grundlegende Architektur eines Händlersystems entspricht im Wesentlichen der eines klassischen oder IP-basierten TK-Systems. Hinzu kommen ggf. weitere Server-Rollen für die Schaltung von Mehrpunkt-Konferenzen sowie die Bereitstellung eines Instant-Messaging-Dienstes. Zentrale Archivierungssysteme erfassen die durch die Händler geführten Gespräche. Aufgrund der hohen und ggf. vom allgemeinen Kommunikationssystem abweichenden Verfügbarkeitsanforderungen können dedizierte Systemkomponenten für die Händlerumgebung aufgebaut werden. Hier besteht weiterhin die Möglichkeit, einen gemeinsamen oder einen dedizierten Amtsübergang zu nutzen. Im Wesentlichen ergeben sich somit die in Abbildung 44 dargestellten Architekturvarianten:

- konsolidiertes Händlersystem
- dediziertes Händlersystem inklusive Mitbenutzung des Amtsübergangs
- vollständig dediziertes Händlersystem mit eigenständigem Amtsübergang

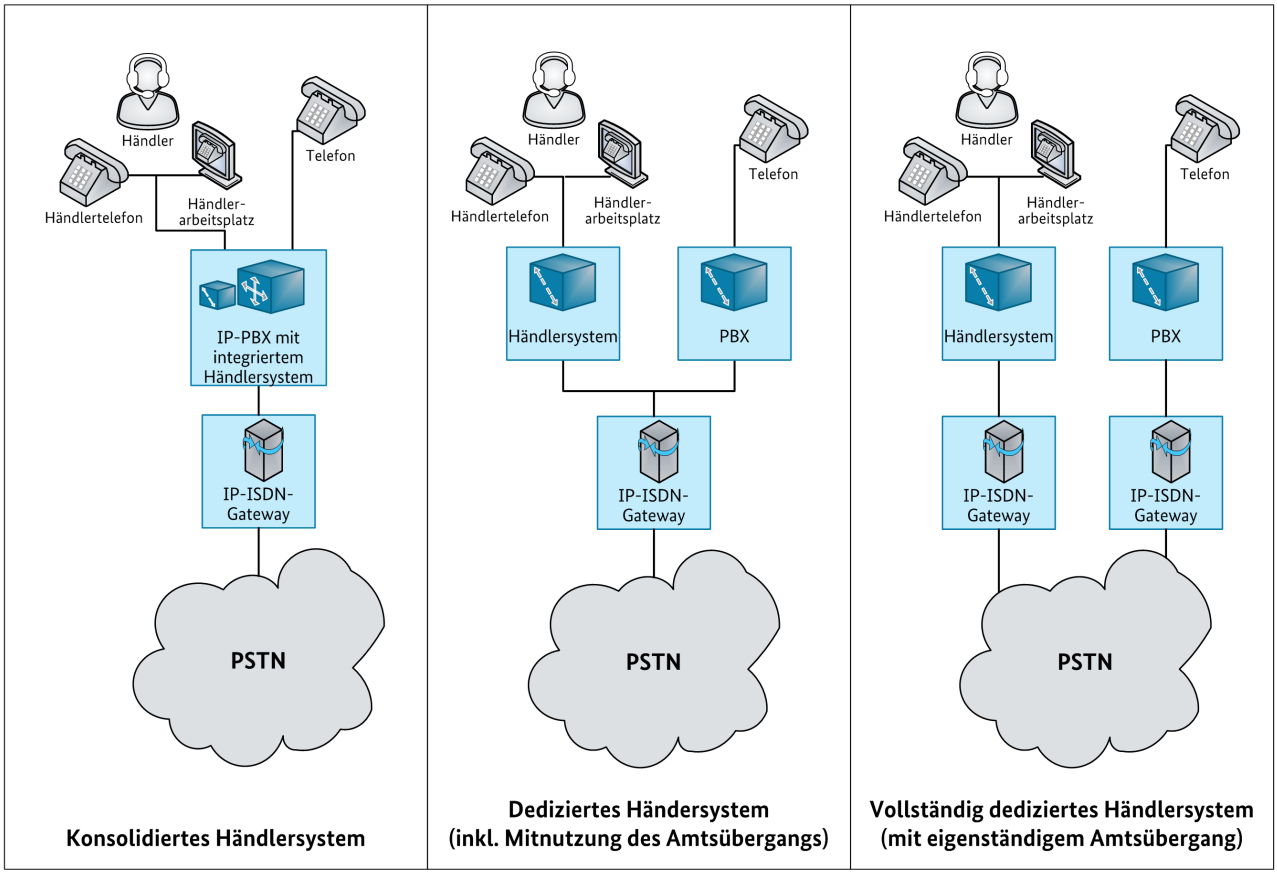


Abbildung 44: Architekturvarianten des Telefonieanteils von Händlersystemen

7.3.2 Gefährdungen

Händlersysteme bilden häufig kritische Geschäftsprozesse ab. Die möglicherweise hohen Handelsvolumina (z. B. Energiehandel) bedingen, dass die Händlersysteme einen signifikanten Einfluss auf den Geschäftserfolg der Organisation oder der verbundenen Organisationen haben. Somit können Ausfälle der Händlersysteme einen hohen wirtschaftlichen Schaden oder hohe Regressforderungen zur Folge haben. Falls dieser Ausfall öffentlich bekannt wird, ist zudem ein erheblicher Imageschaden zu befürchten.

Des Weiteren werden im Händlerumfeld handelsrelevante und teilweise hochsensible Inhalte kommuniziert. Ein Vertraulichkeitsverlust kann in diesem Umfeld schwerwiegende finanzielle Schäden oder Reputationsschädigungen zur Folge haben. Dies gilt auch für eine nachträgliche Enthüllung von aufgezeichneter Kommunikation mit sensiblen Inhalten. Händlersysteme sind somit für Angreifer ein attraktives Ziel zum Abgriff wertvoller Informationen. Aber auch die versehentliche Enthüllung von Informationen durch den Benutzer stellt eine Gefährdung dar.

Die Gefährdungen entsprechen - abgesehen vom erhöhten Schadenspotenzial und Risiko - im Wesentlichen denen der eingesetzten Kommunikationskanäle und -Systeme. Dies betrifft insbesondere die klassische TK-Technik (siehe Kapitel 3.2) oder VoIP (siehe Kapitel 4.2), Instant Messaging und Gruppen-Chat sowie Systeme zur Aufzeichnung und Archivierung von Kommunikation (siehe Kapitel 6.2). Spezifische Gefährdungen für Händlersysteme werden im Folgenden dargelegt.

7.3.2.1 Höhere Gewalt

Auf Händlersysteme treffen wie für alle IT-Lösungen allgemein die Gefährdungen durch höhere Gewalt zu, die in den IT-Grundschutz-Katalogen genannt sind. Es ist zu beachten, dass aufgrund von möglicherweise hohen Handelsvolumina (z. B. beim Handel mit Aktien oder Energie) den Händlersystemen ein sehr hoher Stellenwert für den geschäftlichen Erfolg einer Organisation zukommt. Durch höhere Gewalt ergeben sich somit ggf. besonders hohe Risiken für Händlersysteme. Ist dies gemäß Schutzbedarfsanalyse der Fall, so ist der technischen Realisierung der Hochverfügbarkeit und der Überlebensfähigkeit des Händlersystems im Katastrophenfall besonderes Augenmerk zu schenken. Dies muss im Business Continuity Management (BCM) und im Risikomanagement Berücksichtigung finden.

7.3.2.2 Organisatorische Mängel

Organisatorische Mängel treffen Händlersysteme grundsätzlich genauso wie beliebige andere IT-Systeme. Mit der Einführung eines IT-gestützten Händlersystems müssen bestehende Entscheidungen und Konzepte für eine durch das Händlersystem mitgenutzte TK- und IT-Infrastruktur gezielt überprüft werden. Gefährdungen durch organisatorische Mängel ergeben sich analog zu klassischen TK- und VoIP-Systemen.

Besonders zu beachten sind zudem

- die ggf. von der allgemeinen Telekommunikationslösung abweichenden Betriebszeiten (z. B. weltweiter 24h-Handel),
- die organisatorischen Abhängigkeiten vom Betrieb des allgemeinen TK-Systems, falls eine Mitnutzung von Infrastrukturen, z. B. IP-PBX und Amtsübergang, vorgesehen ist, und
- ein möglicherweise erhöhtes Risiko aufgrund der großen Bedeutung des Händlersystems für kritische Geschäftsprozesse der Organisation.

G-TK-94 Mangelnde Abstimmung zwischen IT/TK-Betrieb und Betrieb des Händlersystems

Je nach gewählter Architekturvariante kann das allgemeine TK-System der Organisation oder die Infrastruktur für den Amtsübergang durch das Händlersystem mitgenutzt werden. In diesem Fall müssen betriebliche Aspekte wie z. B. Wartungsfenster und Konfigurationsänderungen zwischen IT/TK-Betrieb und Betrieb des Händlersystems abgestimmt werden. Ist dies nicht der Fall, können nicht kommunizierte Änderungen oder Wartungen den Betrieb des Händlersystems gefährden. Es sind hierbei die ggf. unterschiedlichen Anforderungen an die Service Level der allgemeinen IT/TK-Systeme und des Händlersystems zu beachten. Die Abstimmung wird erleichtert, wenn sich alle betroffenen Systeme in einer Zuständigkeit befinden.

7.3.2.3 Menschliche Fehlhandlungen

Durch den spezialisierten Anwendungsfall und die teilweise komplexe Bedienung von Händlersystemen wächst die Gefahr einer menschlichen Fehlhandlung. Auch die Abhängigkeiten zwischen allgemeiner Kommunikationsinfrastruktur und Händlersystem und die daraus resultierende Systemkomplexität haben hierauf einen Einfluss.

Damit gelten – sofern technisch anwendbar – grundsätzlich die im Gefährdungskatalog G.3 „Menschliche Fehlhandlungen“ der BSI IT-Grundschutz-Kataloge (siehe [BSI GSK-2013]) aufgeführten Gefährdungen. Es gelten insbesondere die folgenden Gefährdungen:

- G 3.3 „Nichtbeachtung von Sicherheitsmaßnahmen“
- G 3.7 „Ausfall der TK-Anlage durch Fehlbedienung“

Spezifische Gefährdungen durch menschliche Fehlhandlungen sind:

G-TK-95 Versehentliches Enthüllen von Informationen durch Händler

Durch die Vielzahl der gleichzeitig geschalteten Verbindungen, die Kommunikation mit unterschiedlichsten Adressatenkreisen und den schnellen Wechsel des jeweiligen Kommunikationskontextes kann ein Mitarbeiter leicht versehentlich Informationen an die falschen Adressaten weitergeben. So kann z. B. eine Information in einem Gesprächskreis mit anderen Händlern geäußert werden, die eigentlich für einen anderen Adressatenkreis (z. B. Bankhaus) gedacht war.

G-TK-96 Fehlkonfiguration des Händlersystems und mitgenutzter Systeme

Durch Fehlkonfiguration des Händlersystems, z. B. der bei Handelsbeginn automatisch aufgebauten, dauerhaften Konferenzschaltungen (auch Gesprächskreise genannt), kann es zu Betriebsbeeinträchtigungen und Fehlfunktionen kommen, die die Verfügbarkeit des Systems und Vertraulichkeit der Kommunikation betreffen. So kann z. B. durch Fehlkonfiguration von Gesprächskreisen unbeabsichtigt ein nicht autorisierter Teilnehmer hinzugefügt werden. Auch durch Fehlkonfigurationen von mitgenutzten Systemen, z. B. von ISDN-Gateways, kann die Funktionsfähigkeit und Verfügbarkeit des Händlersystems gefährdet sein.

7.3.2.4 Technisches Versagen

Für Händlersysteme gelten prinzipiell die in den IT-Grundschutz-Katalogen genannten Gefährdungen, wie Stromausfall, Datenbankausfall, mangelnde Verschlüsselung, sofern diese für ein konkretes System technisch anwendbar sind. Es gelten hier zudem, sofern technisch anwendbar, die Gefährdungen der Basistechnologien sowie sonstiger genutzter TK-Technologien, z. B. UCC.

7.3.2.5 Vorsätzliche Handlungen

Im Bereich der vorsätzlichen Handlungen besteht die wesentliche Gefährdung darin, dass Angriffe aufgrund der exponierten Stellung von Händlersystemen einen hohen wirtschaftlichen Schaden verursachen können und somit von Angreifern als besonders lohnende Ziele eingeordnet werden. Die Gefährdungslage konzentriert sich dabei auf die klassische oder IP-basierte Telekommunikationstechnik, die Aufzeichnungssysteme und ergänzende Kommunikationsmedien, z. B. Instant Messaging und Gruppen-Chat.

Für Händlersysteme ist mit folgenden spezifischen Gefährdungen durch vorsätzliche Handlungen zu rechnen:

G-TK-97 Abhören der Händlerkommunikation

Durch ein Abhören der Händlerkommunikation können einem Angreifer Wettbewerbsvorteile gegenüber dem angegriffenen Händler bzw. dessen Organisation entstehen. Als Angriffspunkte eignen sich die Übertragung der Sprachkommunikation über das Netz, die eingesetzten Spezialendgeräte oder Clients und ggf. eingesetzte Konferenzbrücken. Dies gilt gleichermaßen für die Sprach- und die Schriftkommunikation (Instant Messaging und Gruppen-Chat).

G-TK-98 Manipulation der Händlerkommunikation

Durch die Kompromittierung eines Kommunikationskanals und die Manipulation von Kommunikation, z. B. durch das Streuen von Falschinformationen im Namen eines Händlers, kann ein Angreifer den Handel zu seinem Vorteil beeinflussen. So kann das Lancieren einer Fehlinformation beispielsweise eine heftige Reaktion an der Börse auslösen, von der ein Angreifer profitieren könnte. Einfacher als die Sprachkommunikation kann die Schriftkommunikation per Instant Messaging und Gruppen-Chat manipuliert werden.

7.3.3 Sicherheitsmaßnahmen

Im Folgenden werden die Maßnahmen zur Anwendung auf Händlersysteme beschrieben. Als Grundlage sind die Sicherheitsmaßnahmen der IT-Grundschutz-Kataloge und der in diesem Dokument beschriebenen Basistechnologien, klassische TK- und VoIP-Systeme und – je nach Ausprägung der Systemarchitektur – für weitere Kommunikationskanäle anzuwenden (siehe Kapitel 3.3, 4.3 und 6.3).

Der Maßnahmenkatalog zur Absicherung der Nutzung und des Betriebs von Händlersystemen ist in die folgenden Blöcke aufgeteilt:

- Server und Anwendungen, siehe Kapitel 7.3.3.1
- Endgeräte und Clients, siehe Kapitel 7.3.3.2
- Netzwerk, siehe Kapitel 7.3.3.3
- Netz- und Systemmanagement, siehe Kapitel 7.3.3.4
- Übergreifende Aspekte, siehe Kapitel 7.3.3.5

7.3.3.1 Server und Anwendungen

Es gelten sinngemäß die für VoIP, Instant Messaging und Audiokonferenzen aufgeführten Maßnahmen bzgl. Server und zentraler Komponenten. Insbesondere ist die Umsetzung der folgenden Maßnahmen anzustreben.

M-TK-31 „Durchgängige Verschlüsselung des Medienstroms“

M-TK-32 „Durchgängige Verschlüsselung der Signalisierung“

M-TK-100 „Sicherung von Konferenzräumen“

M-TK-101 „Sicherer Umgang mit Gesprächs- und Konferenzaufzeichnungen“

Ergänzende Maßnahmen werden im Folgenden dargestellt.

M-TK-137 Verwendung dedizierter Händlersysteme

Die Gefahr einer Beeinträchtigung des Händlersystems durch Fehlkonfiguration eines mitbenutzten Systems kann durch die Verwendung eines dedizierten Händlersystems und dedizierter IT-Infrastrukturen vermindert werden. Dies ist insbesondere dann in Betracht zu ziehen, wenn aufgrund getrennter Zuständigkeiten oder anderer Hindernisse keine Harmonisierung des Betriebs der jeweiligen Systeme möglich ist.

M-TK-138 Festlegung dedizierter Gesprächskreise

Um eine versehentliche Fehlkonfiguration von Gesprächskreisen und die Hinzunahme von nicht autorisierten Teilnehmern zu vermeiden, sollten Gesprächskreise möglichst dauerhaft, mindestens aber vor Handelsbeginn, vorkonfiguriert werden. Sofern diese auf der eigenen Konferenzinfrastruktur realisiert werden, sollten sie als geschlossene Konferenzen mit Zugangsschutz durch Teilnehmerauthentisierung konfiguriert werden (siehe M-TK-100 „Sicherung von Konferenzräumen“). Die angemeldeten Teilnehmer sollten durch den Anwender anhand einer Teilnehmerliste überprüft werden können (siehe M-TK-108 „Ständiges Einblenden der Teilnehmerliste auf den Endgeräten“).

7.3.3.2 Endgeräte und Clients

Es gelten sinngemäß die für klassische Telekommunikationstechnik bzw. VoIP aufgeführten Maßnahmen bzgl. der Endgeräte (siehe Kapitel 4.3.2) sowie die Maßnahmen bzgl. Instant Messaging, Konferenzen und Aufzeichnung (siehe Kapitels 6.3.2). Darüber hinaus ergeben sich folgende Maßnahmen:

M-TK-139 Vermeidung von Fehlbedienung durch intuitive Bedienkonzepte

Insbesondere im Bereich des Handels sind aufgrund des hohen Kommunikationsaufkommens Fehlbedienungen zu erwarten. Durch die Verwendung von intuitiv bedienbaren Endgeräten und Clients kann eine Fehlbedienung wirkungsvoll vermieden werden. Neben einem einfachen und schnellen Wechsel zwischen unterschiedlichen Gesprächskreisen, zählen insbesondere die Unterscheidbarkeit parallel genutzter Kommunikationskanäle und die übersichtliche Darstellung der jeweiligen Adressaten eine entscheidende Rolle. Diese Aspekte sollten bei Auswahl und Beschaffung eines Händlersystems Berücksichtigung finden.

7.3.3.3 Netzwerk

Es gelten sinngemäß die für klassische Telekommunikationstechnik bzw. VoIP aufgeführten Maßnahmen bzgl. des Netzwerkes (siehe Kapitel 3.3.3 und 4.3.3).

7.3.3.4 Netz- und Systemmanagement

Es gelten sinngemäß die für klassische Telekommunikationstechnik bzw. VoIP sowie für Unified Communications and Collaboration aufgeführten Maßnahmen bzgl. Netz- und Systemmanagement (siehe Kapitel 3.3.4, 4.3.4 und 6.3.4).

7.3.3.5 Übergreifende Aspekte

Es gelten sinngemäß die für klassische Telekommunikationstechnik bzw. VoIP aufgeführten Maßnahmen bzgl. übergreifender Aspekte (siehe Kapitel 4.3.5). Zudem sollten die relevanten Maßnahmen in Hinblick auf Instant Messaging, Konferenzen und Aufzeichnungen (siehe Kapitel 6.3.5) umgesetzt werden. Darüber hinaus sind die folgenden Maßnahmen für Kontaktcenter (siehe Kapitel 7.2.3.5) auch für Händlersysteme umzusetzen, um das Risiko der Fehlbedienung und des Vertraulichkeitsverlusts zu minimieren:

M-TK-135 „Schulung von Kontaktcenter-Administratoren und Schichtleitern/Supervisoren“

M-TK-136 „Zutrittsbeschränkung für Kontaktcenter-Räumlichkeiten

7.3.4 Zusammenfassung

Händlersysteme decken die speziellen Kommunikationsanforderungen im Handelsbereich ab und greifen dazu im Wesentlichen auf Telefoniefunktionen, Audiokonferenzen und Instant Messaging zurück. Wegen regulatorischer und rechtlicher Anforderungen wird häufig bei Händlersystemen die Kommunikation aufgezeichnet und archiviert.

Für die Implementierung kommen im Wesentlichen drei Architekturvarianten in Betracht:

- konsolidiertes Händlersystem
- dediziertes Händlersystem mit Mitnutzung des Amtsübergangs einer TK-Lösung
- vollständig dediziertes Händlersystem

Die Angriffsrisiken sind in Abhängigkeit von den verwendeten Komponenten, dem Gesamtsystem und dem Stellenwert des Händlersystems am Organisationserfolg zu bewerten und entsprechend zu minimieren.

Besonders zu beachten sind dabei

- die möglichen Wechselwirkungen zwischen Telekommunikationssystem, IT-Infrastruktur und Händlersystem,
- die Nutzungsintensität und das Risiko von Fehlbedienungen,

- die Zahl und Sensibilität der genutzten Gesprächskreise sowie ggf. deren unterschiedliche Autorisierung und
- die Möglichkeiten zur Manipulation der Informationen und die Konsequenzen hieraus.

Die Erarbeitung und Umsetzung einer Sicherheitskonzeption umfasst neben den generell zu ergreifenden Maßnahmen (siehe Kapitel 10) und den auf das Händlersystem anwendbaren Maßnahmen der Technologien Klassische Telekommunikationstechnik (siehe Kapitel 3.3), VoIP (siehe Kapitel 4.3) und UCC (siehe Kapitel 6.3) die folgenden Aspekte.

Grundabsicherung der Teillösungen des Händlersystems

Es muss eine Grundabsicherung der Teillösungen aus dem Bereich der klassischen Telekommunikationssysteme bzw. VoIP-Systeme sowie UCC-Systeme vorgenommen werden. Diese Maßnahmen dienen in erster Linie der Sicherstellung von Vertraulichkeit, Verfügbarkeit und Integrität der Handelskommunikation.

Eine Maßnahme zur Minimierung der systemübergreifenden Auswirkungen von Fehlbedienungen ist die Entkopplung des Händlersystems vom allgemeinen Kommunikationssystem. Dies ist vor allem bei hohen erwarteten Verlusten im Falle einer Nichtverfügbarkeit des Händlersystems sinnvoll. Neben den Kommunikationssystemen ist besonders die geeignete Absicherung von (Sprach-)Aufzeichnungssystemen zu berücksichtigen.

Absicherung bzw. gezielte Beschränkung von Kommunikationsbeziehungen

Die Absicherung von Konferenzschaltungen und die Vorkonfiguration wichtiger Gesprächskreise mindert das Risiko von unautorisierten Zuhörern und Manipulationen.

Vermeidung von Fehlbedienungen

Die gezielte Produktauswahl nach Kriterien einer guten Bedienbarkeit, die Vorkonfiguration von wesentlichen Gesprächskreisen und die intensive Schulung der Händler beugen den Risiken einer Fehlbedienung in Hinblick auf Vertraulichkeit und Verfügbarkeit wirksam vor.

Organisatorische Maßnahmen

Um einen verlässlichen und sicheren Betrieb von Händlersystemen zu gewährleisten, sind organisatorische Maßnahmen sinnvoll, die eine Harmonisierung zwischen Betrieb des Händlersystems sowie mitgenutzter IT- und Kommunikationsinfrastruktur herbeiführen. Ideal ist eine Zusammenlegung der entsprechenden Betriebsverantwortungen. Hierdurch kann eine Abstimmung der - teilweise sehr verschiedenen - Betriebsanforderungen und eine Harmonisierung der Wartung ideal umgesetzt werden.

7.4 Alarmierungssysteme

Alarmierungssysteme können als geschlossene Systeme betrieben werden. In diesem Fall werden die über Sensoren wie Thermometer und Bewegungssensoren aufgenommenen Hinweise auf außergewöhnliche Situationen bzw. persönliche Kennzeichen zur Personenausstattung im Rahmen von Sucheinrichtungen über einen lösungseigenen Kommunikationspfad zu einer zentralen Einheit geleitet. Diese zentrale Einheit zeigt dann die Ereignisse an, protokolliert diese Ereignisse eventuell auch und nimmt die Alarmierung vor. Beispiele für den Einsatz einer derartigen zentralen Einheit sind das Auflaufen von Ereignissen einer Einbruchmeldeanlage auf einem zentralen Tableau oder die Verwendung eines zentralen Meldesystems für eine oder mehrere Meldeanlagen, siehe auch Kapitel 7.4.1.1.

Der eigene Kommunikationspfad des Alarmierungssystems kann beispielsweise in einer nur durch das Alarmierungssystem genutzten Verkabelung zwischen Sensoren und zentraler Einheit bestehen. Die Alarmierung kann durch direkt an die zentrale Einheit angeschlossene Ausgabeperipherie wie z. B. Signalhorn, Hupe oder Blinklicht erfolgen.

Eine solche geschlossene Anordnung als Alarmierungssystem gehört zunächst nicht in den Geltungsbereichs des vorliegenden Dokuments. Der Wirkbereich eines derartigen geschlossenen Systems mit Blick auf den Melderadius ist entweder vergleichsweise begrenzt oder aber das System muss eine ausgedehnte Meldeinfrastruktur umfassen. Diese erfasst dann einen Bereich, der parallel für andere Informationsflüsse über andere Kommunikationsinfrastrukturen versorgt wird.

Wird aus Wirtschaftlichkeitserwägungen die zentrale Einheit des Alarmierungssystems für die Informationsweiterleitung und Alarmierung bei besonderen Ereignissen an eine vorhandene Telekommunikationsinfrastruktur angeschlossen, entsteht eine Gesamtarchitektur, die über die genutzte Kommunikationsinfrastruktur und die darauf realisierten Dienste in den Fokus des vorliegenden Dokuments rückt.

Beispiele solcher Synergien sind:

- Anschluss einer Alarmierungslösung an eine ISDN- oder VoIP-basierte TK-Anlage zwecks Alarmierung mittels Telefonanruf(en) an vordefinierten Teilnehmerkreis
- Nutzung einer SMS-Gateway-Funktion von ISDN- oder VoIP-Anlage zwecks Alarmweiterleitung
- Erweiterung solcher Weiterleitungsautomatismen auf verschiedene Dienste einer UCC-Lösung (automatische E-Mail an festgelegten Verteiler, ...)
- Nutzung der Lokalisierbarkeit von Mobiltelefonen als Sensorik für Personensucheinrichtungen (synonym: Personensuchanlagen)

Typisch sind die folgenden Szenarien für die Kopplung von Alarmierungssystem und TK-Infrastruktur (siehe Abbildung 45):

- Das Alarmierungssystem wird zwecks Weiterleitung von Alarmen an die TK-Infrastruktur angeschlossen (Szenario 1).
- Das Alarmierungssystem realisiert Funktionalitäten durch Mitnutzung von TK-Lösungen (Szenario 2). Die Endpunkte des Alarmierungssystems, insbesondere Sensoren, sind in diesem Szenario aus Sicht der TK-Lösung wie „normale“ TK-Endgeräte einzustufen.
- Auch können Endgeräte der genutzten Kommunikationsinfrastruktur als Sensoren für die Alarmierungslösung mitgenutzt werden (Szenario 3).

Mindestens an der Schnittstelle zwischen Alarmierungslösung und der durch diese mitgenutzten Kommunikationsinfrastruktur muss gezielt die Informationssicherheit gestaltet werden. Hierbei sind die spezifischen Gefährdungen der genutzten Kommunikationslösung sowie die besonderen Anforderungen der durch die Alarmierungslösung abgedeckten Thematik zu berücksichtigen. Soweit technisch möglich, können zudem die für die Kommunikationsinfrastruktur ergriffenen Sicherheitsmaßnahmen sinngemäß

auch auf das Alarmierungssystem übertragen werden. In diesem Sinne sind die Ausführungen unter Kapitel 7.4.1 zu verstehen.

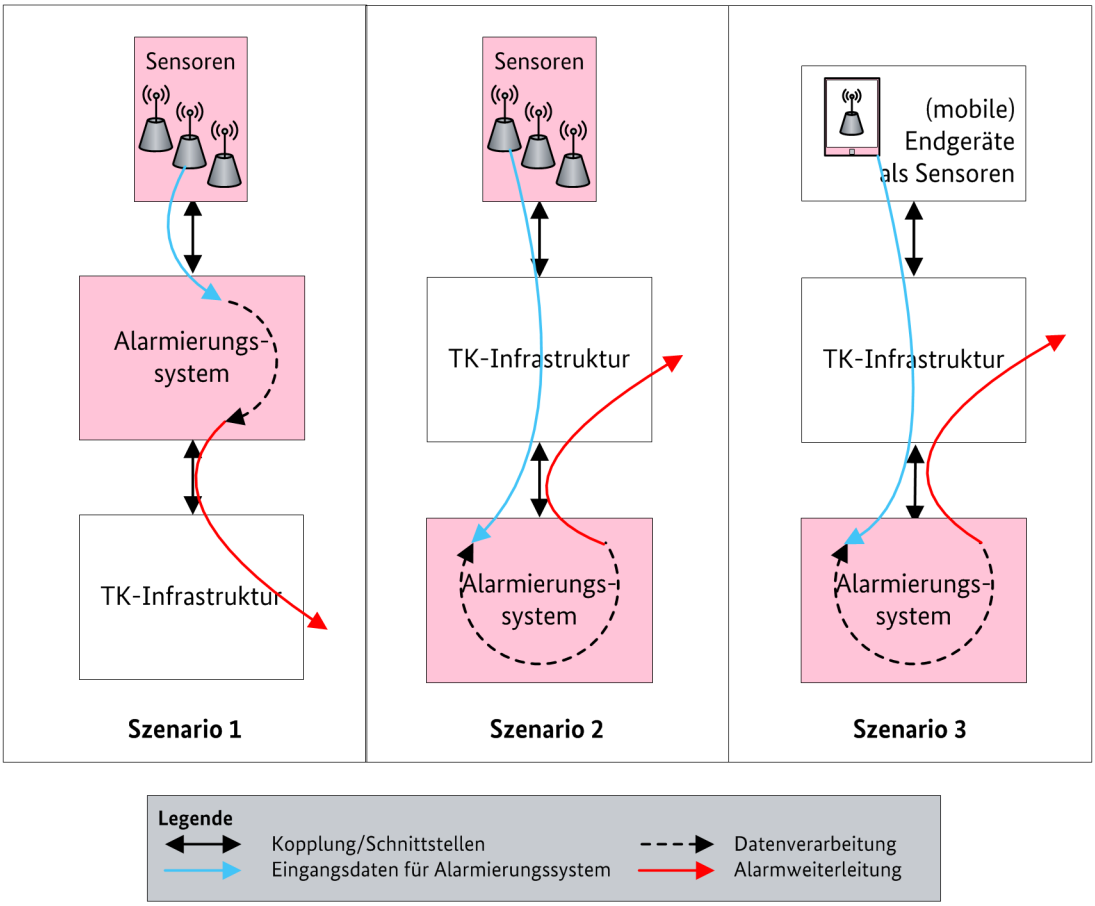


Abbildung 45: Szenarien einer Alarmierungslösung

7.4.1 Basiswissen

Nachfolgend werden zunächst wichtige Praxisbeispiele für Alarmierungslösungen beschrieben. Mit dem so gewonnenen Verständnis können Gefährdungslage und Maßnahmenempfehlungen für solche und andere Alarmierungssysteme leichter nachvollzogen werden.

7.4.1.1 Alarm-Server

Alarm-Server benachrichtigen beim Auftreten von Störungen oder anderen Ereignissen definierte Personen oder Personengruppen. An der Schnittstelle zwischen Gebäudeleittechnik und Kommunikationstechnik sammeln sie Informationen aus den Kommunikationsnetzwerken sowie der im Gebäude eingesetzten Sensorik und werten diese aus. Bei definierten Ereignissen löst der Alarm-Server dann einen Alarm aus und veranlasst, dass alle zuständigen Personen über den Alarm informiert werden. Darüber hinaus sind weitere Gegenmaßnahmen (z. B. die Aktivierung der Sprinkleranlage bei Feueralarm) mithilfe eines Alarm-Servers realisierbar.

Der Einsatzbereich von Alarm-Servern ist breit gefächert. Zum einen kommen diese bei klassischen Aufgaben der Sicherheitstechnik wie Einbruch- und Brandschutz zum Einsatz (siehe auch 7.4.1.3). Zum anderen übernehmen sie Aufgaben wie z. B. die Überwachung von Produktionsprozessen oder der Netzwerkinfrastruktur. So vielfältig wie die Einsatzzwecke sind auch die einzuleitenden Gegenmaßnahmen. Die wichtigste und wohl allgemeingültigste ist das zeitnahe Informieren der für die

Koordination der Gegenmaßnahmen zuständigen Personen. Damit diese Aufgabe bestmöglich erfüllt wird, muss der Alarm-Server in der Lage sein, jedes zur Verfügung stehende Kommunikationsmittel zu nutzen. Dementsprechend verfügen Alarm-Server über eine Vielzahl von Schnittstellen, welche einer Reihe von Gefährdungen ausgesetzt sind.

Ein Alarm-Server ist in der Regel in die Kommunikationsinfrastruktur der Organisation eingebettet, z. B. zur Benachrichtigung von Verantwortlichen per Anruf, Fax oder Textnachricht, kann andererseits aber auch zum Betrieb einer Notrufnummer zur Auslösung eines Alarms genutzt werden. Weiterhin kann eine Anbindung eines Alarm-Servers an IP-basierte Dienste wie VoIP, E-Mail oder Web erfolgen.

Bei der Überwachung der Netzwerkinfrastruktur bzw. zur Alarmauslösung kommt oft das Simple Network Management Protocol (SNMP) zum Einsatz.

Maßgebliche Gefährdungen und zu deren Entschärfung relevante Maßnahmen im Sinne des vorliegenden Dokuments ergeben sich über die Schnittstellen zu durch den Alarm-Server genutzten Elemente einer vorhandenen Telekommunikationsinfrastruktur.

7.4.1.2 Personensucheinrichtungen

Eine Personensucheinrichtung (PSE) bzw. Personensuchanlage (PSA) dient einer Zeitoptimierung zum Auffinden von Personen. Je nach Lösungsarchitektur und Funktionalitätsumfang können PSE-Lösungen verschiedenartig angewendet werden, z. B.

- zum Anstoßen einer Rückmeldung durch eine Person,
- zur Feststellung des Aufenthaltsorts vermisster Personen (typische Anwendungsgebiete sind hier z. B. Verdacht auf Unfall, auf Orientierungsverlust, auf gesundheitlichen Notfall),
- zum Lokalisieren einer Person als Reaktion auf ein durch diese aktiviertes Notsignal,
- zum Durchsuchen des Wirkbereichs eines Schadensereignisses (Explosion, Brand, ...) auf anwesende, ggf. zu bergende / zu versorgende Personen,
- zur Prüfung, ob und ggf. wo sich Personen in einem Gefahrenbereich befinden, insbesondere zur Einhaltung gesetzlicher Bestimmungen zum Arbeitsschutz (z. B. Auflage zur Zusammenarbeit von mindestens zwei Personen zwecks gegenseitiger Überwachung und nötigenfalls gegenseitiger Rettung aus akuten Gefahrenlagen).

Einfache Formen von PSE-Lösungen kombinieren eine Rundruflösung mit flächendeckender Anbringung von (internen) Telefonen: Über eine Lautsprecheranlage o. Ä. erfolgt ein Ausrufen der gesuchten Person, verbunden mit der Aufforderung, sich an einem bestimmten Ort einzufinden oder zunächst eine bestimmte Nummer anzurufen. Die gesuchte Person kommt dieser Aufforderung nach, bei Rückrufaufforderung mit Hilfe des nächstgelegenen Telefons. So kann sie mindestens ihren derzeitigen Aufenthaltsort benennen, darüber hinaus ist eine weiterführende Kommunikation unmittelbar möglich.

Eine derartige Lösungsarchitektur kommt ohne besondere Ausstattung für die zu suchenden Personen aus. In den Geltungsbereich des vorliegenden Dokuments rückt eine solche Architektur bei Nutzung einer Telefoninstallation für die Rückmeldung durch die gesuchte Person. Bei entsprechender Funktionalität von Telefonendgeräten (inkl. eingebautem Lautsprecher) und zentraler Telekommunikationsanlage kann zudem die TK-Lösung auch als Rundruflösung verwendet werden. Je nach Wichtigkeit, in einer Zielumgebung auf diesem Wege eine Person zu finden bzw. die Kommunikation mit einer Person herbeizuführen, ist die Verfügbarkeit der Installation und ihrer Elemente einzustufen.

Aufwändigere Formen von Personensucheinrichtungen ermöglichen das Lokalisieren einer Person unabhängig davon, ob diese Person in der Lage ist, selbst eine Rückmeldung zu ihrer aktuellen Position zu geben. Neben einer reinen Spontansuche zur unmittelbaren Positionsbestimmung kann eine solche PSE über automatisierte Feststellung und Speicherung von Positionsinformationen ergänzend eine „Spurbildung“ (engl. Tracking) ermöglichen. Bei fallweisen Schwierigkeiten zur Spontanbestimmung der Position einer Person lassen sich über die Spurinformationen die letzten Bewegungen der vermissten Person rekonstruieren. Dies lässt zumindest grobe Schlüsse auf den Aufenthaltsort der vermissten Person zu, der dann bei einer Suchaktion durch suchende Personen als Ausgangspunkt dienen kann. PSE-

Architekturen, die auch ohne Mitwirkung der gesuchten Personen auskommen, weisen folgende signifikante Elemente auf:

- Ausstattung der gesuchten Personen mit einem (persönlichen) technischen Kennzeichen zur Kontaktaufnahme

  Dieses technische Kennzeichen wird in einer technischen Ausstattung realisiert, die von einer zentralen Lösung aus lokalisiert werden kann. Hierzu hat das Kennzeichen eine Sendefunktion (z. B. Funksender) bzw. Sende- und Empfangsfunktion (z. B. Pager oder PSE-spezifische Kombination aus Funksender und -empfänger). Besteht nur eine Sendefunktion, so sendet das Gerät unaufgefordert, d. h. ständig bzw. in regelmäßigen Abständen, oder nach manueller Auslösung ein Signal aus. Über dieses Signal kann dann die Position bestimmt werden. Bei Kombination aus Sende- und Empfangsfunktion kann dieser Sendevorgang im Bedarfsfall von der zentralen Komponente ausgelöst werden, etwa zur Schonung der notwendigen Batterie bzw. Akku des Gerätes und zur gezielten regelmäßigen Funktionskontrolle. Soll über eine derartige Ausstattung nicht nur kontrolliert werden können, ob sich Personen in einem bestimmten Bereich aufhalten und wie viele, sondern eine gezielte Aufenthaltsbestimmung einer bestimmten Person möglich sein, so muss das technische Kennzeichen der jeweiligen Person fest zugeordnet sein. Hierzu ist eine eindeutig zum technischen Kennzeichen gehörende Information zu senden.

- Lösung zur Kontaktaufnahme mit technischen Kennzeichen zu Personengruppen

  Das zentrale Architekturelement der Personensucheinrichtung empfängt die ausgesendeten Signale der Personenkennzeichen, initiiert je nach Lösung auch gezielt eine Kommunikation mit der betreffenden Personenausstattung und leistet die Auswertung der so erhaltenen Informationen. Je nach Zweck und Konfiguration der PSE umfasst diese Auswertung auch die Speicherung von Positionsinformationen zur Spurbildung. Mindestleistungsumfang ist die Ermittlung und Darstellung der aktuellen Positionsinformationen.

In den Geltungsbereich des vorliegenden Dokuments kommt eine solche Architektur aus technischer Personenkennzeichnung und zentraler PSE-Einheit fallweise über verschiedene Aspekte:

- Nutzung einer Telekommunikationstechnologie zwecks Kommunikation zwischen Personenkennzeichen und zentraler PSE-Einheit

  Mobile Telekommunikationsendgeräte (z. B. Mobiltelefone) können als technisches Personenkennzeichen verwendet werden, sofern eine feste Zuordnung von Gerät zu Person mindestens als organisatorische Lösung verwaltet wird. Alternativ können persönliche Kennzeichen Telekommunikationstechnologie zur Kommunikation mit der zentralen PSE-Einheit nutzen, aber als zweckgebundene Sonderausstattung realisiert sein.

- Nutzung einer Telekommunikationslösung zur Alarmweiterleitung

  Eine solche Konstellation fällt z. B. an, wenn ein persönliches Kennzeichen als Notruflösung verwendet wird. Beispiele sind Notsignalsender für manuelle Auslösung in Gefahrensituationen (etwa für Skifahrer oder für den Aufenthalt in besonderen Gefahrenbereichen). Ein weiteres Beispiel ist eine Notsignalsenderfunktion als Teil einer Totmanneinrichtung; hier wird die Ausstattung von Personen automatisch überwacht und ggf. Meldung an die zentrale Einheit gegeben. Eine Totmanneinrichtung dient der Arbeitssicherheit. In der jeweiligen Arbeitssituation als gefährlich zu meldende Aspekte können waagerechte Körperlage oder auch schon längere Bewegungslosigkeit sein. In Kombination mit einer PSE-Intelligenz wird so ein schnelles Eingreifen zur Vermeidung von Personenschäden möglich.

  Bei Kopplung einer PSE-intelligenten Lösung mit einer Telekommunikationslösung wird über die entsprechende Schnittstelle eine gezielte (automatische) Alarmierung geleistet, um notwendige Notfallmaßnahmen (medizinische Versorgung, Rettung, Bergung etc.) durch hierfür zuständige Personen zeitnah zu initiieren. Die Kopplung kann z. B. durch direkte Anschaltung einer zentralen PSE-Einheit an eine Telekommunikationsanlage (ISDN- oder VoIP-basiert) oder unter Vorschaltung eines Alarm-Servers erfolgen (siehe auch 7.4.1.1). Die maßgeblichen technischen Schnittstellen ergeben sich durch die Art der Telekommunikationslösung, beispielsweise durch einen analogen bzw. digitalen Anschluss an eine klassische TK-Anlage oder durch einen SIP-Trunk für die VoIP-Nutzung, durch

Schnittstellen zu genutzten IT-Diensten wie E-Mail-Service oder Faxservice bei Nutzung von Unified-Communications-Teillösungen.

Da die beschriebenen aufwändigeren Personensucheinrichtungen dem Schutz von Personen dienen, ist bzgl. ihrer Verfügbarkeit in der Regel ein erhöhter Schutzbedarf anzusetzen. Dies ist zunächst für die Maßnahmenauswahl zur Nutzung von Telekommunikationstechnologie innerhalb der PSE-Lösung selbst zu berücksichtigen. Erfolgt eine Kopplung an bestehende Telekommunikationslösungen wie TK-Anlage oder Alarm-Server, so vererbt sich der Schutzbedarf der PSE-Lösung mindestens auf die durch diese genutzten Schnittstellen und Funktionalitäten.

7.4.1.3 Brandmeldeeinrichtungen

Einrichtungen zur Brandmeldung bilden eine Gefahrenmeldeanlage mit Schwerpunkt Brandschutz (Brandmeldeanlage, BMA). Typische Anwendungsformen sind:

- Weiterleitung von Brandmeldungen an eine ständig besetzte Leitstelle

  Diese alarmiert eine umgebungseigene oder örtliche Feuerwehr nach Vorprüfung auf einen möglichen Fehlalarm.
- Automatische Weiterleitung von Meldungen über Anzeichen für die manuelle Einleitung schadensbegrenzender Sofortmaßnahmen, etwa bis zum Eintreffen der zuständigen Feuerwehr
- Absetzen einer Brandmeldung als Basis eines automatisierten Auslösens von schadensbegrenzenden Sofortmaßnahmen

  Beispiele für derartige automatisch ausgelöste Sofortmaßnahmen sind das Öffnen von Rauchableitungseinrichtungen, das Schließen von Feuerschutztüren, die Ansteuerung von Aufzügen (Sperrung der Nutzung im Brandfall) oder das Auslösen einer vorhandenen Objektlöschanlage.

Typische Sensoren sind im Falle einer solchen Meldeeinrichtung Brandmelder, einzeln oder für verschiedene Meldebereiche jeweils zu Gruppen zusammengeschaltet.

Die durch Brandmelder oder Brandmeldergruppen erfassten Ereignisse können zunächst auf weiteren Endpunkten einer Brandmeldelösung auflaufen, die mindestens der strukturierten Ereignisanzeige und der Meldungsquittierung dienen:

Feuerwehr-Anzeigetableau (FAT)

Bei einem Feuerwehr-Anzeigetableau (FAT) handelt es sich um eine Zusatzeinrichtung zu einer Brandmeldeanlage zur Anzeige von Alarmmeldungen sowie Sonderzuständen der Anlage wie Störungen oder Abschaltungen (etwa im Zuge von Instandhaltungs- und Instandsetzungsarbeiten), siehe auch [DIN 14662]).

Feuerwehr-Bedienfeld (FBF)

Auch ein Feuerwehr-Bedienfeld (FBF) dient als Zusatzeinrichtung zu einer Brandmeldeanlage der Visualisierung eingegangener Brandmeldungen sowie der Anzeige von Anlagenzuständen. Ergänzend umfasst ein Feuerwehr-Bedienfeld die Möglichkeit der Übertragung zur Feuerwehr (automatische Alarmierung). Feuerwehr-Bedienfelder weisen genormte Anzeige- und Bedienelemente auf (siehe [DIN 14675]), was die schnelle Lagesichtung und Bedienung durch die Feuerwehr in jeder Zielumgebung erleichtert. In der Regel ist ein Feuerwehr-Bedienfeld mit einem Schloss der umgebungseigenen oder örtlichen Feuerwehr versehen, sodass ein Betätigen der Funktionstasten sowie das Rücksetzen des Alarms nur durch Personal der Feuerwehr erfolgen kann.

Brandmeldezentrale (BMZ)

Typischerweise kombinieren BMZ-Installationen ein Feuerwehr-Bedienfeld mit einer Steuereinheit zur Anlagensteuerung und verfügen über einen direkten Anschluss an das Meldenetz der örtlichen Feuerwehr.

Voraussetzung für einen solchen Meldenetzanschluss ist die Einhaltung von durch die jeweilige Feuerwehr spezifizierten technischen Anschlussbedingungen (TAB). Diese basieren entsprechend den Komponenten und Schnittstellen einer BMZ in der Regel auf den folgenden Normen:

- DIN VDE 0833 „Gefahrenmeldeanlagen für Brand, Einbruch und Überfall“ (siehe [DIN VDE-0833])
- DIN 14661 „Feuerwehrwesen - Feuerwehr-Bedienfeld für Brandmeldeanlagen“ (siehe [DIN 14661])
- DIN 14662 „Feuerwehrwesen - Feuerwehr-Anzeigetableau für Brandmeldeanlagen“ (siehe [DIN 14662])
- DIN 14675 „Brandmeldeanlagen - Aufbau und Betrieb“ (siehe [DIN 14675])
- DIN EN 54 „Brandmeldeanlagen“ (siehe [DIN EN 54])

Darüber hinaus spezifizieren die technischen Anschlussbedingungen Detailforderungen der jeweiligen Feuerwehr, z. B.:

- verbindliche Forderung nach Ausstattung der BMZ mit einem Feuerwehr-Anzeigetableau
- Installation einer analogen Meldeanzeige oder einer Registriereinrichtung (z. B. Protokolldrucker)
- Zugangsschutz für die BMZ über ein vorgegebenes Schließsystem oder Schloss (Feuerwehrschließung) zwecks Beschränkung des Zugangs auf Feuerwehrpersonal
- Vorgaben zu Positionierung und Kennzeichnung von Brandmeldern
- Vorgaben zur Bereitstellung und Pflege von Orientierungsplänen für die Feuerwehr (Feuerwehrpläne, Feuerwehrlaufkarten mit Angaben bzgl. kürzester Wege zu Punkten, für die eine Meldung angezeigt wird)
- Auflagen bzgl. Inbetriebnahme, Abnahme und Betrieb inklusive Instandhaltung und Wartung einer angeschlossenen BMA
- Mitteilungspflichten gegenüber der Feuerwehr bei baulichen / betrieblichen Änderungen mit Blick auf die Anlage

Ergänzend zum Anschluss an ein bestehendes Feuerwehrmeldenetz wird eine Brandmeldeanlage in der Praxis auch oft an eine zentrale Gefahrenmeldeanlage mit der Funktion eines Alarm-Servers angeschlossen. Hierüber werden definierte Personen oder Personengruppen über festgelegte Meldewege über Brandmeldungen informiert, insbesondere zur Umsetzung interner Vorgaben bzgl. Meldepflichten und Alarmierung. Alternativ kann eine Brandmeldeanlage direkt an eine vorhandene Telekommunikationsinfrastruktur angeschlossen werden. Durch Anschaltung an derartige TK-Einrichtungen, unmittelbar oder mittelbar via Alarm-Server, rückt eine Brandmeldeeinrichtung in den Geltungsbereich des vorliegenden Dokuments. Die maßgeblichen Gefährdungen und zu erwägenden Maßnahmen ergeben sich über die zur Mitnutzung vorhandener Kommunikationslösungen verwendeten Schnittstellen und Technologien.

Da Brandmeldeeinrichtungen insbesondere dem Schutz von Personen dienen, ist neben der grundsätzlichen Realisierung maßgeblicher Normen und gesetzlicher Vorschriften typischerweise ein erhöhter Schutzbedarf bezüglich der Verfügbarkeit anzusetzen. Auf die entsprechenden Schnittstellen und genutzten Funktionalitäten solcher Lösungen vererbt sich dieser Schutzbedarf.

7.4.1.4 Sicherheitsmechanismen bei Alarmierungssystemen

Alarmierungssysteme wie Brandmeldeeinrichtungen und Personensucheinrichtungen wurden in der Vergangenheit lange Zeit typisch als geschlossene Systeme betrieben. Dies wurde zum Teil für bestimmte Alarmierungszwecke aufgrund der besonders hohen Anforderungen bezüglich Verfügbarkeit gezielt so gefordert. Schwerpunktanforderungen an die Sicherheit von Alarmierungssystemen waren typischerweise Verfügbarkeitsaspekte. Die Integrität und die Vertraulichkeit wurden nachrangig behandelt. Als Konsequenz hieraus gibt es derzeit nur im Ausnahmefall Sicherheitsmechanismen, die speziell für die Absicherung der Kommunikation zu Alarmierungslösungen spezifiziert sind.

Des Weiteren gilt: Werden Alarmierungssysteme aus zuvor genannten Gründen im Rahmen des vorliegenden Dokuments berücksichtigt, so liegt der Fokus dabei auf Sicherheitaspekten, die durch die Kopplung von Alarmierungslösungen und TK-Lösungen ergeben.

Insofern sollten mit der Ankopplung von Alarmierungssystemen an TK-Infrastrukturen die Umsetzung der TK-relevanten Sicherheitsmechanismen umgesetzt werden.

7.4.2 Gefährdungen

Es gibt diverse Zwecke von Alarmierung und entsprechend eine Reihe unterschiedlicher Ausprägungen von Alarmierungssystemen. Wichtige Beispiele beschreiben Kapitel 7.4.1.1 bis 7.4.1.3. Diese Beispiele wurden allerdings ohne Anspruch auf Vollständigkeit gewählt, sondern vorrangig als repräsentative Basis für das notwendige Verständnis spezifischer Gefährdungslagen und Rahmenbedingungen.

Entsprechend müssen die maßgeblichen Gefährdungen aus den IT-Grundschutz-Katalogen im konkreten Einzelfall unter Berücksichtigung der folgenden Hinweise bestimmt werden:

- Für die einzelnen Elemente einer Alarmierungslösung sind die Grundschutz-Gefährdungen der Infrastruktur-Schicht je nach Rahmenbedingungen am Aufstellungs- bzw. Montageort zu berücksichtigen.

  Zentrale Einheiten wie ein Alarmierungs-Server oder eine zentrale Gefahrenmeldeanlage sollten nach Möglichkeit unter Beachtung der Gefährdungen untergebracht werden, die in den Bausteinen B 2.9 „Rechenzentrum“ (optimal) oder B 2.4 „Serverraum“ gelistet sind.

  Für Endpunkte wie Sensoren (Brandmelder, Bewegungsmelder etc.) ist häufig eine Montage in schlecht schützbaren oder sogar frei zugänglichen Umgebungen notwendig. Für die gezielte Gefährdungsbetrachtung können je nach konkreten Optionen für Montagepunkte hier die Gefährdungen aus den Bausteinen B 2.7 „Schutzschränke“ bzw. mindestens B 2.11 „Besprechungs-, Veranstaltungs- und Schulungsräume“ als Ausgangsbasis herangezogen werden.
- Mindestens für die Schnittstelle zwischen Alarmierungssystem und TK-System sind die für das TK-System relevanten Grundschutz-Gefährdungen auf Relevanz zu prüfen.

  Wenn dieselbe Technologie sowohl für TK-Systeme als auch für ein Alarmierungssystem zum Einsatz kommt, gelten die technologiespezifischen Gefährdungen für das zugrunde liegende System. Diese müssen jedoch ggf. für das Alarmierungssystem höher bewertet werden.

Die im Folgenden referenzierten Gefährdungen aus den IT-Grundschutz-Katalogen ergänzen beispielhaft diese grundsätzlichen Erläuterungen zur Bestimmung der relevanten Gefährdungslage.

7.4.2.1 Höhere Gewalt

Ergänzend zu den relevanten Gefährdungen der IT-Grundschutz-Kataloge gelten die spezifischen Ausprägungen der Gefährdungen für die verwendete TK-Basistechnologie (siehe Kapitel 3 „Klassische Telekommunikationstechnik“ und Kapitel 4 „Voice over IP“).

Außerdem sind die Gefährdungen zur Einbindung Mobiler Endgeräte (siehe Kapitel 9) sinngemäß zu übertragen.

Ein Beispiel in diesem Sinne ist G-TK-148 „Unzureichende Planung für den Einsatz in widrigen Umgebungsbedingungen“. Dies betrifft als Teil einer Alarmierungslösung eingesetzte Telekommunikationsendgeräte, bei Verwendung von Drahtlostechnik auch Infrastrukturkomponenten wie WLAN Access Points und Sensor-artige Endpunkte einer Alarmierungslösung.

7.4.2.2 Organisatorische Mängel

Über die als relevant erkannten Gefährdungen der IT-Grundschutz-Kataloge hinaus sind für Alarmierungssysteme die nachfolgend beschriebenen spezifischen Gefährdungen auf Relevanz zu prüfen.

Die Relevanz ergibt sich dabei fallweise über Berührungspunkte zwischen TK-Technologie und Alarmierungssystem. Die entsprechend relevanten Passagen des vorliegenden Dokuments bestimmen sich über

- TK-Systeme mit Schnittstelle zum betrachteten Alarmierungssystem oder
- TK-Systeme, die funktional in die Alarmierungslösung eingebunden werden.

Zusätzlich zu den Gefährdungen für die zugrunde liegenden Basistechnologien (siehe Kapitel 3 „Klassische Telekommunikationstechnik“ und Kapitel 4 „Voice over IP“) gelten die folgenden Gefährdungen:

G-TK-99 Unzureichende Regelungen für den Einsatz von Alarmierungssystemen

Soweit eine Alarmierungslösung eine TK-Infrastruktur mitnutzt und zu diesem Zweck mit dieser gekoppelt wird, müssen ggf. Details geregelt werden, deren Einhaltung Voraussetzung für den Anschluss an diese TK-Lösung sind. Beispielsweise müssen im notwendigen Umfang Spezifikationen erfolgen, welche physikalische Schnittstelle das Alarmierungssystem mitbringen muss, um an die TK-Infrastruktur angeschlossen werden zu können. Gegebenenfalls müssen auch für Anschlüsse an diese Infrastruktur geltende betriebs- und sicherheitsrelevante Vorgaben auf den Alarmsystemanschluss übertragen werden. Andernfalls drohen Störungen durch Kompatibilitätsprobleme oder eine Schwächung des Sicherheitsniveaus aus Sicht der TK-Infrastruktur.

Je nach Art von Endpunkten der Alarmierungslösung sind sicherheitsrelevante Regelungen für den Einsatz von TK-Endgeräten auf diese Endpunkte des Alarmierungssystems zu übertragen, sodass von solchen Endpunkten ausgehende Sicherheitsvorfälle, die auf ein TK-System übergreifen können, vermieden werden.

Im Falle von PSE-Lösungen sind Regelungen für den sachgemäßen Umgang mit der personenbezogenen Ausstattung notwendig, damit Fehlfunktionen oder Fehlalarme vermieden werden. Beispiele sind Festlegungen zur korrekten Vorgehensweise beim Übergang der Ausstattung auf eine andere nutzende Person sowie Festlegungen, ob und inwieweit Einweisungen in den Umgang mit solcher Ausstattung nötig sind. Werden TK-Endgeräte, etwa Mobiltelefone, als Basis für die Lokalisierung von Personen durch die PSE-Lösung mitgenutzt, sind im notwendigen Umfang Details zu regeln, um diese Lokalisierungsfunktion wie beabsichtigt nutzen zu können. Ein Beispiel ist die Klärung, inwieweit ein Pool-Handy in diesem Sinne verwendet werden kann und was zur Wahrung des Personenbezugs dabei zu beachten ist.

Durch Kombination von Alarmierungssystem und TK-Infrastrukturelementen entsteht ein Gesamtsystem, bei dessen Betrieb Verfügbarkeits- und Sicherheitsanforderungen beider Einzelsysteme gleichwertig berücksichtigt werden müssen. Entsprechend besteht auch hier Regelungsbedarf. Beispielsweise dürfen Wartungen, Software-Änderungen wie Release-Wechsel oder das Einspielen von Patches, die einen Neustart der TK-Lösung erfordern, nicht unabgestimmt vollzogen werden. Dem Betreiber des Alarmierungssystems muss Gelegenheit gegeben werden, auf den vorübergehenden Wegfall der TK-Lösung durch kompensatorische Maßnahmen zu reagieren oder Zeiten anzumelden, während derer ein so eingeschränkter Nutzen der Alarmierungslösung hingenommen werden kann. Umgekehrt müssen Eingriffe in das Alarmierungssystem, die (z. B. wegen abschließender Tests) Auswirkungen auf Auslastung der TK-Infrastruktur oder störungsähnliche Zustände der genutzten Schnittstelle zur TK-Lösung mit sich bringen können, dem Betreiber der TK-Anlage mindestens vorangekündigt werden.

G-TK-100 Unzureichende Regelungen mit Blick auf Einhaltung maßgeblicher Gesetze und Vorschriften für den Einsatz von Alarmierungssystemen

Neben der Einhaltung je nach Alarmierungszweck, Zielumgebung oder eingesetzter Technologie maßgeblicher spezifischer gesetzlicher Regelungen, technischer Normen und sonstiger Vorschriften (siehe Kapitel 7.4.1) können allgemeine sicherheitsrelevante Vorschriften relevant sein. Entsprechende Details zu Technologieauswahl, Feinkonfiguration,

Betrieb und Nutzung eines Alarmierungssystems sind grundsätzlich auch für TK-Systeme maßgeblich, die durch ein Alarmierungssystem mitgenutzt werden. Ein Beispiel sind Regelungen für den Einsatz der Spurbildungsfunktion einer Personensucheinrichtung zwecks Vermeidung von Verletzungen des Datenschutzes. Hier können zur Umsetzung entsprechender Vereinbarungen mit den zu suchenden Personenkreisen Detailfestlegungen notwendig sein, wer wann auf entsprechende personenbezogene Informationen Zugriff haben darf. Je nach Architektur der Mitnutzung einer TK-Lösung für die PSE-Lösung kann dies auch Konfigurationsdetails für die TK-Lösung nach sich ziehen, damit nicht Administratoren oder Nutzer der TK-Lösung unzulässigen Zugriff auf Spurinformationen erhalten können.

Durch Kopplung zwischen Alarmierungssystem und einem TK-System entsteht ein Gesamtsystem, bei dem insbesondere eine Abstimmung bezüglich betrieblicher Details an den Übergabepunkten zwischen den beiden Systemlösungen mit Blick auf Verfügbarkeitssicherung notwendig ist. Beispiele sind

- ein Abgleich von Detailpflichten im Rahmen von Instandhaltung und Wartung sowie
- Regelungen für einen geeigneten und koordinierten organisatorischen Ablauf bei Eingriffen im Rahmen von Wartung / Instandsetzung und geplanten Änderungen sowie Zustandskontrollen und Funktionstests.

Andernfalls drohen vermeidbare Störungssituationen oder Verletzung von für den Anlagenbetrieb maßgeblichen Vorschriften.

G-TK-101 Unzureichende Planung (der TK-Mitnutzung) von Alarmierungssystemen

Ohne geeignete Planung drohen zunächst Fehler bei der Produktauswahl (mangelhafte Produktunterstützung zur Umsetzung von Vorschriften oder Erfüllung zweckdienlicher Anforderungen). Des Weiteren muss die Architektur von Alarmierungs- und TK-System gleichwertig sein, soweit Verfügbarkeitsaspekte betroffen sind. Andernfalls droht durch Störungen eines Systems über die Kopplung von Alarmierungs- und TK-System eine inakzeptable Beeinträchtigung der Verfügbarkeit des anderen Systems. Generell gilt, dass Störungen über Kopplungsschnittstellen von einem auf das andere System übergreifen können.

Insbesondere wichtig bei der Produktauswahl ist auch die notwendige Kompatibilität von TK- und Alarmierungsprodukten bzgl. Schnittstellen, über die TK- und Alarmierungssysteme gekoppelt werden sollen. Dies gilt für Hard- und Software-Aspekte, für reine Aspekte des stabilen Funktionierens solcher Schnittstellenübergänge ebenso wie für die Unterstützung von Sicherheitsanforderungen. Bei Versäumnissen droht mindestens Mehraufwand (Zusatzinvestitionen, erhöhter Betriebsaufwand) aufgrund einer ggf. aufwändigen Lösungsfindung zur Umgehung von Inkompatibilitäten. Mittelbar können hierdurch Fehlfunktionen oder eine erhöhte Anfälligkeit für Sicherheitsvorfälle die Folge sein.

Werden nicht alle notwendigen Wissens- und Kompetenzträger frühzeitig in die Planung eingeschaltet, sodass eine zunächst unzureichende Planung im Nachhinein korrigiert werden muss, so drohen Verzögerungen bei der Inbetriebnahme und Mehraufwand durch notwendige Nachbesserungen an bereits erfolgten Installationen.

G-TK-102 Unzureichende Kontrolle von Zugangs- und Zugriffsmöglichkeiten zu Elementen einer Alarmierungslösung

Im Falle von Alarmierungssystemen ist hier eine erhöhte Brisanz gegeben, da die Alarmierung häufig dem Schutz der Unversehrtheit von Personen dient. Dabei ist als Rahmenbedingung bei Alarmierungssystemen die zumindest teilweise Notwendigkeit zur Anbringung von Sensoren o. Ä. in schlecht zu schützenden und öffentlich zugänglichen Bereichen zu bedenken. Typische Grundschutzmaßnahmen zum Zugangsschutz lassen sich also nur bedingt umsetzen. Bei Kopplung eines Alarmierungssystems an eine TK-Lösung besteht grundsätzlich die Möglichkeit, dass über die koppelnde Schnittstelle ein Sicherheitsvorfall vom Alarmierungs-

system auf die TK-Lösung übergreift. Dies ist beim Umgang mit der Gefährdungslage hinsichtlich Zugang / Zugriffen auf das Alarmierungssystem zu berücksichtigen.

G-TK-103 Unzureichender Schutz personenbezogener Daten bei Verwendung durch eine Alarmierungslösung

Zweckbindung ist eine typische Bedingung für die notwendige Zustimmung einer Person zur Verwendung von auf diese Person bezogenen Daten. Beispiele für Daten, bei denen die Gefahr einer Auswertung zu anderen Zwecken als der reinen Rettung von Personen entstehen kann, sind Spurdaten im Rahmen einer PSE oder Alarmierungsdaten über eine Totmannlösung. Von diesen könnten z. B. Rückschlüsse über Pausenzeiten oder den Gesundheitszustand einer Person unrechtmäßig gezogen werden.

7.4.2.3 Menschliche Fehlhandlungen

Soweit TK-Systeme (siehe Kapitel 3 und 4) durch eine Alarmierungslösung mitgenutzt werden, sind alle zum jeweiligen Systemtyp gehörenden spezifischen Gefährdungen in Form menschlicher Fehlhandlungen auch für die konkrete Alarmierungssystemlösung relevant.

G-TK-104 Unzureichende Prüfung der Identität von Kommunikationspartnern bei eingehenden Alarmen

Für Alarmierungssysteme verwendete Produkte weisen entsprechend der Historie als „geschlossen betriebene Systeme“ zum Teil nur bedingt Möglichkeiten zur technischen Authentizitätsprüfung eingehender Alarme auf. Soweit derartige Einschränkungen gegeben sind, muss eine umso genauere Prüfung vorgesehen werden, ob ein bewusst generierter Fehlalarm vorliegen könnte.

Gezielte Fehlalarme durch Missbrauch eines Alarmierungssystems können Teil eines vorsätzlichen Angriffs sein. So kann etwa eine Ablenkung und Bindung von Ressourcen der Zweck solcher gefälschten Alarme sein, sodass diese Ressourcen dann für die schnelle Erkennung und Abwehr eines nächsten Angriffsschritts nicht rechtzeitig zur Verfügung stehen. Weiterhin kann mittelbar auch ein schädlicher Einfluss auf ein angekoppeltes TK-System die Folge sein, etwa durch eine Flut von Fehlalarmen und in der Folge eine erhöhte Nutzung des TK-Systems zum Umgang mit den gemeldeten vermeintlichen Schadensereignissen.

G-TK-105 Ungeeigneter Umgang mit Nutzerzugängen und -ausstattung zu Alarmierungslösungen

Diese Gefährdung betrifft zunächst Alarmierungslösungen zur Lokalisierung oder Ereignismeldung bzgl. einzelner Personen. Fehler in der Handhabung, der Zustandsprüfung vor Verwendung (z. B. Akkuladezustand) oder bei der Übergabe können zu Fehlfunktionen oder Fehlinterpretationen führen und so die Schutzwirkung durch die Alarmierungslösung deutlich einschränken. Vergleichbares gilt für Endpunkte zur notwendigen gezielten Aktivierung und Deaktivierung von Alarmierungslösungen. Hier drohen Fehlalarme bei Aktivierung zum falschen Zeitpunkt oder Wegfall der Schutzwirkung durch Versäumnisse bzgl. Reaktivierung der Alarmierungslösung. Ein Bezug zu Telekommunikationssystemen entsteht z. B. über erhöhte Ressourcenbindung am TK-System durch gehäufte Fehlalarme oder zur Klärung der Lage nach einem Fehlalarm. Auch kann fallweise bei der Ursachenfindung zu einem durch Fehlbedienung ausgelösten Alarm eine mit der Alarmierungslösung gekoppelte TK-Lösung zunächst mit in die Analyse eingeschlossen werden (Verdacht auf technische Fehlfunktion als Ursache des Fehlalarms). Dies bindet dann unnötig Ressourcen beim TK-Anlagenbetreiber, wenn eine Fehlbedienung an der Alarmsystemlösung die eigentliche Ursache darstellt.

7.4.2.4 Technisches Versagen

Sofern Lösungen für mobile Telekommunikation zur Unterstützung von Alarmierungslösungen eingesetzt werden, sind technologiebedingt zu berücksichtigen:

G-TK-139 „Ausfall oder Störung eines öffentlichen Funknetzes“

Die Ursache kann auf Seiten des Betreibers oder im Bereich höhere Gewalt zu suchen sein. Aus Sicht einer Alarmierungslösung, die ein Funknetz als Teil der Alarmierungsinfrastruktur nutzt und betrachtet, ist der Blickwinkel eher auf das so gegebene zumindest anteilige technische Versagen dieser Infrastruktur gerichtet, im Sinne von

G-TK-106 Ausfall der mitgenutzten TK-Infrastruktur

Schädliche Folgen für Alarmierungslösungen sind etwa die Beeinträchtigung einer PSE-Lösung bei Mitnutzung einer TK-Infrastruktur, z. B. bei Verwendung von Mobiltelefonen als persönliches Merkmal, oder die Beeinträchtigung der Alarmweiterleitung, sofern die betroffenen TK-Strecken ebenfalls für die Alarmweiterleitung benötigt werden.

Entsprechend ist im Rahmen der Planung einer Alarmierungslösung je nach Zweck und resultierendem Verfügbarkeitsbedarf zu prüfen, ob und in welchem Umfang eine Abstützung auf Mobilfunktechnik überhaupt geeignet ist.

G-TK-107 Technisch bedingte Fehlalarme

Fehlfunktionen oder Fehlinterpretationen im Rahmen automatisierter Auswertung und Aufbereitung eingehender Basisinformationen können zu Fehlalarmen durch Alarmierungssysteme führen.

Solche Fehlalarme können betriebsrelevant sein, falls TK-Lösungen als Informationsquelle für Alarmierung mitgenutzt werden bzw. zur Alarmweiterleitung mit einem Alarmierungssystem gekoppelt sind und durch gehäufte Fehlalarme die Ressourcen der TK-Lösung unnötig in Anspruch genommen werden. Auch kann fallweise im Rahmen der Ursachenfindung zu Fehlalarmen eine unnötige Ressourcenbindung auf Seiten des TK-Anlagenbetreibers entstehen, wenn die Verursachung durch die Alarmierungslösung nicht zügig zu erkennen ist.

7.4.2.5 Vorsätzliche Handlungen

Mindestens im Falle von Personensucheinrichtungen mit Spurfunktion (Nachverfolgung des Wegs, Tracking) ist die Gefährdung G-TK-126 „Profilbildung und Tracking von Personen“ (siehe Kapitel 8.1) zu verallgemeinern bzw. auf diese Art von Alarmierungssystemen zu übertragen. Im Falle der Personensuche ist allerdings zwischen dem Interesse der betroffenen Person an persönlicher Unversehrtheit, z. B. an schneller Rettung aus Gefahren- und Notsituationen, und dem Interesse an Datenschutz, Selbstbestimmung usw. abzuwägen. Erfassung und Zugang zu Tracking-Informationen müssen gezielt auf solche Fälle und solchen Umfang begrenzt werden, die der schnellen Lokalisierung von Personen in Notfall- und Gefahrensituationen dienlich sind.

Darüber hinaus sind für Alarmierungssysteme insbesondere bei deren Mitnutzung von TK-Infrastrukturen die folgenden spezifischen Gefährdungen zu berücksichtigen:

G-TK-108 Denial-of-Service-Angriffe auf bzw. über Alarmierungssysteme

Soweit es sich um Sabotage-artige Angriffe auf die Hardware handelt bzw. um den bewussten Missbrauch von Endpunkten einer Alarmierungslösung, besteht diese Gefährdung in Abhängigkeit von der Möglichkeit zum unberechtigten Zugang und Zugriff auf solche Endpunkte (siehe G-TK-107 „Technisch bedingte Fehlalarme“).

Im Fall von Kopplungen zwischen Alarmierungssystem und TK-Systeminfrastruktur kommt der Aspekt möglicher DoS-Angriffe auf die TK-Infrastruktur ausgehend vom Alarmierungssystem und umgekehrt als zu berücksichtigende Gefährdungsausprägung hinzu (Beispiel: übergreifende Lastangriffe).

G-TK-109 Alarmierungssysteme als Ausgangspunkt für Angriffe auf TK-Lösungen

Soweit TK-Lösungen durch Alarmierungssysteme mitgenutzt oder zwecks Weiterleitung von Alarmen mit Alarmierungssystemen gekoppelt werden, können über die Kopplungspunkte Angriffe übergreifend wirken bzw. gezielt so angelegt werden.

Ein Angreifer kann gezielt Elemente des Alarmierungssystems so angreifen, dass eine übergreifende Wirkung auf die TK-Lösung entsteht. Ein Beispiel ist eine gezielte Häufung vorgetäuschter Fehlalarme durch Manipulationen am Alarmierungssystem mit dem Ziel, eine schädlich erhöhte Ressourcenbindung am mitgenutzten TK-System zu provozieren.

Insbesondere bei intelligenten zentralen Einheiten von Alarmierungssystemen (Beispiel: Alarm-Server) besteht die Möglichkeit, dass ein Angreifer zunächst das zentrale Alarmierungssystem übernimmt, um von dort aus gezielt weitere Angriffsschritte auf die TK-Infrastruktur vorzunehmen. Diese Folgeschritte nutzen gezielt die Schnittstellen zwischen Alarmierungssystem und TK-Infrastruktur und die Tatsache, dass das übernommene Alarmierungssystem aus Sicht der TK-Infrastruktur einen berechtigten Kommunikations-teilnehmer darstellt.

7.4.3 Sicherheitsmaßnahmen

Dieses Kapitel beschreibt Maßnahmen zur Absicherung von Alarmierungssystemen, soweit diese in den Geltungsbereich des vorliegenden Dokuments fallen, d. h.

- für Alarmierungssysteme, deren Funktionalitäten durch Mitnutzung von TK-Lösungen realisiert werden bzw.
- für Alarmierungssysteme, die zwecks Weiterleitung von Alarmen an TK-Infrastrukturen angeschlossen werden.

Entsprechend konzentrieren sich die Ausführungen zu Maßnahmen auf den Umgang mit Gefährdungen, die aus einer Kopplung von Alarmierungs- und TK-Systemlösung resultieren. Die Maßnahmen-beschreibung erfolgt unter besonderer Berücksichtigung eines erhöhten Schutzbedarfs.

Der Maßnahmenkatalog mit diesem Schwerpunkt ist in die folgenden Blöcke aufgeteilt:

- Zentrale Systeme, Server und Anwendungen, siehe Kapitel 7.4.3.1
- Endpunkte von Alarmierungssystemen, siehe Kapitel 7.4.3.2
- Netzwerk, siehe Kapitel 7.4.3.3
- Netz- und Systemmanagement, siehe Kapitel 7.4.3.4
- Übergreifende Aspekte, siehe Kapitel 7.4.3.5

7.4.3.1 Zentrale Systeme, Server und Anwendung

Die Möglichkeit zur Absicherung zentraler Einheiten von Alarmierungssystemen wird geprägt von der Art des Alarmierungssystems und des damit verbundenen typischen Software-Umfangs solcher zentraler Einheiten. So besteht in diesem Sinne z. B. ein deutlicher Unterschied zwischen einer typischen Brandmeldezentrale und einem zentralen Gefahrenmeldesystem mit Funkionen eines Alarmierungs-Servers.

M-TK-140 Schaffung geeigneter Umgebungsbedingungen für zentrale Elemente eines Alarmierungssystems

Zentrale Elemente eines Alarmierungssystems sind entsprechend dem Schutzbedarf geeignet unterzubringen. Maßgeblich sind dabei typische Gefährdungen mit Blick auf unbefugten Zugang zu und Zugriff auf solche Installationen und Gefährdungen der Kategorie höhere Gewalt. Beim Umgang mit Aspekten höherer Gewalt ist dabei zu berücksichtigen, dass

bestimmte Alarmierungssysteme ihrerseits der Früherkennung (sich anbahnender) Schadensereignisse dienen. Für derartige Alarmierungslösungen ist der Schutzbedarf entsprechend hoch anzusetzen und die Präventivwirkung der Umgebungsgestaltung demgemäß besonders wirksam auszulegen.

Server-artige Elemente wie zentrale Konsolen oder Alarm-Server sollten in jedem Fall, auch bei geringem Funktionsumfang, in Räumen untergebracht werden, die mindestens die Grundschutzmaßnahmen gemäß Baustein B 2.6 „Raum für technische Infrastruktur“ umsetzen.

Müssen zentrale Anzeige- und Bedieneinheiten zweckbedingt einem größeren Personenkreis zugänglich sein, so sind sie nötigenfalls von anderen Alarmierungsaufgaben zu trennen und separat unterzubringen.

Beispiel: Soll ein zentrales Anzeige- und Bedienfeld zu einem Einbruchmeldesystem zwecks Quittierung von akustischen (Fehl-)Alarmen für den gesamten Personenkreis zugänglich sein, der in den besonders geschützten Bereichen aufenthaltsberechtigt ist, so ist eine Kombination dieser Bedieneinheit mit Zugriff auf andere Alarmierungsfunktionen wie Brandmeldetechnik bedenklich. Es kann sogar ein Verstoß gegen Auflagen für Installationen zu bestimmten Alarmierungszwecken drohen. Bei entsprechendem Analyseergebnis sind getrennte Bedieneinheiten für Einbruchmeldung und andere Alarmierungsfunktionalitäten vorzusehen, auch wenn ein Produkt eingesetzt wird, dass die Bedienung verschiedener Systeme mit derselben Konsole technisch unterstützt. Nur das Bedienfeld für die Einbruchmeldelösung wird dann so angebracht, dass es dem hierfür vorgesehenen Personenkreis leicht zugänglich ist.

Müssen zentrale Elemente einer Alarmierungslösung zweckbedingt in Umgebungen angebracht werden, in denen ein angemessener Schutz durch Zugangs- und Umgebungsgestaltung nur bedingt realisiert werden kann, ist eine Kompensation durch zusätzliche Maßnahmen der Überwachung solcher Installationen zu erwägen (siehe Kapitel 7.4.3.4).

M-TK-141 Sichere Konfiguration zentraler Elemente einer Alarmierungslösung

In Abhängigkeit vom Schutzbedarf und Funktionsumfang der Software zentraler Elemente einer Alarmierungslösung ist die Konfiguration gezielt unter Sicherheitsgesichtspunkten vorzunehmen.

Relevante Aspekte sind hierbei je nach Produkteigenschaften

- die gezielte Wahl eines zweckgebundenen Umfangs der installierten Software,
- die gezielte Beschränkung aktivierter Funktionalitäten und Zugriffsmöglichkeiten sowie
- die Verwendung vom Produkt unterstützter Sicherheitsfunktionalitäten bzgl. Benutzer- und Rechtemanagement, Authentisierung im Rahmen von Kommunikationsbeziehungen und Verschlüsselungsoptionen (Verschlüsselung der Kommunikation, ggf. auch Verschlüsselung lokal gespeicherter Informationen).

Soweit Elemente einer TK-Infrastruktur als zentrale Elemente einer Alarmierungslösung mitgenutzt werden, können entsprechende Maßnahmen für die sichere Konfiguration zentraler TK-Systeme unmittelbar umgesetzt werden. Andernfalls sind zum betrachteten Element eines Alarmierungssystems passende Maßnahmen sinngemäß zu berücksichtigen.

Können zu technischen Eigenschaften des Alarmsystemelements passende Maßnahmen produktbedingt nur eingeschränkt umgesetzt werden, ist gezielt die Möglichkeit zur Kompensation zu prüfen (siehe auch M-TK-142 „Absicherung der Anbindung von Alarmierungssystemen an TK-Infrastrukturen“ und anwendbare Maßnahmen gemäß Kapitel 7.4.3.4).

M-TK-142 Absicherung der Anbindung von Alarmierungssystemen an TK-Infrastrukturen

Die Anbindung eines Alarmierungssystems, z. B. eines Alarm-Servers, an eine TK-Anlage entspricht der Rolle eines TK-Endgerätes und muss daher denselben Schutzmaßnahmen unterzogen werden (siehe auch Kapitel 4.1.2).

Zusätzlich ergibt sich für im Zuge einer solchen Kopplung eventuell genutzter Notrufnummern eine erhöhte Gefahr eines Folgeschadens bei Missbrauch, weshalb man den direkten Zugriff auf entsprechende Schnittstellen der TK-Infrastruktur auf interne, gezielt vor Fremdzugriff geschützte Systeme beschränken sollte.

Ist ein Zugriff von außerhalb erforderlich, so sollte dieser durch eine für die genutzte Art der TK-Systemlösung aktuelle, hinreichend komplexe Authentisierungsmethode geschützt werden (siehe z. B. M-TK-102 „Absicherung des telefonischen Zugriffs auf UCC-Anwendungen durch eine PIN“).

Die Anbindung eines Alarmierungssystems an IP-basierte Dienste wie VoIP oder E-Mail sollte mindestens bei erhöhtem Schutzbedarf bzgl. Vertraulichkeit durch angemessene Verschlüsselungsmechanismen gesichert werden.

Für eine Alarmauslösung mittels eines der oben genannten Dienste gelten darüber hinaus dieselben Gefährdungen wie für eine auf klassischer Telefonie basierenden Notruf-Hotline. Hier ist insbesondere die Authentisierung der alarmauslösenden Partei notwendig (z. B. die Abfrage einer PIN oder eines Passworts bzw. die Vorlage eines Zertifikats).

Zu schützen sind auch für die Benachrichtigung von Mitarbeitern verwendete Accounts zu externen Kommunikationsdiensten. Die Kommunikation mit dem Anbieter derartiger Dienste erfolgt mittlerweile in der Regel IP-basiert und verlässt die Netzwerkgrenzen der Organisation, sodass ein besonderer Schutzbedarf vorliegt.

Je nach Art der zwischen Alarmierungssystem und TK-Lösung transportierten Informationen ist die Kommunikation über die koppelnde Schnittstelle gezielt mit Blick auf Vertraulichkeit zu sichern. Dies kann je nach Produktunterstützung durch die zu koppelnden Systeme erfolgen über

- (Verschlüsselungs-)Mechanismen der zwischen den Systemen genutzten Kommunikationsprotokolle,
- eine ausreichend wirksame Trennung des zur Systemkopplung genutzten Kommunikationswegs von anderen Netzbereichen oder
- eine Kombination aus beiden Ansätzen.

Die in Frage kommenden Mechanismen genutzter Kommunikationsprotokolle ergeben sich aus den für die jeweilige TK-Technologie zur Verfügung stehenden Optionen.

Grundsätzlich ist im Kontext von Alarmierungssystemen die Verfügbarkeit von besonderer Bedeutung, mit folgenden Konsequenzen:

- Falls essenzielle, ggf. sogar lebenswichtige Funktionen durch die Alarmierungslösung realisiert werden, sind alle Anbindungen an genutzte Kommunikationsnetzwerke redundant auszulegen.

  Dies gilt sowohl in Bezug auf die Kabelinfrastruktur als auch in Bezug auf die Stromversorgung und die notwendigen Anschlusskomponenten (redundante Ausstattung mit Baugruppen wie Netzteilen, Lüftern etc. sowie Einsatz zueinander redundanter Komponenten).
- Vor Anschaltung eines Alarmierungssystems an eine Kommunikationsinfrastruktur ist eine redundante Auslegung der Kommunikationsinfrastruktur zu verifizieren und nötigenfalls nachträglich zu realisieren. Die Redundanzvorkehrungen müssen den im Rahmen des Alarmierungssystems getroffenen Redundanzen mindestens gleichwertig sein.

Bei sehr hohem Schutzbedarf bzgl. Verfügbarkeit ist der Einsatz einer Mehrfachredundanz zu prüfen.

Die Anbindung an Gebäudeinfrastruktur oder Produktionsanlagen muss, je nach Gefährdung und Wichtigkeit der realisierten Funktionen, ebenfalls geschützt werden. Grundlegende Aspekte sind der Schutz vor physischem Zugriff durch Unbefugte sowie die eventuell redundante Auslegung der Kabelanbindung.

M-TK-143 Verstärkte Absicherung der von Alarmierungssystemen mitgenutzten TK-Installationen

Bei Kombination von Alarmierungssystem und TK-Lösung im Rahmen einer Gesamtarchitektur bestimmen der Schutzbedarf des Alarmierungssystems sowie die Umsetzbarkeit möglicher Sicherheitsmaßnahmen für das Alarmierungssystem die für die mitgenutzten TK-Installationen zu ergreifenden Maßnahmen.

Besteht auf Seiten des Alarmierungssystems produktbedingt nur begrenzt die Möglichkeit zur notwendigen präventiven Absicherung, so ist als Kompensation die Möglichkeit eines verstärkten Einsatzes von Maßnahmen auf Seiten des TK-Systems zu prüfen. Zweck einer solchen Kompensation ist die angemessene Minimierung des Risikos, dass Sicherheitsvorfälle von einer Systemart auf die andere übergreifen können.

7.4.3.2 Endpunkte von Alarmierungssystemen

M-TK-144 Ausstattung und Anbringung der Endpunkte unter Berücksichtigung von Sicherheitsaspekten

Auch bei Notwendigkeit zur Installation von Sensoren und ähnlichen Endpunkten von Alarmierungssystemen in schlecht zu schützenden oder frei zugänglichen Umgebungen sind im Rahmen des Möglichen Vorkehrungen zu treffen, um einen unberechtigten Zugang zumindest zu erschweren. Als Beispiel ist eine Anbringung an einer Stelle zu nennen, die ohne Hilfsmittel (z. B. Leiter) nicht unmittelbar zugänglich ist, oder ein Schutz durch ein abschließbares Gitter.

Des Weiteren ist - ohne dass hierdurch Konflikte mit dem zu erreichenden Alarmierungszweck resultieren - eine Anbringung und evtl. ein gezielter Schutz so zu realisieren, dass derartige Endpunkte möglichst gut vor widrigen Umgebungsbedingungen oder Gefährdungen durch Schadensereignisse höherer Gewalt geschützt sind. Insbesondere ist hier ein angemessener Schutz vor Staub, Verschmutzung, Feuchtigkeit bzw. Nässe sowie vor elektromagnetischen Störungen zu gewährleisten.

Als Vorbild können entsprechende Ausführungen in Maßnahmentexten (Maßnahmenspezifikation im Rahmen des IT-Grundschutzes oder des vorliegenden Dokuments) herangezogen werden, soweit deren Umsetzung nicht die Erreichung des Alarmierungszwecks auf vorgesehenem Niveau gefährden könnte. Weiterführende Hinweise auch für den erhöhten Schutzbedarf können den BSI-Dokumenten wie der Broschüre „Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte“ (siehe [BSI DrKoSi-2009]) entnommen werden, soweit diese sich auf die Montage von Komponenten außerhalb spezialisierter Räumlichkeiten der Schutzqualität „Raum für technische Infrastruktur“ oder höher beziehen.

Mindestens bei erhöhtem Schutzbedarf ist zu prüfen, inwieweit durch den Alarmierungszweck oder ungünstige Gegebenheiten am Installationsort bestehende Einschränkungen der Umsetzbarkeit präventiver Schutzmaßnahmen über Zusatzmaßnahmen kompensiert werden können und sollen. Derartige Zusatzmaßnahmen können eine erhöhte Frequenz bei den Inspektionsintervallen (Sichtprüfung) oder der Videoüberwachung sein (siehe auch Kapitel 7.4.3.4).

M-TK-145 Verbindliche Regelungen für den Umgang mit Endpunkten zu Alarmierungssystemen

Je nach Alarmierungssystem und der im Rahmen der gewählten Lösung eingesetzten Endpunkte sind Regelungen für den Umgang mit Endpunkten zum Alarmierungssystem verbindlich festzulegen, soweit sicherheitsrelevante Zustände auf festgelegtem Niveau einer solchen Festlegung bedürfen. Zu regelnde Aspekte können hier insbesondere sein:

- Technische Vorgaben für die direkte Anschaltung von Alarmierungsendpunkten an eine TK-Infrastruktur bzw. resultierende notwendige Produkteigenschaften
- Vorgaben für die korrekte Handhabung beweglicher Endpunkte zu Alarmierungssystemen

  Ein wichtiges Beispiel ist der korrekte Umgang mit persönlichen Merkmalen zu Alarmierungssystemen. Derartige Vorgaben fallen mindestens dann in den Geltungsbereich des vorliegenden Dokuments, wenn mobile TK-Endgeräte als derartige persönliche Merkmale verwendet werden. In diesem Zusammenhang ist als zu regelnder Aspekt auch zu sehen:

  - Vorgaben bzw. Grenzen für die Nutzung von TK-Endgeräten als Endpunkte für Alarmierungssysteme
  - Vorgaben für die korrekte Übergabe personenbezogener Ausstattung zu Alarmierungssystemen
  - Vorgaben für die Vorgehensweise bei Wartungs- und Instandsetzungsarbeiten an Endpunkten zu Alarmierungssystemen zwecks Vermeidung von Fehlalarmen

7.4.3.3 Netzwerk

Sicherheitsmaßnahmen auf Netzebene fallen in den Geltungsbereich des vorliegenden Dokuments, soweit Alarmierungssysteme mit TK-Lösungen zu einer Gesamtarchitektur verbunden werden. Gleichwertig zu berücksichtigende Schwerpunkte der Absicherung sind dabei:

M-TK-146 Absicherung der Kommunikation zwischen Elementen eines Alarmierungssystems

Eine Absicherung derartiger Kommunikation kann zunächst realisiert werden über die gezielte Verwendung von durch die eingesetzten Produkte unterstützte Sicherheits-mechanismen. Die gezielte Verwendung betrifft insbesondere:

- Protokolle, die Sicherheitsmechanismen zumindest optional umfassen, sind solchen ohne derartige Sicherheitselemente vorzuziehen.
- Unterstützte Optionen zur Authentisierung / Identitätsprüfung mit Blick auf Kommunikationspartner innerhalb der Alarmierungslösung sollten genutzt werden.
- Die Möglichkeiten zur Verschlüsselung der Kommunikation sollte genutzt werden.

Weisen die eingesetzten Produkte gemessen am Schutzbedarf eine derartige Sicherheits-unterstützung nur unzureichend auf, so sind Möglichkeiten zur Kompensation über Zusatzmaßnahmen im Rahmen der Kommunikationsinfrastruktur zur prüfen (siehe z. B. M-TK-64 „Zugangskontrolle zum Netzwerk“ und M-TK-67 „Netztrennung für VoIP“).

7.4.3.4 Netz- und Systemmanagement

Eine zu realisierende Grundanforderung bei Kopplung von Alarmierungssystem- und TK-Lösungen ist ein durchgängiges Sicherheitsniveau und damit eine aus der Sicherheitsperspektive einheitliche Güte der Wahrnehmung gleichartiger Betriebsaufgaben. Dementsprechend sind für mit TK-Lösungen im Verbund genutzte Alarmierungssysteme sämtliche sicherheitsrelevanten Ansätze als Maßnahmen zu prüfen,

- die sich durch sinngemäße Übertragung von Grundschutz-Bausteinen und -Maßnahmen ergeben, die zu im Rahmen der Alarmierungssystemlösung eingesetzten Technologien passen, bzw.

- die im Rahmen des vorliegenden Dokuments für TK-Lösungen spezifiziert werden, soweit diese Technologien einsetzen, die auch Teil der Alarmierungssystemlösung sind.

Mindestens im Falle erhöhten Schutzbedarfs sind für Alarmierungssysteme in angemessenem Umfang insbesondere zu realisieren:

M-TK-147 Automatisierte Überwachung der Komponenten von Alarmierungssystemen

Soweit die Funktionalitäten der eingesetzten Produkte dies ermöglichen, sollte eine automatisierte Statuserfassung aller wesentlichen Elemente einer Alarmierungslösung erfolgen. Abweichungen von festgelegten Betriebszuständen, die ein verlässliches Funktionieren von Alarmierung und zugehöriger Sicherheitsmechanismen beeinträchtigen können, sollen im Rahmen einer solchen Statusüberwachung automatisch erkannt, protokolliert und aktiv gemeldet werden (Alarm).

Dies kann vollständig mit Mitteln der Alarmierungslösung oder durch Mitnutzung einer vorhandenen Lösung zur Systemüberwachung realisiert werden, soweit hierdurch nicht gegen maßgebliche Auflagen zur Trennung solcher Management-Lösungen und zugehöriger Kommunikation verstoßen wird.

Die Kommunikationsinhalte derartiger Überwachungslösungen können als Informationen zur Vorbereitung von Angriffen auf die überwachten Systeme missbraucht werden. Daher ist eine derartige Kommunikation geeignet gegen Kenntnisnahme und Manipulation durch Unbefugte zu sichern (Erweiterung vorhandener Konzeption für sicheres Management in der Zielumgebung auf die Alarmierungssysteme).

M-TK-148 Erhöhte Frequenz gezielter Sicht- und Zustandsprüfungen

Gezielte Sicht- und Zustandsprüfungen von Anlagen und Installationen sind grundsätzlich eine routinemäßige Aufgabe des sicheren Betriebs. Insbesondere kann eine besonders häufige Durchführung solcher Prüfungen eine angemessene Zusatzmaßnahme darstellen für Alarmierungssysteme,

- für die erhöhter Schutzbedarf festgestellt wurde bzw.
- bei denen typische, dem Schutzbedarf angemessene präventive Sicherheitsmaßnahmen nicht oder nur eingeschränkt realisiert werden können.

7.4.3.5 Übergreifende Aspekte

Durch die Anbindung von Alarmsystemen an TK-Infrastrukturen bzw. die Mitnutzung von TK-Lösungen durch Alarmierungslösungen darf kein erhöhtes oder unbehandeltes Risiko für die TK-Infrastrukturen entstehen.

Entsprechend sind für Alarmierungssysteme im Rahmen derartiger Szenarien unmittelbar (für die mitgenutzten TK-Lösungen) und mittelbar (durch sinngemäße Übertragung auf die Alarmierungssysteme) alle Maßnahmen zu berücksichtigen, die im vorliegenden Dokument mit Blick auf übergreifende Aspekte zu den jeweiligen TK-Technologien spezifiziert sind.

Ergänzend bzw. vertiefend sind die folgenden Maßnahmen dem Alarmierungszweck, zugehörigen Vorschriften sowie dem festgestellten Schutzbedarf entsprechend umzusetzen:

M-TK-149 Schulung der Administratoren bzw. des Betriebspersonals von Alarmierungssystemen

Ergänzend zu den Maßnahmen in Kapitel 10.7 sind entsprechend dem typischerweise - mindestens bzgl. Verfügbarkeit - erhöhten Schutzbedarf für Alarmierungslösungen alle Personen, die Konfigurations- und Betriebsaufgaben mit Relevanz für die Alarmierungslösung wahrnehmen, speziell zu schulen. Die Schulung muss über die allgemeine Schulung gemäß Maßnahme M-TK-249 „Schulung der Administratoren von TK-Lösungen“ hinaus insbesondere die technischen und organisatorischen Besonderheiten von Alarmierungslösungen umfassen. Dies schließt ein:

- Schulung des Betriebspersonals der Alarmierungslösung
- Schulung der Administratoren zu Software auf zentralen Systemen zur Alarmierungslösung, z. B. auf dem zentralen Alarmierungs-Server
- Schulung der Administratoren von TK-Installationen, die für die Alarmierungssystem-lösung mitgenutzt werden, mit Blick auf sicherheitsrelevante Aspekte zur Einbindung der Alarmierungssystemlösung

Maßgebliche interne Regelungen und einzuhaltende externe Vorschriften (gesetzliche Auflagen, Vorgaben für den Betrieb derartiger Alarmierungsanlagen, maßgebliche Normen usw.) müssen bekannt sein. Festgelegte Abläufe für die Wahrnehmung von Betriebsaufgaben müssen bekannt sein, insbesondere mit Blick auf eine abgestimmte Betriebswahrnehmung für die TK-Infrastruktur und die Alarmierungslösung. Einstellmöglichkeiten und Handhabung sicherheitsrelevanter Produktdetails müssen sicher beherrscht werden, insbesondere mit Blick auf genutzte Schnittstellen und Kopplungspunkte zwischen TK-Infrastruktur und Alarmierungssystemen.

M-TK-150 Bedarfsgerechte Notfallplanung und -vorsorge für Kopplung von Alarmierungssystemen und TK-Lösungen

Die Planung und Umsetzung von Notfallvorsorge zur Aufrechterhaltung bzw. im Notfall zur schnellen Wiederherstellung des ordnungsgemäßen Betriebszustands eingesetzter Alarmsysteme wird als Ausgangsbasis vorausgesetzt (siehe Baustein B 1.3 „Notfallmanagement“ der IT-Grundschutz-Kataloge und Maßnahme M-TK-246 „Notfallvorsorge für alle Teilsysteme der TK-Lösung“). Die dort spezifizierten Maßnahmen sollten auf die eingesetzten Alarmierungslösungen entsprechend angewendet werden.

Soweit Alarmsysteme an TK-Lösungen angeschlossen werden sollen, ist eine spezielle Notfallplanung unter Berücksichtigung des erhöhten Schutzbedarfs des Alarmsystems vorzunehmen.

Beispiel: Alarmierung bzgl. Aspekten, die für die Unversehrtheit von Personen relevant sind (Brandmeldung, Personensuche in Gefahrensituationen etc.) haben typisch einen erhöhten Schutzbedarf. Eine Anschaltung einer derartigen Alarmlösung an eine TK-Lösung zwecks Alarmweiterleitung ist in der Notfallplanung wie die Anschaltung eines Notruftelefons einzustufen. Für Notfallsituationen sind somit für die Sicherstellung von Notrufen typische Maßnahmen auch für den Alarmsystemanschluss zu erwägen (z. B. Berücksichtigung des Alarmsystemanschlusses im Rahmen von Notbetriebsformen zur TK-Lösung, Festlegung entsprechender Sofortmaßnahmen und Vorgehensweisen zur Aktivierung des Notbetriebs für den Alarmsystemanschluss). Als Vorbild können z. B. entsprechende Ausführungen zu M-TK-85 „Notfallvorsorge für das VoIP-System“ herangezogen werden.

M-TK-151 Erarbeitung sicherheitsrelevanter Regelungen für den Einsatz von Alarmierungssystemen

Typische Themen für derartige Regelungen sind insbesondere:

- Maßgebliche, zwingend einzuhaltende externe Vorschriften

  Hierunter fallen Gesetze, Normen, Verordnungen oder Vorgaben durch Betreiber von Infrastrukturen, an die ein internes Alarmierungssystem angeschlossen werden soll, z. B. technische Anschlussbedingungen für den Anschluss an das vorhandene Meldenetz der örtlichen Feuerwehr.
- Regelungen bzgl. zulässiger physikalischer Schnittstellen und Protokolle zur Kopplung von Alarmierungssystemen und TK-Installationen
- Regelungen für den Betrieb von Schnittstellen zur Kopplung von Alarmierungs- und TK-Lösungen

Je nach Sinnfälligkeit können hier z. B. Detailvorgaben für die Konfiguration solcher Schnittstellen oder Beschränkung des (administrativen) Zugriffs auf solche Schnittstellen formuliert werden. Derartige Details sind explizit im Sicherheitskonzept zu regeln.

- Regelungen zum gleichartigen Betrieb von Alarmierungssystem und TK-Infrastruktur, die mit diesem gekoppelt bzw. durch dieses mitgenutzt wird

  Insbesondere sind maßgebliche Festlegungen für den Betrieb der jeweiligen TK-Technik sinngemäß auf angeschlossene Alarmierunglösungen zu übertragen. Sofern TK-Installationen als Teil einer Alarmierungssysteminstallation genutzt werden sollen, ist festzuschreiben, inwiefern für das Alarmierungssystem maßgebliche Vorschriften als Detaillierung von Regelungen für den TK-Betrieb zu berücksichtigen sind.

- Regelungen für abgestimmte und koordinierte Eingriffe in die entstehende Gesamt-architektur aus Alarmierungs- und TK-Lösung

  Eingriffe in die Systemlösung (z. B. Wartungsarbeiten, Änderungen im Rahmen von Release-Pflege, Systemneustarts zur Störungsbehebung) müssen so erfolgen, dass der Betreiber der damit gekoppelten anderen Systemlösung geeignet vorab informiert ist und Auswirkungen auf die Verfügbarkeit dieser anderen Systemlösung minimiert werden.

- Regelungen für den zweckgerechten Einsatz von Endsystemen im Rahmen von Alarmierungssystemlösungen

  Beispiele sind Vorschriften zur Installation/ Anbringung derartiger Endsysteme bzw. verbindliche Vorgaben für den Umgang mit mobiler, als persönliche Ausstattung zu einem Alarmierungssystem verwendeter Geräte. Insbesondere sollte hier explizit festgeschrieben werden, wenn bewusst Entscheidungen getroffen wurden, dass TK-Endgeräte nicht als Endgeräte für bestimmte Alarmierungszwecke verwendet werden sollen.

- Nötigenfalls gezielte Festlegungen bzgl. Einschränkungen des Wirkbereichs von Alarmierung, z. B. nicht in einen Verteiler zu Alarmen aufzunehmende Personenkreise sowie Beschränkungen bzgl. des Zugangs zu Alarminformationen und -Protokollierung

- Vorgaben zu Art und Umfang von Schulungen für Betreiber/ Administratoren bzw. Nutzer von Alarmierungssystemen

- Themen / (Mindest-)Inhalte eines Konzepts zur integrierten Nutzung von Alarmsystemen und TK-Lösungen

- Festlegungen, inwieweit Umsetzungsdetails zu Regelungen der genannten Art in anderen maßgeblichen Dokumenten für TK-Systeme und Alarmsysteme zielgruppenspezifisch festzuschreiben sind

  Es sollte vermieden werden, dass der Betreiber eines TK-Systems ein detailliertes Dokument für den Betrieb einer Alarmsystemlösung vollständig lesen muss, um die für ihn relevanten Details zum TK-Systembetrieb zu kennen, oder umgekehrt.

M-TK-152 Erstellung einer Konzeption zur integrierten Nutzung von Alarmierungssystem und TK-Lösungen

Durch aufeinander abgestimmte Ergänzungen bestehender Konzepte für Alarmierungssystem und TK-Lösung(en) oder in Form eines separaten Integrationskonzepts sind insbesondere alle Planungsergebnisse festzuhalten mit Blick auf:

- technische Umsetzung maßgeblicher Regelungen
- technische und organisatorische Details zur reibungslosen Kopplung über definierte Schnittstellen
- konzeptionelle Details zur Realisierung von Sicherheitsmaßnahmen, die folgende Punkte berücksichtigen:
  - Kopplung über definierte Schnittstellen
  - spezifische Funktionalitäten und Konfigurationsmöglichkeiten der Elementen der einzusetzenden Alarmierungslösung(en)
  - Schaffung der notwendigen Verfügbarkeit
- Detailfestlegungen bzgl. kontrolliertem Zugang und Zugriff auf Elemente von Alarmierungssystemen sowie durch diese mitgenutzte Elemente und Funktionalitäten von TK-Infrastrukturlösungen
- Details mit Blick auf spezifische Notfallplanung zur integrierten Nutzung von Alarmierungssystemen und TK-Infrastrukturlösungen

M-TK-153 Produktauswahl von Alarmierungssystemlösungen unter Sicherheitsgesichtspunkten

Bei der Auswahl einer benötigen Alarmierungslösung sind nicht nur funktionale Aspekte aus Sicht des Alarmierungszwecks zu berücksichtigen, sondern auch auf eine möglichst gute Basis für die technische Unterstützung vorgesehener Sicherheitsmaßnahmen zu achten. Basis sind entsprechende Festlegungen über maßgebliche Regelungen und eine resultierende Konzeption (siehe M-TK-151 „Erarbeitung sicherheitsrelevanter Regelungen für den Einsatz von Alarmierungssystemen“ und M-TK-152 „Erstellung einer Konzeption zur integrierten Nutzung von Alarmierungssystem und TK-Lösungen“).

Basierend auf M-TK-228 „Produktauswahl von TK-Lösungen unter Berücksichtigung von Sicherheitsaspekten“ muss die Produktauswahl von Alarmierungslösungen die speziellen technischen und organisatorischen Gegebenheiten solcher Systeme umfassend berücksichtigen.

M-TK-154 Einweisung, Schulung und Sensibilisierung der Nutzer von Alarmierungssystemen

Nicht nur Betreiber und Administratoren von Alarmierungssystemen und mitgenutzten TK-Infrastrukturen sind gezielt mit Blick auf die entstehende Gesamtarchitektur zu schulen (siehe Maßnahmen in Kapitel 10.7 und M-TK-149 „Schulung der Administratoren bzw. des Betriebspersonals von Alarmierungssystemen“).

Soweit durch Fehlbedienung oder andere Formen unsachgemäßen Umgangs durch zugangs- und zugriffsberechtigter Personen der Einsatzzweck oder die Sicherheit einer Alarmierungslösung oder einer hiermit gekoppelten TK-Lösung beeinträchtigt werden kann, ist dem in geeignetem Umfang und mit angemessener Häufigkeit über gezielte Einweisungs-, Schulungs- und Sensibilisierungsmaßnahmen entgegenzuwirken.

Entsprechende Maßnahmen und zugehörige Hilfsmittel (Schulungsunterlagen, Merkblätter, Formulare zum Durchführungsnachweis) sind gezielt vorzubereiten und zu pflegen. Die Durchführung entsprechender Maßnahmen sollte mit Blick auf den typischen Schutzbedarf, insbesondere die Bedeutung des Alarmierungszwecks (Unversehrtheit von Personen etc.) verbindlich dokumentiert und kontrolliert werden.

7.4.4 Zusammenfassung

Alarmierungssysteme fallen in den Geltungsbereich des vorliegenden Dokuments, falls sie TK-Lösungen zur Alarmweiterleitung nutzen, TK-Endgeräte als Sensoren einsetzen (insbesondere für Personensucheinrichtungen) oder die Kommunikation zwischen Elementen des Alarmierungssystems über die vorhandene TK-Infrastruktur bzw. die für die Telekommunikation verwendete Basistechnologie erfolgt. Für die so entstehende Gesamtarchitektur aus Alarmierungssystem und TK-Lösung sind als Angriffspunkte zu berücksichtigen:

- zentrale Elemente des Alarmierungssystems
- Endpunkte des Alarmierungssystems, insbesondere Sensoren
- Anschlusspunkte von zentralen Elementen des Alarmierungssystems an die TK-Infrastruktur
- Anschlusspunkte von Sensoren des Alarmierungssystems an die TK-Infrastruktur

Unmittelbar im Geltungsbereich des vorliegenden Dokuments sind die durch Alarmierungssysteme genutzten TK-Systeme sowie die hierzu notwendigen Schnittstellen zwischen den beiden Systemlösungen. Die Möglichkeiten zur Absicherung der Alarmierungssystemkomponenten sind nur mittelbar von Relevanz. Eine entsprechende Detailkonzeption obliegt dem Verantwortlichen für den Anlagenbetrieb des Alarmierungssystems.

Auf Seiten einer TK-Infrastruktur entstehen mit Blick auf Alarmierungssysteme Angriffsrisiken. Diese sind in Abhängigkeit von den zwischen TK-Infrastruktur und Alarmierungssystem genutzten Schnittstellen und bestehenden Wechselwirkungen sowie den über diese Schnittstellen ausgetauschten Daten zu bewerten und entsprechend zu minimieren.

Aus Sicht der Zielumgebung sind dabei die folgenden Aspekte zu beachten:

- die über den Alarmierungszweck entstehenden Verfügbarkeitsansprüche
- einzuhaltende gesetzliche oder ähnliche Auflagen für die genutzten Alarmierungssysteme und ggf. für die gekoppelte TK-Lösung
- die Bedeutung einer Alarmierungslösung und deren Funktionen (z. B. dem Absetzen von Notrufen) für die Unversehrtheit von Personen
- die über Alarme ausgelöste Notwendigkeit zu weiterer Kommunikation über die TK-Infrastruktur, z. B., zur Notfallbehandlung (ggf. erhöhte Inanspruchnahme der TK-Infrastruktur).

Die Erarbeitung einer Sicherheitskonzeption zu TK-Lösungen, die von Alarmierungssystemen mitgenutzt werden, umfasst neben den generell zu ergreifenden Maßnahmen (siehe Kapitel 10) und den für das Alarmierungssystem relevanten Maßnahmen der zugrunde liegenden Technologie, klassische Telekommunikationstechnik (siehe Kapitel 3.3) oder VoIP (siehe Kapitel 4.3), die folgenden Aspekte.

Absicherung der zentralen Anlagenelemente

Für zentrale Einheiten von Alarmierungssystemen sind die im vorliegenden Dokument benannten Mindestanforderungen für Sicherheitsmaßnahmen zu berücksichtigen. Beispielsweise sind, soweit möglich, Zugangsschutz und Umgebungsbedingungen so zu gestalten, dass sie dem erhöhten Verfügbarkeitsbedarf von Alarmierungssystemen gerecht werden. Insbesondere sind geltende gesetzliche und sonstige verbindliche Auflagen für den Betrieb solcher Anlagen zu beachten.

Für Alarmierungszwecke genutzte zentrale TK-Systeme ist zu überprüfen, ob die vorgesehenen Sicherheitsmaßnahmen auf einem Niveau angelegt sind, das dem durch die Mitnutzung für Alarmierung entstehenden Schutzbedarf angemessen ist. Nötigenfalls sind Zusatzmaßnahmen zu ergreifen, die mindestens für die Schnittstellen und Anschlusspunkte zur Kopplung mit Alarmsystemelementen wirksam sind.

Da Alarmierungssysteme nur bedingt Möglichkeiten zur Absicherung bieten, müssen Sicherheitsmaßnahmen für das TK-System umso gezielter angesetzt werden, um das angestrebte Sicherheitsniveau zu erreichen. Der Umfang entsprechender TK-seitiger Maßnahmen zur angemessenen Prävention wechselseitiger schädlicher Auswirkungen hängt insbesondere von der Art der für die Alarmierung genutzten TK-Funktionalitäten und Dienste ab.

Außerdem ist der Zugriff auf zentrale Anlagenelemente und deren Funktionalitäten gezielt abzusichern. Bei zentralen Elementen von Alarmsystemen betrifft dies vor allem die Beschränkung des zum Bedienerzugriff berechtigten Personenkreises sowie einen separierten Zugriff für administrative Zugriffe.

Absicherung der administrativen Zugänge zu Anlagenelementen

Administrative Zugänge zum Alarmsystem und zu mitgenutzten TK-Systemen müssen dem Schutzbedarf des Alarmierungszwecks entsprechend abgesichert werden. Gegebenenfalls sind für das Alarmierungssystem maßgebliche gesetzliche oder ähnliche verbindliche Auflagen sinngemäß auf die TK-Anlage zu übertragen.

Absicherung der Kommunikation

Die Kommunikation von Alarmierungssystemen ist angemessen abzusichern. Je nach Alarmierungszweck und Inhalten der Datenströme ist ein Schutz durch Maßnahmen wie Netztrennung und Verschlüsselung zu schaffen. Fehlen auf Seiten des Alarmierungssystems Möglichkeiten zur Absicherung der Kommunikation zwischen Endpunkten und zentralen Elementen, ist eine physische Trennung zu erwägen. Eine Verschlüsselung konzentriert sich dann auf die Kommunikation zwischen zentralen Elementen des Alarmierungssystems (z. B. zentraler Alarmierungsserver) und der TK-Lösung.

Sicherheitsmaßnahmen im Bereich Endpunkte der Lösung

Fest montierte Endpunkte einer Alarmierungslösung sind unter Beachtung von Sicherheitsaspekten anzubringen. Können Zugang und Funktionsfähigkeit durch präventive Maßnahmen nur unzureichend geschützt werden, ohne dass die Funktionalität des Alarmierungssystems dadurch beeinflusst wird, ist ein erhöhtes Maß an Zustandsprüfung zu erwägen. Dies schließt neben automatisierter Zustandsüberwachung auch das Mittel besonders häufiger Sichtprüfungen ein.

Wegen der möglichen Folgewirkungen von Fehlalarmen oder ausbleibenden Alarmen auf die TK-Lösung (z. B. durch erhöhte Belastung bei häufigen Fehlalarmen) ist ein geeigneter Umgang mit Endpunkten einer Alarmierungslösung auch für die Sicherheit der gekoppelten TK-Lösungen wichtig.

Übergreifende Maßnahmen

Übergreifende Maßnahmen betreffen sämtliche Aspekte des abgestimmten Einsatzes miteinander gekoppelter Anlagen, insbesondere:

- Beachtung übergreifender Gefährdungen, Risiken und Schutzbedarfsaspekte
- abgestimmte Produktauswahl mit Blick auf Schnittstellen zur Kopplung der Systeme und deren Absicherung
- durchgängige Gestaltung technischer Sicherheitsmaßnahmen auf einheitlichem Niveau
- Harmonisierung des Betriebs für die gekoppelten Anlagensysteme
- gleichwertige Schulung und Sensibilisierung der Nutzer / Bediener bzw. Administratoren der verschiedenen beteiligten Systeme und Endgeräte
- übergreifende Notfallplanung für das entstehende Gesamtsystem, inklusive Notbetriebsformen im Sinne des Alarmierungszwecks

8 Provider-basierte TK-Dienste

Organisationen nutzen häufig neben den organisationsinternen TK-Diensten auch externe Dienste, die von einem Dienstleister (engl. Provider) bereitgestellt und betrieben werden. Gleichfalls können die organisationsinternen TK-Dienste vollständig oder teilweise zu einem Provider ausgelagert werden, z. B. Application Hosting.

Im Rahmen dieser Technischen Leitlinie werden die folgenden Provider-basierten TK-Dienste beschrieben, die potenziellen Gefährdungen analysiert und entsprechende Sicherheitsmaßnahmen spezifiziert:

- Nutzung von bzw. Kopplung an öffentliche Soziale Netzwerke und Soziale Medien, siehe Kapitel 8.1
- Auslagerung (engl. Outsourcing) von organisationsinternen TK-Diensten bzw. externe Bereitstellung von organisationsintern genutzten Diensten, z. B. UC as a Service, siehe Kapitel 8.2

Organisationsinterne Soziale Netzwerke, z. B. Social Business Software, sind der Technologie Unified Communication and Collaboration (siehe Kapitel 6) zuzurechnen und werden hier nur unter dem Aspekt des Outsourcing betrachtet.

8.1 Soziale Netzwerke und Soziale Medien

Wie in Kapitel 2.3.6.1 erläutert, beziehen sich die Begriffe Soziale Netzwerke und Medien (SNM) in dieser Technischen Leitlinie ausschließlich auf öffentlich zugängliche Webplattformen (z. B. Facebook, LinkedIn, Xing) zur Vernetzung und Kommunikation von Anwendern und zur Bereitstellung von durch Nutzer erzeugten Inhalten.

Dass eine Betrachtung dieser Kommunikationsform auch für Organisationen unabdingbar geworden ist, begründet sich nicht allein mit dem Nutzen, den Soziale Netzwerke und Medien durch die Möglichkeit zur Vernetzung und Kommunikation dem Einzelnen versprechen. Zunehmend durchdringen diese Medien die Lebensbereiche der Mitarbeiter. Dies gilt insbesondere für jüngere Mitarbeiter, für die die private Nutzung von SNM die Normalität darstellt. So ist auch im Unternehmens- und Behördenumfeld der Umgang mit Sozialen Netzwerken und Medien bereits gebräuchlich – oftmals ohne Kenntnis der Verantwortlichen und ggf. gegen die Richtlinien der Organisation. So zeigt die Tatsache, dass im Jahr 2012 mehr Postings bei Facebook über mobile Endgeräte gemacht wurden als über PCs und Laptops, dass durch die Nutzung privater Smartphones und Tablets auch Soziale Netzwerke und Medien in das Organisationsumfeld Einzug halten.

Auf diese Weise setzen sich Organisationen diversen Gefährdungen aus, z. B. indem über Mitteilungen in Sozialen Netzwerken vertrauliche Informationen abfließen können oder eine negative Außenwirkung hervorgerufen werden kann. Dies geschieht häufig unbeabsichtigt, denn wie viele Beispiele zeigen, mangelt es oft an einem ausreichenden Sicherheitsbewusstsein der Anwender. Diese erkennen nicht alle Konsequenzen von datenschutzrelevanten Einstellungen wie Kontaktsynchronisation oder von Möglichkeiten zur Industriespionage über die gezielte Auswertung von Mitteilungsinhalten.

Um derartigen Gefährdungen entgegenzuwirken, muss daher insbesondere eine exakte Abgrenzung bezüglich der Einsatzgebiete und der Schnittstellen derartiger Angebote innerhalb der Organisation vorgenommen werden. Zudem benötigt man organisationsinterne Richtlinien für den Umgang des Personals mit solchen öffentlichen Plattformen.

8.1.1 Basiswissen

Ein Soziales Netzwerk ist eine Verbindung von Menschen in einer Netzgemeinschaft. Generieren die Nutzer dieses Netzwerkes eigene Inhalte, so spricht man von Sozialen Medien.

Der Unterschied zu Social Business Software (SBS) besteht darin, dass bei SBS die organisationsinterne Kommunikation und Zusammenarbeit sowie Vernetzung, Informations- und Identitätsmanagement des internen Personals einer Organisation im Fokus steht. SBS wird daher häufig auch als organisationsinterne Lösung in einer Private Cloud betrieben. Soziale Netzwerke und Medien hingegen dienen der Kommunikation und Vernetzung außerhalb von Organisationen und sind Dienste aus der Public Cloud. Als Überbegriff, der Soziale Netzwerke und Soziale Medien wie auch Social Business Software als Untermenge abdeckt, ist Social Software gebräuchlich. Im Fokus dieser Technischen Leitlinie stehen öffentliche Soziale Netzwerke und Medien unter Konzentration auf ihre Relevanz für die organisationsinterne und organisationsübergreifende Kommunikation.

8.1.1.1 Überblick Soziale Netzwerke und Medien

Verschiedene Soziale Netzwerke und Medien bieten auf verschiedene Art und Weise eine Plattform zum Austausch von Informationen. Trotzdem haben sie im Aufbau und bei ihren Funktionen gewisse Gemeinsamkeiten. Als Anwender erstellt man in der Regel ein Profil, mit dem man sich in der Gemeinschaft oder einer geschlossenen Nutzergruppe präsentiert. Über dieses vernetzt und organisiert man sich in Kontaktgruppen und tauscht je nach Art der Plattform Mitteilungen, Statusnachrichten und Inhalte (z. B. Bilder, Videos und Informationen zu Veranstaltungen) aus.

Zum Schutz der ausgetauschten Informationen und der Identität des Nutzers dienen Nutzer-authentisierung, Verschlüsselung und Einstellungen zu Privatsphäre und Datenschutz. Eine Verschlüsselung wird häufig angeboten, allerdings wird sie bei Nutzung der Standardeinstellungen meist nur bei der Anmeldung des Nutzers, nicht aber zum Schutz der übertragenen Inhalte genutzt. Eine manuelle Aktivierung der durchgängigen Verschlüsselung der Übertragung wird allerdings bei verschiedenen Plattformen angeboten.

Folgend Beispiele illustrieren typische öffentliche Soziale Netzwerke:

- Facebook

  Facebook ist das größte Soziale Netzwerk mit weltweit über 1 Milliarde Nutzern - in Deutschland sind es ca. 25 Millionen. Der Großteil der Nutzer ist zwischen 18 und 34 Jahren alt. Facebook bietet eine sehr große Bandbreite an Funktionen, die ständig erweitert wird. Zum Beispiel hat das Unternehmen im Jahr 2012 auch die für Twitter typische Hashtag-Funktion übernommen. Die Hashtag-Funktion ermöglicht Markierung und Durchsuchen von Inhalten mittels Schlagworten, denen ein # (englisch Hash) vorangestellt wird. Auch die Zahl an Drittanwendungen innerhalb der Plattform steigt stetig, was ein erhebliches Sicherheitsrisiko darstellt. Des Weiteren gestalten sich die Datenschutzeinstellungen sehr unübersichtlich und ungeübte Nutzer übermitteln leicht versehentlich ihre gesamten Kontakte, Adressbücher oder sonstige sensible Daten. Wie auch andere Soziale Netzwerke verfügt Facebook zunächst über Möglichkeiten zur schriftlichen Kommunikation (Nachrichten, Chat), erweitert diese jedoch zunehmend durch Echtzeitmedien wie Audio und Video. Der Fokus des Netzwerkes liegt auf dem Privatanwender, der über vielfältige Angebote adressiert wird. Hierdurch ist Facebook aber auch zunehmend als Marketing- und Kommunikationsplattform für diverse Organisationen relevant.

- Twitter

  Twitter ist ein Microblogging-Dienst, über den kurze Nachrichten veröffentlicht werden können. Eine Nachricht (ein Tweet) ist maximal 140 Zeichen lang und kann von jedem gelesen werden. Auf diese Weise lassen sich nahezu in Echtzeit Ereignisse verfolgen. Weltweit gibt es nach eigenen Angaben mehr als 230 Millionen Nutzer, die mindestens einmal im Monat aktiv sind. In Deutschland sind es ca. 500.000 Nutzer. Twitter ist hier das nach Facebook meistbesuchte Soziale Netzwerk. Nutzer sind neben Privatpersonen häufig Journalisten, aber auch Organisationen nutzen die Plattform zur Öffentlichkeitsarbeit und Kommunikation.

- Google Plus

  Google Plus (Google+) ist ein Soziales Netzwerk, welches von Google Inc. betrieben wird. Bezüglich Funktionsumfang und der adressierten Zielgruppe ähnelt es Facebook und stellt somit ein direktes Konkurrenzprodukt dar. Im Gegensatz zu Facebook werden Kontakte und Beziehungen nicht nur in Form einer Kontaktliste, sondern in sogenannten „Kreisen" organisiert. Ein Kreis kann beispielsweise eine Interessengruppe innerhalb der eigenen Kontaktliste sein. Hierüber lassen sich Informationen selektiv an bestimmte Nutzerkreise kommunizieren. Google bewirbt Google+ als Ergänzung zu seinen sonstigen Webprodukten für Privatleute und Firmen und integriert Google+ beispielsweise in Angebote wie Google Apps for Business. Google+ ist mit weltweit 500 Mio. Nutzern mittlerweile das zweitgrößte Soziale Netzwerk. Neben Privatanwendern wird es auch von Organisationen zunehmend frequentiert.

- LinkedIn

  LinkedIn ist ein Soziales Netzwerk zur Pflege von Geschäftskontakten sowie zum Aufbau neuer geschäftlicher Beziehungen. Mit weltweit 259 Millionen Nutzern ist LinkedIn das größte Netzwerk dieser Art, im deutschsprachigen Raum sind es mehr als 4 Millionen Nutzer. Das Angebot adressiert hierbei primär den einzelnen Mitarbeiter sowie gesamte Organisationen. Die Nutzung von LinkedIn erfolgt üblicherweise durch den einzelnen Anwender mit seinem Privataccount. Zudem wird LinkedIn verstärkt durch Organisationen zur Personalakquise genutzt. Der Verbreitungsschwerpunkt von LinkedIn liegt im angloamerikanischen Raum. Aber auch in Deutschland wird LinkedIn zunehmend genutzt.

- Xing

  Xing ist ein Soziales Netzwerk mit Sitz in Hamburg. Wie LinkedIn dient es vorrangig dem Verwalten von beruflichen Kontakten und bietet Organisationen die Möglichkeit zur Außendarstellung und zum Veröffentlichen von Stellenanzeigen. Über themenspezifische Gruppen können Beiträge zu verschiedenen Themen kanalisiert verfolgt werden. Die „Mitgliedschaft" in einer Gruppe ist auch Basis einer „Newsletter"-Benachrichtigungsfunktion und einem ähnlichen schnellen Zugang bzgl. neuesten Beiträgen zum Thema der Gruppe. Gruppen können für die berufliche Tätigkeit relevante Themen betreffen; Beispiele für IT-nahe Themengruppen sind IPv6, Wireshark, ISO 27001, IT-Grundschutz. Xing weist 12 Millionen Nutzer weltweit auf, davon ca. 6 Millionen im deutschsprachigen Raum. Um weitere Funktionen freizuschalten, kann ein Nutzer sich für den kostenpflichtigen Premium-Account entscheiden. Die Nutzung von Xing als Kommunikationsplattform im beruflichen Umfeld ist in Deutschland weit verbreitet. Dies wird in der Regel durch den einzelnen Mitarbeiter getrieben, der sein persönliches (privates) Dienstkonto zur Pflege geschäftlicher Beziehungen nutzt. Xing wird zudem zunehmend durch Organisationen zur Mitarbeiterakquise verwendet.

- Snapchat

  Snapchat ist eine Anwendung für Smartphones und Tablets, mit der Fotos an Freunde versendet werden können, die nur eine bestimmte Anzahl Sekunden sichtbar sind und dann automatisch vernichtet werden sollen. Aufgrund dieser fehlenden Historie und des dadurch vermeintlich besseren Schutzes der Privatsphäre erfreut sich Snapchat großer Beliebtheit. Weit verbreitet ist unter Jugendlichen das sogenannte Sexting, wo Nutzer freizügige Nachrichten und Fotos im dem Glauben versenden, dass diese ohne Spuren gelöscht würden. Allerdings ist es sehr einfach, die Mitteilungen wiederherzustellen. Eine Nutzung von Snapchat durch Organisationen ist nach heutigem Stand nicht sehr verbreitet. Es ist aber wahrscheinlich, dass Soziale Medien wie Snapchat durch den Mitarbeiter ausgehend von der zunehmenden privaten Nutzung auch in die Organisation hineingetragen werden.

Die neben der privaten Nutzung von SNM zunehmende Nutzung durch Organisationen als Präsenzplattform schließt ein, dass auch Sachinformationen vermehrt über SNM zur Verfügung gestellt werden. Medienorganisationen stellen Nachrichten oder Begleitinformationen zu aktuellen Meldungen etc. auch über solche Dienste zur Verfügung, um die Zielgruppen zu erreichen, die bevorzugt SNM nutzen. Auch öffentliche Einrichtungen wie Ministerien, Städte, Universitäten usw. sind im Rahmen ihrer digitalen Angebote in SNM aktiv. Zum Teil werden umfassende Informationsportale unter anderem auf diesem Wege zugänglich gemacht. Insofern entwickeln sich SNM zu Quellen, die für den beruflichen Informationsbedarf ausgeschöpft werden können.

Bei der Nutzung von SNM hinterlassen Anwender typischerweise vielfältige Informationen zu ihrer Person und ihren Aktivitäten. Dies reicht von bewusst eingestellten Informationen (Name, Kontaktinformationen, Geburtsdatum, Lebenslauf) bis hin zu unbewusst dokumentierten Metadaten (z. B. Nutzungshäufigkeit, Nutzungszeiten, Interessen und Aufenthaltsort). Das Geschäftsmodell einiger Sozialer Netze basiert auf der systematischen Auswertung dieser Informationen zu Werbezwecken, andere finanzieren sich teilweise oder vollständig durch spezielle Premium-Abonnements. Aber auch von anderen Nutzern der Plattform oder externen Angreifern können die Anwenderdaten ausgewertet werden, soweit nicht durch gezielte Gestaltung der Zugriffsberechtigungen durch den Anwender Beschränkungen vorgenommen werden. Den Privatsphäre-Einstellungen und Sicherheitsmechanismen der jeweiligen Plattform kommt somit eine besondere Bedeutung zu.

8.1.1.2 Anwendungsfälle in Organisationen

Öffentliche Soziale Netzwerke finden im Bereich der Kommunikation einer Organisation in verschiedenster Form Anwendung. Anwendungsszenarien sind die Verwendung als Datenquelle für Kontaktverzeichnisse, Außendarstellung und Kundenkanal der Organisation, organisationsübergreifende Kommunikation (Föderation) und als Informationsquelle für organisationsintern interessante Themen und Belange. Dabei spielt die Außendarstellung zur Organisationspräsentation vielleicht die wichtigste Rolle. Das liegt daran, dass diese Art von Diensten eine schnelle Verbreitungsgeschwindigkeit aufweist und man sehr schnell viele Leute ansprechen kann. Insbesondere folgende Ziele kann eine Marketingstrategie in öffentlichen Sozialen Netzwerken verfolgen:

- Neukundengewinnung
- Bestandskundenpflege
- Personalgewinnung

Dieser heute meistgenutzte und wichtige Anwendungsfall für Organisationen ist jedoch nur eines von vielen Szenarien, in denen SNM in einer Organisation eingesetzt werden. Weitere relevante Anwendungsszenarien sind:

- interaktive Recherchen zu Sachthemen mit Relevanz für beruflich ausgeübte Tätigkeiten

  Bei Diskussionen, die via SNM-Lösung geführt werden, besteht die Problematik der Trennung zwischen persönlicher Meinung und Stellungnahme als Vertreter der Organisation, zu der der Anwender gehört. Dies gilt insbesondere bei:

  - Nutzung privater SNM-Accounts am Arbeitsplatz

    Bei der Nutzung privater Accounts von Sozialen Netzwerken und Medien am Arbeitsplatz kann nicht nur die verlorene Arbeitszeit der Organisation einen Schaden bringen. Durch Analyse von geteilten Inhalten können Interna bekannt werden und Rückschlüsse auf die Organisation gezogen werden. Über den privaten Account gemachte Aussagen werden evtl. der Organisation zugeordnet, für die diese Person tätig ist. Die Verschmelzung von Privatem und Dienstlichem ist kritisch zu sehen. Eine Sperrung des Zugangs zu derartigen Diensten über die organisationseigene Außenanbindung ist in Zeiten, in denen jeder Mitarbeiter über sein privates Smartphone den Dienst nutzen kann, aber kein umfassend wirksames Gegenmittel.

  - Nutzung von SNM für die organisationsinterne Kommunikation

    Es ist im Gegenteil sogar denkbar, organisationsinterne Kommunikation über die integrierten Nachrichten- und Mitteilungsfunktionen von SNM-artigen Lösungen in Erwägung zu ziehen. Es lassen sich Mitteilungen unter Mitarbeitern verschicken, Nachrichten zu aktuellen Themen veröffentlichen (beispielsweise in einer internen Gruppe) oder Bilder von Betriebsausflügen teilen. Bei einer Entscheidung zu einer derartigen Nutzungsweise von SNM ist besonders darauf zu achten, dass keine vertraulichen Inhalte über solche öffentlichen Plattformen kommuniziert werden.

- Öffentliche SNM-Plattformen (z. B. Facebook) zur Außendarstellung der Organisation

  Unkritische Inhalte können auch zur Präsentation der Organisation auf öffentlichen Plattformen wie z. B. Facebook veröffentlicht werden. Unter Vorschaltung einer kontrollierenden Instanz (Pressestelle, Unternehmenskommunikation, ...) kann eine Organisation so mit der Öffentlichkeit in Kontakt treten und die schnelle Verbreitung innerhalb Sozialer Netzwerke und Medien für ein gezieltes Marketing nutzen („virales Marketing“).

- Öffentliche SNM-Plattformen (z. B. Xing) als Ergänzung organisationsinterner Adressverzeichnisse

  Die Nutzer Sozialer Netzwerke pflegen in diesen üblicherweise sehr gewissenhaft und zeitnah ihre persönlichen Kontaktdaten. Dies macht SNM als Kontaktdatenbank attraktiv, da die persönlichen Kontaktdaten durch die Ansprechpartner selbst gepflegt und aktualisiert werden. Über Integrationsschnittstellen lassen sich die SNM öffentlicher Anbieter (z. B. Xing oder LinkedIn) zur Ergänzung organisationsinterner Adressverzeichnisse einbinden. Die Pflege beruflich relevanter Kontakte durch Einzelpersonen als Ergänzung des organisationsinternen Verzeichnisses ist sehr verbreitet. Bei derartiger SNM-Nutzung stellen sich neue (auch rechtliche) Fragen, die geeignet zu regeln sind.

- Föderation mit UCC-Lösungen zur externen Kommunikation

  Öffentliche SNM bieten ihren Mitgliedern teils vielfältige Kommunikationskanäle an. Hierzu zählen textbasierte Medien wie Kurznachrichten, Chat und Gruppen-Chat sowie öffentliche Diskussionsforen, aber auch Echtzeitmedien wie Audio- oder Videokommunikation. Diese Kanäle können zum Kontakt mit Partnern und Kunden bzw. externen Ansprechpartnern im Allgemeinen genutzt werden. Ein Anwendungsbeispiel ist die Kommunikation zwischen Kundenbetreuer und Kunde per Video via Google Hangouts. Ein weiteres Beispiel ist die Klärung einer Fragestellung des SNM-Nutzers durch Kommunikation mit organisationsinternen Fachleuten. Hierzu ermöglichen einige marktrelevante UCC-Lösungen eine Föderation mit öffentlichen SNM. So können Präsenzstatus abgeglichen und organisationsübergreifende Kommunikationskanäle aufgebaut werden. Während die Föderation von Instant Messaging und Presence bereits zum Standardlieferumfang von UCC-Lösungen gehört, befindet sich die Föderation von Audio und Videokanälen noch in einem frühen Stadium.

- Integration in ein Kontaktcenter

  Die Föderation mit öffentlichen SNM-Plattformen eröffnet Chancen für die Kommunikation mit Kunden. Dies gilt insbesondere für Bereiche oder Abteilungen in der Organisation, deren Hauptaufgabe die Pflege des Kundenkontaktes ist und die hierzu Kontaktcenter-Lösungen einsetzen. Moderne Kontaktcenter-Technologie bietet eine Vielzahl von Kommunikationskanälen (Audio, Video, SMS, E-Mail etc.), welche sich mit öffentlichen SNM-Plattformen vernetzen lassen. So kann beispielsweise ein Anruf-Feld in die Firmenpräsenz eines Sozialen Netzwerks eingebunden werden. Der Kunde kann nun per Klick auf dieses Feld einen Videoanruf in das Kontaktcenter des Unternehmens aufbauen, der über die Videofunktion des Sozialen Netzwerks im Browser realisiert wird. Auf ähnliche Art und Weise lassen sich auch andere Kommunikationskanäle wie z. B. Audio-Kommunikation und Chat realisieren. Der Vorteil liegt in der vereinfachten Kontaktaufnahme für den Kunden und dem so verbesserten Kundenzugang.

- Datenerhebung (Data Mining) für Kontaktcenter-Anwendungen

  Eine weitere Anwendungsform bietet die Nutzung Sozialer Medien zwecks Erhebung von Daten und Kommunikation in den SNM. Die so über die Medien gewonnenen Daten lassen sich auswerten, analysieren und Kontaktcenter-Anwendungen zur Verfügung stellen. Ein solcher Data-Mining-Prozess erlaubt es, schnell und gezielt auf so ermittelte Themen, Trends und Kundenmeinungen einzugehen und zu antworten. Fehlentwicklungen wie z. B. unzufriedene Kunden können erkannt und ein größerer Schaden für die Organisation durch gezielte Ansprache und Hilfestellung vermieden werden.

Bei der Bewertung verschiedener Funktionen und Möglichkeiten, die Soziale Netzwerke und Medien im Kommunikationskontext bieten, muss eine Organisation abwägen, welche sich davon mit geeignetem Nutzen und ausreichend kontrolliert nutzen lassen. Die relevanten Aspekte dabei sind:

- Eine Nutzung öffentlicher SNM-Angebote für die interne Kommunikation, insbesondere bei erhöhtem Schutzbedarf, ist aufgrund des geringen Schutzniveaus der öffentlichen SNM zumindest bedenklich.
- Die Integration öffentlicher sozialer Plattformen (z. B. Xing) in organisationsinterne Adressverzeichnisse kann geregelt erfolgen.
- Eine Föderation von SNM mit UCC (Unified Communications and Collaboration) und Kontaktcenter als Kommunikationskanal kann erwogen werden. Hierbei ist aber zu beachten, dass die Kommunikation über einen öffentlichen, nicht vertrauenswürdigen Dienst stattfindet, dessen Schutzniveau in aller Regel noch unter dem des öffentlichen Festnetzes liegt. Somit müssen Maßnahmen zur eindeutigen Abgrenzung zwischen interner und externer Kommunikation und zum Schutz der internen Kommunikationsinfrastruktur umgesetzt werden.

8.1.1.3 Anbindungsarchitektur / Technik

Für die beschriebenen Anwendungsfälle lassen sich die folgenden Varianten zur Kopplung zwischen Kommunikationssystem und Sozialen Netzwerken und Medien implementieren.

8.1.1.3.1 Instant Messaging und Präsenzstatus

Die Anbindung zur Kommunikation mit Mitgliedern von SNM kann über eine Kopplung der internen Kommunikationsplattform via eXtensible Messaging and Presence Protocol (XMPP) vorgenommen werden. Per XMPP ist eine Kommunikation via Instant Messaging und ein Abgleich des Präsenzstatus möglich. Es kann sowohl der Präsenzstatus von SNM-Mitgliedern in der internen Kommunikationslösung angezeigt als auch der interne Präsenzstatus veröffentlicht werden. Zur Kopplung der internen Kommunikationslösung mit öffentlichen SNM wird in der Regel ein XMPP-Gateway eingesetzt. Dieses kann – je nach eingesetztem Produktportfolio – als separate Server-Instanz oder als konsolidierte Server-Rolle auf einem Front-End-Server der Kommunikationslösung realisiert werden. Diese Instanz sorgt sowohl für die Konnektivität zwischen interner und externer Plattform als auch für die Adaption und Filterung der ausgetauschten Informationen. So werden z. B. Präsenzstatus der internen Lösung auf standardisierte Status gemäß XMPP-Protokoll umgesetzt. Auch datenschutz- und sicherheitsrelevante Funktionen wie Einschränken oder Verhindern der Veröffentlichung des Präsenzstatus werden hier realisiert. Aufgrund der externen Konnektivität und der Gateway-Funktion sollte ein XMPP-Gateway in einer separaten Sicherheitszone, z. B. der Web-DMZ, positioniert werden. Die grundlegende Architektur einer XMPP-Kopplung ist Abbildung 46 zu entnehmen.

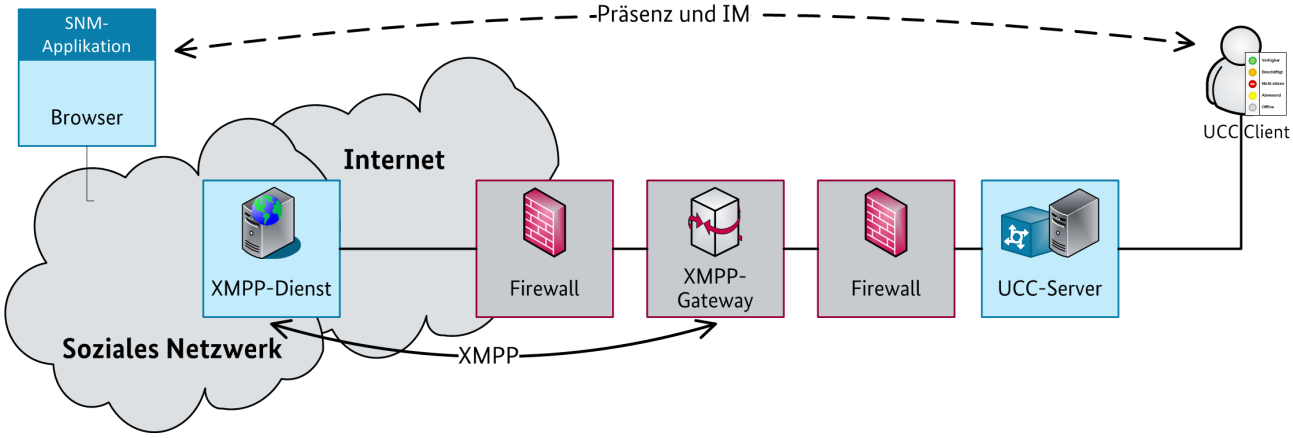


Abbildung 46: XMPP-Föderation zum Austausch von Kurznachrichten und Präsenzstatus

8.1.1.3.2 Echtzeitkommunikation

SNM bieten ihren Teilnehmern vermehrt die Möglichkeit zur internen Echtzeitkommunikation im Browser (z. B. Desktop-Video und Audio über eine Webapplikation). Um eine Echtzeitkommunikation zwischen Teilnehmern eines organisationsinternen Kommunikationssystems mit den Mitgliedern des jeweiligen SNM zu ermöglichen, kann eine Kopplung via IP-Trunk (SIP oder H.323) oder einer vergleichbaren proprietären Technologie erfolgen. Diese Einbindung eignet sich insbesondere für die Kommunikation mit Verbrauchern und Endkunden, welche in Sozialen Netzwerken organisiert sind. Anwendungsszenarien sind somit insbesondere Kontaktcenter im kommerziellen oder Behörden-Umfeld. Die technische Realisierung entspricht im Wesentlichen einer Kopplung via IP-Trunk zur Audio- oder Video-Kommunikation über Vertrauensgrenzen (siehe auch Kapitel 4.1.8 und Kapitel 6.1.14). Sie kann mittels separater Gateways oder konsolidiert auf Front-End-Servern, die die Internet-Konnektivität realisieren, implementiert werden. Eine Kopplung von Echtzeitmedien mit SNM ist derzeit nur für wenige Plattformen verfügbar. Eine zunehmende Nutzung ist aber insbesondere bei voranschreitender Verbreitung von WebRTC (siehe Kapitel 6.1.16) zu erwarten. Die prinzipielle Architektur einer solchen Echtzeitkommunikation ist Abbildung 47 zu entnehmen.

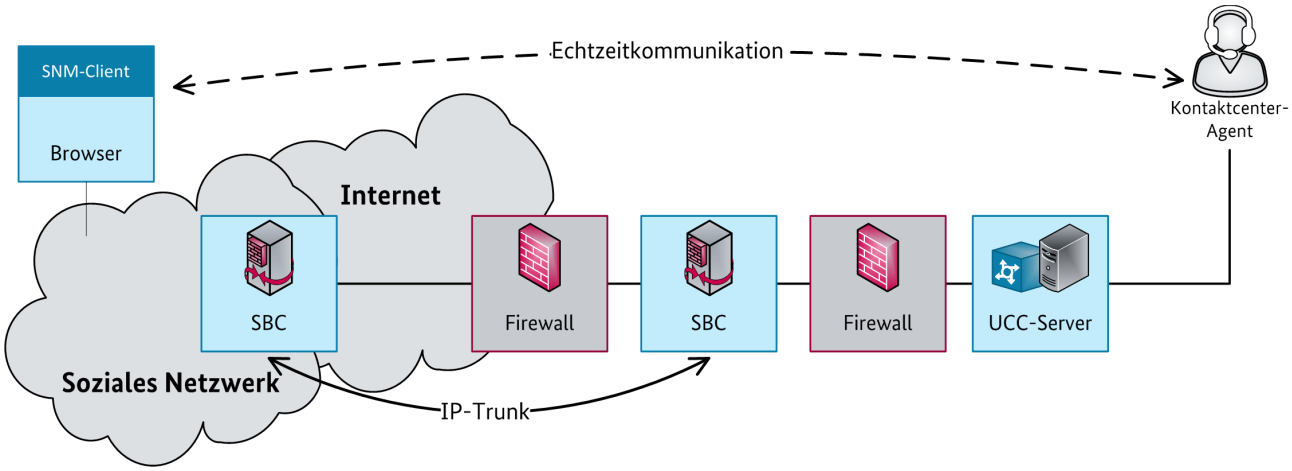


Abbildung 47: Anbindung für Echtzeitkommunikation mittels IP-Trunk

8.1.1.3.3 Synchronisation von Kontaktdaten

Die in Sozialen Netzwerken und Medien von den Anwendern gepflegten Kontaktdaten eignen sich aufgrund der meist hohen Aktualität zur Ergänzung persönlicher und organisationsweiter Kontaktverzeichnisse. Hierzu ist entweder eine Client-seitige oder eine Server-seitige Integration erforderlich.

Für die Client-seitige Integration ist die Installation eines Plug-ins für den Client erforderlich, mit dem auf das Adressbuch zugegriffen wird (in der Regel der E-Mail-Client bzw. Groupware-Client). Es ermöglicht den Abgleich der Kontakte des Adressbuches und übernimmt Änderungen aus der persönlichen Kontaktliste im eigenen SNM-Account. Je nach Konfiguration findet auch eine Rücksynchronisation des Adressbuches in Richtung SNM statt, um so die persönliche Kontaktliste des eigenen Accounts zu vervollständigen. Dies ist insbesondere in Hinblick auf vertrauliche Kontaktdaten als kritisch zu bewerten. Über eine ähnliche Funktionalität verfügen für mobile Endgeräte Apps zum Zugriff auf Soziale Netzwerke und Medien, die einen Abgleich des nativen Kontaktverzeichnisses des mobilen Endgerätes vornehmen. Die Client-seitige Integration ist - insbesondere bei Privatanwendern - weit verbreitet. Die Architektur einer solchen Anbindung ist in Abbildung 48 dargestellt.

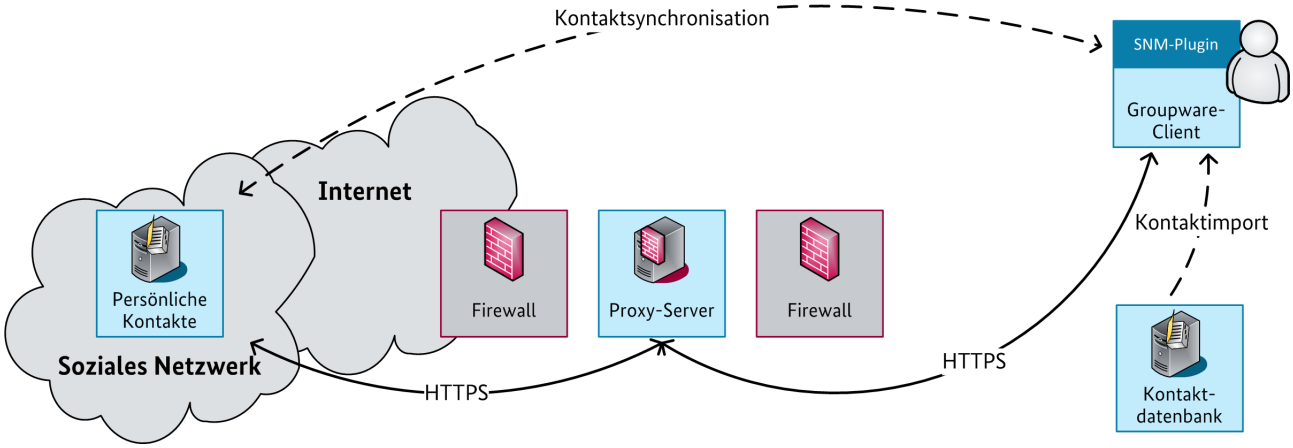


Abbildung 48: Client-seitige Kontaktsynchronisation

Die Server-seitige Integration übernimmt Kontaktdaten aus dem SNM-Account einer Organisation, in dem eine Vielzahl von externen Kontakten der Organisation hinterlegt ist. Dies könnten beispielsweise Interessenten für das im SNM beworbene Produkt eines Unternehmens sein. Über einen Konnektor werden diese Kontakte in das Organisationsverzeichnis importiert. Umgekehrt kann eine Veröffentlichung von Kontakten aus dem Organisationsverzeichnis auf dem SNM-Auftritt der Organisation vorgenommen werden. Die Server-seitige Integration besitzt nach heutigem Stand einen geringen Verbreitungsgrad und wird in der Regel projektspezifisch implementiert. Die schematische Darstellung der Anbindung ist Abbildung 49 zu entnehmen.

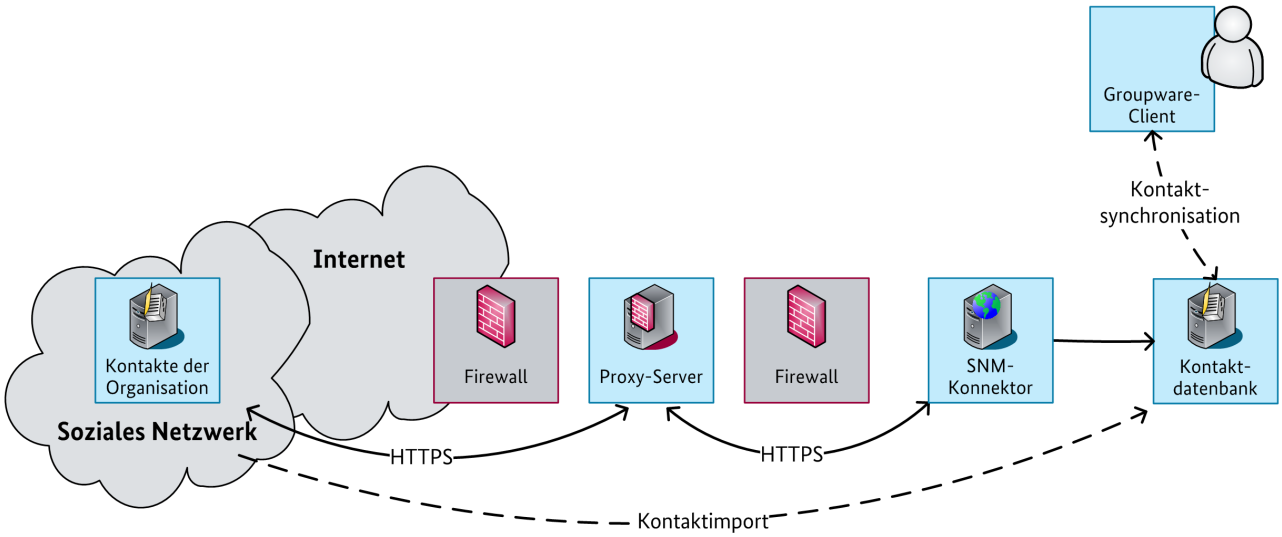


Abbildung 49: Server-seitige Kontaktsynchronisation

8.1.1.3.4 Datenerhebung und -analyse

Zur Analyse der Nutzeraktivitäten in SNM kann eine Integration zwischen öffentlichen SNM und internen Kommunikationsplattformen vorgenommen werden. Diese basiert auf plattformspezifischen Programmierschnittstellen (API) oder auf standardisierten Mechanismen wie z. B. Really Simple Syndication (RSS). Über plattformspezifische API ermöglichen SNM-Betreiber bestimmten Kundengruppen Zusatzfunktionen, beispielsweise die zielgerichtete Suche nach nutzergenerierten Inhalten anhand von Schlagworten oder die Nachverfolgung von Beiträgen im SNM-Angebot einer Organisation. Ein gängiges Anwendungsszenario ist die zielgerichtete Suche nach negativen Äußerungen eines Kunden zum Produkt eines Unternehmens. Auf diese Äußerung, die z. B. auf einen Produktfehler

zurückzuführen ist, kann dann mit einem Kommunikationsangebot reagiert und weiterer Schaden für die Reputation des Unternehmens abgewendet werden. Um die Kontaktaufnahme über die Kommunikationsplattform des Unternehmens zu realisieren, wird ein SNM-Konnektor bzw. eine SNM-Middleware mit Klassifizierungsintelligenz mit dem Kommunikationssystem gekoppelt. Die Architektur eines solchen Szenarios ist Abbildung 50 zu entnehmen.

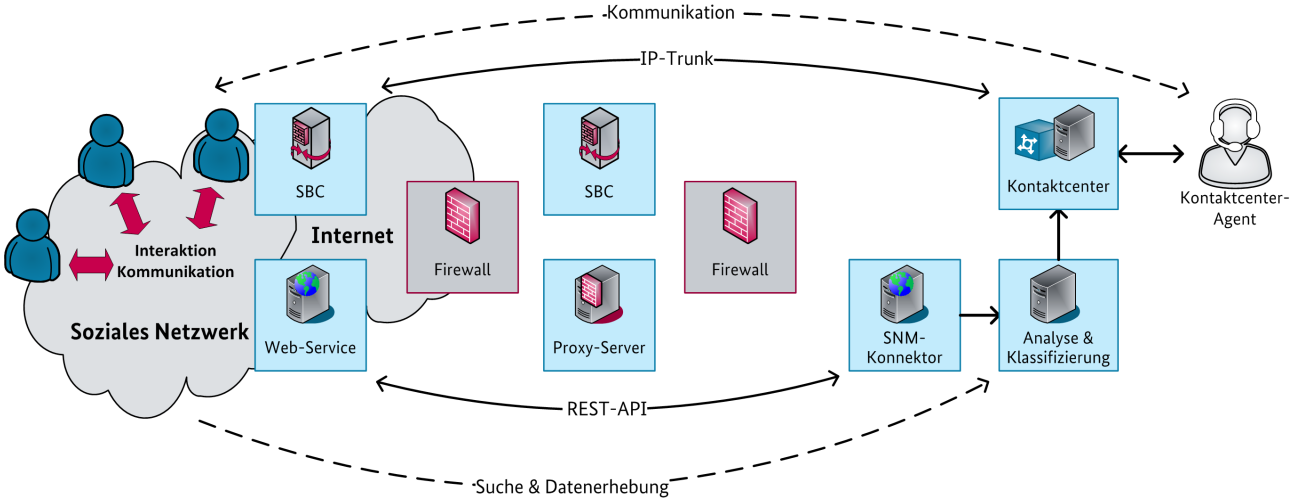


Abbildung 50: Anbindung und Steuerung des organisationsinternen Kontaktcenters über SNM-Konnektor und Klassifizierungssystem

8.1.2 Gefährdungen

8.1.2.1 Höhere Gewalt

Auf Soziale Netzwerke und Medien treffen allgemein die Gefährdungen durch höhere Gewalt zu, die in den IT-Grundschutz-Katalogen genannt sind. Dies beinhaltet beispielsweise Gefährdungen durch Feuer, Wasser, Blitzeinschlag, Staub und Verschmutzung. Da hier ausschließlich auf die Nutzung und Integration öffentlicher Sozialer Netzwerke und Medien eingegangen wird, muss diesen Gefährdungen jedoch durch die jeweiligen Betreiber der Dienste begegnet werden. Falls für die Einbindung dieser Dienste in das Kommunikationssystem erhöhte Verfügbarkeitsanforderungen bestehen, sollten die Gefährdungen durch höhere Gewalt für die organisationseigenen Integrationsschnittstellen (z. B. Gateways) beachtet und entsprechende Maßnahmen umgesetzt werden.

8.1.2.2 Organisatorische Mängel

Vertraulichkeit, Verfügbarkeit und Integrität von Sozialen Netzwerken und (Sozialen) Medien (SNM) sind durch organisatorische Mängel auf Seiten des Betreibers einerseits und der Anwender bzw. der SNM nutzenden Organisation andererseits gefährdet. Es sind zunächst allgemein die Gefährdungen durch organisatorische Mängel zu berücksichtigen, die in den IT-Grundschutz-Katalogen genannt sind. Bei Fremdbetrieb, wie er üblicherweise bei der Nutzung öffentlicher Sozialer Netzwerke und Medien vorliegt, muss den organisatorischen Mängeln primär durch den Betreiber begegnet werden. Diese Gefährdungen sind nicht im Fokus dieser Technischen Leitlinie. Hinweise zur Vertragsgestaltung zwischen nutzender Organisation und Betreiber eines SNM-Angebots zwecks Umsetzung von Anforderungen des Grundschutzbausteins B 1.11 „Outsourcing“ sind langfristig denkbar. Zum heutigen Zeitpunkt ist dies aber aus verschiedenen Gründen noch nicht sinnvoll möglich. In der Regel ist derzeit noch kein Vertragsabschluss zwischen einer Organisation und einem SNM-Anbieter für alle Dienstkonten einer Organisation möglich. Mit zunehmender Bedeutung der SNM für die dienstliche Nutzung kann sich dies jedoch ändern. In diesem Fall sollte bei der Vertragsgestaltung dringend die zum fraglichen Zeitpunkt etablierte Rechtsprechung zu relevanten Details berücksichtigt werden.

Die verbleibenden, im Folgenden behandelten Gefährdungen durch organisatorische Mängel auf Seiten der Organisation wirken vorrangig auf die Anwenderseite sowie ggf. auf organisationsinterne Systeme zur Kopplung mit öffentlichen Sozialen Netzwerken. Hier sind – sofern auf die konkrete Art der SNM-Nutzung zutreffend – grundsätzlich die im Gefährdungskatalog G 2 „Organisatorische Mängel“ der BSI IT-Grundschutz-Kataloge aufgeführten Gefährdungen zu berücksichtigen. Für SNM-Nutzung sind sinngemäß insbesondere die folgenden Gefährdungen relevant:

- G 2.1 „Fehlende oder unzureichende Regelungen“
- G 2.2 „Unzureichende Kenntnis über Regelungen“
- G 2.7 „Unerlaubte Ausübung von Rechten“
- G 2.28 „Verstöße gegen das Urheberrecht“
- G 2.54 „Vertraulichkeitsverlust durch Restinformationen“
- G 2.61 „Unberechtigte Sammlung personenbezogener Daten“
- G 2.66 „Unzureichendes Sicherheitsmanagement“
- G 2.84 „Unzulängliche vertragliche Regelungen mit einem externen Dienstleister“
- G 2.87 „Verwendung unsicherer Protokolle in öffentlichen Netzen“
- G 2.96 „Veraltete oder falsche Informationen in einem Webangebot“
- G 2.103 „Unzureichende Schulung der Mitarbeiter“
- G 2.105 „Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen“
- G 2.162 „Fehlende Zulässigkeit der Verarbeitung personenbezogener Daten“
- G 2.163 „Nichteinhaltung der Zweckbindung bei der Verarbeitung personenbezogener Daten“
- G 2.164 „Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten“
- G 2.165 „Fehlende oder unzureichende Datenvermeidung und Datensparsamkeit bei der Verarbeitung personenbezogener Daten“
- G 2.166 „Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten“
- G 2.167 „Fehlende oder nicht ausreichende Vorabkontrolle“
- G 2.168 „Gefährdung der Rechte Betroffener bei der Verarbeitung personenbezogener Daten“
- G 2.169 „Fehlende oder unzureichende Absicherung der Datenverarbeitung im Auftrag bei der Verarbeitung personenbezogener Daten“
- G 2.170 „Fehlende Transparenz für den Betroffenen und die Datenschutz-Kontrollinstanzen“
- G 2.171 „Gefährdung vorgegebener Kontrollziele bei der Verarbeitung personenbezogener Daten“
- G 2.172 „Fehlende oder unzureichende Absicherung der Verarbeitung personenbezogener Daten im Ausland“
- G 2.173 „Unzulässige automatisierten Einzelfallentscheidungen oder Abrufe bei der Verarbeitung personenbezogener Daten“
- G 2.174 „Fehlende oder unzureichende Datenschutzkontrolle“

Generell sollte der Aspekt des Datenschutzes bei der Nutzung und Weitergabe von personenbezogenen Daten berücksichtigt werden.

Es bestehen zudem die folgenden spezifischen Gefährdungen durch organisatorische Mängel:

G-TK-110 Mangelhafte Trennung zwischen privater und dienstlicher Nutzung

Durch mangelhafte Trennung von privater und dienstlicher Nutzung Sozialer Netzwerke und Medien löst sich die Grenze zwischen Privat- und Berufsleben auf. So können private Äußerungen auf die Organisation bezogen aufgefasst werden und auf diese Weise Schaden anrichten. Über Zugriff von Außen entsteht ein erhöhtes Sicherheitsrisiko für das Organisationsnetzwerk und die Gefahr des Datenabflusses.

G-TK-111 Fehlende Richtlinien zum Umgang mit Sozialen Netzwerken und Medien

Wurden in einer Organisation keine Richtlinien zum Umgang mit Sozialen Netzwerken und Medien getroffen oder sind diese den Mitarbeitern nicht ausreichend kommuniziert worden, so besteht eine erhöhte Gefahr der versehentlichen Fehlbedienung und des Angriffs auf eine Organisation über SNM.

Ohne entsprechende Regelungen kann nicht davon ausgegangen werden, dass alle SNM-Nutzer durch geeigneten Umgang mit SNM-basiert vorgehaltenen Daten die aus Sicht der Organisation notwendige Datenverfügbarkeit sicherstellen.

Zudem besteht die Gefahr der Rechtsunsicherheit für die Organisation und den Mitarbeiter bei Sicherheitsvorfällen im Rahmen der dienstlichen Nutzung oder der privaten Nutzung im dienstlichen Umfeld.

G-TK-112 Fehlende oder nicht ausreichende Vorabkontrolle der Außendarstellung über Soziale Netzwerke und Medien

Soweit ein SNM-Account einen unmittelbaren Bezug des Kontoinhabers zu einer Organisation herstellt, muss davon ausgegangen werden, dass über diesen Account erfolgende Veröffentlichungen, insbesondere Stellungnahmen u. Ä., auf diese Organisation bezogen werden. Werden rein persönliche, private Veröffentlichungen über einen SNM-Account nicht ausreichend als solche gekennzeichnet, so droht eine negative Außenwirkung für die Organisation. Das gilt auch, wenn Veröffentlichungen im Sinne der Organisation nicht genügend reglementiert oder gestaltet werden oder die für andere Kommunikationsformen geltenden Regeln bei SNM-Nutzung versehentlich unterwandert oder gezielt umgangen werden.

G-TK-113 Mangelhafte Integration der Nutzung von Sozialen Netzwerken und Medien in etablierte Abläufe

Soziale Netzwerke und Medien können als Hilfsmittel für Aufgaben herangezogen werden, die bislang mit anderen Mitteln in geregelter Form durchgeführt wurden. Die mit den bisherigen Regelungen verfolgten Zielsetzungen dürfen durch eine solche SNM-Nutzung nicht untergraben werden. Informationsflüsse müssen mit und ohne SNM-Nutzung gleichwertig erfolgen. Qualitätssichernde bzw. schadensvermeidende Aufgaben müssen bei SNM-basierte Informationsflüssen ebenso verlässlich und durch dafür eindeutig Zuständige wahrgenommen werden wie bei Informationsflüssen über andere Kanäle.

Beispiele hierfür sind:

- Bei fehlenden Zuständigkeiten können etwa bei der dienstlichen Nutzung Sozialer Netzwerke und Medien Inhalte veröffentlicht werden, die der Organisation schaden (siehe G-TK-112 „Fehlende oder nicht ausreichende Vorabkontrolle der Außendarstellung über Soziale Netzwerke und Medien“). So können ohne geeignete Kontrolle und hiermit verbundener Gestaltung und Qualitätssicherung rufschädigende oder als rufschädigend aufgefasste Nachrichten übermittelt oder sonstige Veröffentlichungen vorgenommen werden.
- Bei Fehlen einer Autorisierungsinstanz für die Veröffentlichung von Inhalten in SNM ist es möglich, dass Interna versehentlich nach außen getragen werden.

- Verteiler oder ähnliche Festlegungen bzgl. zu informierender Personenkreise sollten von bereits etablierten Kommunikationslösungen auf SNM übertragen werden. Andernfalls können interne Abläufe spürbar behindert, im ungünstigsten Fall Mehraufwand oder Sicherheitsvorfälle provoziert werden.
- Werden bislang zentral oder koordiniert verwaltete Datenbestände neuerdings anteilig in SNM-Lösungen in nicht abgestimmter Weise vorgehalten, drohen inkonsistente oder nicht allen Zielgruppen in der Organisation ausreichend zugängliche Datenbestände.

G-TK-114 Mangelhafte Verwaltung der Zugriffsrechte für dienstliche Accounts in Sozialen Netzwerken oder Medien

Es besteht die Gefahr einer missbräuchlichen Verwendung des dienstlichen Accounts, z. B. auch durch nicht erfolgten Entzug der Zugriffsrechte nach dem Ausscheiden aus der Organisation.

G-TK-115 Keine Information der Mitarbeiter bei Preisgabe persönlicher Daten

Es muss darauf geachtet werden, dass keine persönlichen Daten der Mitarbeiter weitergegeben werden, sofern diese nicht darüber informiert wurden und dieser Vorgehensweise zugestimmt haben. Es ist zudem möglich, dass z. B. bei der Kontaktsynchronisation oder dem Kontaktaustausch mit einem anderen Unternehmen der Schutz privater Rechte von Mitarbeitern verletzt wird.

G-TK-116 Fehlende oder unzureichende Regelungen bzgl. Nutzungsrechten einer Organisation an Daten in Sozialen Netzwerken und Medien

Werden bestimmte, für die Organisation relevante Daten durch ihr Personal ausschließlich im Rahmen von SNM-Lösungen vorgehalten, so kann der Zugriff auf diese Informationen gefährdet sein. Das gilt insbesondere bei Ausscheiden oder längerer Krankheit des zuständigen Personals.

Ohne geeignete rechtsgültige Vorkehrungen ist ein SNM-Betreiber nicht verpflichtet, eventuell auch gar nicht dazu berechtigt, Daten an eine Organisation herauszugeben, die unter einem persönlichen Account vorgehalten werden. Bei plötzlicher schwerwiegender Erkrankung des Account-Inhabers in einer Form, dass eine Datenübergabe durch diesen berechtigten Nutzer an die Organisation nicht möglich ist, sind derartige Daten für die Organisation für die Dauer dieses Krankheitsfalls nicht verfügbar.

Scheidet Personal aus einer Organisation aus, so besteht mindestens bei einem sowohl dienstlich als auch privat genutzten Account ohne entsprechende Regelung in Form einer rechtsverbindlichen Vereinbarung eine unklare Situation, ob und welche Daten, die über einen solchen SNM-Account vorgehalten werden, der Organisation rechtzeitig bis zum Ende des Beschäftigungsverhältnisses zu übergeben sind.

Wird nicht rechtzeitig unter Einbeziehung entsprechend technisch sachkundiger Know-how-Träger festgelegt, über welche Schritte und unter Beachtung welcher Detailaspekte eine solche Übergabe erfolgen soll, so können ungewollt Fehler passieren. Übergebene Daten sind dann womöglich nicht vollständig oder unbrauchbar. Falls nach der Übergabe eine Löschung dieser Daten im SNM erfolgte, so sind sie bei Erkennen des Problems womöglich nicht mehr rekonstruierbar. Ein erfolgreicher zweiter Übergabevorgang ist dann nicht realisierbar. Dies gilt selbst bei Mitwirkungsbereitschaft der aus der Organisation ausgeschiedenen Person.

8.1.2.3 Menschliche Fehlhandlungen

Durch die Integration von Sozialen Netzwerken und Medien in die Kommunikationsinfrastruktur steigt die Komplexität des Gesamtsystems. Zudem besteht durch die Exposition der Inhalte öffentlicher SNM ein hohes Risiko für die Vertraulichkeit von Informationen. Das Risiko einer menschlichen Fehlhandlung ist als sehr hoch einzustufen, wenn z. B. für den Umgang mit Informationen in Sozialen Netzwerken mangels

geeigneter Schulung keine Sensibilität beim Anwender besteht. Auch die Arbeitseffizienz kann durch den fehlerhaften Umgang mit SNM gefährdet sein.

Damit sind – sofern auf die konkrete Form der SNM-Lösung und -Nutzung zutreffend – grundsätzlich die im Gefährdungskatalog G 3 „Menschliche Fehlhandlungen“ der BSI IT-Grundschutz-Kataloge aufgeführten Gefährdungen gültig. Insbesondere sind die folgenden Gefährdungen relevant:

- G 3.13 „Weitergabe falscher oder interner Informationen“
- G 3.16 „Fehlerhafte Administration von Zugangs- und Zugriffsrechten“
- G 3.37 „Unproduktive Suchzeiten“
- G 3.43 „Ungeeigneter Umgang mit Passwörtern“
- G 3.44 „Sorglosigkeit im Umgang mit Informationen“
- G 3.45 „Unzureichende Identifikationsprüfung von Kommunikationspartnern“
- G 3.105 „Ungenehmigte Nutzung von externen Dienstleistungen“
- G 3.107 „Rufschädigung“

G-TK-117 Unzureichende Absicherung des Nutzeraccounts

Bei der Erstellung und dem Verwalten von Nutzeraccounts muss darauf geachtet werden, diese geeignet zu sichern. Dies gilt für privat genutzte Accounts ebenso wie für dienstliche. Durch Verwendung von schwachen Passwörtern oder identischen Passwörtern für verschiedene Plattformen kann der Passwortschutz gebrochen werden. Ein Angreifer könnte so Inhalte in fremdem Namen übermittelten. Bei erfolgreichen Angriffen auf den Nutzeraccount des SNM wäre bei gleichem Passwort z. B. auch das E-Mail-Konto nicht mehr sicher. Somit könnte jeder Nutzeraccount von allen Plattformen, auf denen diese E-Mail-Adresse zur Anmeldung hinterlegt wurde, kompromittiert werden.

G-TK-118 Unverschlüsselte Nutzung von Sozialen Netzwerken und Medien

Wenn Soziale Netzwerke und Medien unverschlüsselt genutzt werden, bestehen vielfältige Angriffsmöglichkeiten. Beispielsweise kann bei der Nutzung ohne Verschlüsselung in öffentlichen Wireless LANs (WLANs) ein Angreifer die sogenannte Firesheep-Attacke durchführen. Hierbei werden Session Cookies mitgeschnitten, mit welchen es möglich ist die Identität des Nutzers zu stehlen und diese unberechtigt im SNM zu nutzen. Der Angreifer erlangt vollen Zugriff auf den so kompromittierten Account.

Insbesondere bei der Verwendung mobiler Endgeräte wie Smartphones und Tablets ist diese Gefährdung gegeben, weil bei vielen mobilen Geräten – im Gegensatz zu einem Standardbrowser auf einem PC – der Status mit Blick auf Verschlüsselung nicht angezeigt wird. Der Anwender kann daher ohne manuellen Eingriff die Sicherheit der Verbindung nicht kontrollieren.

G-TK-119 Fehlkonfiguration der Datenschutzeinstellungen

Leicht können durch den Anwender im SNM fehlerhafte Datenschutzeinstellungen getroffen oder angenommen werden, die einer Organisationsrichtlinie zum Datenschutz widersprechen. Auf diese Weise werden einem Dienstbetreiber oft umfangreiche und teilweise unwiderrufliche Nutzungsrechte hochgeladener Inhalte erteilt. Dies kann beim Anlegen eines Accounts oder späterem Zurücksetzen auf die Standardeinstellung passieren. Ebenfalls besteht die Gefahr, dass durch den Anbieter veränderte Datenschutzbestimmungen ungeprüft akzeptiert werden. Zudem sind bei vielen Diensten die Datenschutzeinstellungen sehr irreführend aufgebaut und missverständlich oder unvollständig erklärt. Es besteht somit die Gefahr, dass persönliche Daten des Anwenders oder anderer betroffener Personen sowie schützenswerte Informationen der Organisation ungewollt preisgegeben werden.

G-TK-120 Versehentliche, unautorisierte Preisgabe von schützenswerten Informationen

Bei intensiver Nutzung Sozialer Netzwerke und Medien können Organisationsinterna nach außen dringen. Dies ist insbesondere der Fall, wenn SNM für die interne Kommunikation eingesetzt werden oder unkontrolliert Inhalte durch die Mitarbeiter in den SNM freigegeben werden können. So sind in der Vergangenheit beispielsweise Details zu neuen Produkten verfrüht bekannt geworden oder Kunden- und Geschäftsbeziehungen durch Standortbestimmung und Profilbildung zum Nutzers eines SNM-Accounts aufgedeckt worden.

G-TK-121 Ungerechtfertigtes Vertrauen in Informationen und Absender

Viele Angriffe auf einen Account werden auf dem Weg über fremde Accounts mit dem Status „Freund“ beziehungsweise „direkter Kontakt“ in einem Sozialen Netzwerk begangen. Diesen wird durch den Inhaber eines Accounts eine Vertrauensstellung eingeräumt (z. B. Zugriff auf die Kontaktdaten), die vielfach über den beabsichtigten Zweck hinausgeht und schädlich ausgenutzt werden kann.

Gründe für den Erfolg von Angriffen auf dieser Basis können eine mangelnde Identitätsbestimmung zu einem „befreundeten Account“ oder ein vom Angreifer ausgenutzter mangelnder Integritätsschutz der Accounts eines SNM sein. So kann durch einen Angreifer ein gefälschter Account angelegt oder der Account eines direkten Kontakts o. Ä. übernommen werden. Durch Vernetzung mit gehackten oder gefälschten Accounts können sich Malware und Malicious Hyperlinks sehr schnell verbreiten, da die Quelle vermeintlich vertrauenswürdig ist. Zudem können so „Friend-in-the-Middle“-Attacken durch geführt werden, um Profilinhalte des Nutzers auszuspähen oder Aktionen in deren Namen auszuführen.

G-TK-122 Verletzung von Urheberrechten

Durch die absichtliche oder unbeabsichtigte Veröffentlichung von urheberrechtlich geschütztem Material, das zweckgebunden, einzelplatzbezogen, personengebunden oder nur für den internen Gebrauch lizenziert ist, kann eine Urheberrechtsverletzung durch den Anwender erfolgen, für die ggf. die Organisation haftbar gemacht wird. Insbesondere das inkorrekte Zitieren oder Aneignen von externen Inhalten ist problematisch, da man nicht davon auszugehen kann, dass dies ungeschützte Inhalte sind.

G-TK-123 Preisgabe vertraulicher Informationen durch Client-Software

Soziale Netzwerke und Medien bieten häufig dedizierte Client-Software (insbesondere zur Nutzung auf dem mobilen Endgerät) und/oder Plug-ins zur Integration in weit verbreitete Client-Anwendungen. Zum Beispiel ermöglicht ein Outlook Plug-in die Synchronisation von Kontakten. Im Organisationsumfeld ist dies als kritisch anzusehen, da Fehlkonfiguration des Plug-ins oder ungefragte Synchronisation außerhalb der Einflussmöglichkeit der unter Sicherheitsgesichtspunkten geregelten und gezielten IT-Administration liegen. Infolgedessen besteht die Gefahr einer unkontrollierten und ungewollten Offenlegung von organisationsinternen Kontakten und Daten.

8.1.2.4 Technisches Versagen

Bei der Nutzung von Sozialen Netzwerken und Medien kann es zu einem technischen Versagen des Systems kommen. Es muss bei der Risikobetrachtung berücksichtigt werden, dass das technische Versagen eines Systems nur durch den Betreiber zu verhindern wäre und dies durch die Organisation bzw. den Anwender nicht erzwungen werden kann. Es ist zu berücksichtigen, dass nicht nur die Dienst- und Datenverfügbarkeit, sondern auch die Vertraulichkeit kritischer Daten durch technisches Versagen gefährdet ist. Beispielsweise kann der Schutz von Daten oder Datenübertragung durch Verschlüsselung Schwächen aufweisen oder völlig versagen.

Die Organisation kann hingegen nur dafür Sorge tragen, das Risiko eines technischen Versagens der Schnittstellen zu öffentlichen SNM zu minimieren. Hierbei ist, neben den Gefährdungen der mitgenutzten Netz- und Server-Infrastruktur, insbesondere ein vorhandenes Gateway zur Anbindung öffentlicher SNM

(SNM-Gateway) zu berücksichtigen. Dabei übertragen sich im Wesentlichen die in den BSI IT-Grundschutz-Katalogen genannten Gefährdungen, denen allgemein ein Application Layer Gateway (ALG) ausgesetzt ist, auf das SNM-Gateway.

8.1.2.5 Vorsätzliche Handlungen

Im Bereich der vorsätzlichen Handlungen besteht die wesentliche Gefahrenquelle darin, dass Soziale Netzwerke und Medien durch die Verknüpfung von personenbezogenen Daten, Informationen zur Organisation und nutzungsbedingt anfallenden Metadaten vielfältige Angriffsvektoren auf die Informationssicherheit einer Organisation oder einzelner Personen bieten.

Es treffen zunächst – sofern technisch anwendbar – grundsätzlich die im Gefährdungskatalog G 5 „Vorsätzliche Handlungen“ der BSI IT-Grundschutz-Kataloge aufgeführten Gefährdungen zu. Es gelten insbesondere die folgenden Gefährdungen:

- G 5.2 „Manipulation an Informationen oder Software“
- G 5.7 „Abhören von Leitungen“
- G 5.18 „Systematisches Ausprobieren von Passwörtern“
- G 5.19 „Missbrauch von Benutzerrechten“
- G 5.22 „Diebstahl bei mobiler Nutzung des IT-Systems“
- G 5.25 „Maskerade“
- G 5.42 „Social Engineering“
- G 5.64 „Manipulation an Daten oder Software bei Datenbanksystemen“
- G 5.71 „Vertraulichkeitsverlust schützenswerter Informationen“
- G 5.72 „Missbräuchliche Groupware-Nutzung“
- G 5.73 „Vortäuschen eines falschen Absenders“
- G 5.85 „Integritätsverlust schützenswerter Informationen“
- G 5.90 „Manipulation von Adressbüchern und Verteillisten“
- G 5.104 „Ausspähen von Informationen“
- G 5.143 „Man-in-the-Middle-Angriff“
- G 5.157 „Phishing und Pharming“
- G 5.158 „Missbrauch sozialer Netzwerke“
- G 5.172 „Umgehung der Autorisierung bei Webanwendungen“

Gefährdungen, die im Hinblick auf eine organisationsinterne Nutzung von SNM zu Kommunikationszwecken vorrangig durch die Organisation zu entschärfen sind, sind insbesondere die folgenden.

G-TK-124 Phishing und Betrug über Soziale Netzwerke und Medien

Durch das Ausnutzen von Vertrauensstellungen oder das Klicken auf manipulierte Links werden Angreifern Phishing-Attacken ermöglicht. Die so vorgenommene Sammlung von personenbezogenen Informationen kann auch der Vorbereitung von weiterführenden Betrugsversuchen dienen. Durch die Vielzahl von personenbezogenen Daten in Profilen auf SNM-Plattformen wird zudem eine gezielte Phishing-Attacke (sog. Spear-Phishing) und die Identifizierung von Zielen für Phishing-Attacken auf besonders interessante Zielpersonen (sog. Whaling) stark vereinfacht.

G-TK-125 Identitätsdiebstahl und Social Engineering in Sozialen Netzwerken und Medien

Es besteht die Gefahr, dass auf Basis von Sozialen Netzwerken und Medien gezielt personenbezogene Daten des Nutzers gesammelt und korreliert werden. Die Auswertung dieser Daten kann z. B. zur Vortäuschung falscher Identitäten und zur Erlangung von Zugriffsrechten dienen oder eine vorbereitende Maßnahme für weitere Attacken sein.

Wenn beispielsweise ein Account- bzw. Sitzungsdiebstahl durch Abfangen der Session Cookies (Firesheep-Attacke) durchgeführt wird, kann der Angreifer Zugriff unter anderem auf Passwörter erlangen und kann als vermeintlich vertrauenswürdige Person mit Dritten interagieren.

G-TK-126 Profilbildung und Tracking von Personen

Einzelanwender und Personen von besonderer Wichtigkeit für die Organisation, z. B. Entscheidungsträger oder Geheimnisträger, können über ihre Aktionen und Mitteilungen überwacht werden. Dies beinhaltet Gewohnheiten, Aufenthaltsort, Abwesenheit und Ähnliches. Durch Profilbildung können weitere Straftaten vorbereitet werden, beispielsweise Social Engineering zur Vorbereitung von Angriffen auf die IT-Infrastruktur, aber auch Einbruch, Diebstahl, Raub, Erpressung oder Entführung zur Durchsetzung von gegen die Organisation gerichteten Interessen.

G-TK-127 Rekonstruktion von internen Organisationsinformationen

Durch Sammeln und Korrelieren von Daten aus Sozialen Netzwerken können unter Umständen interne Organisationsinformationen rekonstruiert werden. Betroffene Informationen können Entscheidungswege, Motivationslage, Strukturen und Hierarchien oder die finanzielle Situation der Organisation (z. B. drohende Insolvenz eines Unternehmens) sein. Diese Daten können auch für Social Engineering und zur Vorbereitung gezielter Hacker-Angriffe verwendet werden.

G-TK-128 Herbeiführen eines Reputationsverlustes

Durch Übernahme eines unzureichend gesicherten Accounts können Äußerungen im Namen der Organisation oder von Mitarbeitern der Organisation getätigt werden. Dies kann beispielsweise Reputationsverlust und wirtschaftliche Nachteile für die Organisation oder den Mitarbeiter zur Folge haben.

G-TK-129 Behinderung der Kommunikation durch Manipulation von Kontaktdaten

Es besteht die Möglichkeit der gezielten Manipulation von Kontaktdaten innerhalb des Sozialen Netzwerks oder Mediums. Wenn Kontaktdaten aus diesen Diensten durch gezielte Manipulation führend in das elektronische Telefonbuch bzw. das Adressverzeichnis der Organisation eingespeist werden, kann so die Kommunikation der Organisation behindert oder sogar unterbunden werden.

8.1.3 Sicherheitsmaßnahmen

Im Folgenden werden die Maßnahmen aufgeführt, die für die Nutzung und Integration von Sozialen Netzwerken und Medien empfohlen werden.

Die beschriebenen Ansätze greifen zum Teil auch für andere vernetzte IT-Systeme bzw. auch bei normalem Schutzbedarf. Je nach Szenario und insbesondere für erhöhten Schutzbedarf kommt es darauf an, aus dieser Gesamtheit der Maßnahmen jeweils angemessene Pakete zu bilden.

Für die Nutzung von Sozialen Netzwerken und Medien treffen, sofern auf Art und Nutzungsweise des SNM-Angebots anwendbar, die Maßnahmen der BSI IT-Grundschutz-Kataloge (siehe [BSI GSK-2013]) zu. Relevant im Sinne der identifizierten Gefährdungen sind insbesondere die Maßnahmen:

- M 5.155 „Datenschutz-Aspekte bei der Internet-Nutzung“

- M 5.156 „Sichere Nutzung von Twitter“
- M 5.157 „Sichere Nutzung von sozialen Netzwerken“

Für die Nutzung von SNM-Angeboten aus der Umgebung einer Organisation heraus können Gateways oder ähnliche Übergänge verwendet werden, die durch die Organisation selbst betrieben werden (z. B. Gateway zum XMPP). In einem solchen Fall greifen typische für die Sicherheit auf der Schicht IT-Systeme relevante Grundschutzmaßnahmen, soweit diese für die verwendete Technologie anwendbar sind. Im Einzelnen ergeben sich die in diesem Sinne relevanten Maßnahmen zum Beispiel über die zu den Übergangssystemen inhaltlich passenden Grundschutz-Bausteine.

Ergänzend bzw. detaillierend sind die nachfolgend beschriebenen für SNM-Nutzung spezifischen Maßnahmen zu beachten.

Der entsprechende Maßnahmenkatalog zur Absicherung der Nutzung und der Integration von SNM ist in die folgenden Blöcke aufgeteilt:

- Server und Anwendungen, siehe Kapitel 8.1.3.1
- Endgeräte und Client-Anwendungen, siehe Kapitel 8.1.3.2
- Netzwerk, siehe Kapitel 8.1.3.3
- Netz- und Systemmanagement, siehe Kapitel 8.1.3.4
- Übergreifende Aspekte, siehe Kapitel 8.1.3.5

8.1.3.1 Server und Anwendungen

M-TK-155 Berechtigungskonzept zur Steuerung der Freigabe des Präsenzstatus

Durch Berechtigungskonzepte kann die Preisgabe von Präsenzinformationen in öffentlichen SNM am XMPP-Gateway gesteuert werden. Es sollte generell keine Preisgabe von nutzerbezogenen Informationen ohne vorherige Information und Zustimmung der Anwender erfolgen. Die individuelle Freigabe von Informationen je Kommunikationspartner, beispielsweise durch Hinzufügen eines Kontakts zur Kontaktliste, ist ein sinnvoller Steuerungsmechanismus. Allerdings setzt dies die Integrität der Authentisierung am Sozialen Netzwerk und die verschlüsselte Übertragung der Präsenzinformationen voraus. Ist dies nicht gewährleistet, muss zur Vermeidung auf die Anzeige der Präsenzstatus verzichtet werden.

M-TK-156 Berechtigungskonzept und technische Umsetzung für externe Kommunikation mit Sozialen Netzwerken und Medien

Die Echtzeitkommunikation zu externen Teilnehmern in Sozialen Netzwerken und Medien sollte auf diejenigen Anwender beschränkt werden, welche hieraus einen dienstlichen Nutzen ziehen. In Bereichen mit erhöhtem Schutzbedarf muss eine technische Verhinderung von unkontrollierter Echtzeitkommunikation über SNM erwogen werden. Zur externen SNM-Kommunikation berechtigte Anwender müssen in jedem Fall über das geringe Schutzniveau der Kommunikation via öffentlicher SNM-Plattformen belehrt werden.

M-TK-157 Kanalisierung des Zugriffs auf dienstliche Accounts in Sozialen Netzwerken und Medien über Portallösung

Die Einbindung von Sozialen Netzwerken und Medien in eine organisationsinterne Portallösung kann mit Unterstützung von iFrame-Regelwerken erfolgen. Zudem kann über das Portal eine Nutzerauthentisierung (z. B. per OAuth oder ähnliche Mechanismen) zur Benutzung der organisationseigenen SNM-Accounts erfolgen. So findet eine Bedienung von SNM nur innerhalb der eigenen Portallösung statt und die hierüber realisierte Authentisierung erlaubt die Verwaltung der Zugriffsrechte mehrerer Anwender über einen „technischen Firmen-Account“ im SNM. Ebenso wird das Lifecycle-Management der Nutzerberechtigungen stark vereinfacht und eine kontextbasierte Authentisierung möglich (z. B. keine Social-Media-Nutzung bei gleichzeitigem Zugriff auf bestimmte Daten).

M-TK-158 Dokumentation der Zugriffe und Aktivitäten bei Nutzung von Sozialen Netzwerken und Medien

Um Nachvollziehbarkeit und Rechenschaft durchgeführter Zugriffe, Aktivitäten und Kommunikationsvorgänge in Zusammenhang mit der dienstlichen Nutzung von Sozialen Netzwerken und Medien zu erzielen, sollten diese erfasst und dokumentiert werden. Dies gilt mindestens für im Namen der Organisation durchgeführte Aktivitäten. Es muss dabei beachtet werden, dass die Protokollierung der Privatnutzung von SNM ggf. im Konflikt mit den Regelungen zum Datenschutz steht bzw. im Rahmen von Betriebsvereinbarungen zu regeln ist. Anwender sollten in jedem Fall über eine Protokollierung ihrer Aktivitäten informiert werden, soweit diese zulässig ist und aktiviert werden soll. Eventuelle Konflikte oder Konfliktpotenziale mit dem Datenschutz sollten juristisch abgesichert, dokumentiert und regelmäßig überprüft werden.

8.1.3.2 Endgeräte und Client-Anwendungen

M-TK-159 Vermeiden der bidirektionalen Kontaktsynchronisation mit Sozialen Netzwerken und Medien

Der Zugriff auf Kontakte im Groupware-Client (und ggf. auf weitere Daten) und Lookup der Kontakte in Sozialen Netzwerken ist unter Sicherheitsgesichtspunkten kritisch zu bewerten. Besonders kritisch ist die mögliche Rücksynchronisation von Kontakten und Daten zu den SNM. Daher sollten solche Plug-ins auf schädliches Verhalten geprüft und nur eingesetzt werden, wenn sie nach einer solchen Prüfung als vertrauenswürdig eingestuft werden können. Falls derartige Plug-ins eingesetzt werden sollen, sollten diese durch die IT-Administratoren einer Organisation so vorkonfiguriert werden, dass eine Rücksynchronisation verhindert und eine verschlüsselte und authentisierte Verbindung sichergestellt wird.

Bei erhöhtem Schutzbedarf für Kontaktdaten sollte der Einsatz von Client-seitigen Plug-ins vermieden und auf eine Client-seitige Kontaktsynchronisation mit SNM verzichtet werden. Eine Ausnahme hiervon ist nur zulässig, wenn

- für das Plug-in eine Beschränkung von Synchronisationsvorgängen auf den gewollten Umfang konfiguriert werden kann (z. B. nur Import aus dem SNM) **und**
- die festgelegte Sollkonfiguration sich gegen ungewollte Änderungen geeignet schützen lässt.

Dieser Schutz kann je nach Anwendung, in die das Plug-in eingebettet ist, über die Rechteverwaltung zur Anwendung, die grundlegenden Berechtigungen des Nutzerkontos auf dem Endgerät oder über eine zentrale Lösung zur Konfigurationsverteilung und -änderung realisiert werden.

Bei sehr hohem Schutzbedarf für Kontaktdaten sind zur Vermeidung ungewollter Kontaktabgleiche folgende Lösungsansätze zu erwägen:

- Umsetzung der für den erhöhten Schutzbedarf formulierten Empfehlung, ergänzt durch gezieltes automatisiertes Rücksetzen entsprechender Konfigurationseinstellungen über eine zentrale Administrationslösung, sobald ein Client Verbindung zur internen Infrastruktur hat.
- Vollständiger Verzicht auf Einsatz derartiger Plug-ins, wobei hier die Möglichkeit gegeben sein muss, die Installation von Plug-ins durch den Endgeräteadministrator zu unterbinden.

Funktionen zur Synchronisation der Kontakte aus SNM-Anwendungen für mobile Endgeräte (z. B. „Freunde finden“ oder „Folge Deinen Freunden“) sollten deaktiviert oder auf Basis entsprechender Regelungen und entsprechender Einweisung durch den Anwender gemieden werden. Kann dies nicht sichergestellt werden, so muss bei erhöhtem Schutzbedarf vom Einsatz der entsprechenden Apps abgesehen werden.

Die Installation solcher SNM-Apps kann z. B. durch ein zentrales Management mobiler Endgeräte und der darauf installierten Software (Mobile Device Management bzw. Enterprise Application Management) unterbunden werden. Bei sehr hohem Schutzbedarf sollte eine Entscheidung zum Verzicht auf derartige Apps auch konsequent über solche Mittel verlässlich realisiert werden.

Es bietet sich generell an, die gezielte Umsetzung von Richtlinien über zentrale Systeme zu realisieren. Als Architekturvorlage bietet sich die in Kapitel 8.1.1.3.3 beschriebene Vorgehensweise zur Server-seitigen Kontaktsynchronisation an. Voraussetzung ist die Marktverfügbarkeit geeigneter Produkte. Bei der Eignungsprüfung eines solchen Produktes sollte darauf geachtet werden, dass es geeignete Schnittstellen zu vorhandenen internen Lösungen mitbringt.

M-TK-160 Host-basiertes Data Loss Prevention (DLP) bei Nutzung von Sozialen Netzwerken und Medien

Zur Verhinderung eines möglichen Datenabflusses kann eine Host-basierte DLP-Lösung eingesetzt werden. Diese Maßnahme eignet sich als Ersatz oder Ergänzung eines Netzwerk-basierten DLP-Systems. Sie bietet den Vorteil, dass der Datenverkehr keinen zentralen Netzübergang passieren muss, um die Wirksamkeit des DLP-Systems sicherzustellen. Ein lokaler DLP-Client überwacht Transaktionen auf dem Endgerät, also z. B. die Interaktion mit Sozialen Netzwerken und Medien. Nach vordefinierten Regelwerken werden Transaktionen der als vertraulich eingestuften Inhalte unterbunden. Dies setzt voraus,

- dass das DLP-System die Erkennung spezifischer Transaktionen mit Sozialen Netzwerken, mindestens aber Interaktionen mit generischen Webapplikationen, unterstützt und
- dass die Endgeräte von der Organisation gestellt werden oder vom Anwender für beruflich genutzte private Endgeräte eine derartige DLP-Lösung akzeptiert ist.

8.1.3.3 Netzwerk

M-TK-161 Netzwerk-basiertes Data Loss Prevention (DLP) bei Nutzung Sozialer Netzwerke und Medien

Zur Unterbindung oder Einschränkung der SNM-Nutzung aus einem privaten Netzwerk heraus eignen sich Netzwerk-basierte DLP-Systeme. Diese überwachen den Datenverkehr an einer oder mehreren Stellen im Netzwerk und inspizieren diesen in Hinblick auf vertrauliche Inhalte. Als unzulässig erkannte Transaktionen werden daraufhin unterbunden. Zur Umsetzung eines Netzwerk-basierten DLP-Systems ist der Einsatz einer Vielzahl von Sensoren (engl. Probes) oder die Bündelung des Datenverkehrs über wenige zentrale Netzwerkübergänge notwendig. Da dies nicht immer sinnvoll realisierbar ist, z. B. in Szenarien mit vielen verteilten Internet-Breakouts oder mit mobilen Endgeräten ohne zwangsweises Routing über das Netz der Organisation, muss die Eignung eines Netzwerk-basierten DLP-Systems genau geprüft werden. Zudem muss das DLP-System in der Lage sein, den verschlüsselten Datenverkehr mit SNM zu kontrollieren. Hierzu muss die Ent- und Verschlüsselung der HTTPS-Kommunikation im Sinne eines „Friendly-Man-in-the-Middle“ unterstützt werden. Gegebenenfalls sollte alternativ der Einsatz eines Host-basierten DLP erwogen werden.

M-TK-162 Verhinderung oder Einschränkung der Nutzung von Sozialen Netzwerken und Medien am Netzübergang

Um die Privatnutzung von SNM zu unterbinden, kann eine diesbezügliche Absicherung des Netzübergangs durch Application Layer Firewalls erfolgen. Dies ist insbesondere zu empfehlen, wenn die Nutzung von SNM nicht durch ein DLP-System abgesichert werden kann. Auch eine Einschränkung auf bestimmte Nutzergruppen kann durch die Regelwerke eines solchen Systems erzielt werden. Diese Maßnahme ist ebenso wie ein Netzwerk-basiertes DLP-System nur bei zentralen Netzübergängen wirksam.

Um eine differenzierte Einschränkung der Nutzung zu ermöglichen, bietet sich zusätzlich zur Blockierung des Datenverkehrs in Richtung SNM der Einsatz von Social Media Middleware an (siehe z. B. M-TK-157 „Kanalisierung des Zugriffs auf dienstliche Accounts in Sozialen Netzwerken und Medien über Portallösung“). Durch Integration in maßgeschneiderte Intranet-Lösungen mit entsprechender Nutzerauthentisierung lassen sich Nutzeraktivitäten gezielt und differenziert limitieren. Der den verschiedenen Nutzertypen zugängliche Funktionsumfang von SNM kann auf das notwendige Maß einschränkt werden.

M-TK-163 Netztechnische Isolation von Clients und Infrastrukturteilen mit Zugriff auf Soziale Netzwerke und Medien

Sofern die Nutzung von SNM auf kleine, dedizierte Nutzergruppen beschränkt ist und der Anwendungsfall keine Integration in andere IT-Lösungen voraussetzt, können die betreffenden Infrastrukturen und Clients in einer separaten Netzzone (Sicherheitszone) positioniert werden, um so eine vollständige Isolation von kritischen Infrastrukturen und Datenbeständen zu erzielen.

Dies setzt voraus, dass die betreffenden Clients keinen Zugriff auf besagte Infrastrukturen und Datenbestände benötigen. Andernfalls wäre eine Öffnung der Sicherheitszone, z. B. für die Integration von Webschnittstellen, notwendig. Die besprochenen Gefährdungen ergeben sich jedoch mehrheitlich aus diesen Schnittstellen, sodass eine Aufweichung der Netztrennung den Sicherheitsgewinn aufhebt. In diesem Fall würde diese lediglich zu erhöhten Betriebsaufwänden führen.

8.1.3.4 Netz- und Systemmanagement

M-TK-164 Sichere Administration der Server-Systeme und Gateways zur Anbindung an Soziale Netzwerke und Medien

Die Administration von Servern und Gateways zur Anbindung von Organisationsanwendungen und Kommunikationssystemen an Soziale Netzwerke und Medien muss durch Sicherheitsmechanismen angemessen geschützt werden. Hierzu sind die zutreffenden Maßnahmen der IT-Grundschutz-Kataloge umzusetzen, insbesondere die über die zur konkreten Lösung passenden Grundschutz-Bausteine der Schicht „IT-Systeme“ benannten.

Mit Blick auf die Absicherung der Nutzung von SNM-Angeboten sind beim Betrieb derartiger Server und Gateways darüber hinaus die folgenden Aspekte angemessen zu berücksichtigen:

- Effiziente und wirksame Umsetzung der Festlegungen zur sicheren SNM-Nutzung unter gezielter Verwendung von Produktoptionen der zentralen Übergänge

  Bringen neue Versionen von Firmware bzw. Gateway-artiger Software neue Konfigurationsoptionen mit, welche eine differenzierte Feinkonfiguration erlaubter und blockierter Nutzungsweisen ermöglichen, so ist die bisherige Konfiguration unter Berücksichtigung solcher Neuerungen gezielt zu überprüfen. Die Entscheidung zur Verwendung solcher Neuerungen ist in Abhängigkeit von dem Schutzbedarf, dem mit solchen Änderungen verbundenen Aufwand-Nutzen-Verhältnis und dem Risiko ungewollter Beeinträchtigung vorgesehener SNM-Nutzungsweisen zu treffen.

- Mindestens bei erhöhtem Schutzbedarf bzgl. Vertraulichkeit der durch SNM-Nutzung zu unterstützenden Prozesse und deren internen Daten sollten in festgelegten Abständen bzw. bei festgelegten Anlässen vorhandene Berechtigungsprofile zur SNM-Nutzung und Nutzerzuordnungen zu diesen auf Aktualität überprüft werden.

  Anlässe dieser Art können insbesondere sein:

  - Ausscheiden von Personen
  - Aufgabenwechsel, Wechsel der Abteilungszugehörigkeit usw.

- Änderungen der bisherigen Gründe für den Bedarf zum SNM-Zugriff in bestimmtem Umfang
- Änderung an Vorgaben / Regelungen zur SNM-Nutzung

M-TK-165 Schulung der Administratoren für den Zugang zu Sozialen Netzwerken und Medien

Kommunikationssysteme und deren Integrationsschnittstellen zu Sozialen Netzwerken und Medien können nicht isoliert betrachtet werden. Änderungen an den Eigenschaften eines öffentlichen SNM-Dienstes können sicherheitsrelevante Auswirkungen auf die internen Systeme haben. Neue Funktionalitäten interner Systeme, die unmittelbar oder mittelbar bei Zugriffen auf SNM-Angebote beteiligt sind bzw. aus SNM-Zugriffen stammende Daten verarbeiten, können neue Angriffspunkte darstellen. Gegebenenfalls muss gezielt mit Konfigurationsänderungen reagiert werden, etwa an zentralen internen Übergängen zu externen SNM-Angeboten oder bei der sicheren Konfiguration von Clients für den SNM-Zugriff.

Die zu entschärfenden Risiken durch SNM-Nutzung bzw. die zu diesem Zweck verwendeten Konfigurationsparameter müssen ausreichend verstanden werden, sodass weder Vertraulichkeitsverluste noch eine vermeidbare Behinderung freigegebener SNM-Nutzung durch Administrationsfehler entstehen.

Basierend auf M-TK-249 „Schulung der Administratoren von TK-Lösungen“ müssen daher die Administratoren der jeweiligen Integrationsschnittstellen zu den Wechselwirkungen der Systeme gezielt geschult, auf relevante Sicherheitsrisiken hingewiesen und bzgl. der umzusetzenden Maßnahmen und Regelungen auf aktuellem Kenntnisstand gehalten werden.

8.1.3.5 Übergreifende Aspekte

M-TK-166 Klärung und rechtsverbindliche Regelung juristischer Aspekte zur Nutzung Sozialer Netzwerke und Medien im dienstlichen Kontext

Soziale Netzwerke und Medien können als neue Alternative genutzt werden, um bisher auf anderem Wege realisierte Aufgaben wahrzunehmen. Während für länger etablierte Kommunikationslösungen typische juristische Aspekte durch entsprechende Ergänzungen zur Gesetzgebung oder durch gängige Rechtsprechung geklärt sind, kann bei einer SNM-Nutzung hiervon nicht ungeprüft ausgegangen werden. Zu dieser Rechtsunsicherheit trägt auch die oft stärkere Bindung des SNM-Zugangs an einen durch den Nutzer direkt und persönlich beim externen SNM-Betreiber zu beantragenden Account bei. Die für andere externe Kommunikationsdienste typischerweise verfügbare Option zum Abschluss eines Vertrags zwischen Organisation und Dienstanbieter als Basis von dienstlich genutzten Zugängen ist bei SNM-Angeboten nicht zwingend gegeben, zum Teil sogar (noch) unüblich.

Mit dieser bis auf Weiteres besonderen rechtlichen Ausgangslage muss aus Sicht der Sicherheitsziele einer Organisation gezielt so umgegangen werden, dass Aspekte der folgenden Art geeignet gelöst werden:

- Möglichkeit der Organisation zur verbindlichen Regelung bzgl. über persönliche SNM-Konten durchgeführte Aktionen mit Haftungsrisiko

  Die Pflichten und Verbote bei der Nutzung persönlicher SNM-Konten müssen so verbindlich geregelt sein, dass ein Bezug zur Organisation hergestellt werden kann und dass die Folgen einer Zuwiderhandlung durch den Einzelnen juristisch nicht auf die Organisation zurückfallen können.

- Möglichkeit der Organisation zur verbindlichen Regelung bzgl. über persönliche SNM-Konten durchgeführte Aktionen mit Charakter eines Rechtsgeschäfts

  Die Berechtigung zur Tätigung von Rechtsgeschäften im Namen der Organisation über ein persönliches SNM-Konto muss in geeigneter Form juristisch unterlegt werden (z. B. Mit einer Vollmacht). Bei Fehlen einer solchen Ermächtigung sollte ein explizites Verbot der

Durchführung solcher Aktivitäten erwogen werden. Je nach möglichem Folgeschaden für die Organisation sind ergänzend Ansätze zur technischen Verhinderung entsprechender Vorgänge zu suchen und ggf. zu implementieren.

- Möglichkeit der Organisation zur Sicherung von benötigten Nutzungsrechten an Informationen, die über persönliche Konten verwaltet und SNM-basiert vorgehalten werden

  Soweit nicht geeignet sichergestellt werden kann, dass nur über persönliche SNM-Konten zugängliche Informationen in geeignet synchroner Kopie auch als interne Datenbestände zur Verfügung stehen, muss aus Sicht der Organisation eine belastbare juristische Grundlage für den Zugang zu diesen Daten auch in ungünstigen Situationen geschaffen werden. Es ist zu vermeiden, dass aus rechtlichen Gründen eine Herausgabe an die Organisation verweigert werden kann; ein typisches Beispiel ist hier die Beschränkung von Pflichten des SNM-Dienstanbieters auf Ansprüche durch den Account-Inhaber.

- Rechtssicherheit für Mitarbeiter einer Organisation bei der Durchführung dienstlich zugewiesener Aufgaben mittels persönlicher SNM-Konten

  Nimmt ein Mitarbeiter einer Organisation ihm übertragene Aufgaben mit Wissen der Organisation über ein persönliches SNM-Konto wie beauftragt wahr, so dürfen ihm hieraus bei korrekter, pflichtgemäßer Aufgabenwahrnehmung keine rechtlichen Nachteile entstehen.

- Konformität zu Gesetzen und Vorschriften, die für die SNM-basierte Informationsbereitstellung durch die Organisation gelten.

  Es ist grundsätzlich von der Annahme auszugehen, dass die für etablierte Formen der Externkommunikation und Informationsbereitstellung maßgeblichen Gesetze und Vorschriften zumindest sinngemäß auch auf neue Kommunikationsmöglichkeiten wie SNM-Angebote anzuwenden sind. Beispiel sind hier Impressumspflicht, Aspekte des Urheberrechts bei Weitergabe usw. Will eine Organisation Informationsangebote über SNM-Lösungen zur Verfügung stellen, sollte eine gezielte Prüfung bzgl. entsprechend zu berücksichtigender Aspekte erfolgen. Die für die Ausführung zuständigen Personen sind entsprechend einzuweisen, eine abschließende Kontrolle der entsprechenden Umsetzung durch das SNM-basierte Informationsangebot sollte vor Freischaltung des Zugangs zu neuen / geänderten Informationsangeboten der Organisation erfolgen.

Diese und ggf. weitere für eine Organisation maßgebliche Aspekte sollten für erstmalig vorgesehene SNM-Nutzungsformen im notwendigen Umfang gezielt juristisch vorgeprüft werden. Wichtigstes Kriterium für den Prüfungsumfang ist das mögliche Schadensausmaß. Kann eine geeignet juristische Basis nicht sicher ermittelt werden, so ist ein explizites Verbot derartiger SNM-Nutzungsformen bis zur belastbaren Klärung durch die Gesetzgebung oder Rechtsprechung zu erwägen.

M-TK-167 Geeignete Einbindung der Nutzung von Sozialen Netzwerken und Medien in etablierte Prozesse

Soweit der Umgang mit Informationen, insbesondere deren Nutzung über eine technische Außenanbindung, für bereits bestehende Lösungen zur Externkommunikation in einer Organisation geregelt ist, müssen solche Regeln gleichwertig auf die Nutzung von SNM-Angeboten übertragen werden. Dies schließt ein:

- Festgelegte Prüf- und Freigabeinstanzen

  Soweit vor Veröffentlichung von Informationen der Art, wie sie jetzt über SNM-Lösungen Dritten zugänglich gemacht werden sollen, eine interne Prüfung und Freigabe vorgesehen ist, sollte eine gleichwertige Prüf- und Freigabeverpflichtung vor Einstellen in ein SNM-Angebot festgelegt werden. Typisch ist die Zuweisung der Zuständigkeit für Prüfung und Freigabe an die auch bei Nutzung anderer Kommunikationswege zuständigen Instanzen geeignet und zu empfehlen.

Ist vor Übernahme auf anderem Wege eingegangener Informationen in interne Datenbestände eine Prüfung vorgesehen, so ist diese Regelung auf Eingang solcher Informationen via SNM-Diensten auszuweiten. Prüfpunkte in diesem Sinne können beispielsweise die Prüfung auf Authentizität der Quelle, auf Plausibilität der Inhalte oder auf Rechtmäßigkeit einer Speicherung und weiteren Verarbeitung sein.

- Festgelegte Zuständigkeiten für bestimmte Verwendungszwecke von Informationen und zugehörigen Kommunikationsflüssen

  Dies betrifft insbesondere Informationen, die über Externkommunikation Dritten zugänglich gemacht werden sollen, jetzt eben via SNM. Soweit für solche Externkommunikation grundsätzlich die Zuständigen eindeutig festgelegt wurden (z. B. Unternehmenskommunikation oder Pressestelle), sollte für eine externe Weitergabe via SNM keine Ausnahme von einer solchen grundlegenden Festlegung gemacht werden. Es ist zu prüfen, ob die bisherige Festlegung so allgemein formuliert wurde, dass das Medium zur Veröffentlichung unerheblich ist, also SNM unmittelbar eingeschlossen ist. Wenn nicht, sollte der Geltungsbereich explizit auf Veröffentlichungen via SNM erweitert werden.

- Festlegungen bzgl. zu informierender Personen / Personengruppen

  Sollen Informationen, für die über solche Inhalte zu informierende Personen festgelegt sind, zukünftig über SNM weitergegeben werden, so ist folgendes sicherzustellen:

  - Der festgelegte Personenkreis hat technischen Zugang zu diesen Informationen im SNM.
  - Über die SNM-Lösung erfolgt eine aktive Benachrichtigung über den Eingang solcher Informationen, wenn die bisher zur Weitergabe genutzten Dienste automatisch einen solchen Hinweis erzeugt haben.

    Schließt ein bisher genutzter Dienst Funktionalitäten ein, die einen Eingangsnachweis beim Adressaten beinhalten und für Informationen der fraglichen Art auch genutzt worden sind, so muss bei Weitergabe über SNM-Dienste ein vergleichbarer Nachweis sichergestellt werden. Dies gilt insbesondere, wenn der Nachweis als Basis einer Nichtabstreitbarkeit des Erhalts bzw. der Kenntnisnahme dienen soll.
  - In bislang genutzten Verteilern (organisatorisch oder technisch definierte Listen der zu Informierenden) enthaltene Adressaten können lückenlos auch bei Weitergabe via SNM erreicht werden.

    Hierbei ist mit Blick auf den Schutzbedarf hinsichtlich Vertraulichkeit von Kontaktinformationen der Unterschied zwischen intern vorgehaltenen Adressverzeichnissen und im Rahmen externer SNM-Lösungen gespeicherten Kontaktinformationen zu beachten. Durch den Wechsel auf SNM-basierte Verteilung darf kein Verstoß gegen interne Festlegungen entstehen, die ein externes Verwalten bestimmter Kontakte untersagen.

M-TK-168 Transparente und durchsetzbare Regelungen zur Nutzung Sozialer Netzwerke und Medien im dienstlichen Kontext

Um einen wirksamen Schutz vor dem Missbrauch Sozialer Netzwerke und Medien zu implementieren, ist die Transparenz und Durchsetzbarkeit einer Regelung zu deren Nutzung erforderlich.

Transparenz ist durch explizite und ausreichend verständliche Festlegung von erlaubten und zu unterlassenden Details zur SNM-Nutzung zu schaffen:

- Hierin muss mindestens definiert werden, welcher Anwender welche Dienste nutzen darf und welcher Zweck damit verfolgt wird.
- Zudem ist klar zu formulieren, für welche Nutzergruppen und unter welchen Rahmenbedingungen eine SNM-Nutzung ausdrücklich nicht zulässig ist.

- Soweit vermieden werden soll, dass ungeschickte Äußerungen von Organisationspersonal via SNM negativ auf die Organisation zurückfallen, sollten klare Festlegungen und Hinweise erfolgen, welche Nutzungsweisen vermieden werden sollen bzw. worauf bei Formulierungen zu achten ist.

  Beispiele:

  - Hinweis, dass bei Antworten auf Fragen bzw. Stellungnahmen im Rahmen von via SNM geführter Diskussionen über gezielte Formulierungsdetails („Ich-Form", „meiner persönlichen Ansicht nach" usw.) klar abgegrenzt werden soll, dass hier nicht ein abgestimmter Standpunkt der Organisation, sondern eine persönliche Meinung kundgetan wird
  - Ausdrückliche Beschränkung der Nutzung von SNM-Diensten auf die Informationsbeschaffung, insbesondere explizites Verbot einer aktiven Stellungnahme über (auch) dienstlich genutzte Konten

Es wird empfohlen, Definitionen und Grundregeln zu derartigen Aspekten auf Basis von bereits geregelten, in einer Organisation verbindlich zu verwendenden Klassifizierungen zur Kritikalität von Informationen zu formulieren (z. B. öffentlich, intern, vertraulich). Auf diese Weise gelten allgemein an solche Einstufungen von Informationen gekoppelte Verhaltensmaßregeln zur Wahrung der Vertraulichkeit mindestens sinngemäß auch für den SNM-basierten Informationsaustausch.

Bei den Festlegungen sind maßgebliche Gesetze und Vorschriften (z. B. das Bundesdatenschutzgesetz, BDSG) zu berücksichtigen. Für eine geeignete Transparenz sollte die Maßgeblichkeit für SNM-Nutzung in angemessenem Umfang unter Nennung der Gesetze und Regelungen erwähnt werden.

Basis für die notwendige Durchsetzbarkeit ist eine gezielte juristische Vorklärung sowie Schaffung ausreichender Verbindlichkeit (siehe auch M-TK-166 „Klärung und rechtsverbindliche Regelung juristischer Aspekte zur Nutzung Sozialer Netzwerke und Medien im dienstlichen Kontext"). Mindestens bei erhöhtem Schutzbedarf der betroffenen Informationen wird dringend empfohlen zu prüfen, inwieweit die Einhaltung von Regelungen durch technische Maßnahmen gezielt unterstützt werden kann. Beschlossene Maßnahmen dieser Art sind als Elemente einer Sicherheitskonzeption zur SNM-Nutzung aus der Organisation heraus zu dokumentieren und im zum Schutzbedarf passenden Umfang für die verschiedenen Nutzungsformen und Nutzerkreise zu SNM-Angeboten umzusetzen.

Um eine optimale Wirksamkeit zu gewährleisten, sollten diese Regelungen nicht nur den Mitarbeitern kommuniziert werden, sondern ihre Einhaltung sollte nach Möglichkeit mit technischen Mitteln überwacht und durchgesetzt werden.

M-TK-169 Gezielte Trennung von dienstlichem und privatem Gebrauch von Sozialen Netzwerken und Medien

Für die Nutzung von SNM muss eine klare Regelung zur Trennung von dienstlichem und privatem Gebrauch von SNM-Angeboten erfolgen, insbesondere

- falls Informationen mit erhöhtem Schutzbedarf mittels SNM-Diensten erlangt werden oder Externen zur Verfügung gestellt werden und
- falls die Risiken für die Organisation bei paralleler privater und dienstlicher Nutzung bestimmter SNM-Angebote über dasselbe Nutzerkonto nicht angemessen entschärft werden können.

Typische Ansätze zu einer wirksamen Umsetzung derartiger Regelungen sind insbesondere:

- Eine klare Definition von dienstlichen und privaten SNM-Accounts
- Ausschluss der Privatnutzung von dienstlichen Accounts

- Verbot der Nutzung von dienstlichen E-Mail-Adressen zur Eröffnung privater SNM-Accounts
- Hinweise und Regelungen bzgl. einer klaren Vermeidung unmittelbarer Rückschlüsse von privaten SNM-Konten, privaten Meinungsäußerungen o. Ä. auf die Organisation, der die Kontoinhaber zugehören

  Beispiel: Vermeidung einer Nennung der Organisationszugehörigkeit im Rahmen von Identitätsangaben / Profilinhalten zu einem privaten Nutzerkonto

M-TK-170 Einschränkung oder Verbot der Privatnutzung von Sozialen Netzwerken und Medien am Arbeitsplatz

Bei erhöhtem Schutzbedarf sollten zur Schaffung von Rechtssicherheit in praxisrelevanten Situationen oder bei nicht ausreichender technischer Möglichkeit zum Schutz von Informationen im Rahmen bestimmter externer SNM-Angebote die folgenden Alternativen erwogen werden, sofern dies ohne Verstoß gegen Gesetze, Vorschriften, Betriebsvereinbarungen usw. möglich ist:

- Generelles Verbot der Privatnutzung betroffener SNM-Angebote am Arbeitsplatz
- Verbot der privaten Nutzung von SNM-Angeboten auf dem Dienstgerät, typisch in Verbindung mit Vorgabe zur ausschließlichen Nutzung des Dienstgerätes im Rahmen der beruflichen Tätigkeit

Ein konsequentes Verbot jeglicher Privatnutzung von SNM am Arbeitsplatz ist insbesondere zu empfehlen, falls für die mit erhöhtem Schutzbedarf eingestuften Inhalte bei Kommunikation via SNM keine gezielte und differenzierte Kontrolle (z. B. mittels DLP) möglich ist. Die Durchsetzung dieser Regelung sollte durch technische Maßnahmen (z. B. Application Layer Firewall, Proxy-Konfiguration) unterstützt werden.

M-TK-171 Verbot der ungeschützten Übertragung vertraulicher Inhalte über Soziale Netzwerke und Medien

Aufgrund des nicht sichergestellten Schutzniveaus von Kommunikation und Datenübertragung über öffentliche SNM muss von einer Übertragung vertraulicher oder geheimer Inhalte (ab Kategorie „Nur für den Dienstgebrauch“) unbedingt abgesehen werden. Auch die Übermittlung personenbezogener Daten sollte unterlassen werden, sofern hierfür kein Einverständnis der betreffenden Person(en) vorliegt. Sofern technisch machbar, sollte ein technisches Konzept zur Verhinderung der Übertragung vertraulicher Inhalte implementiert werden (z. B. DLP-System).

M-TK-172 Information und Schulung der Anwender bzgl. sicherer Nutzung von Sozialen Netzwerken und Medien

Sofern eine dienstliche Nutzung von SNM in Erwägung gezogen und die generelle Nutzung nicht unterbunden wird, müssen die Anwender über die internen Regelungen zur Nutzung von SNM informiert werden. Im Rahmen der Anwender-Information zum sicheren Umgang mit IT-Systemen sollte eine Aufklärung und eine Sensibilisierung für Sicherheitsaspekte der SNM-Nutzung erfolgen. Auch wichtige Hinweise für die Privatnutzung von SNM sollten hier Berücksichtigung finden. Als Grundlage eignet sich neben den Inhalten dieser Technischen Leitlinie das Informationsmaterial des BSI zum Thema Social Media im Programm „BSI für Bürger“ (siehe [BSI BSIFB-2014])

M-TK-173 Benennung von Ansprechpartnern

Um einem Missbrauch von oder einem Angriff via SNM in Organisationen vorzubeugen bzw. einen bereits erfolgten Missbrauch oder Angriff aufzuklären und einzudämmen, sollten dedizierte Ansprechpartner benannt werden. Diese sollen den Mitarbeitern als Ansprechpartner zur Meldung ungewöhnlicher Vorkommnisse und bei Verdacht auf missbräuchliche Nutzung von SNM zur Verfügung stehen. Diese Ansprechpartner nehmen idealerweise auch eine Beratung der Anwender in solchen Fällen vor und koordinieren ggf.

einzuleitende Maßnahmen mit der IT-Sicherheit und dem IT-Sicherheitsbeauftragten. Im Falle einer Sicherheitslücke oder eines Missbrauchsverdachts koordinieren sie zudem die notwendigen Maßnahmen mit dem Betreiber der betroffenen SNM-Plattform. Um in solchen Fällen die Reaktionszeit zu verkürzen, sollten bereits im Vorfeld Kommunikationskanäle zu den Betreibern der relevanten SNM-Plattform aufgebaut werden. Diese Ansprechpartner können auch in die Schulung und Sensibilisierung der Nutzer einbezogen werden und als Informationsstelle zum Thema dienen.

8.1.4 Zusammenfassung

Soziale Netzwerke und Medien (SNM) sind durch externe Anbieter betriebene, öffentlich zugängliche Webplattformen zur Vernetzung, Kommunikation und Bereitstellung von Daten. SNM werden hier mit Fokus auf ihre Relevanz für organisationsinterne und -übergreifende Kommunikation betrachtet.

Da es sich bei SNM um einen externen Dienst handelt, wird dieser über den Internetzugang des Anwenders innerhalb einer Organisation genutzt. Die Nutzerkonten und gespeicherten Daten werden vom Dienstanbieter der SNM bereitgestellt und verwaltet. Die Bereitstellung und Verwaltung liegen daher außerhalb der Zuständigkeiten der Organisation, welcher der Nutzer zugehörig ist. Angriffspunkte in diesem Bereich können daher von der betroffenen Organisation nicht beeinflusst oder entschärft werden.

Wesentliche Elemente einer Sicherheitskonzeption für die Nutzung von Sozialen Netzwerken und Medien durch eine Organisation bestehen daher in der Absicherung von Schnittstellen zur Organisation. Diese Schnittstellen sind einerseits Übergänge von der internen Infrastruktur zu externen SNM und andererseits Schnittstellen, welche sich an Endgeräten ergeben, die SNM nutzen (z. B. durch für SNM genutzte Applikationen).

Weiterhin ist von Organisationsseite generell die Entscheidung zu treffen, ob und in welchem Umfang SNM dienstlich genutzt werden soll und in welchem Umfang Daten und Informationen über solche Angebote bereitgestellt werden dürfen.

Die mit Nutzung Sozialer Netzwerke und Medien aus der Infrastruktur einer Organisation heraus verbundenen Angriffsrisiken sind im Rahmen eines Sicherheitskonzepts zu bewerten und über bewusste Gestaltung der Nutzung zu minimieren. Hierbei sind folgende Punkte zu berücksichtigen:

- die Gesamtheit der Angebote in SNM, die durch eine Organisation als signifikant eingestuft werden, und die dafür zur Verfügung zu stellenden Daten und Informationen
- die Wichtigkeit des Zugangs zu Sozialen Netzwerken und Medien für bestimmte Aufgaben
- die mit den verschiedenen Diensten und Dienstanbietern verbundenen Gefährdungspotenziale

Besonders zu beachten sind dabei:

- die Gefahr des Abflusses interner Daten und Informationen durch Fehlbedienung, Fehlkonfiguration (insbesondere bei Verwendung privater Endgeräte im dienstlichen Umfeld), technische Fehler oder gezielter Angriffe auf ein Multifunktionsendgerät
- die Notwendigkeit zur Übertragung von Daten in die Infrastruktur der externen SNM-Anbieter, vor allem im Hinblick auf Vertraulichkeit von personenbezogenen Daten und Gefahren bei ausschließlicher Vorhaltung von Daten in SNM
- die häufige Praxis, mit einem SNM-Nutzerzugang ein direktes Vertragsverhältnis zwischen dem Nutzer eines Kontos und dem Betreiber eines SNM-Angebots zu initiieren, und den hieraus entstehenden rechtlichen Konsequenzen für die Organisation

Die Erarbeitung und Umsetzung einer Konzeption für die sichere Nutzung von Sozialen Netzwerken und Medien durch Personal einer Organisation konzentriert sich neben den generell zu ergreifenden Maßnahmen (siehe Kapitel 10) auf Aspekte der folgenden Art:

Absicherung im Bereich Server und Anwendungen

Sollen Daten und Informationen über SNM bereitgestellt werden, so ist es notwendig, dass geregelt wird, welche Daten und Informationen extern freigegeben werden dürfen. Dies ist besonders relevant, wenn die Daten personenbezogene Anteile enthalten.

Soweit die externe Preisgabe solcher Daten mit Einstellmöglichkeiten des SNM-Dienstes kontrolliert werden kann, sollten solche Möglichkeiten gezielt genutzt werden. Sind keine bzw. keine ausreichend verlässlichen und differenzierten Einstellmöglichkeiten gegeben, sollten die zur Weitergabe freigegebenen Daten auf das notwendige Maß beschränkt werden.

Absicherung im Bereich Endgeräte und Client-Anwendungen

Auf Endgeräten, von denen aus berechtigte Nutzer SNM nutzen können, sind Risiken durch automatisches Zusammenwirken von SNM-Client-Software und anderer auf solchen Endgeräten verfügbaren Anwendungen zu prüfen. Je nach Risikobewertung und Sicherheitseigenschaften derartiger SNM-Client-Software ist zu entscheiden, ob derartige Software überhaupt auf dem Endgerät installiert werden darf:

- Soweit das Risiko eines ungewollten Datenabflusses als zu hoch angesehen wird, muss auf derartige Software verzichtet werden. Dabei muss eine Nachinstallation durch den Nutzer verhindert werden. Informationen zwischen SNM- und anderer Client-Software müssen dann ggf. manuell übertragen werden (minimierte Installation und Konfiguration von SNM-Client-Software auf dem Endgerät).
- Soweit SNM-Client-Software grundsätzlich zum Einsatz freigegeben werden kann und soll, ist zumindest für den erhöhten Schutzbedarf der Einsatz Client-lokaler Ergänzungslösungen zur Verhinderung ungewollten Datenabflusses (Host-basierte Data Loss Prevention) zu prüfen.

Absicherung des Netzwerks

Die Überwachung von Datenströmen zwischen Endgerät und SNM kann über Netzkomponenten zentral realisiert werden.

So können Netzbereiche mit Endgeräten und Systemübergängen zu SNM von anderer Kommunikation isoliert werden. Weiterhin kann der Internetzugang um Systemlösungen ergänzt werden, welche den Datenstrom zwischen Endgerät und Internet kontrollieren können. Datenströme zur Nutzung von SNM können dann gezielt über solche Systemlösungen kanalisiert werden:

- Systeme zur kontrollierten SNM-Anbindung können im Rahmen typischer Protokolle zur Nutzung von SNM-Diensten angebotene Gateway-Lösungen sein (z. B. XMPP-Gateway, Session Border Controller) oder gezielt als zentral kontrollierbares Gateway mit SNM-spezifischer Intelligenz in die Architektur aufgenommen werden („SNM-Connector“).
- Zentrale Gateway-Übergänge zu SNM können als Realisierungspunkte für Sicherheitsmaßnahmen und zur Festlegung von SNM-Nutzungsmöglichkeiten für unterschiedliche Personenkreise genutzt werden. Da sie aber auch Angriffspunkte darstellen, an denen ein Angreifer schädlichen Einfluss auf die Verfügbarkeit des SNM-Zugriffs oder auf die SNM-Datenströme nehmen kann, sind sie entsprechend dem Schutzbedarf zu härten und abzusichern.

Soweit auf solchen Übergängen verfügbare Protokollierungsoptionen zur Erkennung und Behandlung von Sicherheitsvorfällen oder zur Erfüllung gesetzlicher Auflagen genutzt werden sollen, müssen gezielte Regelungen bzgl. Art und Umfang einer zulässigen Protokollierung, Aufbewahrung und Zugriffe auf solcher Daten getroffen und durch eine entsprechende Konfiguration umgesetzt werden.

Gezielte Ausstattung, externe Leistungen

Eine gezielte Ausstattung für SNM bilden Komponenten für zentrale Systeme zur Kanalisierung und sicherheitstechnischen Kontrolle von Datenströmen zur Nutzung von externen SNM-Angeboten.

Soweit die Verfügbarkeit freigegebener SNM-Nutzungsformen für eine Organisation wichtig ist, sollten Wartungs- und Support-Verträge für derartige Systemlösungen entsprechend gestaltet werden.

Organisatorische Maßnahmen

Sämtliche gezielt zur Kanalisierung und Absicherung der Nutzung externer Sozialer Netzwerke und Medien eingesetzten Systeme müssen auf einem abgestimmten Niveau sicher administriert und betrieben werden. Gleiches gilt für den Endgerätebetrieb, soweit spezielle Client-Anwendungen und Client-lokale Sicherheitsmaßnahmen für eine kontrollierte SNM-Nutzung zu administrieren sind.

Administratoren und Nutzer müssen bezüglich besonderer Gefährdungen durch Nutzung externer SNM-Angebote gezielt sensibilisiert werden. Der sichere Umgang mit entsprechender Software und die Einhaltung spezieller Sicherheitsmaßnahmen muss geeignet geschult werden.

Wesentliche Grundlage für eine angemessene Entschärfung von Gefährdungen und Risiken einer SNM-Nutzung aus Sicht einer Organisation sind gezielte, umfassende und ausreichend differenzierte Regelungen. Über solche Regelungen muss insbesondere die nötige Basis dafür geschaffen werden,

- dass bei Ergänzung oder Ablösung bisher etablierter Kommunikationsformen und Dienste durch Soziale Netzwerke und Medien maßgeblichen Gesetzen und Regelungen mindestens sinngemäß weiterhin entsprochen wird,
- dass durch die externe, stark an das einzelne Nutzerkonto gebundene Bereitstellung und Zugriffsgewährung zu Diensten und Daten in Sozialen Netzwerken und Medien keine Nachteile für die Organisation entstehen,
- dass sicherheitsrelevante organisationsinterne Festlegungen für den Umgang mit Daten und Informationen auch eingehalten werden, wenn diese im Rahmen extern betriebener SNM-Angebote verwendet und vorgehalten werden,
- dass etablierte Prozesse, insbesondere Festlegungen bzgl. Zuständigkeiten für Informationsbestände und Verantwortlichkeiten für die Freigabe von Informationen, bei Übergang auf externe Soziale Netzwerke und Medien als IT-Basis nicht unterwandert werden, sowie
- dass für die Organisation keine inakzeptablen Risiken durch Vermischung von privater und dienstlicher Nutzung von Endgeräten und Konten zu Sozialen Netzwerken und Medien entstehen.

8.2 Outsourcing, IP-Centrex, Cloud Computing und UC as a Service

8.2.1 Basiswissen

8.2.1.1 Cloud Computing

Der Begriff des Cloud Computing hat sich in den vergangenen Jahren weiter gefestigt, auch wenn sich bis dato keine Definition allgemeingültig durchsetzen konnte. In Publikationen und Vorträgen findet man häufig Definitionen, die sich zwar sehr ähneln, im Detail jedoch immer wieder variieren.

Eine häufig herangezogene Definition ist die der US-amerikanischen Standardisierungsstelle National Institute of Standards and Technology (NIST, siehe [NIST SP800145-2011]), welche auch von der European Network and Information Security Agency (ENISA, siehe [ENISA CC-2009]) angewendet wird:

> *„Cloud Computing ist ein Modell, das es erlaubt bei Bedarf, jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Management-Aufwand oder geringer Service-Provider-Interaktion zur Verfügung gestellt werden können."*

Nach dieser Definition zeichnet sich Cloud Computing durch die folgenden charakteristischen Eigenschaften aus:

- On-demand Self Service: Die Bereitstellung und Provisionierung von Ressourcen (z. B. Rechenleistung und Speicherkapazitäten) erfolgt automatisiert ohne direkte Interaktion mit dem Dienstanbieter.
- Broad Network Access: Die Dienste sind mit Standardmechanismen über das Netz verfügbar und nicht an einen bestimmten Client gebunden (Client-agnostisch).
- Resource Pooling: Die Ressourcen des Dienstanbieters liegen in einem Pool vor, aus dem sich viele Anwender bedienen können (Multi-Tenant-Modell). Dabei wissen die Anwender nicht, wo sich die Ressourcen befinden, sie können aber vertraglich den Speicherort, also z. B. Region, Land oder Rechenzentrum, festlegen.
- Rapid Elasticity: Die Services können schnell und elastisch zur Verfügung gestellt werden, in manchen Fällen auch automatisch. Aus Anwendersicht scheinen die Ressourcen daher unendlich zu sein.
- Measured Services: Die Ressourcennutzung kann gemessen und überwacht werden und entsprechend bemessen auch den Cloud-Anwendern zur Verfügung gestellt werden.

Das BSI hat folgende Definition für den Begriff Cloud Computing festgelegt (siehe [BSI Bro314-2012]):

> *„Cloud Computing bezeichnet das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software."*

In diesem Dokument wird der Begriff Cloud Computing gemäß dieser Definition verwendet, wobei die charakteristischen Eigenschaften gemäß der Definition des NIST stets zu berücksichtigen sind.

Im Rahmen des Cloud Computing haben sich unterschiedliche Betreibermodelle etabliert. Die Wesentlichen sind:

- Public Cloud: Hier werden durch einen entsprechenden Anbieter über das Internet Cloud-Ressourcen und Dienste der Allgemeinheit zur Verfügung gestellt.
- Private Cloud: Hierbei wird die Cloud-Infrastruktur dezidiert für eine Organisation betrieben. Sie kann von der Organisation selbst oder einem Dritten organisiert und geführt werden und kann dabei im Rechenzentrum der eigenen Organisation oder eines Cloud-Dienstleisters stehen.
- Hybrid Cloud: Diese Cloud-Infrastruktur ist eine Zusammensetzung aus verschiedenen Cloud-Infrastrukturen (Public Cloud oder Private Cloud), die jeweils für sich eigenständig sind und deren Daten bzw. Anwendungen über standardisierte oder proprietäre Technologien gekoppelt werden.
- Virtual Private Cloud: Dies ist eine Spezialform der Private Cloud, die innerhalb einer Public Cloud betrieben wird und durch weitreichende Zugriffsbeschränkungen logisch isoliert ist. Im Gegensatz zur Private Cloud werden benötigte Hardware-nahe IT-Ressourcen in der Regel mit anderen Nutzern der Public Cloud geteilt.

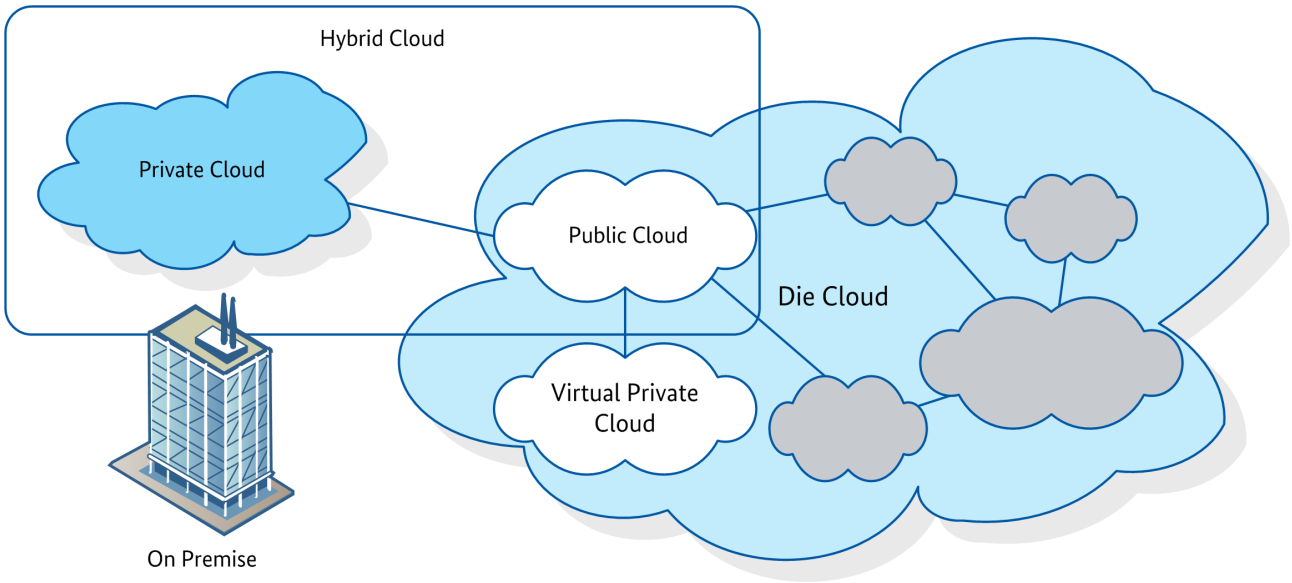


Abbildung 51: Cloud-Betreibermodelle

Das NIST definiert darüber hinaus noch die Community Cloud, bei der Cloud-Ressourcen von mehreren Organisationen mit gemeinsamen Interessen geteilt werden. Sie hat jedoch nur sehr geringe Praxisrelevanz.

In Abhängigkeit der von der Cloud bereitgestellten Dienste sind darüber hinaus die folgenden Servicemodelle zu unterscheiden:

- Infrastructure as a Service (IaaS): Bei IaaS werden Ressourcen wie Rechenkapazität, Speicher oder Netzwerke zur Verfügung gestellt, auf denen Cloud-Kunden beliebige Software und Betriebssysteme installieren und betreiben können. Cloud-Kunden verwalten dabei nicht die zugrunde liegende Cloud-Infrastruktur, sondern haben volle Kontrolle über Betriebssysteme, Speicher und Anwendungen sowie ggf. begrenzte Kontrolle über ausgewählte Netzwerkkomponenten (z. B. Host-Firewalls).
- Platform as a Service (PaaS): Bei diesem Servicemodell wird dem Cloud-Kunden eine Umgebung bereitgestellt, auf dem er Anwendungen betreiben kann, ggf. mit Hilfe von Programmiersprachen, Bibliotheken und Tools, die vom Cloud-Anbieter unterstützt werden. Dies sind z. B. Datenbank-Systeme, Systeme zur Workflow-Steuerung oder Web-Server. Der Cloud-Kunde hat keine Kontrolle über die zugrunde liegende Cloud-Infrastruktur einschließlich Netzwerk, Server, Betriebssysteme oder Speicher. Der Cloud-Kunde hat jedoch volle Kontrolle über die bereitgestellten Anwendungen und eventuell über die Konfigurationseinstellungen für die Hosting-Umgebung der Anwendung.

- Software as a Service (SaaS): SaaS bietet dem Cloud-Kunden die Möglichkeit, Anwendungen zu nutzen, welche vom Cloud-Anbieter bereitgestellt werden. Auf diese Anwendungen kann von verschiedenen Client-Geräten entweder über eine generische Client-Schnittstelle, z. B. einen Web-Browser, oder über eine entsprechende Client-Applikation zugegriffen werden. Der Cloud-Kunde hat keine Kontrolle über die zugrunde liegende Cloud-Infrastruktur einschließlich Netzwerk, Server, Betriebssysteme, Speicher, Speicherort der Daten oder sonstige Konfiguration der Infrastruktur. Lediglich benutzerspezifische Anpassungen der Anwendung können ggf. vorgenommen werden.

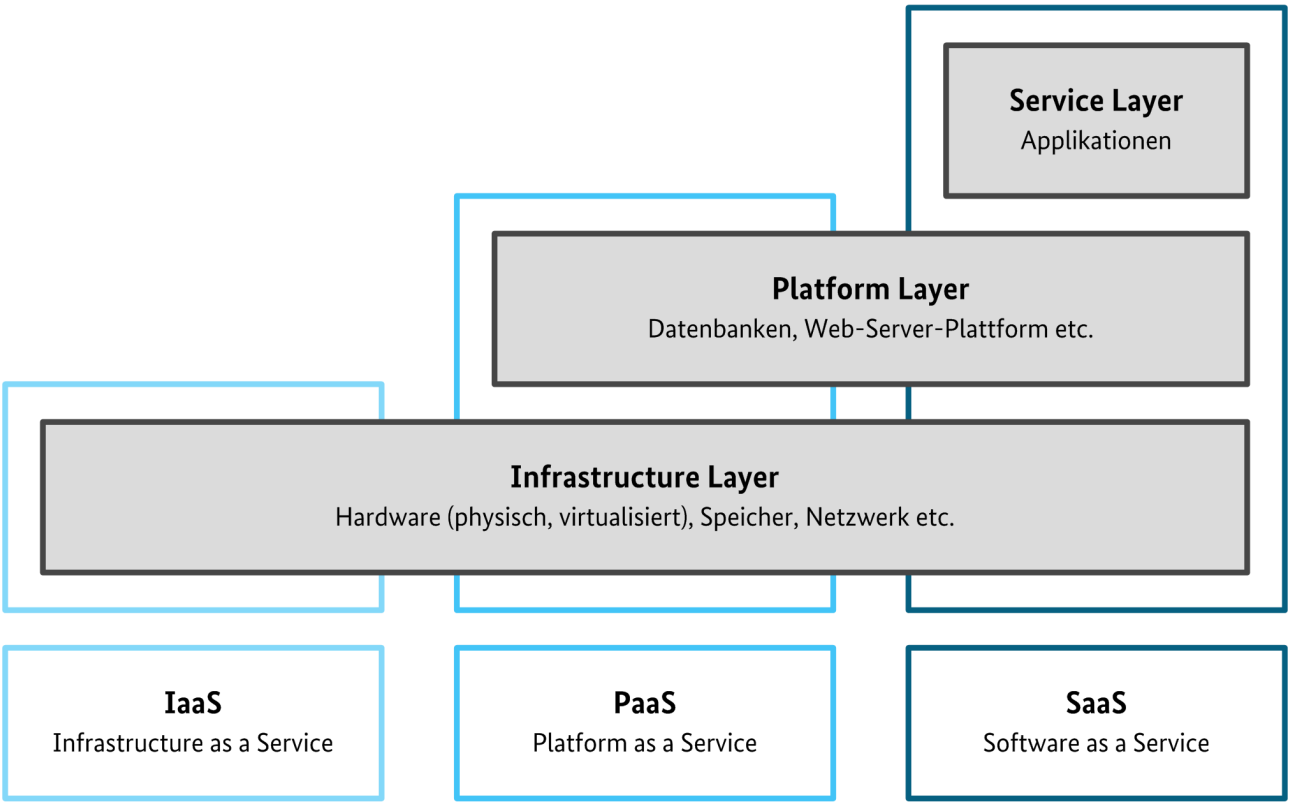


Abbildung 52: Cloud-Servicemodelle

8.2.1.2 Outsourcing

Beim Outsourcing werden Arbeits-, Produktions- oder Geschäftsprozesse einer Organisation ganz oder teilweise zu externen Dienstleistern ausgelagert. Typischerweise steht die benötigte Infrastruktur entweder im Rechenzentrum des Anbieters oder im Rechenzentrum des Outsourcing-Kunden und steht der Organisation exklusiv zur Verfügung (Ein-Mandanten-Prinzip). Zudem werden Outsourcing-Verträge meistens über längere Laufzeiten abgeschlossen. Outsourcing ist darüber hinaus geprägt durch individuelle und fest definierte Leistungen, die zu festen Rahmenbedingungen erbracht werden.

Weitere Informationen zu Outsourcing finden sich in Baustein B 1.11 „Outsourcing“ der BSI IT-Grundschutz-Kataloge.

Outsourcing ähnelt in vielen Aspekten dem Cloud Computing. Ein wesentlicher Unterschied besteht jedoch darin, dass beim Outsourcing die Leistungen in der Regel sehr umfangreich und individuell zugeschnitten sind, während beim Cloud Computing die Leistungen hochgradig standardisiert und sehr granular sind.

Aus technischer Sicht sind die Unterscheide nicht gravierend, auch wenn das Outsourcing die charakteristischen Eigenschaften des Cloud Computing wie z. B. die dynamische Skalierbarkeit nicht notwendigerweise erfüllt. Dennoch gelten hier die entsprechenden Gefährdungen und Sicherheitsmaßnahmen.

8.2.1.3 IP-Centrex

Mit IP-Centrex wird die Übernahme des Prinzips von Centrex auf Voice over IP bezeichnet. Bei diesem Bereitstellungsmodell werden die Funktionen einer TK-Anlage durch einen Dienstleister im öffentlichen Netz zur Verfügung gestellt.

Grundlage hierfür sind Funktionen, wie sie typischerweise durch eine TK-Anlage für eine geschlossene Kommunikationsgruppe bereitgestellt werden. So werden zwischen den angeschlossenen Teilnehmern anlagenspezifische Leistungsmerkmale ermöglicht.

Je nachdem, ob der Anbieter hierfür jeweils eine dezidierte oder mandantenfähige TK-Anlage einsetzt, ist IP-Centrex aus technischer Sicht mit einer Private Cloud bzw. Virtual Private Cloud vergleichbar. Ähnlich wie beim Outsourcing erfüllt IP-Centrex jedoch die charakteristischen Eigenschaften des Cloud Computing nicht. Dennoch gelten auch hier die entsprechenden Gefährdungen und Sicherheitsmaßnahmen.

8.2.1.4 Unified Communications aus der Cloud

Die Nutzung von Cloud-Diensten verspricht Organisationen eine Reihe von Vorteilen, z. B. die Einsparung von teilweise erheblichen Investitionen, keine längerfristige Kapitalbindung und Skalierbarkeit. Auf der anderen Seite soll Unified Communications die zunehmenden Anforderungen an die ortsunabhängige interne und externe Kommunikation von Organisationen unterstützen. Um die Vorteile beider Themenkomplexe miteinander zu vereinen, bietet eine zunehmende Anzahl von Dienstleistern UC-Dienste aus der Cloud an. Hierfür hat sich der Begriff UC as a Service (UCaaS) etabliert. Unter den Anbietern finden sich Technologie-Hersteller und Systemintegratoren sowie Telekommunikations-anbieter und reine Cloud-Service-Anbieter. Dabei sprechen die Anbieter durchaus unterschiedliche Zielgruppen an. Während einige Anbieter mit ihren Public-Cloud-Angeboten eher auf den Privatanwender ausgerichtet sind, zielen die Angebote anderer Anbieter in erster Linie auf den professionellen Einsatz in Organisationen ab. Deren Angebote umfassen UC-Dienste sowohl aus der Public Cloud oder Virtual Private Cloud, aber auch aus Private Clouds, die im Rechenzentrum der Organisation oder im Rechenzentrum des Anbieters angesiedelt sein können. Für professionelle UCaaS-Angebote können folgende Betreibermodelle unterschieden werden:

- UCaaS aus der Public Cloud
- UCaaS aus der Virtual Private Cloud
- UCaaS aus der Private Cloud im Rechenzentrum des Anbieters
- UCaaS aus der Private Cloud im Rechenzentrum der Organisation

Grundsätzlich ist festzuhalten, dass auf alle genannten Betreibermodelle die jeweiligen Gefährdungen und Sicherheitsmaßnahmen, die für die zugrunde liegenden Technologien Voice over IP (siehe Kapitel 4), Unified Communications and Collaboration (siehe Kapitel 6), Soziale Netzwerke und Medien (siehe Kapitel 8.1) sowie Einbindung mobiler Endgeräte (siehe Kapitel 9) genannt sind, zutreffen und zu berücksichtigen sind. Darüber hinaus sind an den Anbieter der Cloud-Dienste die Sicherheitsanforderungen zu stellen, die in [BSI Bro314-2012] beschrieben sind.

UCaaS aus der Public Cloud

Dieses Betreibermodell muss für den Einsatz in Organisationen genau untersucht werden und mit den jeweiligen Sicherheitsanforderungen verglichen werden. Public Clouds zeichnen sich u. a. durch eine mangelnde Mandantenfähigkeit aus: Die Abrechnung der genutzten Cloud-Ressourcen mag zwar mandantenfähig sein, eine vollständige (logische) Trennung der Ressourcen und gespeicherten Daten in den Back-End-Systemen erfolgt jedoch nicht. Aus diesem Grund kann dieses Betreibermodell für den professionellen Einsatz möglicherweise geeignet sein, falls die eigenen Sicherheitsanforderungen sehr niedrig sind. Für Organisationen mit erhöhtem Schutzbedarf ist es allerdings gänzlich ungeeignet, da Vertraulichkeit, Verfügbarkeit und Integrität nicht gewährleistet sind.

UCaaS aus der Virtual Private Cloud

Auch dieses Modell ist für den professionellen Einsatz nur bedingt geeignet, da aufgrund der potenziell unsicheren logischen Trennung die Vertraulichkeit, Verfügbarkeit und Integrität nicht sichergestellt werden kann. Für Organisationen mit erhöhtem Schutzbedarf ist es ebenfalls gänzlich ungeeignet.

UCaaS aus der Private Cloud im Rechenzentrum des Anbieters

Sofern der Anbieter die in [BSI Bro314-2012] genannten Anforderungen erfüllt, kann dieses Betreibermodell auch für Organisationen mit erhöhtem Schutzbedarf in Betracht kommen. Dabei wird vorausgesetzt, dass eine Private Cloud mit einer dezidierten Umgebung für die jeweilige Organisation bereitgestellt wird und nicht mehrere Mandanten bedient. Um den erhöhten Schutzbedarf hinsichtlich Verfügbarkeit sicherzustellen, muss dabei zusätzlich zu den zugrunde liegenden Technologien auch die Vertraulichkeit, Verfügbarkeit und Integrität der Netzwerkverbindung zwischen der Organisation und dem Anbieter sichergestellt sein.

UCaaS aus der Private Cloud im Rechenzentrum der Organisation

Dieses Betreibermodell kann ebenfalls auch für Organisationen mit erhöhtem Schutzbedarf in Betracht kommen, sofern der Anbieter die in [BSI Bro314-2012] genannten Anforderungen erfüllt. Auch hier wird vorausgesetzt, dass die Private Cloud in einer dezidierten Umgebung läuft und damit nicht mehrere Mandanten bedient. Betrachtungen und Überlegungen zur Vertraulichkeit, Verfügbarkeit und Integrität der Netzwerkverbindung zwischen der Organisation und dem Anbieter entfallen, da die Private Cloud im Rechenzentrum der Organisation betrieben wird und damit diese Netzwerkverbindung entfällt. Es sind jedoch die Netzwerkverbindungen in das Rechenzentrum der Organisation zu berücksichtigen, die der Anbieter zu Management-Zwecken unterhält.

Im Folgenden werden die spezifischen Gefährdungen und Sicherheitsmaßnahmen von UCaaS näher beschrieben.

8.2.2 Gefährdungen

8.2.2.1 Höhere Gewalt

Beim Einsatz von Cloud-Diensten treten allgemein die Gefährdungen durch höhere Gewalt, die in den BSI IT-Grundschutz-Katalogen (siehe [BSI GSK-2013]) genannt sind, auf. Hier ist insbesondere zu beachten, dass die Gefährdungen in erster Linie auf den Dienstleister zutreffen, dass also dieser die entsprechenden Maßnahmen umsetzten muss. Bedingt durch die Abhängigkeit vom Wide Area Network (WAN) beziehungsweise Internetzugang müssen die Gefährdungen durch höhere Gewalt für die entsprechenden Schnittstellen besonders beachtet werden.

8.2.2.2 Organisatorische Mängel

In Bezug auf mögliche organisatorische Mängel sind insbesondere die Gefährdungen der UCC-Technologie (siehe Kapitel 6.2.2) sowie die des Bausteins B 1.11 „Outsourcing“ der IT-Grundschutz-Kataloge zutreffend. Hierbei treten die Gefährdungen jedoch hauptsächlich auf Seiten des Dienstleisters auf, sodass dieser die zutreffenden Maßnahmen umsetzen muss. Andererseits gelten gerade im Bezug auf die Nutzung von Public-Cloud-Diensten zusätzlich noch folgende Gefährdungen:

G-TK-130 Fehlende Regelungen und Mechanismen zur Trennung auf Multi-Mandanten-Plattformen

Wenn wie im Falle einer Public Cloud oder Virtual Private Cloud die zur Verfügung gestellte Plattform samt Infrastruktur nicht ausschließlich der eigenen Organisation, sondern zusätzlich weiteren Teilnehmern zur Verfügung gestellt wird, besteht die Gefahr, dass die Trennung der einzelnen Mandanten nicht in ausreichender Form geschieht. Dies stellt vor allem auf der Verwaltungsebene aber auch auf der Datenebene ein Problem dar, denn ohne

geeignete Mechanismen zur Trennung der Mandanten können Daten der Organisation gegebenenfalls durch weitere Mandanten missbräuchlich genutzt werden.

G-TK-131 Unzureichende Regelungen in Bezug auf Wartungsarbeiten

Da der Betrieb und damit insbesondere die Wartung der genutzten Dienste nicht von der Organisation selbst, sondern in Verantwortlichkeit des Dienstleisters ausgeführt werden, besteht hier eine direkte Abhängigkeit vom jeweiligen Dienstleister. Insbesondere fehlende oder unzureichende Regelungen zu geplanten wie ungeplanten Wartungsarbeiten stellen eine wesentliche Gefährdung dar, da in der Zeit möglicherweise einige Dienste oder gar die gesamte Kommunikation nicht zur Verfügung stehen.

8.2.2.3 Menschliche Fehlhandlungen

Durch die Auslagerung der gesamten Kommunikation zu einem externen Dienstleister treten die Gefährdungen durch menschliche Fehlhandlungen sowohl auf Seiten des Dienstleisters wie auch auf Seiten der Organisation auf. Relevant sind daher insbesondere die Gefährdungen, die im Baustein B 1.11 „Outsourcing“ im IT-Grundschutz-Katalog genannt werden, sowie die folgenden Gefährdungen aus den IT-Grundschutz-Katalogen:

- G 3.3 „Nichtbeachtung von Sicherheitsmaßnahmen“
- G 3.13 „Weitergabe falscher oder interner Informationen“
- G 3.16 „Fehlerhafte Administration von Zugangs- und Zugriffsrechten“
- G 3.43 „Ungeeigneter Umgang mit Passwörtern“
- G 3.44 „Sorglosigkeit im Umgang mit Informationen“

8.2.2.4 Technisches Versagen

Bei der Nutzung von Cloud-Diensten kann es hauptsächlich auf Seiten des Dienstleisters zu technischem Versagen kommen. Daher muss der Dienstleister sicherstellen, dass die hier relevanten Gefährdungen, die in den IT-Grundschutz-Katalogen genannt werden, in angemessener Weise berücksichtigt werden. Jedoch ist auch das Netz zwischen Dienstleister und Organisation anfällig für Gefährdungen hinsichtlich technischem Versagen. Das gilt insbesondere dann, wenn der genutzte Cloud-Dienst nicht im Rechenzentrum der Organisation betrieben wird. Daher sind zusätzlich folgende Gefährdungen zu beachten:

G-TK-132 Mangelnde Verfügbarkeit des Weitverkehrsnetzes beziehungsweise des Netzes zwischen Dienstleister und Organisation

Das Netz zwischen Dienstleister und Organisation spielt in Bezug auf die genutzten Dienste eine tragende Rolle, da bei einem Ausfall des Netzes keinerlei Dienste genutzt und damit insbesondere keinerlei Kommunikation getätigt werden können.

G-TK-133 Versagen der Mechanismen zur Trennung auf Multi-Mandanten-Plattformen

Bei Nutzung von Multi-Mandanten-Plattformen kann ein Versagen der Mechanismen zur Trennung von Mandantendaten dazu führen, dass trotz entsprechender Mechanismen die Daten nicht ausreichend geschützt sind. Ist dies der Fall, können personenbezogene Daten wie z. B. Nutzerdaten sowie Dokumente oder sonstige Informationen der Organisation einem großen Personenkreis zugänglich sein.

8.2.2.5 Vorsätzliche Handlungen

Durch den Einsatz eines Dienstleisters, der die entsprechenden UCC-Dienste mittels einer Cloud-Lösung betreibt, ergeben sich eine Vielzahl an Gefährdungen durch vorsätzliche Handlungen. Dies liegt zum einen daran, dass die eigene Organisation nicht primär für den Betrieb der Dienste verantwortlich ist, zum anderen aber auch daran, dass der Zugriff auf die Dienste in der Regel über das öffentliche Internet realisiert wird. Daher sind neben den bekannten Gefährdungen aus den IT-Grundschutz-Katalogen noch die folgenden Gefährdungen zu betrachten:

G-TK-134 Abhören von Leitungen / Lauschangriff im Netz des Dienstleisters

Durch Nutzung eines Weitverkehrsnetzes beziehungsweise des Internets, das sich nicht in unmittelbarer Kontrolle der Organisation befindet, besteht die Gefahr, dass Kommunikation, die über diese Leitungen geführt wird, abgehört und mitgeschnitten werden kann.

G-TK-135 Abfluss von Daten aus dem Netz des Dienstleisters

Da die Daten bei der Nutzung von Cloud-Diensten nicht dem unmittelbaren Zugriff durch die Organisation unterliegen, besteht keine vollständige Kontrolle über den Einsatz, die Verarbeitung und die Verbreitung der Daten. Wenn die Daten nicht ausreichend gegen den Zugriff durch andere geschützt sind, können so sensible Daten und Informationen die Organisation verlassen und damit in Hände Dritter geraten.

Daten können jedoch nicht nur durch unzureichenden Schutz die Organisation unautorisiert verlassen. Dies trifft z. B. auch dann zu, wenn sich die Server, auf denen Daten und Informationen gespeichert sind, nicht in Deutschland befinden und regionale Gesetzte den Zugriff durch dortige Behörden erlauben.

G-TK-136 Manipulation und Verlust von Daten

In Analogie zur oben geschilderten Gefährdung durch den Abfluss von Daten bzw. Informationen kann ein unberechtigter Zugriff auf die Daten auch zur Manipulation der Daten oder im schlimmsten Falle zum unwiderruflichen Verlust der Informationen führen. Beispielsweise können Verbindungsdaten manipuliert werden. Ebenso können Benutzerdaten oder im Cloud-Service gespeicherte Dokumente manipuliert werden.

8.2.3 Sicherheitsmaßnahmen

Der Einsatz von Unified Communications in Kombination mit Cloud-Diensten bietet einerseits durch die flexible Nutzung und Abrechnung von benötigten Ressourcen nicht von der Hand zu weisende Vorteile, andererseits summieren sich die Gefährdungen beider Techniken auf. Um diesen Gefährdungen angemessen zu begegnen, müssen adäquate Maßnahmen zum Schutz der Kommunikation und der Daten getroffen werden. Zunächst ist festzuhalten:

- **Dienste aus der Public Cloud oder der Virtual Private Cloud sind bei dem aktuellen Stand der Technik für die Verarbeitung von Daten mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit oder Integrität nicht geeignet. Dies gilt auch für IP-Centrex-Dienste.**
- **Allenfalls Private-Cloud-Dienste oder klassische Outsourcing-Modelle können zum Einsatz kommen, allerdings auch nur, wenn geeignete Sicherheitsmaßnahmen umgesetzt werden.**

Die Bausteine B 1.11 „Outsourcing“ und B 5.21 „Webanwendungen“ der IT-Grundschutz-Kataloge bilden die Basis, deren Maßnahmen als Grundlage konsequent anzuwenden sind. Des Weiteren sind vom Dienstleister die im Eckpunktepapier „Sicherheitsempfehlungen für Cloud Computing Anbieter“ genannten Maßnahmen einzufordern (siehe [BSI Bro314-2012]).

Der Maßnahmenkatalog zur Absicherung der Nutzung von Cloud- bzw. Outsourcing-Diensten im UCC-Bereich ist in die folgenden Blöcke aufgeteilt:

- Server und Anwendungen, siehe Kapitel 8.2.3.1
- Endgeräte und Clients, siehe Kapitel 8.2.3.2
- Netzwerk, siehe Kapitel 8.2.3.3
- Netz- und Systemmanagement, siehe Kapitel 8.2.3.4
- Übergreifende Aspekte, siehe Kapitel 8.2.3.5

8.2.3.1 Server und Anwendungen

M-TK-174 Konsequente Verschlüsselung bei Transport, Speicherung und Verarbeitung von Daten

Daten mit einem erhöhten Schutzbedarf hinsichtlich Vertraulichkeit oder Integrität sollten weder in einer Public Cloud noch in einer Virtual Private Cloud oder einem IP-Centrex-System verarbeitet werden. Kann aus wichtigen Gründen nicht darauf verzichtet werden, müssen die Daten sowohl bei Transport und Speicherung als auch bei der Verarbeitung angemessen verschlüsselt werden, d. h. es darf kein Verschlüsselungsendpunkt in der Cloud liegen. Hierzu können sogenannte homomorphe Verschlüsselungsmechanismen eingesetzt werden, da diese eine Verarbeitung der verschlüsselten Daten erlauben und somit die Daten während Transport, Speicherung und Verarbeitung durchgängig verschlüsselt sind.

Daten mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit oder Integrität, die in einer Private Cloud oder einem klassischen Outsourcing-Betrieb bei einem Dienstleister, d. h. außerhalb des eigenen Rechenzentrums, verarbeitet werden müssen, sind bei Transport und Speicherung zu verschlüsseln. Auch eine Verschlüsselung bei der Verarbeitung der Daten ist wie oben beschrieben wünschenswert.

Weiterhin darf generell das Schlüsselmaterial ausschließlich berechtigten Nutzern bekannt sein und das Schlüsselmanagement muss den Vorgaben für einen erhöhten Schutzbedarf genügen. Dies beinhaltet beispielsweise ein automatisiertes Schlüsselmanagement im Rahmen einer Authentisierung bzw. eine hinreichende Komplexität der Schlüssel in Verbindung mit einem regelmäßigen Schlüsselwechsel.

Wenn diese Maßnahme nicht hinreichend umgesetzt werden kann, muss auf die Speicherung und Verarbeitung von Daten auf externen Systemen eines Dienstleisters (insbesondere in einer Public Cloud, Virtual Private Cloud oder IP-Centrex) verzichtet werden und die Nutzung solcher Dienste auf Daten mit normalem Schutzbedarf beschränkt werden. Hierzu bietet sich der Einsatz von Konzepten aus dem Bereich Hybrid Cloud an (siehe Abbildung 53). Durch ein einheitliches Identitätsmanagement in Verbindung mit einem Berechtigungskonzept kann der Zugriff auf Daten dabei transparent für den Nutzer erfolgen.

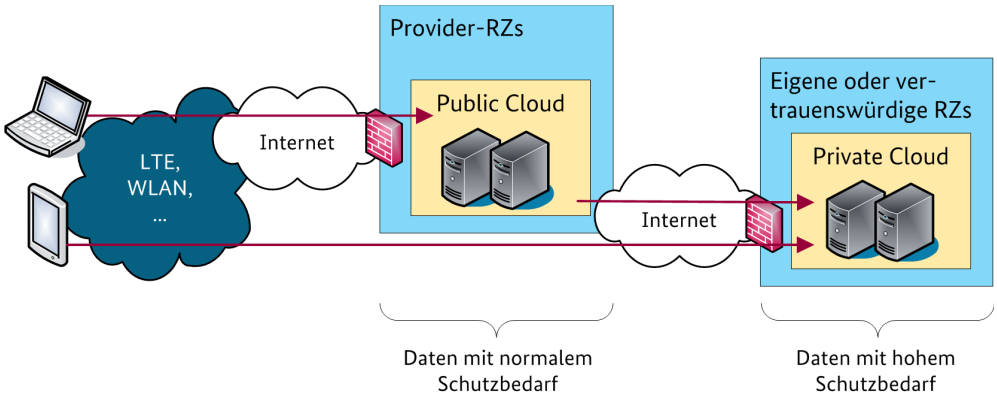


Abbildung 53: Nutzungsformen einer Hybrid Cloud für Daten mit normalem und erhöhtem Schutzbedarf

M-TK-175 Härtung der Virtualisierungsplattform

Beim Einsatz einer Private Cloud im eigenen Rechenzentrum (RZ) ist die Absicherung der gewählten Virtualisierungsplattform entsprechend Maßnahme M-TK-230 „Spezielle Absicherung von virtualisierten TK-Servern“ besonders wichtig, da gerade bei einer Private Cloud RZ-Automatierungstechniken zu einer erheblichen Dynamik virtueller Maschinen (VM) führen. Diese Dynamik kann insbesondere eine Vermischung von VMs unterschiedlichen Schutzbedarfs und Sicherheitsniveaus auf einer gemeinsamen Virtualisierungsplattform nach sich ziehen. Insbesondere muss die Virtualisierungsplattform dem Schutzbedarf der Daten angemessen gehärtet werden.

M-TK-176 Einsatz von UC-fähigem Virenschutz

Der in der Organisation eingesetzte Virenschutz muss in der Lage sein, die Verbreitung von Malware und anderer schadenstiftender Software zu verhindern, in Analogie zu M-TK-97 „Verhindern der Verbreitung von Malware und bösartigen Hyperlinks per Instant Messaging“. Diese Filterung ist jedoch nicht nur auf Instant Messaging zu beschränken, sondern auf alle gesendeten und empfangenen Nachrichtentexte und Dateiübertragungen anzuwenden.

8.2.3.2 Endgeräte und Clients

M-TK-177 Einsatz von Host-basierten DLP-Systemen bei Cloud-Nutzung

Um einen unberechtigten Abfluss von Daten in die Cloud zu verhindern, sollten Host-basierte Data-Loss-Prevention-Systeme (DLP-Systeme) eingesetzt werden. Diese Systeme stellen sicher, dass Daten nicht unbeabsichtigt über das Internet oder das Weitverkehrsnetz in die Cloud, also das Rechenzentrum des Dienstleisters, übertragen werden.

8.2.3.3 Netzwerk

Zum Schutz der Kommunikation sind zunächst die das Netzwerk betreffenden Maßnahmen, die schon im Kapitel 4.3 behandelt wurden, umzusetzen. Insbesondere sind geeignete Firewall-Systeme und Session Border Controller einzusetzen, gemäß G-TK-67 „Ungesicherte Aufzeichnung bzw. Protokollierung von Kommunikation“ sowie M-TK-69 „Erkennung und Abwehr von DoS-Angriffen gegen VoIP und von SPIT durch IPS / IDS“. Zusätzlich sollte noch die folgende Maßnahme umgesetzt werden:

M-TK-178 Einsatz von Netzwerk-basierten DLP-Systemen bei Cloud-Nutzung

Zur Verhinderung von unberechtigtem Datenverkehr sollten zusätzlich zu M-TK-177 „Einsatz von Host-basierten DLP-Systemen bei Cloud-Nutzung“ ebenfalls Netzwerk-basierte DLP-Systeme eingesetzt werden. Hiermit wird auf Netzwerkebene der Datenverkehr entsprechend kontrolliert, sodass Daten mit erhöhtem Schutzbedarf weder unbeabsichtigt noch vorsätzlich die Organisation verlassen können.

8.2.3.4 Netz- und Systemmanagement

Wird eine Private Cloud im eigenen Rechenzentrum betrieben, sind alle Maßnahmen der zugrunde liegenden Technologien VoIP und UCC (siehe Kapitel 4.3.4 und 6.3.4) anzuwenden. Beim Einsatz einer Private Cloud, die im Rechenzentrum des Dienstleisters betrieben wird, sind zusätzlich folgende Maßnahmen in Bezug auf das Management anzuwenden:

M-TK-179 Dem Schutzbedarf angepasste Überwachung der Dienste

Der Dienstleister muss sicherstellen, dass die zur Verfügung gestellten Dienste hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität entsprechend überwacht werden. Sollte es trotz der Überwachung zu einem sicherheitsrelevanten Vorfall kommen, obliegt es dem Dienstleister entsprechende Gegenmaßnahmen einzuleiten.

M-TK-180 Regelmäßige Erstellung von Berichten und Informationspflicht bei Sicherheitsvorfällen

Der Dienstleister muss in regelmäßigen Abständen Berichte über die korrekt durchgeführte Überwachung der Dienste bereitstellen. Des Weiteren hat der Dienstleister bei sicherheitsrelevanten Vorfällen die Organisation unverzüglich über die Art und Dauer des Vorfalls zu unterrichten. Dies entbindet den Dienstleister jedoch nicht von seiner Pflicht, jeglichen Vorfällen dieser Art in angemessener Weise zu begegnen und ihnen entgegen zu wirken.

8.2.3.5 Übergreifende Aspekte

M-TK-181 Nachweis und Überprüfung der Vertrauenswürdigkeit des Dienstleisters

Der Dienstleister, der mit der Implementierung und dem Betrieb der TK-Dienste, insbesondere der Cloud-Dienste beauftragt wird, ist hinsichtlich seiner Vertrauenswürdigkeit zu überprüfen.

M-TK-182 Einsatz von sicherheitsüberprüftem Personal

Das Personal, das für den Betrieb der TK-Dienste bzw. Cloud-Dienste verantwortlich ist, muss unabhängig davon, ob es sich um eigenes Personal oder um das Personal des Dienstleisters handelt, sicherheitsüberprüft sein. Nur so ist eine sichere Verarbeitung von Daten mit erhöhtem Schutzbedarf gewährleistet.

M-TK-183 Regelmäßige Auditierung der Infrastruktur des Dienstleisters

Gerade beim Einsatz von Diensten, die nicht im eigenen Rechenzentrum betrieben werden, ist eine regelmäßige Auditierung der Infrastruktur des Dienstleisters vorzunehmen. Hierbei sollte die regelmäßige Durchführung der Auditierung direkt Bestandteil des Vertrages zwischen Organisation und Dienstleister sein.

M-TK-184 Festlegung des Speicherortes der Daten bei Outsourcing und Cloud-Nutzung

Bei der Vertragsgestaltung ist ebenso darauf zu achten, dass der Speicherort der Daten, also insbesondere das Land, in dem die Server des Dienstleisters stehen, von vornherein festgelegt werden kann. Hierbei kann entweder explizit das Rechenzentrum oder nur das Land beziehungsweise die Region vorgeschrieben werden.

M-TK-185 Lesender Zugriff auf die vom Dienstleister bereitgestellten Komponenten

Der Dienstleister sollte der Organisation lesenden Zugriff auf die bereitgestellten Komponenten gewähren, damit diese hinsichtlich ihrer ordnungsgemäßen Funktionalität überprüft werden können. Außerdem ist nur so eine lückenlose Überwachung der Komponenten gewährleistet.

8.2.4 Zusammenfassung

Beim klassischen Outsourcing werden Prozesse einer Organisation ganz oder teilweise zu externen Dienstleistern ausgelagert. Neben diesem Modell verbreiten sich auch die folgenden externen Bereitstellungsdienste immer weiter:

- IP-Centrex: IP-basierte Bereitstellung von VoIP-Funktionen durch den Betreiber des IP-Netzes
- Cloud Computing: Bereitstellung von Diensten und Infrastruktur in einer Cloud
- UCaas: Unified Communications as a Service, bei denen UC-Dienste in einer Private Cloud, Public Cloud, Virtual Private Cloud oder Hybrid Cloud zur Verfügung gestellt werden

Als Cloud wird dabei eine schnelle, durch den Kunden selbst initiierbare Bereitstellung von Ressourcen und die Nutzung dieses (virtualisierten) Ressourcen-Vorrats bezeichnet. Allgemeine Merkmale einer Cloud sind die flexible Skalierbarkeit, der netzbasierte Abruf der Leistungen und ein nutzungsabhängiges Preismodell.

Die wesentlichen Unterschiede zwischen den Cloud-Varianten ergeben sich aus dem jeweiligen Betreiber (Fremd- oder Eigenbetrieb), dem Standort (On Premise bzw. eigenes Rechenzentrum oder Nutzung des Betreiber-Rechenzentrums) und der geteilten Ressourcennutzung (dedizierte oder mit anderen Kunden gemeinsam genutzte Infrastruktur).

Auch wenn Kommunikationsinfrastrukturen im Rahmen von Outsourcing als IP-Centrex- oder Cloud-Dienst betrieben werden, unterliegen diese zunächst denselben Gefährdungen wie auch eigenständig betriebene Kommunikationslösungen. Es ergeben sich jedoch zusätzliche Gefährdungen durch

- zusätzliche Netzübertragungswege,
- den mangelnden Einfluss auf die umgesetzten Sicherheitsmaßnahmen,
- den Kontrollverlust über die Datenhaltung und -absicherung extern gespeicherter Daten sowie
- die Nutzung von Ressourcen durch mehrere Mandanten, insbesondere bei mangelnden organisatorischen und technischen Mitteln zur Separation von Mandanten.

Es ist festzuhalten, dass unter den derzeitigen technischen und vertraglichen Gegebenheiten bei erhöhtem Schutzbedarf auf eine Nutzung von Outsourcing-Ansätzen mit geteilten Ressourcen – also UCaaS aus Public Cloud und Virtual Private Cloud sowie IP-Centrex – verzichtet werden muss.

Bei den dedizierten Formen von Outsourcing und Private Cloud müssen, neben den anzuwendenden Maßnahmen der zugrunde liegenden Technologien (siehe Kapitel 4.3 und 6.3), zusätzliche Maßnahmen ergriffen werden, um ein erhöhtes Schutzniveau zu erzielen. Diese Maßnahmen sind zumeist vertraglicher Natur, da nur auf diesem Wege Einfluss auf die technische Gestaltung der Gesamtlösung genommen werden kann. Die Umsetzung der notwendigen organisatorischen Maßnahmen und Einhaltung diesbezüglicher Standards muss durch den Dienstleister gewährleistet und in Form von Audits nach anerkannten Standards nachgewiesen werden.

Weitere Maßnahmen umfassen technische Ansätze zur Absicherung der durch den Kunden verantworteten Netzstrecken und -übergänge sowie Monitoring der Kommunikationsinfrastruktur und Meldung von Sicherheitsvorfällen in dieser durch den Dienstleister.

9 Einbindung Mobiler Endgeräte

Moderne Arbeitsmethoden zeichnen sich verstärkt durch mobile und nomadische Nutzung von IT-Ressourcen aus. Mobiltelefone sowie insbesondere Smartphones und Tablets sind seit geraumer Zeit zu einem Standardelement der IT-Infrastruktur von Unternehmen und Behörden geworden und immer mehr Mitarbeiter werden mit solchen Endgeräten ausgerüstet. Klassische Telefone und PCs verlieren in Folge dessen als TK-Endgeräte zunehmend an Bedeutung. In der Vergangenheit war die Telefonie die wesentliche Anwendung für die Anbindung mobiler Endgeräte an eine TK-Anlage. Dies hat sich mit Smartphones und Tablets sowie neuen leistungsfähigeren Mobilfunk- und WLAN-Technologien massiv geändert. Inzwischen ermöglicht das mobile Internet den Zugriff auf die gesamte Anwendungsvielfalt der IT durch mobile Endgeräte und liefert insbesondere im Bereich Unified Communications and Collaboration (UCC) einen erheblichen Mehrwert (siehe Kapitel 6). Damit werden automatisch sehr sensible Daten, z. B. vertrauliche personenbezogene Daten, auf mobilen Endgeräten verarbeitet und auch gespeichert.

Als Konsequenz ist die Wichtigkeit der sicheren Einbindung von mobilen Endgeräten in die TK-Infrastruktur einer Organisation enorm gestiegen.

Die Anbindung mobiler Endgeräte an die IT-Infrastruktur erfolgt über Mobilfunk oder über drahtlose lokale (schnurlose) Kommunikationstechniken, z. B. Wireless Local Areal Network (WLAN). Funkübertragungen sind dabei generell fehleranfällig und können leicht kompromittiert und dabei z. B. abgehört werden. Daher ist die Absicherung solcher Systeme beispielsweise mit kryptografischen Techniken essenziell. Gleichzeitig zeigen gerade die populären mobilen Betriebssysteme wie Android und iOS immer wieder signifikante Schwachstellen auf. Es kann sogar durchaus festgestellt werden, dass sich schadenstiftende Software, Überwachungstools bzw. -Apps und Angriffswerkzeuge (insbesondere für Lauschattacken) verstärkt auf mobile Endgeräte konzentrieren.

9.1 Basiswissen

Mobile Endgeräte wie Smartphones und Tablets stellen eine eigene Kategorie von Endgeräten dar, die mit spezifischen Betriebssystemen laufen. Zunächst werden in Kapitel 9.1.1 die wesentlichen Betriebssysteme kurz vorgestellt und anschließend in Kapitel 9.1.2 die Möglichkeiten der Anbindung an die IT-Infrastruktur kurz dargestellt. Ein besonders wichtiger Aspekt, insbesondere aus dem Blickwinkel der Informationssicherheit, ist dabei die Verwaltung mobiler Endgeräte (Mobile Device Management, MDM), wie in Kapitel 9.1.3 beschrieben. Mit diesen Mitteln ist weitergehend sogar eine Integration von organisationsinterner Telekommunikation (TK) und Mobilfunk möglich (siehe Kapitel 9.1.4).

Der Zugriff auf organisationsinterne Ressourcen durch mobile Endgeräte erfolgt verstärkt über ein Mobilfunknetz und dessen Anbindung an das Internet bzw. direkt an die jeweilige Organisation. Die grundlegenden Techniken und Sicherheitsmechanismen in Mobilfunknetzen werden kurz in Kapitel 9.1.5 skizziert.

Für die organisationsinterne Telekommunikation sind schnurlose Anbindungen von Endgeräten nicht neu. Digital Enhanced Cordless Telecommunications (DECT) ist ein seit Jahren bewährtes System. Auf der Seite der IT-Infrastrukturen hat sich aber mit WLAN eine Technik entwickelt, die mit der Konvergenz von Sprache und Daten auch immer attraktiver für die Sprachübertragung wird. Die grundlegenden Konzepte und Sicherheitsmechanismen für den WLAN-Einsatz werden in Kapitel 9.1.6 vorgestellt. Abschließend werden die Systeme DECT (Kapitel 9.1.7) und Bluetooth (Kapitel 9.1.8) betrachtet.

9.1.1 Mobile Endgerätetypen und mobile Betriebssysteme

Die Palette mobiler Endgeräte reicht heute von traditionellen Mobiltelefonen über Smartphones, Tablets und Notebooks bis hin zu Hybridformen[27].

Smartphones sind dabei eine Kombination von Mobiltelefon und Personal Digital Assistant (PDA) und haben PDAs praktisch vom Markt verdrängt. Als Basissystem findet man PDAs nur noch in Spezialgeräten wie z. B. manchen Barcode-Scannern.

Tablets sind aus der Kreuzung der Funktionalität und Bediensystematik des Smartphones mit dem Format eines miniaturisierten Notebooks, dem sogenannten Netbook entstanden. Im Gegensatz zum Smartphone verzichten die meisten Tablets auf eine unmittelbare Telefonfunktion, auch wenn die Geräte meist über eine Mobilfunk-Schnittstelle verfügen, um Datendienste nutzen zu können. Durch das größere Display sind Tablets prinzipiell auch für komplexere Anwendungen geeignet. Allerdings stellt die Nutzerschnittstelle häufig insbesondere hinsichtlich der Anbindung von Maus und Tastatur eine gewisse Einschränkung dar.

Trotzdem gilt insgesamt, dass viele Anforderungen, denen früher nur ein PC gerecht wurde, nun mit eben diesen mobilen Endgeräten abgedeckt werden können.

Speziell Smartphones vereinen dabei nicht nur Telekommunikation, UCC und PC-Anwendungen, es entstehen auch vollständig neue Nutzungsformen durch die Kombination der Kommunikationsmöglichkeiten. Smartphones sind üblicherweise mit einer Kamera und einem Empfänger für das Global Positioning System (GPS) ausgerüstet. Hiermit ist mehr als Fotografieren und Navigation möglich. Beispielsweise kann die Umgebung des Smartphones erkannt werden und es können positionsabhängig Dienste bereitgestellt werden. Eine solche „erweiterte Realität“ (engl. Augmented Reality)[28] ist erst mit Smartphones und Tablets für einen breiteren Nutzerkreis möglich geworden. Auch wenn solche Anwendungen derzeit oft noch im Consumer-Bereich verwurzelt sind, sind Anwendungspotenziale in Unternehmen und Behörden vorhanden. Diese Möglichkeiten bergen natürlich auch erhebliche Risiken für die Informationssicherheit und den Datenschutz. Die vielfältigen Varianten der Erstellung von Bewegungsprofilen, z. B. durch unberechtigtes Abgreifen von Positionsdaten durch eine App oder sogar durch den Hersteller des Betriebssystems selbst, sind nur eine Facette der resultierenden Bedrohungen.

Neben einer nahezu unüberschaubaren Vielzahl von Hardware-Herstellern konkurrieren verschiedene Betriebssysteme in unterschiedlichen Ausprägungen um den Markt der mobilen Endgeräte. Beispiele für Betriebssysteme für Smartphones und Tablets sind Google Android, Apple iOS, Windows Phone 8 (bzw. Windows 8 für Tablets) und RIM Blackberry 10.

Typisch für diese Betriebssysteme ist die Kapselung der Anwendungen (Apps) in sogenannten Sandboxes, über die kein direkter Zugriff auf den Speicher anderer Apps erlaubt ist und deren Kommunikation untereinander und deren Zugriff auf System-Ressourcen eingeschränkt ist, wie in Abbildung 54 exemplarisch dargestellt.

27 Außerdem gibt es immer mehr Spezialgeräte (z. B. Messgeräte oder Anlagen), die über Mobilfunk an eine Zentrale z. B. zur Auswertung von Messungen und zur Wartung angebunden werden. Solche Spezialgeräte werden allerdings in der vorliegenden Technischen Leitlinie nicht weiter betrachtet.

28 Augmented Reality kombiniert die realen Wahrnehmungen eines Menschen mit durch Computer bzw. Smartphones erzeugten Ergänzungen, die in Echtzeit die realen Wahrnehmungen aufwerten. Bekannte Beispiele von Augmented Reality sind das Einblenden der Bestmarke beim Skispringen im Fernsehen sowie das Anzeigen von zusätzlichen Informationen zu Sehenswürdigkeiten im Smartphone.

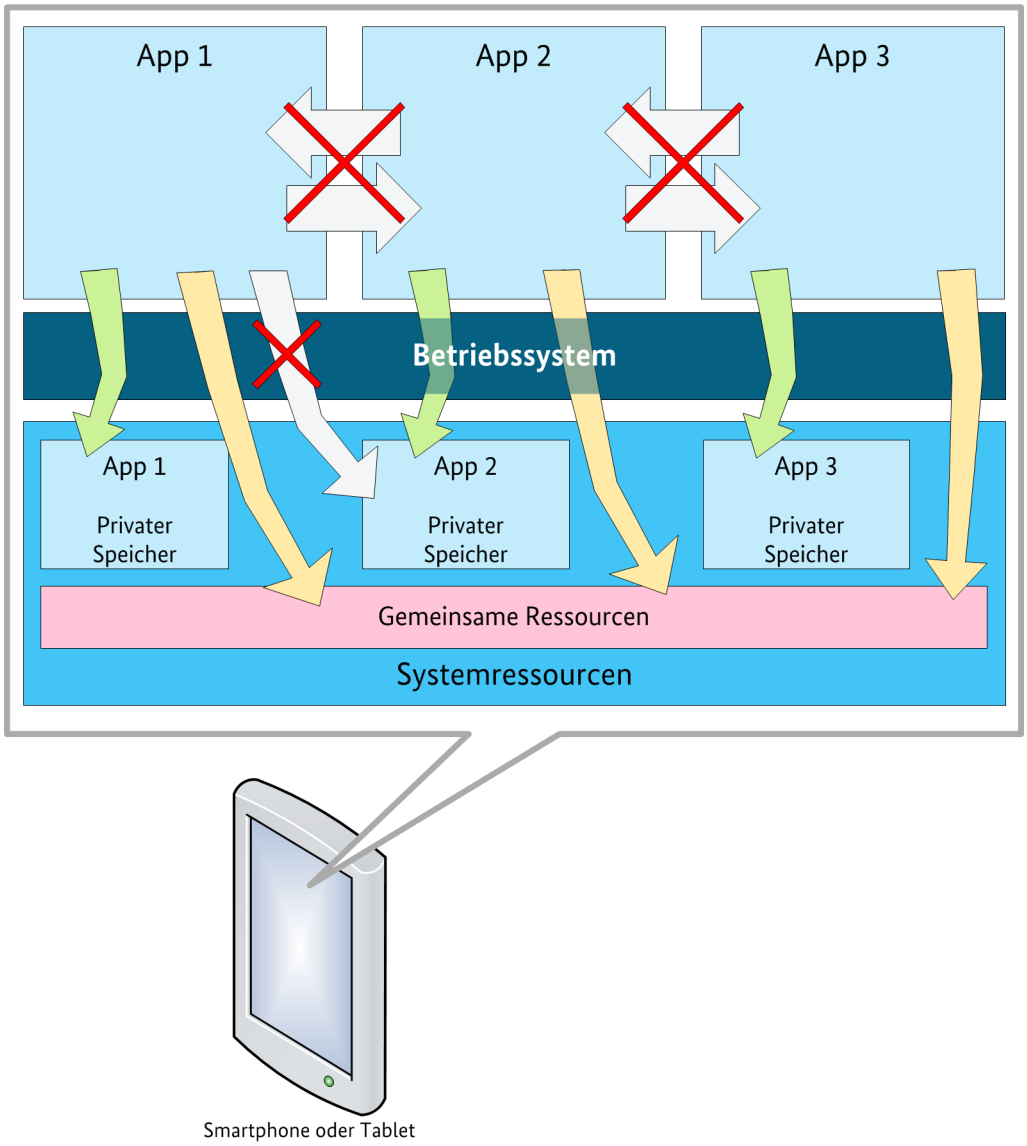


Abbildung 54: Exemplarische Darstellung des Sandbox-Prinzips

Android verwendet beispielsweise zur Ausführung von Applikationen virtuelle Maschinen, wodurch eine grundlegende Kapselung erzielt wird. Eine Android App kann, neben dem privaten Speicherbereich, lesend auf ein gemeinsames, unverschlüsseltes Dateisystem für Nutzerdaten zugreifen. Der Arbeitsspeicherinhalt wird ebenfalls nicht verschlüsselt. Unter Android sind Applikationen durch ein Rechtesystem voneinander getrennt. Anwendungen können aber immer eine Liste der installierten und ausgeführten Programme einsehen und andere Applikationen starten. Zudem können während der Installation weitere Rechte durch den Nutzer angefordert werden (z. B. Zugriff auf Ortsinformationen), die der Anwender gewähren darf. So kann das Rechtesystem zur Kontrolle der Systemressourcen aufgeweicht werden.

Anhand dieses Beispiels wird deutlich, dass die Betriebssystem-eigenen Sandboxing-Mechanismen zwar geeignet sind, um Applikationen voneinander zu isolieren, nicht jedoch, um den Zugriff auf Systemressourcen zu unterbinden. Zudem können Exploits im Betriebssystem genutzt werden, um die Isolation der Anwendungsdaten zu durchbrechen.

Die Sicherheitsfunktionen, die auf Ebene der mobilen Endgeräte zu erwarten sind, entsprechen grundsätzlich denen, die auch für konventionelle PCs etabliert sind, und beinhalten unter anderem folgende Punkte:

- Verschlüsselung der auf dem mobilen Endgerät gespeicherten Daten auf Ebene des Betriebssystems und bei Bedarf ergänzend auf Ebene der Apps
- Zugangsschutz durch Authentisierung des Nutzers durch PIN bzw. Passwort am mobilen Endgerät und bei Bedarf dedizierte Authentisierung für die Nutzung spezifischer Apps
- Befristete oder vollständige Sperre und ggf. sogar Löschung (engl. Wipe) des mobilen Endgerätes bzw. einer App bei mehrfacher fehlerhafter Authentisierung
- Automatische Sperrung bei Inaktivität des Nutzers für einen gewissen Zeitraum
- Kontrolle und Einschränkung der Berechtigungen von Apps

Rollen und Berechtigungskonzepte für mobile Endgeräte, die es beispielsweise dem Nutzer nicht erlauben würden, gewisse Systemeinstellungen zu ändern, sind oft nicht von Betriebssystemen für mobile Endgeräte vorgesehen bzw. nur rudimentär umsetzbar. Daher ist die Kontrolle der Konfiguration und das Erzwingen von Einstellungen durch ein zentrales Mobile Device Management (MDM) von besonderer Bedeutung (siehe Kapitel 9.1.3).

Viele heute besonders populäre mobile Endgeräte und ihre Betriebssysteme adressieren den Consumer-Markt. Dies wird insbesondere in der Art und Weise deutlich, wie Apps über sogenannte App Stores, die spezifisch für die mobilen Betriebssysteme sind, den Nutzern zur Verfügung gestellt werden. Ein Nutzer wird hier im Normalfall nicht hinsichtlich der Auswahl einer App eingeschränkt. Konzepte, die sicherstellen, dass ein Nutzer nur eine beschränkte, ggf. gruppenspezifische Auswahl von Anwendungen erhält, die entsprechend geprüft und zugelassen sind, werden mit sogenannten Company (oder Enterprise) App Stores umgesetzt, die jedoch auf der Basis der Kanäle für die systemspezifischen App Stores aufgebaut sind (siehe Kapitel 9.1.3).

Allgemein spricht man bei dem Trend, verstärkt Consumer-Produkte (Geräte und Software) in der IT einer Organisation einzusetzen, von der „Consumerization of IT“. Dieser Trend hat erhebliche Konsequenzen für die Informationssicherheit, da bei Consumer-Produkten eher nicht davon auszugehen ist, dass bei der Produktentwicklung auch Anforderungen der Informationssicherheit umfänglich beachtet werden und dass Sicherheitsmaßnahmen, die z. B. bei PCs seit Jahren etabliert sind, sich ohne Probleme auch auf diese Consumer-Produkte anwenden lassen.

Kernelement der Absicherung mobiler Endgeräte ist der Schutz der dienstlichen Daten vor unberechtigten Zugriffen. Im Idealfall werden auf dem mobilen Endgerät keine dienstlichen Daten verarbeitet und gespeichert, sondern lediglich angezeigt, wie es bei einem Zugriff über Server-based Computing, d. h. über ein Terminal-Server-Protokoll, der Fall ist (siehe hierzu auch Kapitel 4.1.9). Dies ist allerdings oft nicht praktikabel, da offline (z. B. in einem Funkloch) kein Zugriff auf Anwendung und Daten bestünde. In Folge dessen kann oft auf Anwendungslogik und Datenhaltung auf den Endgeräten nicht verzichtet werden.

Erschwerend kommt hinzu, dass die private Nutzung mobiler Endgeräte insbesondere angesichts moderner Arbeitsmethoden oft kaum noch untersagt, geschweige denn unterbunden werden kann. In dieser Lage ist die sichere Trennung von dienstlichen Daten und privaten Daten auf Smartphone und Tablet unerlässlich.

Zur Datentrennung sind zunächst Container-Technologien zu nennen, die auf Ebene einer App eine Umgebung für Verarbeitung und Speicherung von dienstlichen Daten liefern können. Konsequenter ist der Einsatz von Virtualisierungstechniken, bei denen über einen Hypervisor das Endgerät zwischen einem privaten und einem dienstlichen Kontext umschalten kann.

Unterschiedliche Techniken sind dabei auf dem Markt verfügbar:

- Typ-2-Hypervisoren werden auf Ebene einer App realisiert, d. h. ein virtuelles Smartphone bzw. Tablet wird als App realisiert und benötigt hierfür erhebliche Rechte auf dem zugrunde liegenden Betriebssystem des Smartphones bzw. Tablets.
- Alternativ kann ein Hypervisor oder ein vergleichbarer Trennungsmechanismus in das Betriebssystem integriert werden.

- Besser ist der Einsatz eines Typ-1-Hypervisor, der direkt auf der Hardware des mobilen Endgerätes aufsetzt. Die eigentlichen Betriebssysteme und Apps laufen dann als virtuelle Maschine (VM) auf dem Hypervisor und werden auf dieser Ebene voneinander getrennt (siehe Abbildung 55). Hiermit kann eine besonders sichere Umgebung für des Vorhalten und das Umschalten zwischen privatem und dienstlichem virtuellem Smartphone bzw. Tablet geschaffen werden. Dabei können ergänzend zur Kapselung der Systeme durch Virtualisierung mit kryptografischen Mitteln insbesondere die Daten einer dienstlichen VM im Speicher und beim Datentransport zusätzlich geschützt werden.

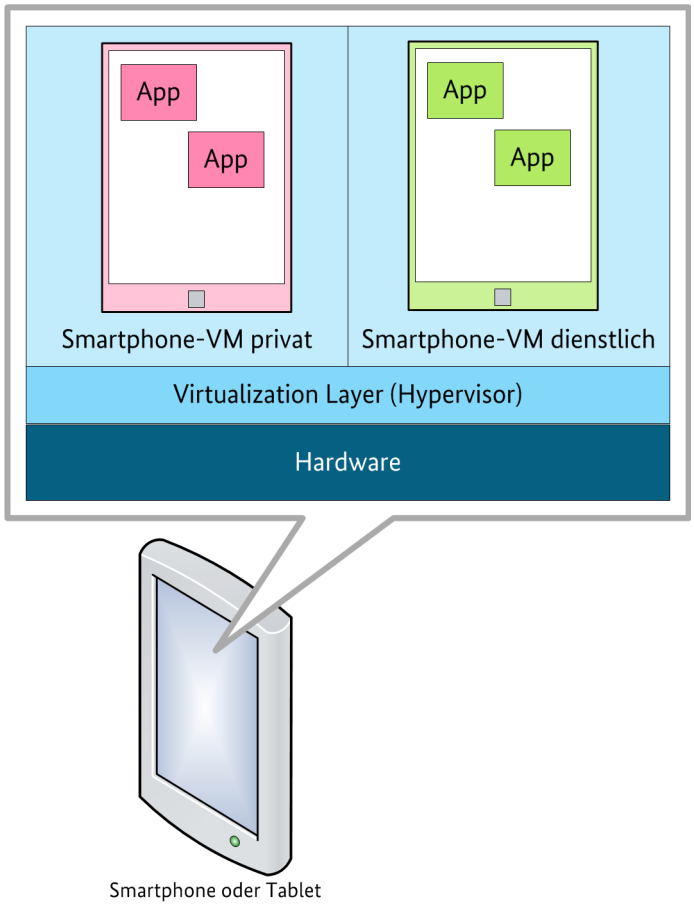


Abbildung 55: Virtualisierung von mobilen Endgeräten mit einem Typ-1-Hypervisor

In diesem Zusammenhang muss insbesondere auf abhörsichere Mobiltelefone hingewiesen werden, die umgangssprachlich auch als Cryptophones oder Krypto-Handys bezeichnet werden. Hierbei handelt es sich um proprietäre Produkte, welche – wie der Name bereits andeutet – zunächst die konsequente Verschlüsselung der Daten eines mobilen Endgerätes bei Transport und bei Speicherung auf dem Endgerät ermöglichen.

Diese Absicherung betrifft insbesondere auch die Sprachübertragung. Dabei wird – unabhängig von einer Verschlüsselung auf der Ebene des Mobilfunknetzes oder der schnurlosen Kommunikation – eine Ende-zu-Ende-Absicherung der Sprachübertragung entweder direkt zwischen den mobilen Endgeräten oder zwischen einem mobilen Endgerät und einem zentralen Gateway der Organisation hergestellt. In moderneren Produkten wird dabei vermehrt eine VoIP-Übertragung zur Infrastruktur der jeweiligen Organisation genutzt.

Darüber hinaus sind solche Endgeräte und entsprechende Hersteller, die für einen erhöhten Schutzbedarf infrage kommen, oft besonders geprüft, indem der Hersteller z. B. durch eine Zertifizierung nach Common Criteria[29] nicht nur einen Funktionsumfang, sondern auch seine Vertrauenswürdigkeit im Umgang mit

29 Common Criteria ist als internationaler Standard spezifiziert in ISO/IEC15408:2005 (Common Criteria Version 2.3) bzw. ISO/IEC15408:2006 (Common Criteria 3.1)

dem Produkt nachweist. Weiterhin sind bei abhörsicheren Mobiltelefonen für den Einsatz im Behördenumfeld entsprechende Zulassungen der Produkte für die Verarbeitung, Speicherung und Übertragung von Daten (inklusive Sprache), die als Verschlusssachen zu behandeln sind, zu beachten.

9.1.2 Infrastrukturanbindung mobiler Endgeräte

Mobiltelefone, Smartphones und Tablets haben eine entscheidende gemeinsame Eigenschaft: Sie kommunizieren ausschließlich (von USB-Synchronisation abgesehen) über drahtlose Techniken, d. h. primär Mobilfunk oder WLAN. Bei WLAN kann dabei sowohl ein öffentlicher Zugang (WLAN-Hotspot) als auch ein Zugang über die eigene Infrastruktur auf dem Campus einer Organisation genutzt werden.

Der Zugriff auf Daten im Netz einer Organisation erfolgt oft über das Internet, auf das über Mobilfunk oder über einen WLAN-Hotspot ein Zugang hergestellt wird. Zum Einsatz kommen dabei Webapplikationen, Webportale, Virtual Private Network (VPN, z. B. auf Basis von IP Security (IPsec) oder Transport Layer Security, TLS) oder Server-based Computing. Die Übertragung wird dabei mit den Mitteln abgesichert, die auch für die Remote-Anbindung von PCs eingesetzt werden, d. h. Authentisierung beispielsweise mit Zertifikaten, Verschlüsselung der Kommunikation z. B. mit Advanced Encryption Standard (AES) sowie Entkopplung der Kommunikation durch Gateways in einer Demilitarized Zone (DMZ) für die Außenanbindung. Abbildung 56 illustriert das Grundprinzip.

Bei einem WLAN-Zugang auf dem Campus einer Organisation ist grundsätzlich ein direkter Zugang zu Ressourcen möglich, sofern die Kommunikation auf der Luftschnittstelle angemessen abgesichert ist (siehe Kapitel 9.1.6).

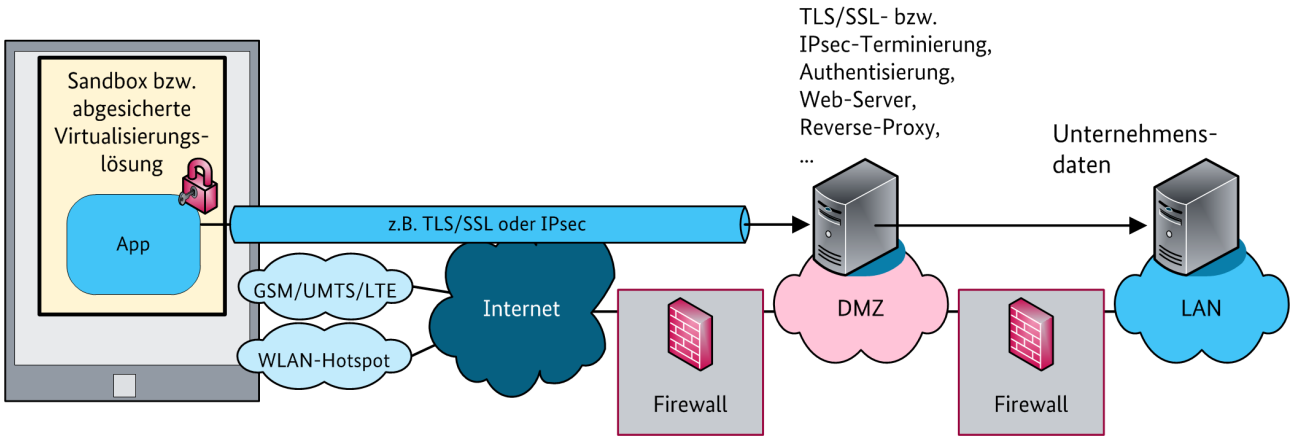


Abbildung 56: Mobiler Zugriff auf Daten in der Infrastruktur einer Organisationen

Eine weitere Form der Anbindung mobiler Endgeräte ist der sogenannt Private Access Point Name (APN). Dabei wird durch den Mobilfunkbetreiber der paketvermittelte Datenverkehr eines mobilen Endgerätes nicht in das Internet ausgekoppelt, sondern über ein VPN an einen Router in der jeweiligen Organisation geschickt, der der Private APN zugeordnet ist. Weitere Details zur Realisierung eines Private APN sind in Kapitel 9.1.5 zu finden.

Für die Sprachkommunikation wird entweder der Sprachdienst des Mobilfunknetzes genutzt oder die Übertragung erfolgt über Voice over IP (VoIP) unter Verwendung einer entsprechenden Softphone-App bzw. UCC-App auf dem Smartphone oder Tablet. Bei Nutzung von VoIP wird entweder das VoIP-System der jeweiligen Organisation oder ein Provider-Dienst genutzt, wie in Kapitel 4.1 beschrieben.

In diesem Zusammenhang ist der Standard „Sichere Netzübergreifende Sprachkommunikation“ (SNS) des Bundesamt für Sicherheit in der Informationstechnik (BSI) von besonderer Bedeutung (siehe hierzu [BSI Bro321-2012]). Kernelement dieser Technik ist zunächst eine spezielle Hardware für die Verschlüsselung der Sprachkommunikation, die dann über einen Circuit-Switched-Datendienst (CS) des jeweiligen Mobilfunkanbieters übertragen wird, sowie für die Verschlüsselung der Nachrichten des Short Message Service (SMS). Die Verwendung eines CS-Datendienstes war ursprünglich damit begründet worden, dass

ein solcher Dienst am besten zu den Antwortzeitanforderungen einer Sprachübertragung passt. Moderne Mobilfunksysteme favorisieren jedoch inzwischen paketvermittelte Dienste auf Basis des Internet Protocol (IP). SNS über IP ist daher ein zentrales Element der modernen Absicherung der Sprachkommunikation. SNS kann als integrierte Komponente eines mobilen Endgerätes (z. B. Smartphone oder Tablet) oder als separate Hardware realisiert werden, die z. B. über Bluetooth mit einem mobilen Endgerät verbunden wird. Ferner sind Festnetzgegenstellen für die Anschaltung an die Kommunikationsinfrastruktur der jeweiligen Organisation über die klassische TK (Integrated Services Digital Network, ISDN) oder IP verfügbar.

9.1.3 Verwaltung mobiler Endgeräte - Mobile Device Management

Die wesentliche Aufgabe eines Mobile Device Management (MDM) besteht in der Unterstützung des zentralen Betriebs der mobilen Endgeräte einer Organisation. Dies beinhaltet insbesondere die folgenden Punkte:

- Inventarisierung, Rollout und Fernkonfiguration
- Systemmanagement und Endgeräteüberwachung
- Fernwartung und Support

Solche Funktionen, wie z. B. die Konfiguration aus der Ferne und die damit verbundene Möglichkeit Konfigurationsprofile zu erzwingen und überwachen zu können, sind jedoch auch wesentliche Sicherheitsfunktionen, von denen typischerweise MDM-Lösungen eine ganze Palette bieten. In diesem Sinne ist MDM eine der wichtigsten Sicherheitsmaßnahmen zur Integration mobiler Endgeräte.

9.1.3.1 Inventarisierung, Rollout und Fernkonfiguration

Zur Erfassung eines neuen Endgerätes muss oft zunächst eine spezielle App für das MDM auf dem mobilen Endgerät installiert und das Gerät dem zentralen MDM bekannt gemacht werden. Diese Erfassung eines neuen Endgerätes erfolgt entweder durch einen Administrator oder sogar durch den Nutzer selbst an einem Selbstbedienungs-Portal (engl. Self-Service Portal).

Nach der Inventarisierung und der damit verbundenen Anbindung an das zentrale MDM der Organisation kann das Gerät dann Over-the-Air (OTA) unabhängig vom Endgerätestandort mit Einstellungen konfiguriert werden. Dabei werden oft unterschiedliche Nutzergruppen unterschieden und entsprechende gruppenspezifischen Policies angesetzt.

Für die Software-Verteilung werden oft sogenannte Company App Stores (auch als Corporate App Stores oder Enterprise App Stores bezeichnet) eingesetzt, die jedoch auf den App Stores der eingesetzten mobilen Betriebssysteme und den hier bestehenden Verteilungsmechanismen basieren. Dabei handelt es sich – zumindest für die aktuell besonders populären mobilen Betriebssysteme – letztendlich um Dienste, die über eine Public Cloud bereitgestellt werden, was mit erheblichen Sicherheitsbedenken verbunden ist (siehe auch Kapitel 8.2). In einem solchen Company App Store können dann für die Arbeit erforderliche oder selbst entwickelte Anwendungen für den Nutzer bereitgestellt und freigegeben werden. Auch eine Fernlöschung der Apps von den Endgeräten ist bei Bedarf möglich. Trotz der genannten Sicherheits-bedenken ist ein Company App Store von besonderer Wichtigkeit, da nur über diesen Weg auch sichergestellt werden kann, dass nur freigegebene Apps verwendet werden und die Apps auch nur die wirklich benötigten Zugriffsrechte erhalten.

9.1.3.2 Systemmanagement und Endgeräteüberwachung

Das Systemmanagement muss unmittelbar bei Anmeldung eines Nutzers aktiv werden und bei Bedarf aktualisierte Konfigurationsdaten, Apps oder Sperr- und Löschkommandos übermitteln können (auch als Push-Down-Funktion bezeichnet). Kommandos zum Sperren oder sogar Löschen (engl. Wipe) können dabei eine App oder das komplette Endgerät betreffen.

Ein weiteres Element des Systemmanagements ist die regelmäßige Sicherung (Backup) der Daten von einem mobilen Endgerät auf die zentrale Infrastruktur einer Organisation, um das Risiko von Datenverlusten bei Defekt oder Verlust des Gerätes zu minimieren.

Die Endgeräteüberwachung beinhaltet folgende Punkte:

- Event-Logs: Es werden Logfiles mit unterschiedlichem Detaillierungsgrad über Systemzugriffe und Anwenderaktivitäten erstellt.
- Reporting: Die erfassten Ereignisse werden in Reports zu Statistiken verdichtet.
- Kostenkontrolle: Das Volumen von Sprach- und Datenverkehr wird überwacht und dokumentiert. Entsprechende Grenzwerte können vordefiniert werden und geben bei Überschreitung einen Warnhinweis.

Fernwartung und Support

Es werden durch das MDM-System Werkzeuge zur Verfügung gestellt, die eine Ferndiagnose und einen Fernzugriff auf das Gerät ermöglichen. Dadurch kann der IT-Support den Anwender, unabhängig von seinem Standort, bei der Behebung möglicher Probleme unterstützen. Zur Erfassung und Bearbeitung von Störungen und Wartungstätigkeiten kann dabei ein MDM-System auch an ein System für das Störungsmanagement (engl. Incident Management System) angebunden werden.

Sicherheitsfunktionen

Folgende Sicherheitsfunktionen können von MDM-Lösungen (in unterschiedlichen Ausprägungen) realisiert werden:

- Erzwingung von Sicherheitsrichtlinien: Es kann ein Passwort-Schutz sowie eine angemessene Komplexität des Passwortes erzwungen werden. Ebenso kann festgelegt werden, wie viele Fehlversuche gestattet sind und wie darauf reagiert werden soll (z. B. Sperrung des Gerätes oder Löschung aller Daten oder bestimmter Inhalte). Auch sollte eine Bildschirmsperre des Gerätes nach einem definierbaren Zeitintervall erzwingbar sein.
- App-Richtlinien: Über Blacklists und Whitelists können bestimmte Apps explizit gesperrt bzw. freigegeben werden. Sofern vom Betriebssystem des Endgerätes unterstützt, können einzelne App-Berechtigungen unterdrückt werden. Auch ist eine Fernlöschung unerwünschter Apps nach dem Abgleich mit der Blacklist/Whitelist möglich.
- Remote-Wipe: Hierunter wird das Sperren und Löschen des Endgerätes per Fernadministration verstanden. Diese Funktion versetzt den IT-Betrieb bzw. den Anwender in die Lage, im Falle eines Endgeräteverlusts oder -diebstahls die auf dem Endgerät gespeicherten sensiblen Daten vor unbefugtem Zugriff zu schützen. Ggf. können Daten auch selektiv gelöscht werden. Manche Hersteller unterstützen auch eine Funktion, bei der die Daten nach einer festgelegten Zeitspanne ohne erfolgreiche Anmeldung am zentralen MDM automatisch gelöscht werden.
- Kill-Switch: Ein Kill-Switch stellt eine (zunehmend integrierte) Funktionalität im mobilen Endgerät dar, die die obigen Funktionalitäten erweitert. Über Sperren und Löschen des mobilen Endgerätes per Fernadministration oder bei Verletzung der Sicherheitsrichtlinien hinaus wird durch einen Kill-Switch verhindert, dass das Gerät mit einer anderen oder gänzlich ohne SIM-Karte betrieben werden kann. Eine Kill-Switch-Sperre kann dabei nicht mit einem Reset (z. B. nach Tausch der SIM-Karte) oder einer Neuinstallation auf Betriebssystem-Ebene umgangen werden. Das Gerät kann einzig durch die Eingabe eines speziellen Benutzerpasswortes wieder reaktiviert werden.

Eine solche Funktionalität ist derzeit noch kein Standard in vielen MDM-Lösungen, bekommt jedoch zunehmend einen hohen Stellenwert. Wird ein Smartphone gestohlen und der Kill-Switch durch Verletzung der Sicherheitsrichtlinien oder durch Abschalten bzw. Entnahme der SIM-Karte aktiviert, so wird es für einen unberechtigten Nutzer praktisch gänzlich unbrauchbar.

- Endgeräte-Audits: Die auf einem mobilen Endgerät installierte MDM-Software kann, ggf. angestoßen und gesteuert durch eine zentrale MDM-Komponente, regelmäßig und bei Bedarf eine Überprüfung auf Einhaltung von Richtlinien und Konfigurationsvorgaben durchführen. Dies beinhaltet insbesondere die Feststellung, ob erweiterte Berechtigungen auf dem mobilen Endgerät vorliegen (Jailbreak oder Root-Rechte), sodass entsprechende Maßnahmen eingeleitet werden können.
- Behandlung von Sicherheitsvorfällen (Security Incidents): Wird bei der Prüfung eines Endgerätes ein Sicherheitsvorfall erkannt, können je nach Dringlichkeit unterschiedliche Aktionen angestoßen werden, die von der Information des Nutzers, der Benachrichtigung der IT-Abteilung bis hin zu einem Remote-Wipe rangieren können.
- Verschlüsselung gespeicherter Daten: Durch das MDM wird erzwungen, dass Daten der jeweiligen Organisation auf dem Gerät und auf austauschbaren Speicherkarten nur verschlüsselt gesichert werden. Hierzu wird entweder die bordeigene Verschlüsselungsmethode des Endgerätes oder aber ein eigenes Verfahren der MDM-Lösung verwendet.
- Container-Bildung: Die Daten werden in einer speziell gesicherten Container-App der MDM-Lösung verschlüsselt gespeichert (siehe auch Kapitel 9.1.1). Der Zugang zur App ist mit einem eigenen Passwort geschützt. Die Verwendbarkeit der hier abgelegten Daten außerhalb des geschützten Containers kann per Richtlinie konfiguriert werden.
- Gesicherte Verbindungen: Der Zugang zum Netz einer Organisation erfolgt ausschließlich über gesicherte Verbindungen.

Aufbau einer MDM-Lösung

Für den Aufbau einer MDM-Lösung in einem organisationseigenen Rechenzentrum sind üblicherweise folgende Komponenten erforderlich:

- Mobile Device Services: Über einen Server in einer DMZ erhalten die mobilen Endgeräte ihre Konfigurationsdaten. Die Kommunikation erfolgt hier meist über HTTPS.
- Secure Application Gateways: Über Application-Gateways in einer DMZ erfolgt der Zugriff auf die eigentlichen Anwendungs-Server der Organisation (z. B. Exchange). Über einen solchen Weg kann auch eine sichere Browser-Umgebung für mobile Endgeräte geschaffen werden, indem sich eine Browser-App über das Internet stets mit der organisationsinternen Proxy-Infrastruktur verbindet und erst von hier das eigentliche Ziel im Internet erreicht.
- Management-System für MDM-Komponenten: Zunächst werden die zentralen Komponenten des MDM-Systems über ein Management-System verwaltet. Zudem erfolgen gewisse Elemente von Inventarisierung, Rollout und Fernadministration lösungsabhängig über das Management-System. Typische Beispiele sind die Administration des Company App Store oder die Verwaltung von Zertifikaten und anderen Credentials für die Authentisierung von Endgeräten und Nutzern. Für den Zugriff auf einen Company App Store ist eine Kommunikation mit dem eigentlichen, externen App Store erforderlich. Aus diesem Grund wird der entsprechende Server üblicherweise in einer eigenen DMZ platziert.

Hinweis: Manche MDM-Lösungen benötigen eine zentrale Komponente in der Infrastruktur des jeweiligen Herstellers, über die der gesamte Verkehr zu den mobilen Endgeräten läuft. Aus Sicherheitsgründen ist eine solche Lösung bedenklich, da einerseits die Verfügbarkeit durch die zusätzliche Komponente in jedem Fall eingeschränkt ist und andererseits das grundsätzliche Risiko der Kompromittierung von Daten über die Infrastruktur des Herstellers besteht. Aus ähnlichen Gründen sind Cloud-basierte MDM-Lösungen kritisch zu sehen.

Abbildung 56 zeigt exemplarisch einen möglichen Aufbau der Infrastruktur.

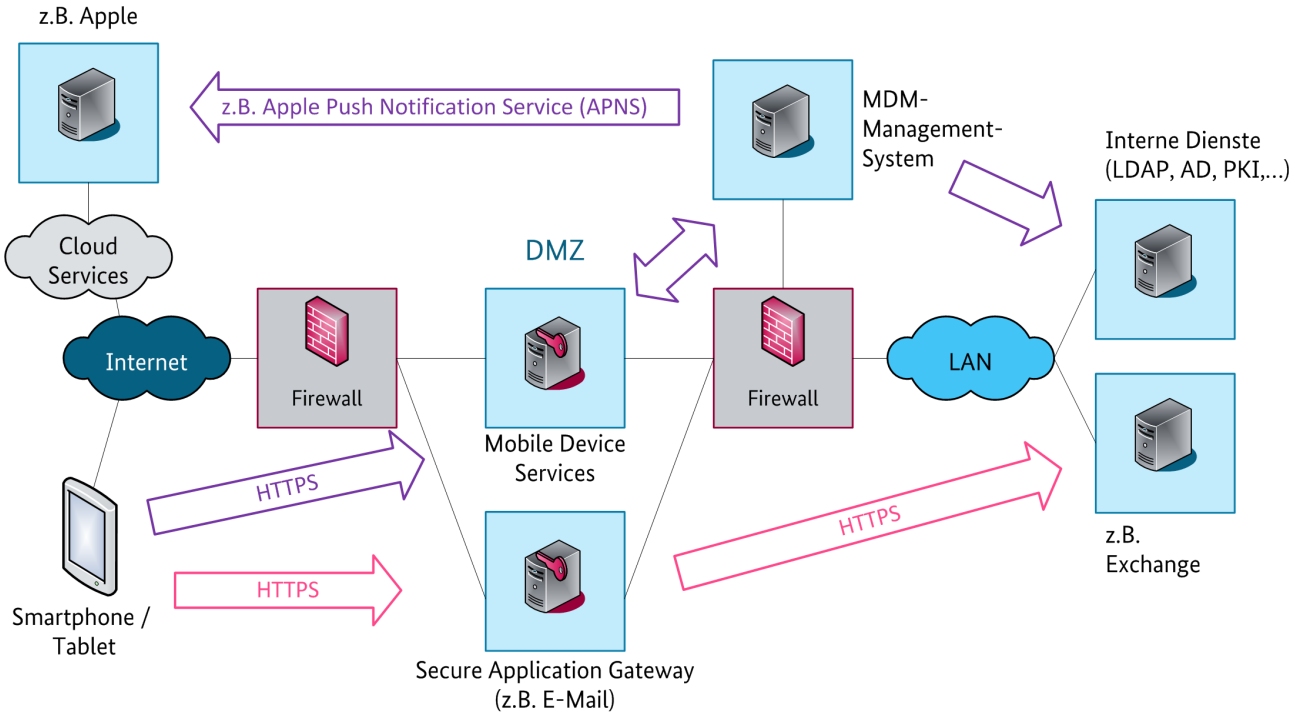


Abbildung 57: Beispielhafter Aufbau einer MDM-Infrastruktur

9.1.4 Organisationsinterne Telekommunikation und Mobilfunk: Fixed Mobile Convergence

Unter Fixed Mobile Convergence (FMC) wird eine Verbindung zwischen einem Festnetz und einem Mobilfunknetz verstanden, die netzübergreifend Leistungsmerkmale zu einem einheitlichen Dienst integriert. Ein typisches Beispiel ist die Erreichbarkeit unter einer einzigen Rufnummer im Festnetz und im Mobilfunknetz (One Number Service). Dabei erfolgt eine Anbindung von GSM- bzw. UMTS-Mobiltelefonen an eine lokale TK-Anlage derart, dass der Teilnehmer einerseits am Mobiltelefon unter seiner Festnetznummer erreichbar ist und andererseits auf die vom Festnetzanschluss gewohnten Leistungsmerkmale zurückgreifen kann.

FMC kann als integraler Bestandteil von UCC realisiert werden, jedoch auch als eigenständiger Lösungsansatz zur Integration von Mobilfunk in die TK-Lösung umgesetzt werden.

9.1.4.1 Architektur

Unter dem Begriff FMC werden unterschiedliche technische Lösungen zusammengefasst, die sich in der Art und Weise der Verbindung der Netze unterscheiden. Im Wesentlichen können zwei Alternativen unterschieden werden:

- Aufbau einer FMC-Lösung als Ergänzung einer TK-Anlage
- Aufbau einer FMC-Lösung als Bestandteil eines GSM/UMTS-Mobilfunknetzes

Für die Betrachtungen in dieser Technischen Leitlinie ist primär die erste Alternative wichtig, da hier die organisationsinterne Telekommunikation im Vordergrund steht.

Manche FMC-Systeme basieren auf den in TK-Anlagen bereitgestellten Rufumleitungsfunktionen und erfordern für die Bereitstellung von Leistungsmerkmalen eine spezielle Software auf dem Mobiltelefon. Aus dem Blickwinkel der TK-Anlage und des Nutzers ist das Mobiltelefon praktisch eine weitere Nebenstelle geworden und das Mobilfunknetz wird als transparentes Kommunikationsmedium

verwendet. Solche FMC-Lösungen nutzen neben den Diensten zur Sprachübertragung auch Datendienste (siehe Kapitel 9.1.5) und Messaging-Dienste zur spezifischen Signalisierung zwischen der Komponente auf dem Mobiltelefon und der TK-Anlage (z. B. Synchronisation von Kontakten). Ein eingehender Ruf kann parallel sowohl auf dem Festnetztelefon als auch auf dem Mobiltelefon angezeigt werden. Nimmt der Teilnehmer das Gespräch beispielsweise auf dem Festnetzapparat an, kann das Gespräch bei vielen Lösungen anschließend „auf Knopfdruck“ an das Mobiltelefon übergeben und dort nahtlos fortgesetzt werden.

Unterstützt das Mobiltelefon zusätzlich eine WLAN-Schnittstelle mit einem VoIP-Client, so gestatten es manche FMC-Lösungen, dass sich das Endgerät bei Empfang des heimatlichen WLAN automatisch in dieses Netz einbucht und die Sprachkommunikation automatisch über WLAN geführt wird. Bewegt sich das Mobiltelefon aus dem Abdeckungsbereich des WLAN hinaus, wird wieder über GSM/UMTS kommuniziert (siehe Abbildung 58). Dabei kann auch eine nahtlose Gesprächsübergabe (Handover) zwischen WLAN und GSM/UMTS realisiert werden.

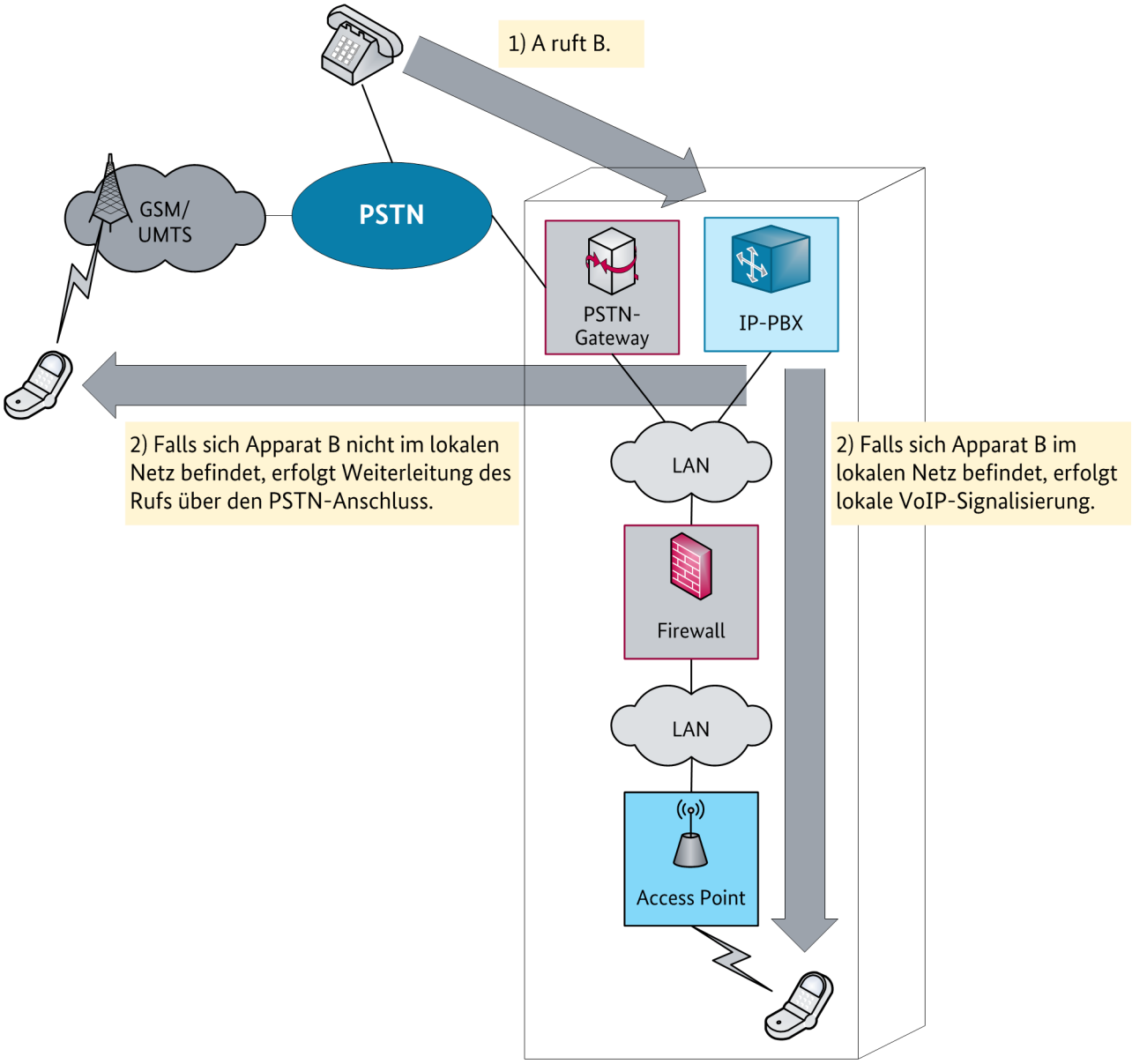


Abbildung 58: Beispiel einer Rufvermittlung bei einer FMC-Lösung

9.1.4.2 Sicherheitsmechanismen

Zunächst gelten die für GSM/UMTS eingesetzten Sicherheitsmechanismen (siehe Kapitel 9.1.5.2), d. h. die Mobilstation muss sich bei der Anmeldung an ein GSM/UMTS-Netz gegen das Heimat-GSM/UMTS-Netz authentisieren und die Sprachinformationen werden auf der Luftschnittstelle zwischen Mobilstation und Basisstation verschlüsselt übertragen. Für den Datendienst General Packet Radio Service (GPRS) wird zwischen Mobilstation und Serving GPRS Support Node (SGSN), einer Komponente des Core-Netzes, verschlüsselt. Trotzdem werden in wesentlichen Teilen der GSM/UMTS-Infrastruktur sowohl Nutz- als auch Signalisierungsdaten unverschlüsselt und nicht authentisiert übertragen. Weiterhin haben zumindest die Verfahren, die in GSM/UMTS und GRPS auf der Luftschnittstelle eingesetzt werden, gewisse Schwächen, welche für die Übertragung von Daten mit erhöhtem Schutzbedarf bedenklich sind, wie in Kapitel 9.1.5.2 beschrieben.

Für die Übertragung im (W)LAN wirken zunächst die dort eingesetzten Sicherheitsmechanismen (siehe Kapitel 9.1.6.2). Damit sich nur gewünschte Endgeräte mit dem (W)LAN verbinden können, kann am (W)LAN-Zugang eine Authentisierung mit IEEE 802.1X verwendet werden. Für WLANs bietet IEEE 802.11i (siehe [IEEE 802.11-2012]) die weitergehende Möglichkeit zur Verschlüsselung der Kommunikation auf der Luftschnittstelle.

Generell gilt auch, dass Sicherheitsmechanismen auf den mobilen Endgeräten erforderlich sind. Zu nennen sind die Zugangskontrolle zu Diensten sowie der Zugriffsschutz für Daten auf dem Endgerät inklusive Berechtigungskonzept. Hier haben viele mobile Endgeräte erhebliche Schwächen (siehe Kapitel 9.1.1).

Für eine FMC-Lösung als Ergänzung einer TK-Anlage können produktabhängig Sicherheitsmechanismen zwischen Mobiltelefon und TK-Anlage wirken. Grundsätzlich kann beispielsweise zwischen der FMC-Komponente auf dem Mobiltelefon und der TK-Anlage eine Authentisierung zumindest des Mobiltelefons erfolgen. Eine Verschlüsselung der Kommunikation zwischen der FMC-Komponente auf dem Mobiltelefon und der TK-Anlage ist ebenfalls denkbar.

9.1.5 Mobilfunknetze im Überblick

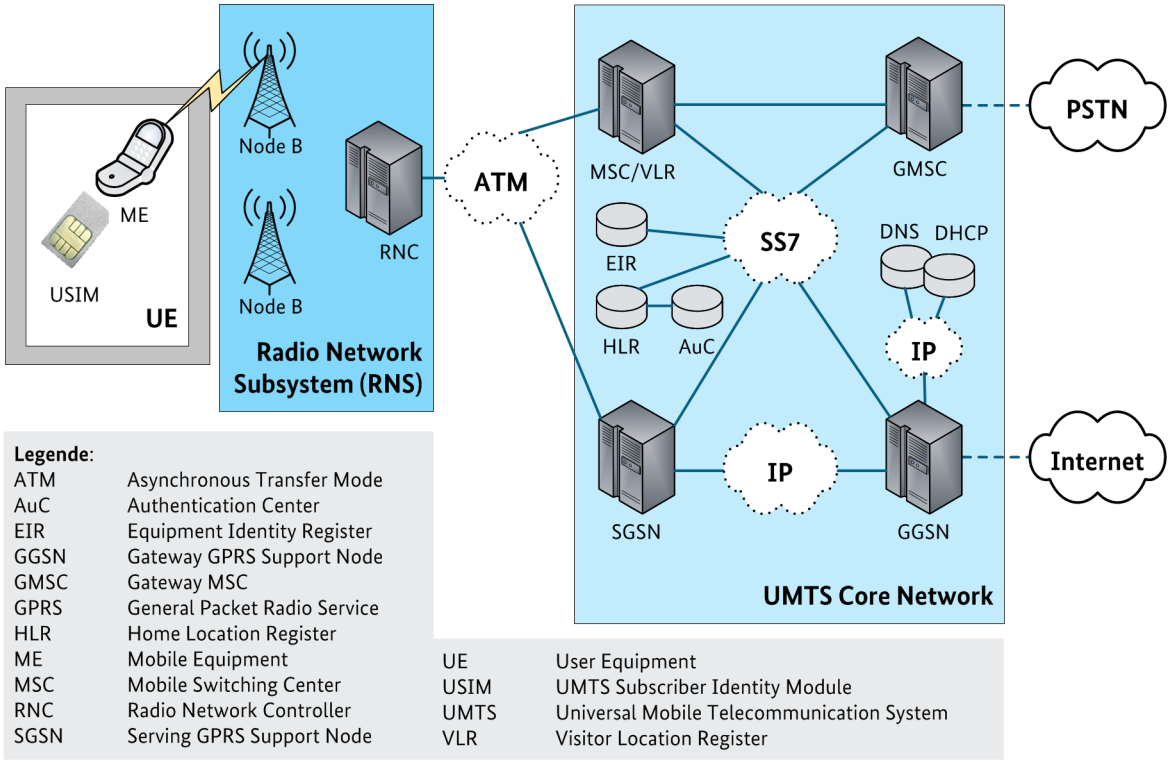
9.1.5.1 Architektur

Nach der ersten, analogen Generation des Mobilfunks hat der Mobilfunk in der zweiten, digitalen Generation mit dem Global System for Mobile Communications (GSM) eine weltweite und in vielen Regionen flächendeckende Verbreitung und durch preiswerte Mobiltelefone eine enorme Nutzung erfahren. Mit dem General Packet Radio Service (GPRS) ist auch ein paketvermittelter Datendienst zu GSM in die zweite Generation hinzugekommen, der einen mobilen Internetzugang ermöglicht. In der Praxis werden Datenraten von bis zu 53,6 kbit/s Downlink und 26,8 kbit/s Uplink möglich. Mit der Optimierung Enhanced Data Rates for GSM Evolution (EDGE) können Datenraten bis 220 kbit/s im Downlink und 110 kbit/s im Uplink erreicht werden.

Das Universal Mobile Telecommunications System (UMTS) ist der wesentlichste Vertreter der sogenannten dritten Generation mobiler Kommunikationssysteme (3G). UMTS wurde in einem 3GPP-Standard (3rd Generation Partnership Project) zunächst in der Release 99 spezifiziert. Die Datenraten betragen hier im Downlink je nach Zeichenkodierung 64 / 128 / 384 kbit/s und im Uplink 64 kbit/s. Anschließend wurden die Releases 4, 5, 6 und 7 veröffentlicht, in denen UMTS näher spezifiziert wurde. Die Implementierung neuer Releases wird in den Mobilfunknetzen der unterschiedlichen Betreiber unterschiedlich schnell durchgeführt.

Zwischen Sprach- und Datendiensten wird in UMTS klar getrennt (siehe Abbildung 59). Der Aufbau der UMTS-Netzarchitektur ist dem Aufbau von GSM/GPRS-Netzen dabei sehr ähnlich. Dennoch bestehen technische Unterschiede in diversen Teilbereichen sowie in der Nomenklatur. Wie Abbildung 59 zu entnehmen ist, vereint das UMTS Core Network sowohl Komponenten analog zu GSM in einem System für leitungsvermittelnde Dienste (primär Sprache) als auch Komponenten analog zu GPRS in einem paketvermittelten IP-Netz. Zum Beispiel ist der Gateway GPRS Support Node (GGSN) – wie auch in der

GPRS-Architektur – für die Anbindung an externe paketbasierte Netze und für die Nutzungsabrechnung zuständig. Auch die Anbindung an andere Provider-Netze wird über den GGSN realisiert.



Legende:

ATM	Asynchronous Transfer Mode
AuC	Authentication Center
EIR	Equipment Identity Register
GGSN	Gateway GPRS Support Node
GMSC	Gateway MSC
GPRS	General Packet Radio Service
HLR	Home Location Register
ME	Mobile Equipment
MSC	Mobile Switching Center
RNC	Radio Network Controller
SGSN	Serving GPRS Support Node
UE	User Equipment
USIM	UMTS Subscriber Identity Module
UMTS	Universal Mobile Telecommunication System
VLR	Visitor Location Register

Abbildung 59: Vereinfachte Darstellung der UMTS-Netzarchitektur nach Release 99

High Speed Packet Access (HSPA) ist eine Weiterentwicklung von UMTS, die höhere Datenraten ermöglicht. Hier können mit (High Speed Downlink Packet Access (HSDPA) bzw. mit High Speed Uplink Packet Access (HSUPA) höhere Datenraten im Downlink bzw. im Uplink erreicht werden. HSDPA basiert vollständig auf der oben beschriebenen UMTS-Infrastruktur.

Nahezu alle Mobilfunk-Netzbetreiber bieten HSDPA für deutlich höhere Datenraten im Downlink an. HSDPA ist Teil des Release 6 von UMTS. Unter optimalen Bedingungen ist damit eine theoretische Datenübertragungsrate von 14,4 Mbit/s brutto möglich. Die erzielbare Datenrate hängt dabei auch von dem verwendeten Endgerät ab.

Mit dem Aufbau des High Speed Uplink Packet Access (HSUPA) kann die maximal verfügbare Datenrate vom Endgerät zum Festnetz (Uplink) zunächst auf 5,8 Mbit/s gesteigert werden. HSUPA ist wie HSDPA Teil des Release 6 von UMTS und gehört zur sogenannten Generation 3,5 (3.5G) der Mobilfunknetze.

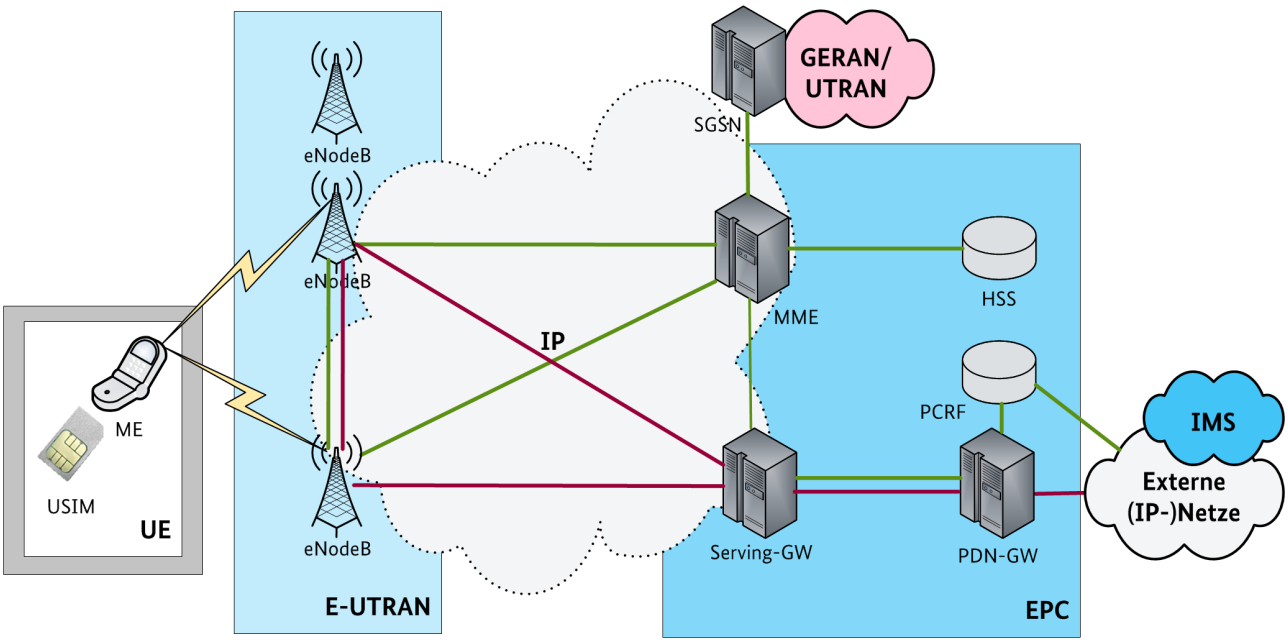
Long Term Evolution (LTE), auch als 3.9G bezeichnet, ist ebenfalls ein Standard im Rahmen des 3GPP. Eine erste Standardisierung von LTE findet sich in 3GPP-Standard, Release 8. LTE bietet eine erhöhte spektrale Effizienz durch verbesserte Antennentechnologie, verbesserte Modulationsverfahren und eine verbesserte Kodierung.

LTE Advanced, die Weiterentwicklung von LTE, erfüllt schließlich die Anforderungen der ITU für Mobilfunkstandards der 4. Generation, z. B. eine Datenrate von 100 Mbit/s. Die verwendete Technik ermöglicht im Access-Bereich bei stationärer Nutzung sogar 1 Gbit/s.

Die LTE-Netzarchitektur ist gegenüber der von UMTS deutlich vereinfacht. Es gibt nur noch eine paketorientierte Datenübertragung über IP (siehe Abbildung 60). Die Radio Network Controller (RNC) fallen weg und der Datenverkehr führt direkt vom evolved Node B (eNodeB) zum Gateway (GW). Die Mobility Management Entity (MME) ist ein reiner Kontrollknoten zur Signalisierung.

LTE ist also ein reines Datenübertragungsnetz, das ausschließlich auf IP basiert. Sprachübertragung und SMS sind als Netzarchitekturelemente nicht vorgesehen und müssen als Anwendungen realisiert werden.

Eine langfristig anvisierte Lösung für dieses Problem bietet das auf dem Session Initiation Protocol (SIP) basierende IP Multimedia Subsystem (IMS), das aber eine komplexe Implementierung benötigt. Eine weitere Option bietet Voice over LTE via Generic Access Network (VoLGA). Hierbei erfolgt über das LTE-Netz eine Anmeldung am GSM-Netz. Dies hat den Vorteil, dass am Vermittlungsnetz kaum Änderungen notwendig sind. Der VoLGA Access Network Controller (VANC) verhält sich gegenüber dem Mobile Switching Center (MSC) wie ein Base Station Controller (BSC). Als dritte Option, welche die aktuelle Praxis darstellt, ist ein Circuit Switched Fallback möglich, d. h. die Verwendung des 2G- oder 3G-Netzes zur Telefonie.



Legende:		GW	Gateway	PDN-GW	Packet Data Network GW
eNodeB	evolved Node B	HSS	Home Subscriber Server	RAN	Radio Access Network
EPC	Evolved Packet Core	ME	Mobile Equipment	UE	User Equipment
E-UTRAN	Evolved UTRAN	MME	Mobility Management Entity	USIM	UMTS Subscriber Identity Module
GERAN	GSM EDGE RAN	PCRF	Policy&Charging Rules Function	UMTS	Universal Mobile Telecommunication System

Abbildung 60: LTE-Netzarchitektur (vereinfacht)

9.1.5.2 Sicherheitsmechanismen

Die verschiedenen Mobilfunktechniken besitzen auch unterschiedliche Sicherheitsmechanismen. In unterschiedlichen Ausprägungen sind aber die folgende Punkte vertreten:

- Anonymisierung der Identität
- Authentisierung
- Verschlüsselung der Kommunikation

Die Anonymisierung erfolgt in den Netzen über verschiedene temporäre Identitäten, die bei Funkzellenwechsel und/oder in regelmäßigen Abständen gewechselt werden, um beispielsweise das Erstellen von Bewegungsprofilen zu verhindern.

Die Authentisierung ist bei GSM und bei GPRS jeweils einseitig, d. h. nur das Endgerät, genauer die Mobilstation, authentisiert sich gegenüber dem Netz, aber nicht umgekehrt. Seit UMTS ist die Authentisierung beidseitig.

Die Verschlüsselung der Kommunikation in GSM, UMTS und LTE erfolgt auf der Luftschnittstelle und basiert auf Pre-Shared Keys, die auf der USIM und im Authentication Center (AuC) verschlüsselt gespeichert sind, und weiteren Verschlüsselungsalgorithmen. Je Mobilfunktechnik können Endgerät und

Netz verschieden starke Algorithmen aushandeln. Diese werden mit GPRS Encryption Algorithm (GEA), UMTS Encryption Algorithm (UEA) und Evolved Encryption Algorithm (EEA) bezeichnet.

Im GSM-Netz ist die Basisstation der Verschlüsselungsendpunkt für die Sprachkommunikation. Der am häufigsten verwendete Verschlüsselungsalgorithmus ist GEA1 (auch A5/1 genannt), eine Stromchiffre. Diese wurde über Reverse Engineering nachgestellt und es sind viele Angriffsmöglichkeiten bekannt. GEA0 bedeutet keine Verschlüsselung und von der Verwendung von GEA2 wird seitens 3GGP wegen erheblicher Schwächen abgeraten. Erst GEA3, der auf UEA1 aufbaut, wird noch als sicher angesehen. Die Möglichkeit, eine unsichere oder keine Verschlüsselung auszuhandeln, lässt sich zusammen mit der einseitigen Authentisierung in GSM für eine Man-in-the-Middle-Attacke ausnutzen. Eine solche IMSI-Catcher-Attacke gestattet es dem Angreifer, eine Basisstation vorzutäuschen und so Gespräche abzuhören und SMS abzufangen (siehe [BSI ÖMS-2008]). Des Weiteren ist die Kommunikation zwischen den Basisstationen unverschlüsselt und bei der Übertragung beispielsweise mittels Richtfunk abhörbar.

Im UMTS-Netz ist für die Sprachkommunikation der Verschlüsselungsendpunkt das RNC, weshalb der letztgenannte Punkt hier nicht zum Tragen kommt. Eine Attacke wie mit dem IMSI-Catcher ist auch wegen der beidseitigen Authentisierung nicht möglich. Allerdings könnte durch die meist mögliche Abwärtskompatibilität ein Endgerät durch Signalunterdrückung zur Nutzung von GSM gezwungen werden, wodurch diese Gefährdung wieder zum Tragen kommt.

Bei der paketvermittelnden Datenkommunikation mit GPRS oder UMTS erfolgt die Verschlüsselung auf der LLC-Schicht (Logical Link Control) zwischen Mobilstation und Serving GPRS Support Node (SGSN). Die zuvor angesprochene Attacke ist auch hier nicht möglich. Die Sicherheit der Übertragung zwischen SGSN und GGSN liegt im Verantwortungsbereich des Netzbetreibers. Der unsichere Bereich, d. h. das Internet, beginnt am GGSN. Bei LTE wird die Kommunikation auf der Luftschnittstelle und ggf. auch im Festnetz verschlüsselt. Für die Übertragung der Nutzdaten sind das mobile Endgerät, eNodeB[30] und Serving-Gateway die Verschlüsselungsendpunkte. Für die IP-Kommunikation zwischen eNodeB und Serving-Gateway wird IPsec verwendet (siehe [ETSI TS133401-2010]).

Im Zusammenhang mit der Internet-Anbindung mobiler Endgeräte ist die Funktion eines sogenannten Private Access Point Name (APN) von Interesse. Hier wird die Datenkommunikation, z. B. für UMTS, am GGSN nicht direkt in das Internet ausgekoppelt, sondern über ein Site-to-Site-VPN (z. B. mit IPsec) vom GGSN zu einem VPN-Gateway im Netz der Organisation geleitet. Das mobile Endgerät wird dann mit dem Private APN konfiguriert und der IP-Verkehr wird per VPN automatisch in das Organisationsnetz geleitet. Von dort kann ein Internetzugang erfolgen, der sich in keiner Weise mehr von einem Zugang über ein lokal am LAN angeschlossen Endgerät unterscheidet (siehe Abbildung 61).

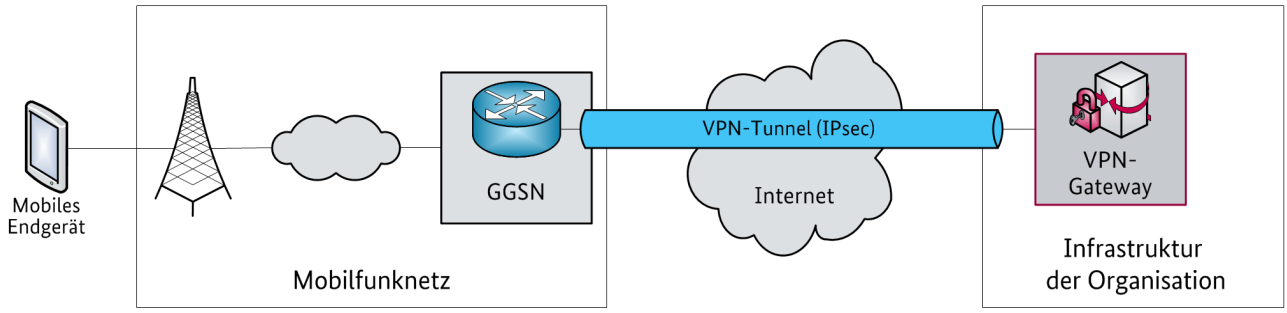


Abbildung 61: Kommunikation via Private APN

Die Tatsache, dass in Mobilfunknetzen der Form GSM/UMTS/LTE nicht zwingend vollumfänglich verschlüsselt wird, war in der Vergangenheit immer wieder ein Angriffspunkt.

Daher sind trotz der Absicherung der Kommunikation zwischen Mobilstation und Node B, Mobilstation und SGSN bzw. Mobilstation, eNodeB und Gateway bei der Nutzung von GSM/UMTS/LTE stets weitergehende Maßnahmen (z. B. eine Ende-zu-Ende-Verschlüsselung) zur Sicherung vertraulicher Daten notwendig.

30 eNodeB = Evolved UMTS Terrestrial Radio Access Network Node B bzw. Evolved Node B

9.1.6 Wireless LAN

Wireless-LAN-Technologie (WLAN) hat sich als drahtlose Erweiterung für traditionelle kabelbasierte LANs etabliert. WLANs operieren in den unlizenzierten Frequenzbereichen bei 2,4 GHz und bei 5 GHz, die in Deutschland von der Bundesnetzagentur unter anderem für die WLAN-Nutzung zur Verfügung gestellt wurden. Im 2,4-GHz-Bereich, einem sogenannten ISM-Band (Industrial, Scientific and Medical Band), operieren neben WLAN eine Vielzahl unterschiedlicher Systeme. Beispiele sind Mikrowellenherde, Bewegungsmelder und Bluetooth.

Als Standard für WLAN hat sich IEEE 802.11 durchgesetzt (siehe [IEEE 802.11-2012]). Der Standard ist seit seiner ersten Auflage 1997 durch diverse Ergänzungen erweitert worden, die beispielsweise verschiedene physikalische Übertragungsverfahren (IEEE 802.11a für den 5-Ghz-Bereich, und IEEE 802.11b sowie IEEE 802.11g für den 2,4-GHz-Bereich und IEEE 802.11n für 2,4 GHz und 5 GHz), Anpassungen des Kanalzugriffs zur Unterstützung von Quality-of-Service-Konzepten (IEEE 802.11e) oder verbesserte Sicherheitsmechanismen (IEEE 802.11i) beschreiben. WLANs nach IEEE 802.11a und IEEE 802.11g operieren mit einer Bruttodatenrate von maximal 54 Mbit/s auf der physikalischen Schicht. Der Standard IEEE 802.11n kann durch spezielle Funkübertragungstechniken diese Datenrate theoretisch auf brutto bis zu 600 Mbit/s erweitern. Die verfügbaren Produkte unterstützen jedoch maximal 450 Mbit/s.

Mit IEEE 802.11ac und IEEE 802.11ad stehen inzwischen sogar Technologien zur Verfügung, die theoretisch Datenraten bis zu fast 7 Gbit/s brutto auf der Luftschnittstelle realisieren können (siehe [IEEE 802.11ac-2013] und [IEEE 802.11ad-2012]). Während IEEE 802.11ac als Optimierung von IEEE 802.11n in den bestehenden Frequenzbereichen operiert, was allerdings für höhere Datenraten nur bei 5 GHz möglich ist, verwendet IEEE 802.11ad einen Frequenzbereich bei 60 GHz. Während mit IEEE 802.11ac die Nachfolgetechnik von IEEE 802.11n vorliegt, die insbesondere für flächendeckende WLANs geeignet ist, adressiert IEEE 802.11ad andere Anwendungsfelder, da der Frequenzbereich sich nur für eine punktuelle Funkversorgung und eine Peer-to-Peer-Kommunikation zwischen Endgeräten im Bereich von wenigen Metern eignet.

9.1.6.1 Architektur

Die Verwendung autonomer Access Points, die als Layer-2-Bridges an ein kabelbasiertes LAN (Ethernet) angeschlossen werden, ist in vielen WLAN-Installationen durch das sogenannte Controller-basierte WLAN-Design (siehe Abbildung 62) abgelöst worden. In einem Controller-basierten WLAN-Design werden WLAN-Funktionen durch zentral positionierte WLAN-Controller realisiert und die Aufgaben der Access Points auf die reine Funkübertragung reduziert. Daher werden Access Points in einem Controller-basierten Design oft auch als Thin Access Points bezeichnet. In der Internet Engineering Task Force (IETF) hat die Gruppe CAPWAP (Control and Provisioning of Wireless Access Points, siehe [IETF RFC5415-2009]) einen Standard für die Kommunikation zwischen Thin Access Points und WLAN-Controllern erarbeitet. Es gibt jedoch auch heute noch diverse herstellerspezifische Protokolle.

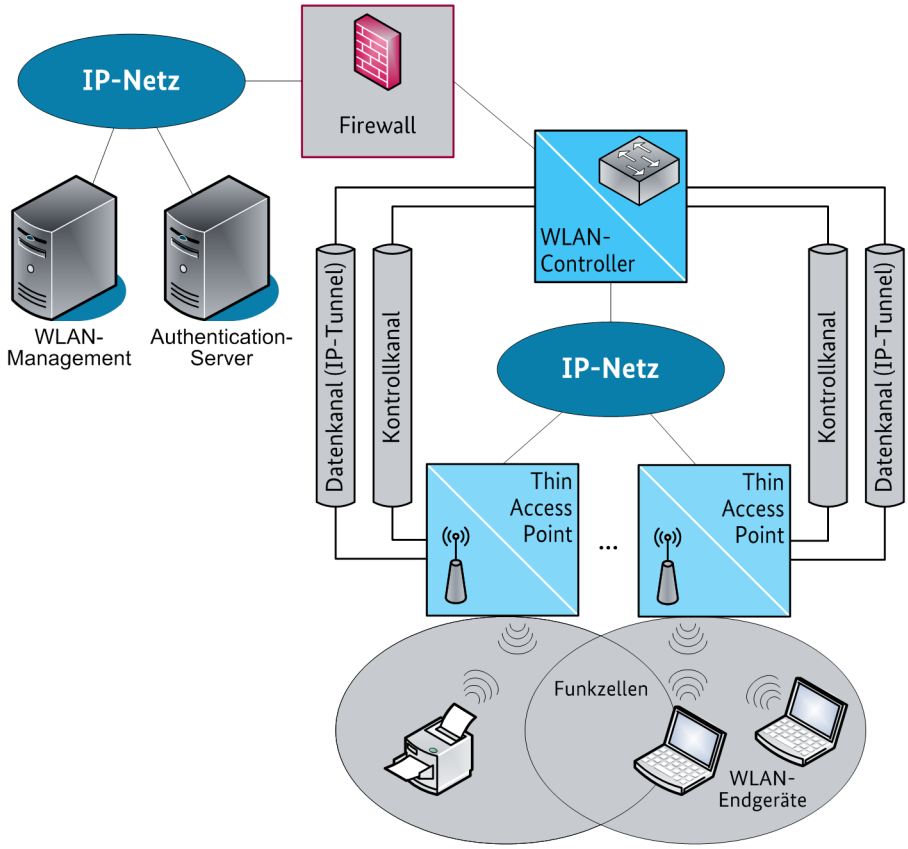


Abbildung 62: Controller-basiertes WLAN-Design

Die Kommunikation zwischen WLAN-Controller und Thin Access Point erfolgt IP-basiert typischerweise über zwei Kanäle (siehe Abbildung 62), die auf dem Transport Layer (Layer 4) durch unterschiedliche Ports bereitgestellt werden. Im Kontrollkanal werden alle Daten für das Management der Thin Access Points transportiert. Die Verwaltung und Überwachung der WLAN-Funktionen erfolgt zentral über den WLAN-Controller. Der optionale Datenkanal ist ein IP-Tunnel, über den die gesamte Kommunikation der WLAN-Clients zum WLAN-Controller geschickt werden kann. Hiermit ist der Aufbau des WLANs als Overlay-Netz möglich, d. h. aus dem Blickwinkel der WLAN-Endgeräte ist die zugrunde liegende Netzstruktur zwischen Thin Access Points und WLAN-Controller transparent. Der WLAN-Verkehr der Endgeräte wird dabei erst am WLAN-Controller in das Netz ausgekoppelt. Bei einem zentralen WLAN-Controller hat dies den Vorteil, dass der WLAN-Verkehr bei Bedarf auf eine einfache Weise über ein zentrales Sicherheitselement (z. B. Firewall) geleitet und dort gefiltert werden kann.

Für den Aufbau eines WLAN kann bei einer Controller-basierten Lösung die vorhandene LAN-Infrastruktur genutzt werden. Durch die Verwendung eines IP-Tunnels für den Datenkanal besteht analog zu einem VPN eine logische Trennung des WLAN-Verkehrs von der sonstigen Kommunikation im LAN. Während der Kontrollkanal jedoch meist von den Herstellern durch eine Verschlüsselung geschützt wird, ist die Möglichkeit der Verschlüsselung des Datenkanals produktabhängig und wird auch nicht von allen Herstellern unterstützt. Bei entsprechenden Sicherheitsanforderungen kann eine weitergehende Trennung durch Virtual LAN (VLAN) oder sogar eine separate physikalische Infrastruktur für das WLAN, d. h. eigene aktive Komponenten, erfolgen.

Das Tunnel-Konzept einer WLAN-Controller-Lösung hat in manchen Situationen auch Nachteile. Stellt man sich ein Szenario mit Außenstellen vor, bei dem die WLAN-Controller in der Zentrale aufgestellt sind und Thin Access Points in den Außenstellen über eine WAN-Strecke angebunden werden, kann sich folgende Situation ergeben: Wenn in einer Außenstelle über VoIP kommuniziert wird und ein lokales Telefonat geführt wird oder wenn von einem WLAN-Client eine Datei zu einem lokalen Drucker geschickt wird, wird der gesamte Verkehr erst in die Zentrale zum WLAN-Controller und dann wieder zurück zur

Außenstelle übertragen. Die kostbare WAN-Strecke wird also nicht nur unnötig, sondern sogar doppelt passiert. Zur Lösung dieses Problems bieten die meisten Hersteller die Möglichkeit den Verkehr lokal am Thin Access Point auszukoppeln. Damit gehen natürlich die Eigenschaften des Overlay-Netzes verloren.

9.1.6.2 Sicherheitsmechanismen

Kernelement ist die Absicherung der Funkübertragung. Hierzu dient der Standard IEEE 802.11i[31], der folgende Elemente beschreibt:

- Authentisierung von WLAN-Clients und WLAN-Infrastruktur
- Verschlüsselung und Integritätsprüfung der Daten auf der Luftschnittstelle
- Schlüsselmanagement zur Aushandlung und Auffrischung des Schlüsselmaterials

Für die Verschlüsselung und Integritätsprüfung sind zwei Verfahren festgelegt worden: Das Temporal Key Integrity Protocol (TKIP) basiert auf dem Stromchiffrierer RC4 und wird von vielen, auch älteren WLAN-Geräten unterstützt. Seit November 2008 sind deutliche Schwächen von TKIP bekannt (siehe [ACM BeTe-2009]). Unter gewissen Rahmenbedingungen ist es nämlich möglich, gewisse Teile eines mit TKIP verschlüsselten Verkehrs ohne Kenntnis des Schlüssels zu entschlüsseln. TKIP ist daher keinesfalls mehr zu empfehlen und als Altlast einzustufen. Der zweite Mechanismus, Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP), basiert auf AES mit einer Schlüssellänge von 128 Bit. CCMP ist die derzeit zu empfehlende Variante.

Die Authentisierung erfolgt entweder über IEEE 802.1X (in diesem Fall erfolgt das Schlüsselmanagement auch über IEEE 802.1X) oder implizit über Pre-Shared Keys (PSKs).

Für eine Authentisierung nach IEEE 802.1X kommuniziert ein WLAN-Client (in der Terminologie von IEEE 802.1X als Supplicant bezeichnet) auf Layer 2 mit einer Funktion im Access Point bzw. WLAN-Controller, dem Authenticator. IEEE 802.1X verwendet hierzu eine für die LAN-Übertragung angepasste Version des Extensible Authentication Protocol (EAP). Der Authenticator gestattet bei erfolgreicher Authentisierung die Kommunikation des WLAN-Client mit der Infrastruktur bzw. blockiert andernfalls die Kommunikation. Der Authenticator enthält keine eigene Intelligenz hinsichtlich des verwendeten Authentisierungsverfahrens, sondern leitet EAP-Pakete des Supplicant an einen sogenannten Authentication-Server weiter und dessen EAP-Antworten wieder an den Supplicant zurück. Als Protokoll zwischen Authenticator und Authentication-Server dient üblicherweise der Remote Authentication Dial In User Service (RADIUS), wobei EAP-Nachrichten in einem RADIUS-Attribut gekapselt werden. Eine detailliertere Beschreibung von IEEE 802.1X und EAP kann dem Anhang in Kapitel 13.3.2 entnommen werden.

Für WLAN-Installationen in Unternehmen oder Behörden ist die Verwendung von IEEE 802.1X in den meisten Fällen zu empfehlen. PSKs können nur in sehr kleinen WLANs sinnvoll (und sicher) verwaltet werden. Als Authentisierungsmethode kann für viele Einsatzbereiche Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) empfohlen werden.

Das Herstellerkonsortium Wi-Fi Alliance[32] zertifiziert Produkte hinsichtlich Interoperabilität und Konformität zu Standards der Reihe IEEE 802.11. Für die Absicherung von WLANs wurde im ersten Quartal 2003 zunächst Wi-Fi Protected Access (WPA) veröffentlicht. WPA basierte auf einem Draft zu IEEE 802.11i und unterstützt nur eine Teilmenge der in diesem Draft spezifizierten Funktionen (insbesondere TKIP). Im Jahr 2004 wurde WPA2 verabschiedet und seit 2006 ist WPA2 ein zwingender Bestandteil einer Wi-Fi-Zertifizierung (und hat damit WPA abgelöst). WPA2 deckt alle zwingenden Anforderungen von IEEE 802.11i ab und unterstützt insbesondere auch den AES-Modus CCMP.

31 IEEE 802.11i ist Bestandteil des WLAN-Gesamtstandards in der Fassung von 2012 (siehe [IEEE 802.11-2012]).

32 Wi-Fi wird häufig mit „Wireless Fidelity“ gleichgesetzt, wurde ursprünglich jedoch lediglich als Marketingbegriff für das Firmenkonsortium Wi-Fi Alliance erfunden.

Es gibt zwei Profile für WPA2:

- Das Profil WPA2-Enterprise ist für größere WLAN-Installationen gedacht und verwendet für die Authentisierung und Schlüsselverwaltung IEEE 802.1X mit RADIUS.
- WPA2-Personal (auch als WPA2-PSK bezeichnet) wurde für kleinere WLAN-Installationen und den SOHO-Bereich (Small Office / Home Office) spezifiziert und operiert mit Pre-Shared Keys operiert.

Weitere Informationen zur Absicherung von WLANs, insbesondere unter Berücksichtigung eines erhöhten Schutzbedarfs, finden sich in der Informationsschrift „Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte“ des BSI (siehe [BSI DrKoSi-2009]).

Für den erhöhten Schutzbedarf hinsichtlich Vertraulichkeit und Integrität sieht die genannte Informationsschrift neben dem Einsatz von IEEE 802.11i und IEEE 802.1X die Verwendung eines VPN vor. Auf diese Weise besteht auch bei Kompromittierung eines einzelnen Mechanismus (etwa durch einen Konfigurationsfehler) ein Schutz durch Authentisierung und Verschlüsselung. Bei erhöhten Anforderungen an die Verfügbarkeit werden eine Überwachung der Luftschnittstelle und der Einsatz von Systemen zur Angriffserkennung und -verhinderung empfohlen.

9.1.6.3 VoIP over WLAN

Für die Übertragung von VoIP über WLANs ist der in IEEE 802.11 spezifizierte Kanalzugriff ohne zusätzliche Mechanismen nicht zufriedenstellend geeignet. Der Grund ist, dass der Kanalzugriff in einem WLAN nach IEEE 802.11 ein zufallsgesteuerter Mechanismus ist, der zunächst weder eine Priorisierung unterschiedlicher Verkehrsklassen noch eine explizite Bandbreitenreservierung vorsieht. Als Konsequenz ist die Antwortzeit in einem WLAN nach IEEE 802.11 stets gewissen Schwankungen unterworfen. Diese Schwankungen sind neben der Qualität des Funkkanals abhängig von der Anzahl der Clients, die an einem Access Point assoziiert sind, und vom Verkehrsverhalten (also von den Anwendungen) dieser Clients.

Für die Übertragung von Sprache und anderen Daten, die höhere Anforderungen an das Antwortzeitverhalten haben, ist der Kanalzugriff daher mit IEEE 802.11e um Mechanismen zur Zusicherung von Dienstgüte (Quality of Service, QoS) erweitert worden. Auf einem Draft zu IEEE 802.11e basiert der Industriestandard Wi-Fi Multimedia (WMM) des Herstellerkonsortiums Wi-Fi Alliance, nach dem diverse WLAN-Produkte zertifiziert sind. Das Kernelement von IEEE 802.11e und WMM ist die abwärtskompatible Erweiterung des Kanalzugriffs um einen Priorisierungsmechanismus. Der grundsätzliche Zufallsmechanismus des Kanalzugriffs in WLANs bleibt aber erhalten. Es werden vier Prioritätsklassen unterschieden: Voice Priority als höchste Priorität, gefolgt von Video Priority, dann Best Effort Priority und schließlich Background Priority.

Wird VoIP in einem flächendeckenden WLAN, bestehend aus mehreren überlappenden Funkzellen (Access Points) genutzt, bestehen hohe Anforderungen an den Zellwechsel (Handover). Gewisse Ausfallzeiten der Verbindung sind bei einem Handover unvermeidbar. Für VoIP müssen sich diese Ausfallzeiten in tolerablen, d. h. kaum wahrnehmbaren, Grenzen bewegen. Da ein Zellwechsel vom Endgerät initiiert wird, muss an dieser Stelle eine Optimierung für VoIP realisiert werden. Dies ist jedoch herstellerspezifisch.

9.1.7 DECT

Der Standard Digital Enhanced Cordless Telecommunications (DECT) des European Telecommunications Standards Institute (ETSI, siehe [ETSI EN300175]) spezifiziert ein digitales System zur drahtlosen Übertragung von Sprache und Daten, das sich im Vergleich zu analogen Schnurlostelefon-Standards durch eine hohe Sprachqualität und Optionen für eine höhere Abhörsicherheit auszeichnet. DECT arbeitet in Europa im explizit reservierten Frequenzband zwischen 1880 MHz und 1900 MHz.

Typische Einsatzbereiche von DECT sind in erster Linie Bürogebäude, das Gelände von Organisationen sowie Heimbereiche.

Seit Ende 2006 steht mit CAT-iq (Cordless Advanced Technology – internet and quality) eine Erweiterung des DECT-Standards zur Verfügung, die unter anderem eine verbesserte Sprachqualität, die Anbindung von

DECT an IP-Netze sowie eine verbesserte Interoperabilität beinhaltet. Die ETSI standardisiert diese Technologien unter dem Namen New Generation DECT (NG-DECT, siehe [ETSI TS102527]).

Im August 2013 hat ETSI eine Verbesserung der Sicherheitsmechanismen des Common-Interface-Moduls herausgegeben (siehe siehe [ETSI EN300175]). Auf dieser Basis erschienen kurze Zeit später Verbesserungen am DECT-Standard, welche insbesondere die Sicherheit der DECT-Technologie betreffen. Problematisch ist jedoch die Tatsache, dass diverse Hersteller trotz der Verbesserungen des DECT-Standards noch eine ältere Version in ihre Produkte implementieren.

Im Januar 2011 wurde die Arbeit an einer energiesparenden Version von DECT, DECT ULE (Ultra Low Energy) begonnen (siehe [ETSI TS103159-2014]). DECT ULE fokussiert insbesondere auf Geräte mit geringen Rechen- und Energieressourcen. Hierzu gehören auch Geräte aus dem Bereich des Internet of Things, z. B. ferngesteuerte Steckdosen, Bewegungs- und Rauchmelder. Seit 2013 sind entsprechende Geräte im Handel zu erwerben.

9.1.7.1 Architektur

Mit DECT-Systemen können komplette schnurlose Nebenstellenanlagen aufgebaut werden. Neben den normalen Telekommunikationsverbindungen über einen Amtsanschluss können dann zwischen mehreren mobilen Endgeräten (Portable Parts, PPs) gebührenfrei interne Kommunikationsverbindungen über die DECT-Basisstation (sogenannte Fixed Parts, FPs) aufgebaut werden.

DECT ist multizellenfähig und unterstützt Verfahren wie Roaming[33] und Handover[34]. Bei Mehr-Zellen-Systemen besteht ein DECT-Netz aus mehreren FPs, die an eine zentrale Vermittlungskomponente (DECT Fixed System, DFS) angeschlossen sind. Das DFS verfügt hierzu über eine Datenbank zur Nutzer- bzw. Endgeräte-Verwaltung und ist an eine Nebenstellenanlage angeschlossen oder als Modul einer Nebenstellenanlage realisiert. Zur Versorgung eines größeren Gebiets können mehrere DFSs und ggf. auch Nebenstellenanlagen eingesetzt und zu einem größeren Netz verbunden werden. Die Anpassung der DECT-spezifischen Protokolle an die Protokolle des analogen Telefonnetzes bzw. des ISDN erfolgt durch die sogenannte Interworking Unit (IWU, siehe Abbildung 63).

In einem kleinen DECT-System bestehend aus einem einzelnen FP (wie im Heimbereich üblich) werden die Funktionen des DFS im FP realisiert.

Zur Erweiterung eines DECT-Systems können auch sogenannte Wireless Relay Stations (WRS), auch Relais oder Repeater genannt, eingesetzt werden. Mit Nutzung eines Repeater ist in der Regel eine automatische Deaktivierung der Verschlüsselung verbunden!

Damit ein problemloses Zusammenspiel von PPs verschiedener Hersteller gewährleistet ist, gibt es das Generic Access Profile (GAP), das in [ETSI EN300444-2013] spezifiziert ist und Minimalanforderungen für Fernsprechdienste festlegt. Sogenannte Interworking Profiles definieren die Schnittstellen zu anderen Netzen (z. B. ISDN). Weiterhin können auch schnurlose Datennetze mit entsprechenden Geräten auf DECT-Basis aufgebaut werden. In sogenannten Application Profiles sind Kommunikationsdienste für spezielle Anwendungen spezifiziert.

DECT unterstützt auch Datendienste. Der DECT Packet Radio Service (DPRS, siehe [ETSI EN301649-2012]) und das DECT Multimedia Access Profile (DMAP, siehe [ETSI EN301650-2011]) ermöglichen beispielsweise Datenkommunikation mit höheren Datenraten (vergleichbar z. B. mit denen von Bluetooth).

33 Wechsel eines PP zwischen verschiedenen DECT-Netzen

34 Wechsel eines PP zwischen zwei benachbarten Funkzellen, d. h. zwischen den durch FPs versorgten Bereichen, unter Aufrechterhaltung der Ende-zu-Ende-Verbindung

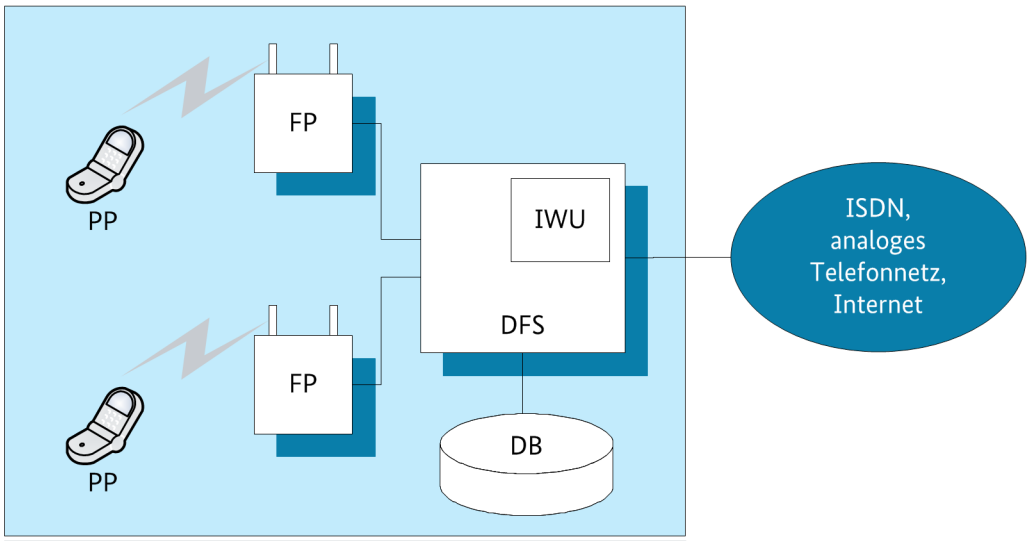


Abbildung 63: Vereinfachter Aufbau eines DECT-Systems (Quelle: [BSI DrKoSi-2009])

Die prinzipielle Architektur von CAT-iq entspricht der von DECT, d. h. ein CAT-iq-System besteht weiterhin aus FPs und PPs. Aufgrund der Abwärtskompatibilität können bestehende PPs weiterhin an einem CAT-iq-System betrieben werden. Dies bezieht sich auf PPs, welche GAP unterstützen. Die Nutzung der CAT-iq-Funktionen erfordert jedoch neue Komponenten, die sich von bisherigen teilweise unterscheiden. CAT-iq legt hierzu für PPs folgende Profile fest:

- CAT-iq 1.0 „HD Sound“ für breitbandige Sprachübertragung,
- CAT-iq 2.0 „Multi-Line“ für erweiterte Breitband-Dienste für das Sprachsignal,
- CAT-iq 3.0 „Internet Ready“ Datentransport von IP-Paketen über DRPS und Software-Updates Over The Air, und
- CAT-iq 4.0 „Intelligent Networking“ für Dienste wie Plug & Play oder Instant Messaging.

Ein Schwerpunkt von CAT-iq liegt in der Integration von DECT und IP. Der hierfür nötige Transport von Paketen der IP-Version 4 (IPv4) und IP-Version 6 (IPv6) erfolgt in CAT-iq-Systemen auf Basis von DPRS innerhalb des Protokoll-Stack für Nutzerdaten. Eine transparente Übertragung von IP-Paketen ist sowohl für den FP als auch den PP eines CAT-iq-Systems verpflichtend. Dabei wird zwischen zwei Konfigurationen unterschieden:

- IEEE 802.3 over DECT: In dieser Konfiguration werden Ethernet Frames (bis auf Präambel und Prüfsumme) per DECT transportiert,
- IP over DECT: In dieser Konfiguration werden IP-Pakete direkt per DECT transportiert.

Sprachdaten werden aus Gründen des geringeren Overhead und der damit verbundenen geringeren Verzögerung bei CAT-iq nicht über IP übertragen, d. h. zwischen FP und PP findet auf der DECT-Luftschnittstelle keine Nutzung von VoIP statt. CAT-iq setzt jedoch einen Breitband-Codec ein, der eine bessere Sprachqualität im Vergleich zu klassischem DECT liefert (von den Herstellern auch als „HD-Telefonie“ bezeichnet).

Die CAT-iq-Funktionalität ist häufig nur eine Teilkomponente eines Kombigerätes. Weitere mögliche Funktionen sind insbesondere der Internetzugang sowie integrierte TK-Anlagen für Heim- oder kleinere Büroumgebungen einschließlich PSTN-Zugang. Neben dem PSTN-Zugang für analoge oder digitale Telefone ist auch die Internettelefonie häufig Bestandteil des Funktionsumfangs. Die Anbindung der Komponenten einschließlich des VoIP-Kommunikationspfades in einem solchen Szenario ist

exemplarisch in Abbildung 64 dargestellt. Hierbei wird die Sprache auf der DECT-Luftschnittstelle weiterhin TDM-basiert übertragen, während die Übertragung zwischen FP und dem VoIP-Dienstanbieter (Internet Telephony Service Provider, ITSP) mittels IP erfolgt.

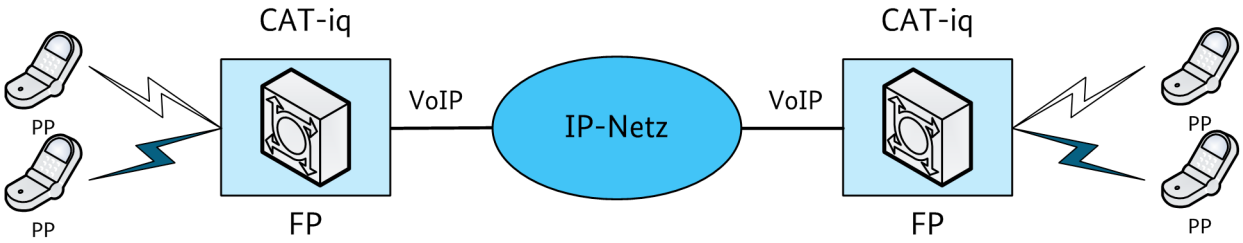


Abbildung 64: Kommunikationsfluss eines Gesprächs (Quelle: [BSI DrKoSi-2009])

9.1.7.2 Sicherheitsmechanismen

Da DECT ein funkbasiertes Verfahren ist, besteht grundsätzlich die Gefahr, dass unberechtigte DECT-fähige Geräte die DECT-Kommunikation mithören bzw. sich aktiv in die Kommunikationsverbindung einschalten. Neben nicht-kryptografischen Verfahren zum Schutz gegen Übertragungsfehler sieht die Spezifikation kryptografische Authentisierungs- und Verschlüsselungsalgorithmen vor.

Um unberechtigte Netzzugriffe zu verhindern, muss sich jeder PP vor einem Verbindungsaufbau authentisieren. Die Authentisierung basiert auf einem sogenannten Challenge-Response-Verfahren. Eine Authentisierung des FPs gegenüber dem PP ist dagegen optional.

Die Sicherheitsmechanismen von DECT-Lösungen hängen insbesondere davon ab, auf welchen Standards die jeweiligen Lösungen basieren. Lösungen können zum Schutz der Vertraulichkeit auf der Funkschnittstelle die Daten optional verschlüsselt übertragen werden. Die Verschlüsselung erfolgt mit dem DECT Standard Cipher (DSC). Dabei wird ein 64 Bit langer Chiffrier-Schlüssel verwendet. Selbst für einen normalen Schutzbedarf ist diese geringe Schlüssellänge als bedenklich einzustufen. Weiterhin gibt es bei diesen Geräten keine kryptografische Absicherung der Integrität der übertragenen Daten. Ein Angreifer kann also gezielt Nachrichten manipulieren. DECT-Lösungen, die neuere DECT-Standards implementieren (siehe hierzu Part 7 „Security Features“ von [ETSI EN300175]), unterstützen zur Authentisierung den DECT Standard Authentication Algorithm Version 2 (DSAA2) und zur Verschlüsselung der Kommunikation DSC2. DSAA2 und DSC2 verwenden AES mit einer Schlüssellänge von 128 Bit. DSC2 unterstützt einen regelmäßigen Schlüsselwechsel innerhalb einer Sitzung (Re-keying). Für die Nutzung von DSAA2 und DSC2 müssen beide Geräte (FP und PP) diese Standards implementieren, um eine Verbesserung der Sicherheit erzielen zu können. Wenn beispielsweise nur ein Gerät DSAA2 unterstützt und das andere DSAA, dann fällt die Authentisierung auf das vergleichsweise weniger sichere Verfahren DSAA zurück. Obwohl diese Standards mit verbesserten Sicherheitsmaßnahmen bereits länger verfügbar sind, sind nach wie vor auch neuere Produkte auf dem Markt verfügbar, welche die Standards nicht implementieren.

Einstellungen an DECT-Geräten können üblicherweise erst nach Eingabe einer meist 4- bis 8-stelligen Geheimnummer, der persönlichen Identifikationsnummer (PIN), vorgenommen werden. Für die Anmeldung eines PPs bei einem FP (als Subscription bezeichnet) ist in der Regel ebenfalls die Eingabe einer PIN erforderlich.

Die Sicherheitsmechanismen für CAT-iq unterscheiden sich nicht grundlegend von klassischem DECT. Es sei aber darauf hingewiesen, dass die stark wachsende Anzahl von Kombigeräten, die neben DECT weitere Schnittstellen wie beispielsweise Ethernet, USB, WLAN, Mobilfunk oder Bluetooth besitzen, äußerst kritisch zu betrachten ist. Es gibt sogar DECT-FPs mit nahezu allen erdenklichen Smartphone-Funktionalitäten. Hieraus leiten sich diverse Gefährdungen ab, insbesondere bei der Verbindung von DECT und Internetdiensten, da die DECT-Sicherheitsmechanismen als nicht sicher genug einzustufen sind. Dennoch könnten diese Geräte Sicherheitsmechanismen auf Basis von IP oder höher nutzen, da der Transport von IP explizit in CAT-iq vorgesehen ist. Dies würde die Nutzung von als sicher geltenden Algorithmen ermöglichen und damit eine deutliche Aufwertung der Sicherheit bei DECT ermöglichen.

Eine detailliertere Beschreibung von DECT und den zugehörigen Sicherheitsmechanismen kann der Broschüre „Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte“ des BSI entnommen werden (siehe [BSI DrKoSi-2009]). Dabei ist insbesondere für DECT-Systeme, die noch nicht auf Basis des aktuellen DECT-Standards abgesichert werden können, auch der Sicherheitshinweis des BSI vom 14. Februar 2012 zu beachten (siehe [BSI SiDECT-2012]), in dem von der Benutzung von DECT grundsätzlich abgeraten wird, wenn man vertrauliche Gespräche führt.

9.1.8 Bluetooth

Bluetooth ist ein offener Industriestandard der Bluetooth Special Interest Group (BSIG) für die kabellose Sprach- und Datenkommunikation zwischen IT-Geräten im Nahbereich (Kabelersatz und Ad-hoc Networking). Die derzeit aktuelle Version der Spezifikation ist Version 4.1 (siehe [BSIG BTspec-2013]), wobei die entsprechenden Endgeräte erst gegen Ende 2014 erwartet werden. Gebräuchlich sind momentan Geräte, die die Spezifikationen V4.0 und V3.0 umsetzen). Seit der Spezifikation 4.0 gibt es zwei grundsätzliche Bluetooth-Technologiesysteme: Basic Rate (BR) und Low Energy (LE). Das Basic Rate System schließt die Spezifikationen Enhanced Data Rate (EDR), Alternate Media Access Control (MAC) und die Physical Layer Extension (PHY) ein.

Mit BR/EDR können Bruttodatenraten bis zu 3 Mbit/s erreicht werden. Bluetooth arbeitet wie WLAN nach IEEE 802.11b bzw. IEEE 802.11g im 2,4-GHz-ISM-Frequenzband. Generell können sich WLAN- und Bluetooth-Geräte gegenseitig stören. Bedingt durch die Bluetooth-Technik wird dabei meist das WLAN stärker gestört[35]. Je nach Bluetooth-Gerät kann die Störung auch im Abstand von einigen Metern noch zu einem signifikanten Leistungseinbruch im WLAN führen. Der im Bluetooth-Standard spezifizierte Mechanismus Adaptive Frequency Hopping (AFH) mildert lediglich diese Störungen.

Das LE-System zielt auf Anwendungen ab, die weniger Verbrauch, Komplexität, Kosten und Datendurchsatz als das BR/EDR-System benötigen. Geräte, die beide Systeme unterstützen, werden Smart Ready genannt.

9.1.8.1 Architektur

Um die Interoperabilität unterschiedlicher Geräte sicherzustellen, hat die Bluetooth Special Interest Group (SIG) Anwendungs-Profile definiert. Beispiele sind:

- Generic Access Profile: GAP ist ein grundlegendes Profil zur herstellerübergreifenden Kommunikation von Bluetooth-Geräten[36]. Auf GAP basieren viele Anwendungsprofile.
- Headset Profile und Handsfree Profile: Diese beiden Profile beschreiben Funktionen, die ein Mobiltelefon im Zusammenspiel mit einer Freisprecheinrichtung benötigt. Neben der reinen Übertragung von Sprache in beiden Richtungen spielt beim Handsfree Profile auch die Fernbedienung des Mobiltelefons eine Rolle.
- Dialup Network Profile (DUN-Profile) und Fax Profile: Diese Profile beschreiben Protokolle und Funktionen zur drahtlosen Anbindung von Modems oder Mobiltelefonen an Rechner mit dem Ziel, darüber Wählverbindungen zur Daten- oder Faxübertragung aufzubauen.
- File Transfer, Object Push und Synchronization Profile: Diese Profile werden zum Austausch von Dateien über Bluetooth genutzt. Wichtigste Anwendung ist die Synchronisierung von Kontakten, Terminen, Aufgaben und Mails zwischen tragbaren Geräten (Personal Information Manager, PIM) und Servern.

35 Bluetooth verwendet zur Übertragung ein Frequenzsprungverfahren (Frequency Hopping), bei dem üblicherweise nach einem Paket auf einen anderen Kanal gesprungen wird. Die Sprungsequenz belegt letztendlich das gesamte zur Verfügung stehende Spektrum. Dieses Verfahren ist robust gegenüber Interferenzen.

36 Das Bluetooth-GAP ist nicht zu verwechseln mit dem DECT-GAP; der „Generic Access“ bezieht sich lediglich auf den allgemeinen Zugriff durch Geräte verschiedener Hersteller innerhalb einer Technologie. Die ETSI-Spezifikationen für DECT sind nicht kompatibel zu den Spezifikationen der Bluetooth SIG.

Damit jedes Bluetooth-Gerät als Kommunikationspartner eindeutig zu identifizieren ist, verfügt es über eine 48 Bit lange, öffentlich bekannte und weltweit eindeutige Geräteadresse, die sogenannte Bluetooth Device Address.

Der Verbindungsaufbau erfolgt über die Prozeduren Inquiry und Paging.

- Per Inquiry kann ein Bluetooth-Gerät feststellen, ob sich andere Geräte im Sendebereich befinden. Nach einem Inquiry liegen alle Geräteadressen der gefundenen kommunikationsbereiten Geräte vor. Voraussetzung für das Auffinden eines Gerätes mittels Inquiry ist, dass dieses Gerät als erkennbar konfiguriert ist (engl. discoverable). Geräte ab der Spezifikation V2.1 + EDR unterstützen ein erweitertes Inquiry, bei dem zusätzlich Gerätename und unterstützte Dienste bekannt gemacht werden.
- Durch eine Paging-Anforderung kann eine Kommunikationsverbindung zu einem per Inquiry gefundenen Gerät aufgebaut werden. Das Gerät, das die Verbindung aufbaut, wird Master genannt, das andere Slave. Während des Paging sendet der Master seine Geräteadresse und seinen Zeittakt an den Slave.

Neben einer Punkt-zu-Punkt-Verbindung zwischen zwei Bluetooth-Geräten unterstützt Bluetooth auch Punkt-zu-Mehrpunkt-Verbindungen. Bis zu 255 Bluetooth-Geräte (im Sonderfall auch mehr) können in einem sogenannten Piconet als Slaves im Park-Mode mit einem Master vernetzt sein. Innerhalb eines Piconet können bis zu 7 Slaves gleichzeitig aktiv mit dem Master kommunizieren.

9.1.8.2 Sicherheitsmechanismen

Basis der in Bluetooth vorgesehenen kryptografischen Verfahren sind Verbindungsschlüssel (engl. Link Keys), die während der sogenannten Paarbildung (engl. Pairing) zwischen jeweils zwei Bluetooth-Geräten vereinbart werden. Es gibt verschiedene Pairing-Modelle, wobei kompliziertere Modelle, wie das Numeric Comparison, von LE-Systemen nicht unterstützt werden. Für ein erfolgreiches Numeric Comparison Pairing bei BR/EDR muss in beide Geräte die gleiche PIN eingetragen werden. Die PIN kann 1 bis 16 Byte lang sein und ist entweder durch den Nutzer konfigurierbar oder fest voreingestellt. Weitere Modelle, die bei BR/EDR den gleichen Namen tragen, bieten bei LE im Vergleich zu BR/EDR aufgrund der geringeren Komplexität schwächeren Schutz.

Zur Authentisierung wird ein Challenge-Response-Verfahren auf Basis eines symmetrischen Chiffrier-Verfahrens verwendet. Es wird grundsätzlich eine einseitige Authentisierung genutzt, d. h. ein Gerät (sog. Claimant) authentisiert sich gegenüber einem anderen Gerät (sog. Verifier). Wollen sich beide Geräte gegenseitig authentisieren, wird die Authentisierung mit vertauschten Rollen wiederholt.

Die Verschlüsselung kann optional verwendet werden, wenn sich mindestens eines der beiden kommunizierenden Geräte gegenüber dem anderen authentisiert hat. Dabei kann die Verschlüsselung sowohl vom Master, als auch vom Slave beantragt werden. Die Verschlüsselung selbst wird jedoch immer vom Master gestartet, nachdem er die notwendigen Parameter mit dem Slave ausgehandelt hat.

Weitere Informationen zu Bluetooth finden sich in der Broschüre „Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte“ des BSI (siehe [BSI DrKoSi-2009]).

9.2 Gefährdungen

Dieses Kapitel analysiert die Gefährdungslage für mobile und drahtlose Endgeräte und Systeme. Hierbei handelt es sich um Systeme, die als Ergänzung der bisher betrachteten kabelgebundenen TK-Systeme dienen:

- Nutzung von GSM/UMTS/LTE im Rahmen einer FMC- bzw. UCC-Lösung, d. h. mit Anbindung an die lokale TK-Anlage bzw. die lokalen UCC-Server
- Nutzung von WLAN für die Telekommunikation durch dedizierte VoIP-fähige WLAN-Handsets, Smartphones, Tablets und Laptops mit Softphone bzw. UCC-Clients und WLAN

- Nutzung von DECT
- Nutzung von Bluetooth, z. B. zwischen einem Headset und einem Tischtelefon oder einem PC

Basis für die folgenden Betrachtungen sind für den normalen Schutzbedarf die Bausteine B 3.404 „Mobiltelefon“, B 3.405 „PDA“ und B 4.6 „WLAN“ der IT-Grundschutz-Kataloge (siehe [BSI GSK-2013]), ergänzt durch die Festlegungen in den Broschüren „Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte“ und „Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte“ des BSI (siehe [BSI ÖMS-2008] und [BSI DrKoSi-2009]) sowie „Smartphones: Information security risks, opportunities and recommendations for users“ der ENISA (European Network and Information Security Agency, siehe [ENISA SmPh-2010]).

9.2.1 Höhere Gewalt

Auf mobile und drahtlose Systeme treffen wie für alle digitalen TK-Lösungen allgemein die Gefährdungen durch höhere Gewalt zu, die in den IT-Grundschutz-Katalogen genannt sind.

Wie bei anderen technischen Systemen kann es bei der Nutzung drahtloser Kommunikationsformen durch Feuer, Verschmutzung usw. zum Totalausfall der Systeme kommen. Dieser Fall kann auftreten, wenn entweder das System selbst oder die verwendeten Kommunikationsinfrastrukturen betroffen sind.

Spezifische Ausprägungen bei einem Einsatz solcher Systeme innerhalb eines Unternehmens oder einer Behörde ergeben sich durch die Nutzung von Systemkomponenten wie z. B. Antennen, die nur unzureichend vor höherer Gewalt geschützt werden können.

Ergänzend zu Gefährdung G 1.17 „Ausfall oder Störung eines Funknetzes“ der IT-Grundschutz-Kataloge sind bei einem erhöhten Schutzbedarf hinsichtlich der Verfügbarkeit für die hier betrachteten Systeme zusätzlich folgende Detaillierungen relevant.

G-TK-137 Störung durch Blitzeinschlag

Eine spezielle Gefährdung entsteht durch die gegebenenfalls erforderliche Montage von Antennen- und Übertragungskomponenten (Basisstationen, DECT Fixed Parts, WLAN Access Points) im Außenbereich durch die Gefahr von Blitzschlägen.

Die Ausprägung der Gefährdung ist abhängig vom Grad der Abstützung auf solche im Außenbereich montierten Systeme:

- Eine nur unterdurchschnittliche Gefährdung ergibt sich, sofern die mobile Telekommunikation ausschließlich als Ergänzung der drahtgebundenen Telekommunikation für wenige Teilnehmer genutzt wird.
- Wird eine große Gruppe von Teilnehmern oder gar ganze Unternehmens- oder Behördenbereiche ausschließlich über solche drahtlosen Systeme in das Gesamtnetz eingebunden, so ist die resultierende Gefährdung als überdurchschnittlich zu bewerten.

G-TK-138 Beeinträchtigung durch Großveranstaltungen

Der öffentliche Mobilfunk sieht im aktuellen Ausbau keine Reserven für eine überdurchschnittliche Belastung des Netzes mit extremen Lastspitzen im Rahmen einer Großveranstaltung vor. Hierdurch kann es bei derartigen Veranstaltungen mit vielen Mobilfunk-Teilnehmern vorkommen, dass ein Mitarbeiter der Organisation keine freie Kapazität erhält.

Auch andere drahtlose Kommunikationssysteme (z. B. WLAN), die bei Großveranstaltungen häufig eingesetzt werden, bedingen ein erhöhtes Störpotenzial für die lokal verwendeten Systeme in der eigenen Organisation.

Die Ausprägung der Gefährdung wird sowohl vom Grad der Abstützung als auch von der Menge der so angebundenen Teilnehmer bestimmt.

G-TK-139 Ausfall oder Störung eines öffentlichen Funknetzes

Eine spezielle Gefährdung ergibt sich bei mobilen Systemen durch die Abhängigkeit von öffentlichen Funknetzen, die nicht vom TK-Betreiber selbst verantwortet werden. Verschärfend kommt hinzu, dass eine Störungsbehandlung unter Einbeziehung von externen Betreibern erfolgen muss.

Der Ausfall oder die Störung eines Funknetzes kann außer den grundsätzlichen Ursachen beim Ausfall zentraler Einrichtungen insbesondere auch elektromagnetische Störungen zur Ursache haben. Derartige Störungen werden z. B. durch andere Funksysteme, aber auch durch höhere Gewalt wie z. B. Sonnenwinde hervorgerufen.

Die Ausprägung der Gefährdung ist abhängig vom Grad der Abstützung auf ein solches Funknetz:

- Eine nur geringe, unterdurchschnittliche Gefährdung ergibt sich, sofern die auf dem Funknetz basierende mobile Telekommunikation ausschließlich als Ergänzung der drahtgebundenen Telekommunikation genutzt wird.
- Wird das Funknetz als primäres Netz zur Telekommunikation verwendet, so ist die resultierende Gefährdung mit einer Großstörung gleichzusetzen, da keine unmittelbare Abstützung auf drahtgebundene Kommunikationsformen möglich ist.

9.2.2 Organisatorische Mängel

Organisatorische Mängel treffen mobile und drahtlose Systeme grundsätzlich genauso wie beliebige andere IT-Systeme. Verstärkt werden diese Mängel jedoch durch die Nutzung von mobilen Endgeräten wie Mobiltelefone oder Smartphones, für die eine angemessene Absicherung nur unzureichend möglich ist.

Ergänzend zu Gefährdung G 1.17 „Ausfall oder Störung eines Funknetzes“ der IT-Grundschutz-Kataloge sind bei einem erhöhten Schutzbedarf hinsichtlich der Verfügbarkeit für die hier betrachteten Systeme zusätzlich folgende Detaillierungen relevant.

G-TK-140 Fehlende oder unzureichende Regelungen sowie unzureichende Kenntnis über Regelungen bei intelligenten mobilen Endgeräten

Grundsätzlich entstehen analog zu G 2.1 „Fehlende oder unzureichende Regelungen“ und G 2.2 „Unzureichende Kenntnis über Regelungen“ der IT-Grundschutz-Kataloge auch bei mobilen und drahtlosen Systemen spezifische Gefährdungen, wenn die Regelungen hinsichtlich Konfiguration und Betrieb eines mobilen Endgerätes fehlen oder unzureichend sind.

Verstärkt werden diese allgemeinen Gefährdungen durch die eingeschränkten Betriebssystem-Funktionalitäten mobiler Endgeräte, insbesondere Mobiltelefone, Smartphones und Tablets:

- Auch Systeme der neuesten Ausprägung haben seitens des Betriebssystems immer noch kein Berechtigungskonzept für Benutzer. Der Nutzer hat weitgehende administrative Berechtigungen auf seinem mobilen Gerät. Somit kann ein Benutzer beabsichtigt oder unbeabsichtigt Sicherheitsmechanismen unterlaufen, kritische Parametereinstellungen vornehmen und die Installation schadenstiftender Software ermöglichen oder erlauben.

  Hier muss eine entsprechende Regelung für den Umgang mit mobilen Endgeräten greifen, die allen Nutzern zur Kenntnis gebracht wird.

- Die Speicherung von kritischen Daten auf einem mobilen Endgerät, speziell einem Smartphone oder Tablet, birgt durch die mangelnde Absicherung solcher Geräte eine erhöhte Gefährdung.

  Es muss geregelt sein, welche Daten auf welchem multifunktionalen Endgerät gespeichert werden dürfen. Diese Regelung muss allen Nutzern bekannt gemacht werden.

G-TK-141 Fehlendes oder unzureichendes Management sowie unzureichende Kontrolle der IT-Sicherheitsmaßnahmen

Ergänzend zu G 2.4 „Unzureichende Kontrolle der Sicherheitsmaßnahmen“ sind mobile Endgeräte aufgrund ihrer flexiblen Einsatzmöglichkeiten nur schwer vollständig in ein Mobile Device Management als automatisiertem Kontrollsystem bzgl. der Sicherheitsmaßnahmen einzubinden. Häufig kann eine Management-Operation, z. B. ein Software-Update, nicht unmittelbar erfolgen bzw. erzwungen werden, z. B. weil das Gerät nicht erreichbar ist. Somit besteht eine erhöhte Gefährdung, dass mobile Endgeräte keine aktuelle Software bzw. inkorrekte Einstellungen haben.

Beispiel: Diverse mobile Systeme sind anfällig gegenüber schadenstiftender Software (Viren, Würmer und Trojaner) und haben zudem Schwachstellen, die einen unberechtigten Zugriff gestatten. Diese Geräte sind aber oft nicht in ein zentrales Patch-Management eingebunden. In Folge wird z. B. ein Patch des Betriebssystems zu spät und nicht auf allen Endgeräten eingespielt.

Daher muss für die Prüfung von Umsetzung und Einhaltung von Sicherheitsmaßnahmen ein höherer Aufwand kalkuliert werden. Insbesondere müssen Regelungen getroffen werden, wie alle Systeme regelmäßig erfasst werden können.

G-TK-142 Unzureichender Schutz vor unberechtigtem Zugriff auf Mobile Endgeräte und deren Daten

Im Bereich der mobilen und drahtlosen Systeme werden insbesondere Mobiltelefone, Smartphones und Tablets mit weitreichenden PC-ähnlichen Funktionalitäten eingesetzt. Eine vergleichbare Absicherung mit einem abgestuften Benutzerkonzept steht jedoch derzeit nicht zur Verfügung. Somit können die z. T. umfangreichen Daten, die auf den Systemen gespeichert sind, auch von anderen, jedoch nicht autorisierten Personen gelesen werden.

Beispiel: Smartphones erlauben eine Speicherung von vielen Daten, insbesondere auch E-Mails, Text- und Tabellen-Dokumenten. Ein Zugangsschutz sieht das Betriebssystem vielleicht zwar vor, wird aber nicht erzwungen und durch Nutzer ggf. nicht aktiviert.

G-TK-143 Ungeordneter Weitergabe oder Außerbetriebnahme

Die Gefährdung G 3.44 „Sorglosigkeit im Umgang mit Informationen“ der IT-Grundschutz-Kataloge trifft auf mobile Endgeräte wie Smartphones und Tablets in besonderem Maße zu, da hier Daten, häufig auch personenbezogene Daten wie Kontaktdaten, auf dem Gerät selbst, auf der SIM-Karte oder auf einem mobilen Datenträger gespeichert werden. Aufgrund des fehlenden Benutzerkonzepts und der mangelnden Absicherung solcher Geräte stehen derartige Daten einem neuen Benutzer ebenfalls zur Verfügung.

G-TK-144 Unzureichendes Schlüsselmanagement bei Verschlüsselung

Aufgrund der erhöhten Abhörgefahr auf der Luftschnittstelle erhält die Verschlüsselung der Kommunikation mit mobilen und drahtlosen Systemen eine besondere Bedeutung. Eine erhöhte Gefährdung ergibt sich durch systemspezifische Mechanismen.

- WLAN: Eine Absicherung der WLAN-Kommunikation mittels WEP (Wired Equivalent Privacy) ist seit geraumer Zeit als vollständig unzureichend nachgewiesen worden. Die Absicherung über WPA2-PSK (Wi-Fi Protected Access – Pre-Shared Key) basiert auf einem gemeinsamen Passwort und damit dessen Komplexität und Wechselintervall. Werden die Passwörter zu selten gewechselt, bieten sie keinen ausreichenden Schutz.
- GSM/UMTS/LTE: Bei der Nutzung von GSM/UMTS/LTE hat der Endnutzer keinen Einfluss auf die eingesetzten Sicherheitsmechanismen. Der Kunde muss eine entsprechende Vertrauensbasis gegenüber dem Provider haben. Selbst wenn die Kommunikation auf der Luftschnittstelle verschlüsselt wird, ist nicht ausgeschlossen, dass gewisse Übertragungs-strecken im Netz des Providers unverschlüsselt genutzt werden.

- DECT: Die bei DECT-Systemen implementierten Sicherheitsmechanismen werden nicht sehr hoch bewertet und stellen somit eine erhöhte Gefährdung dar. Verstärkt wird die Gefährdung durch die üblicherweise unsicheren Voreinstellungen auf den DECT-Systemen sowie durch den Anschluss eines PP, der keine Sicherheitsmechanismen unterstützt.
- Bluetooth: Die in Bluetooth implementierten Sicherheitsmechanismen haben in der Vergangenheit immer wieder Schwachstellen durch eine unsachgemäße Benutzung oder durch Implementierungsfehler gezeigt. Als anfällig hat sich hier insbesondere die Phase der initialen Verbindung (Pairing) erwiesen. In diesem Zusammenhang ist insbesondere die Verwendung schwacher PINs als kritisch einzustufen.

G-TK-145 Einschränkung durch unzureichende Kapazitäten des genutzten Datendienstes

Durch zu gering geplante Kapazitäten kann es im Shared Medium Funk zu deutlichen Leistungsengpässen kommen. Diese können durch eine in der ursprünglichen Planung nicht berücksichtigte vermehrte Nutzung oder gestiegene Nutzerzahl verursacht werden.

Insbesondere bei Nutzung von Datendiensten für Sprache und Video kann bereits ein geringer Nutzungsanstieg einen Engpass für die Sprach- oder Videoübertragung bedeuten und zu einer Verminderung der Dienstgüte führen.

G-TK-146 Unkontrollierter paralleler Aufbau von Kommunikationsverbindungen

Diese allgemein gültige Gefährdung für jede Kommunikationsschnittstelle wird im Bereich der Telekommunikation dadurch verstärkt, dass mobile Endgeräte oft mindestens zwei Kommunikationsmöglichkeiten, GSM/UMTS/LTE und Bluetooth/WLAN, integriert haben.

Hierdurch ist es theoretisch möglich, dass Daten einer internen WLAN/Bluetooth-Verbindung über eine externe GSM/UMTS/LTE-Verbindung abfließen.

G-TK-147 Unzureichende Planung für die Nutzung von VoIP, Video und UCC-Diensten

Je nach eingesetzter Funktechnik, insbesondere für WLAN, ergeben sich durch eine unzureichende Planung Gefährdungen. Ergänzend zu Gefährdung G 2.117 „ Fehlende oder unzureichende Planung des WLAN-Einsatzes“ trifft dies insbesondere für die Nutzung von Sprache, Video und UCC-Diensten zu. Typische Planungsfehler finden sich in der Dimensionierung der Funkzellen für VoIP und Video, im Einsatz von QoS-Mechanismen gemäß WMM bzw. IEEE 802.11e und in der Gestaltung der Absicherung gemäß IEEE 802.11i. Weiterhin bestehen für die drahtlose Telekommunikation erhöhte Anforderungen durch die Mobilität, insbesondere kann der unterbrechungsfreie Wechsel zwischen Funkzellen gestört sein. Die genannten WLAN-Gefährdungen gelten insbesondere auch für FMC-Lösungen.

G-TK-148 Unzureichende Planung für den Einsatz in widrigen Umgebungsbedingungen

Mobile und drahtlose Kommunikationssysteme werden auch in Bereichen eingesetzt, in denen eine drahtgebundene Telekommunikation nur schwer realisierbar ist und die widrigen Umgebungsbedingungen (Temperatur, Luftfeuchtigkeit, Staub, Verschmutzung und Erschütterung) ausgesetzt sind. Insbesondere sind hier Außenbereiche, Industriebereiche und Kellerbereiche zu nennen, aber auch Treppenhäuser, Messehallen usw.

Komponenten in solchen ungeschützten Bereichen sind im Vergleich zu Komponenten, die in dedizierten Technikräumen stehen, vermehrt widrigen Umwelteinflüssen wie unzulässigen Temperatur- und Luftfeuchtebereichen ausgesetzt. Auch die Belastung durch Staub und Verschmutzung ist gegenüber geschützt montierten Systemen deutlich erhöht.

Die Ausprägung der Gefährdung ist abhängig von der Menge der so angebundenen Teilnehmer und dem Grad der Abstützung auf solche Systeme.

9.2.3 Menschliche Fehlhandlungen

Durch die Nutzung von mobilen und drahtlosen Systemen steigt die Komplexität des Gesamtsystems; diese wird weiter verstärkt durch die meist zusätzliche und unkoordinierte Nutzung von drahtlosen Systemen, z. B. Smartphones, zu sonstigen Telekommunikationssystemen. Damit wächst insbesondere das Risiko einer menschlichen Fehlhandlung, da z. B. die Konsequenzen einer Handlung auf andere Teilsysteme mangels geeigneter Schulung nicht bedacht werden.

Damit gelten – sofern technisch anwendbar – grundsätzlich alle in den IT-Grundschutz-Katalogen aufgeführten Gefährdungen im Bereich menschlicher Fehlhandlungen, insbesondere ist folgende spezifische Ausprägung für die hier betrachteten Systeme zu beachten.

G-TK-149 Konfigurations- und Bedienungsfehler bei mobilen Endgeräten

Als Spezialisierung der Gefährdung G 3.38 „Konfigurations- und Bedienungsfehler“ der IT-Grundschutz-Kataloge muss beachtet werden, dass bei diversen mobilen Endgerätetypen, insbesondere bei Smartphones und Tablets, der Endnutzer meist automatisch einen administrativen Zugang hat. Dies führt im Vergleich zu Systemen mit Berechtigungskonzept zu häufiger auftretenden Bedienungsfehlern.

Diese Gefährdung wird verstärkt, wenn sich mobile Endgeräte nicht umfassend zentral konfigurieren und administrieren lassen.

9.2.4 Technisches Versagen

Für den Einsatz von mobilen und drahtlosen Endgeräten gelten prinzipiell alle in den IT-Grundschutz-Katalogen genannten Gefährdungen wie Stromausfall, Datenbankausfall, mangelnde Verschlüsselung usw., sofern diese für ein konkretes System technisch relevant sind. Darüber hinaus gelten folgende spezifische Ausprägungen:

G-TK-150 Verlust von Kontaktdaten und sonstigen gespeicherten Daten

Ergänzend zu Gefährdung G 4.52 „Datenverlust bei mobilem Einsatz“ sind die hier betrachteten mobilen Endgeräte besonders gefährdet, da

- insbesondere auf Smartphones und Tablets neben Kontaktdaten auch andere ggf. kritische Daten gespeichert werden,
- bei der Verwendung mobiler Endgeräte die Zeitspannen zwischen Synchronisationen bzw. Backups meist größer sind als bei fest installierten Geräten,
- bei mobilen Endgerätetypen wie Mobiltelefonen und Smartphones die Verantwortung für Synchronisation und ggf. für Backups beim Nutzer liegt,
- durch das dauerhafte Mitführen eines mobilen Endgerätes auch bei privaten Aktivitäten die Gefährdung durch einen Diebstahl und den damit verbundenen Datenverlust erhöht ist.

G-TK-151 Unerwünschter Datenzugriff durch Apps auf mobilen Endgeräten

Manche Apps greifen unbemerkt auf Daten, z. B. Kontakt- und Positionsdaten, die auf dem mobilen Endgerät gespeichert sind, zu und übertragen diese Daten an eine zentrale Stelle außerhalb der Organisation zur weiteren Auswertung. Wenn eine solche App installiert wird, können bei diversen existierenden Systemen solche Rechte nicht mehr entzogen werden.

Darüber hinaus kann durch einen Fehler oder Fehlkonfiguration im mobilen Betriebssystem ein unberechtigter Zugriff auf Daten einer anderen App oder des Betriebssystems erfolgen.

9.2.5 Vorsätzliche Handlungen

Gerade in der Gefährdungskategorie „Vorsätzliche Handlungen“ ist es wichtig zu beachten, dass im Bereich der mobilen und drahtlosen Systeme häufig eine Infrastruktur genutzt wird, die nicht ausschließlich in der Verantwortung der Organisation liegt.

Ergänzend zu den Gefährdungen der IT-Grundschutz-Kataloge bzgl. PDA und Mobiltelefon sind folgende Gefährdungen für mobile Endgeräte, speziell für Smartphones und Tablets, zu beachten.

G-TK-152 Umfassende bzw. zielgerichtete missbräuchliche Überwachung mobiler Endgeräte und deren Nutzer

Durch Schwachstellen im mobilen Betriebssystem, entsprechende schadenstiftende Software oder unzureichende Berechtigungskonzepte für Apps ist die Erstellung umfassender Profile (Bewegungs- und Nutzungsprofile) einer Vielzahl mobiler Endgeräte und deren Nutzer möglich.

Außerdem ist so auch die zielgerichtete, vollständige Überwachung einzelner mobiler Endgeräte bzw. deren Nutzer möglich.

G-TK-153 Einschränkungen durch Malware

Durch Malware können mobile und drahtlose Systeme derart gestört werden, dass die eigentliche Applikation der Telekommunikation nur noch unzureichend nutzbar ist. Eine solche Gefährdung wird dadurch verstärkt, dass die Infektion mit Malware über die Datendienste eines mobilen Endgerätes erfolgt, die Schadfunktion sich aber auch auf die Telekommunikationsfunktion des Gerätes auswirkt. Beispielsweise startet das Gerät nach einer Infektion nicht mehr oder man kann nicht mehr telefonieren oder das Telefonbuch wird gelöscht. Darüber hinaus gibt es für mobile Endgeräte zusätzliche Möglichkeiten einer Infektion über unterschiedliche Kommunikationsschnittstellen (Bluetooth, lokaler Angriff über WLAN, Internet via WLAN, Internet via UMTS oder LTE).

Dabei ist zu beachten, dass schadenstiftende Software (Malware) mittlerweile mit erheblich steigender Tendenz für verschiedene Betriebssysteme (insbesondere Android) für Mobiltelefone, Smartphones und Tablets vorhanden ist.

9.3 Sicherheitsmaßnahmen

Die Anbindung von GSM/UMTS/LTE-Mobilstationen an eine TK-Anlage und allgemein an die IT-Infrastruktur zur Nutzung von UCC-Diensten erfordert die im Folgenden beschriebenen Maßnahmen. Allgemeine Hinweise zur Nutzung mobiler Endgeräte und mobiler Applikationen gibt [BSI Mobil-2006]. Die Struktur des Maßnahmenkatalogs orientiert sich an den für den Nutzer solcher Systeme relevanten Teilen der Systemarchitektur:

- Maßnahmen auf Ebene der Server und Anwendungen (siehe Kapitel 9.3.1)
- Maßnahmen zur Absicherung der Endgeräte (siehe Kapitel 9.3.2)
- Maßnahmen im Bereich des Netzwerks (siehe Kapitel 9.3.3)
- Maßnahmen zum Netz- und Systemmanagement (siehe Kapitel 9.3.4)

Generell gilt für die Einbindung der hier betrachteten mobilen und drahtlosen Endgeräte:

- Mobilfunk: Für den normalen Schutzbedarf bilden für Mobilfunk die in den Bausteinen B 3.404 „Mobiltelefon“ und Baustein B 3.405 „PDA“ sowie in der Broschüre „Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte“ des BSI beschriebenen Maßnahmen die Grundlage (siehe [BSI ÖMS-2008]).
- WLAN: Die Maßnahmen, die im Baustein B 4.6 „WLAN“ der IT-Grundschutz-Kataloge für den normalen Schutzbedarf sowie in der „Technischen Richtlinie Sicheres WLAN“ und der Broschüre „Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte“ des BSI (siehe [BSI TRWLAN-2005] und

[BSI DrKoSi-2009]) für den normalen und den erhöhten Schutzbedarf festgelegt sind, gelten uneingeschränkt auch für die Anwendung von WLAN im Bereich der Telekommunikation (d. h. primär für VoIP über WLAN). Weiterhin behalten diverse Maßnahmen, die in Kapitel 4.3.2 für kabelbasierte Clients beschrieben sind, auch für WLAN ihre Gültigkeit.

- DECT: Maßnahmen zur Absicherung von DECT-Systemen für den normalen Schutzbedarf sind in der Broschüre „Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte“ des BSI beschrieben (siehe [BSI DrKoSi-2009]). Bei einem erhöhten Schutzbedarf ist der Einsatz von weitergehenden Sicherheitsmechanismen zwingend erforderlich. Für DECT-Systeme, die noch nicht auf Basis des aktuellen DECT-Standards abgesichert werden können, muss bei einem erhöhten Schutzbedarf von der Nutzung von DECT abgeraten werden.
- Bluetooth: Für den normalen Schutzbedarf bilden für Bluetooth die im Baustein B 4.8 „Bluetooth“ sowie in der Broschüre „Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte“ des BSI beschriebenen Maßnahmen die Grundlage (siehe [BSI DrKoSi-2009]).

Für den erhöhten Schutzbedarf sind ergänzend folgende Maßnahmen vorgesehen.

9.3.1 Server und Anwendungen

In diesem Kapitel werden für die einzelnen betrachteten mobilen und drahtlosen Systeme die für Server und Anwendungen relevanten Sicherheitsmaßnahmen erarbeitet:

- Mobilfunk und Fixed Mobile Convergence, siehe Kapitel 9.3.1.1
- Wireless LAN (WLAN), siehe Kapitel 9.3.1.2
- DECT, siehe Kapitel 9.3.1.3
- Bluetooth, siehe Kapitel 9.3.1.4

9.3.1.1 Mobilfunk und Fixed Mobile Convergence

M-TK-186 Gegenseitige Authentisierung von mobilen Endgeräten und einer zentralen Komponente der FMC- bzw. UCC-Lösung

Mobile Endgeräte und eine zentrale Server-Komponente der FMC- bzw. UCC-Lösung müssen sich gegenseitig authentisieren. Nur authentisierte Endgeräte dürfen über die FMC-Lösung kommunizieren. Für die Authentisierung kommen beispielsweise zertifikatsbasierte Verfahren in Betracht.

M-TK-187 Schutz von Servern für mobile Endgeräte

Die zentrale Server-Komponente der FMC- bzw. UCC-Lösung muss einen Zugriff der mobilen Endgeräte gestatten. Hierzu ist die zentrale Server-Komponente entsprechend zu härten und der Zugang entsprechend zu kontrollieren (siehe Maßnahmen M-TK-228 bis M-TK-232). Dies betrifft allgemein Server für mobile Endgeräte (z. B. Server für die Synchronisation mit E-Mail, Kalender usw.). Solche Systeme dürfen im Normalfall nicht direkt an das Internet angebunden werden, sondern nur über Sicherheits-Gateways (je nach Sicherheitsanforderungen eine Kombination aus Firewalls, Application Layer Gateways und Intrusion-Prevention-Systemen).

M-TK-188 Verwendung einer Ende-zu-Ende-Verschlüsselung für die Telekommunikation

Für die Telekommunikation (Sprache, Video, UCC) bei erhöhtem Schutzbedarf muss eine Ende-zu-Ende-Verschlüsselung zwischen den beteiligten Endgeräten oder zumindest zwischen dem verwendeten mobilen Endgerät und einem Gateway bzw. einer Verschlüsselungsbox im Sicherheitsbereich der organisationsinternen TK-Lösung erfolgen. Dies gilt unabhängig davon, ob ein Endgerät gerade über GSM/UMTS/LTE oder WLAN verbunden ist.

Die Schlüssellänge muss mindestens 128 Bit betragen. Als zugrunde liegendes Verschlüsselungsverfahren kommt AES in Frage. Ein sicheres, dynamisches Schlüsselmanagement, z. B. basierend auf Zertifikaten oder dem Diffie-Hellman-Verfahren, muss unterstützt werden. Wenn die Sprachübertragung über IP erfolgt, ist möglichst Secure Real-Time Transport Protocol (SRTP) und Secure RTP Control Protocol (SRTCP) zu verwenden.

M-TK-189 Verschlüsselung von Nachrichten

Nachrichten mit einem erhöhten Schutzbedarf, die per SMS oder MMS übertragen werden sollen, müssen Ende-zu-Ende verschlüsselt werden. Hierzu ist auf den Endgeräten eine entsprechende Anwendung erforderlich.

Die Schlüssellänge muss mindestens 128 Bit betragen. Als zugrunde liegendes Verschlüsselungsverfahren kommt AES in Frage. Ein sicheres, dynamisches Schlüsselmanagement, z. B. basierend auf Zertifikaten oder dem Diffie-Hellman-Verfahren, muss unterstützt werden.

M-TK-190 Einsatz von Server-based Computing

Die Speicherung von organisationsinternen Daten mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit sollte auf mobilen Endgeräten möglichst vermieden werden.

Dies kann durch den Einsatz von Server-based Computing erreicht werden (siehe Kapitel 9.1.2), da hierdurch die Verarbeitung organisationsinterner Daten an zentraler Stelle erfolgt.

Hinweis: Der Einsatz von Server-based Computing ist ggf. mit erheblichen Einschränkungen des Nutzerkomforts beim Bearbeiten von Daten verbunden.

Wenn diese Maßnahme nicht angemessen umgesetzt werden kann, ist M-TK-196 „Schutz der organisationsinternen Daten auf einem mobilen Endgerät“ umzusetzen.

9.3.1.2 Wireless LAN

M-TK-191 Verschlüsselung, Integritätsschutz und Authentisierung auf der Luftschnittstelle

Auf der Luftschnittstelle müssen Verschlüsselung und Integritätsschutz möglichst gemäß IEEE 802.11i bzw. WPA2 erfolgen. Im Ausnahmefall (z. B. zur Unterstützung älterer Systeme) kann WPA eingesetzt werden. Bevorzugt sollte CCMP aktiviert werden, anderenfalls müssen zumindest TKIP-Verschlüsselung und der zugehörige Integritätsschutz genutzt werden.

Die Authentisierung sollte möglichst über IEEE 802.1X (WPA2-Enterprise bzw. WPA-Enterprise) erfolgen. Dabei muss eine dem erhöhten Schutzbedarf angemessene Authentisierungsmethode eingesetzt werden, bevorzugt EAP-TLS. Bei einem Zellwechsel während eines Telefonats (Handover) kann eine Authentisierung per IEEE 802.1X zu einer kurzzeitigen Leistungseinbuße verbunden mit hörbaren Beeinträchtigungen der Übertragungsqualität führen. Eine typische Maßnahme ist an dieser Stelle die Verwendung eines Controller-basierten WLAN-Designs.

In kleineren WLANs, in denen nur eine geringe Anzahl von WLAN-Stationen zu verwalten ist (SOHO-Bereich), können Pre-Shared Keys (d. h. WPA2-Personal) eingesetzt werden.

M-TK-192 Ende-zu-Ende-Verschlüsselung für Medienströme

Für den erhöhten Schutzbedarf muss Maßnahme M-TK-191 „Verschlüsselung, Integritätsschutz und Authentisierung auf der Luftschnittstelle“ möglichst durch eine Ende-zu-Ende-Verschlüsselung der Medienströme ergänzt werden. Auf diese Weise wird die Übertragung auf der Luftschnittstelle zweifach abgesichert und ein Ausfall eines einzelnen Mechanismus (z. B. wenn durch eine Fehlkonfiguration am Access Point auf der Luftschnittstelle unverschlüsselt übertragen wird) führt nicht zwangsläufig zu einem unsicheren WLAN. Weiterhin wird durch diese Maßnahme dafür gesorgt, dass die Kommunikation über die Luftschnittstelle hinaus geschützt wird.

Für die Ende-zu-Ende-Verschlüsselung der Medienströme sollten möglichst SRTP und SRTCP eingesetzt werden. Alternativ können VPN-Techniken (basierend auf IPsec oder TLS) eingesetzt werden, sofern eine dem erhöhten Schutzbedarf angemessene Verschlüsselung mit einer Schlüssellänge von mindestens 128 Bit eingesetzt wird.

M-TK-193 Absicherung Authentication-Server

Über den Authenticator (Access Point bzw. WLAN-Controller) findet ein indirekter Dialog zwischen Supplicant (d. h. einem Client) und dem Authentication-Server statt. Dabei kann ein Supplicant in einer EAP-Methode an einen Authenticator potenziell schadenstiftende Daten übertragen. Der Authentication-Server (typischerweise ein RADIUS-Server) muss also entsprechend gehärtet sein (siehe Maßnahme M-TK-229 „Härtung von Servern des Telekommunikationssystems"). Dabei sind insbesondere ungenutzte RADIUS-spezifische Funktionen und EAP-Methoden zu deaktivieren.

Bei einem erhöhten Schutzbedarf ist außerdem zu empfehlen, die Qualität des RADIUS-Servers und der Implementierung der eingesetzten EAP-Methoden im Rahmen von Penetrationstests eingehend zu prüfen.

9.3.1.3 DECT

Die Absicherung der zentralen Anlage erfolgt gemäß der Basistechnologien Klassische Telekommunikationstechnik und ggf. Voice over IP (siehe Kapitel 3 und 4).

9.3.1.4 Bluetooth

Für Bluetooth als Übertragungssystem gibt es keine zentralen Komponenten.

9.3.2 Endgeräte

In diesem Kapitel werden für die einzelnen betrachteten mobilen und drahtlosen Systeme die für Endgeräte relevanten Sicherheitsmaßnahmen erarbeitet:

- Mobilfunk und Fixed Mobile Convergence, siehe Kapitel 9.3.2.1
- Wireless LAN (WLAN), siehe Kapitel 9.3.2.2
- DECT, siehe Kapitel 9.3.2.3
- Bluetooth, siehe Kapitel 9.3.2.4

9.3.2.1 Mobilfunk und Fixed Mobile Convergence

M-TK-194 Einsatz von abhörsicheren Mobiltelefonen

Bei erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit und Integrität ist der Einsatz von besonders geschützten, abhörsicheren Telefonen in Betracht zu ziehen. Derartige Telefone erlauben die konsequente Verschlüsselung der Daten (inkl. Sprache) bei Übertragung und Speicherung auf dem Endgerät. Außerdem sind diese Endgeräte durch besondere Maßnahmen auf Ebene der Hardware vor unberechtigten Zugriffen geschützt.

M-TK-195 Absicherung aller Kommunikationsschnittstellen des Endgerätes

Neben der GSM/UMTS/LTE-Funkschnittstelle (die automatisch über die in den GSM/UMTS/LTE-Standards spezifizierten Mittel abgesichert wird) verfügt ein Endgerät über weitere Kommunikationsschnittstellen, die – sofern sie nicht deaktiviert sind – abgesichert werden müssen. Dies beinhaltet auch die Absicherung einer WLAN-Schnittstelle gemäß Kapitel 9.3.1.2 und einer Bluetooth-Schnittstelle gemäß Kapitel 9.3.1.4. In diesem

Zusammenhang sollten zur Härtung des Endgerätes auch alle nicht benötigten bzw. sicherheitskritischen Dienste und Leistungsmerkmale deaktiviert werden.

M-TK-196 Schutz der organisationsinternen Daten auf einem mobilen Endgerät

Organisationsinterne Daten mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit und Integrität sind auf einem mobilen Endgerät zwingend zu verschlüsseln. Dabei können z. B. Verschlüsselungstechniken auf Ebene einer Virtualisierungslösung oder einer Container-Technologie (siehe Kapitel 9.1.1) zum Einsatz kommen.

Die Schlüssel zur Entschlüsselung sollten dabei getrennt vom Endgerät in einem sicheren Speicher, z. B. auf einer Smartcard oder der SIM-Karte, aufbewahrt werden. Als Speicherort für personenbezogene Daten (und generell anderen Daten mit erhöhtem Schutzbedarf) kann - sofern technisch möglich - ebenfalls die SIM-Karte verwendet werden.

Diese Maßnahme ist insbesondere dann wichtig, wenn Maßnahme M-TK-190 „Einsatz von Server-based Computing“ nicht geeignet umgesetzt werden kann.

M-TK-197 Erweiterung von Data Loss Prevention auf mobile Endgeräte

Data Loss Prevention (DLP) ist ein Mittel, um den Abfluss von organisationsinternen Daten und sensiblen Informationen aus dem Netz einer Organisation zu unterbinden. Grundlage ist eine generelle Klassifikation aller in der Organisation verarbeiteter Daten, auf deren Basis eine Entscheidung über die Zulässigkeit von Transaktionen (z. B. Weiterleiten von Anhängen, Speicherung auf Wechseldatenträgern) getroffen wird. DLP-Systeme arbeiten entweder Host- oder Netzwerk-basiert.

Werden organisationsinterne Daten mit erhöhtem Schutzbedarf hinsichtlich der Vertraulichkeit auf mobilen Endgeräten gespeichert, so sollte möglichst ein DLP-System genutzt werden.

M-TK-198 Sperrung des mobilen Endgerätes für Nutzereingaben

Für den erhöhten Schutzbedarf muss ein Endgerät die Möglichkeit bieten, dass ein Nutzer das Gerät für Nutzereingaben sperren kann. Bei einem gesperrten Gerät steht nur ein eingeschränkter Dienstumfang (Annahme von Rufen, Absetzen von Notrufen) zur Verfügung. Eine solche Sperre muss (sofern technisch möglich) automatisch nach einer gewissen Zeitspanne ohne Nutzereingabe erfolgen.

Wenn dieser automatische Sperrvorgang nicht möglich ist bzw. der Nutzer diese Funktion deaktivieren kann, muss der Umgang des Nutzers mit der Sperrfunktion organisatorisch geregelt werden.

Das Entsperren muss über die Eingabe einer PIN oder eines Passworts hinreichender Komplexität erfolgen. Das Gerät sollte so konfiguriert werden, dass nach einer gewissen, festlegbaren Anzahl von fehlgeschlagenen Authentisierungsversuchen weitere Anmeldeversuche blockiert werden. Authentisierungsversuche (zumindest fehlgeschlagene Versuche) sollten protokolliert werden.

Der Nutzer sollte diese Funktion nicht deaktivieren dürfen. Andernfalls muss der Umgang des Nutzers mit der Sperrfunktion organisatorisch geregelt werden.

Zum Entsperren muss der Nutzer sich am Endgerät gemäß Maßnahme M-TK-199 „Benutzerauthentisierung am mobilen Endgerät“ authentisieren.

M-TK-199 Benutzerauthentisierung am mobilen Endgerät

Für einen erhöhten Schutzbedarf muss das Endgerät die Möglichkeit einer Nutzer-authentisierung bieten, die über die Eingabe einer PIN zur Freischaltung der SIM-Karte hinausgeht.

Hierzu ist entweder ein Passwort hinreichender Komplexität oder ein Verfahren auf Smartcard-Basis zu verwenden.

Eine Authentisierung mittels biometrischer Merkmale muss im Einzelfall bewertet werden und ggf. ist aus Sicherheits- und Datenschutzgründen sogar davon abzuraten. Ein Beispiel, das kritisch hinterfragt werden muss, ist die Authentisierung am mobilen Endgerät über einen Fingerabdruck. Einerseits besteht die Befürchtung, dass die entsprechenden Daten vom Hersteller des mobilen Endgerätes bzw. des zugehörigen Betriebssystems gesammelt werden können. Andererseits konnte in der Vergangenheit immer wieder nachgewiesen werden, dass durch einen kopierten Fingerabdruck eine Authentisierung erfolgreich durchgeführt werden kann.

Das Gerät muss weiterhin so konfiguriert werden, dass nach einer festlegbaren Anzahl von fehlgeschlagenen Authentisierungsversuchen weitere Anmeldeversuche blockiert bzw. im Extremfall die Daten auf dem Gerät sogar gelöscht werden (engl. Wipe). Geräte, die eine Kill-Switch-Funktionalität unterstützen, müssen dabei so konfiguriert werden, dass der Kill-Switch nach mehrfacher Falscheingabe eines Benutzerpasswortes automatisch aktiviert wird. Authentisierungsversuche (insbesondere fehlgeschlagene Versuche) müssen protokolliert werden.

M-TK-200 Automatische Handlungen bei Verletzung von Sicherheitsrichtlinien auf mobilen Endgeräten

Werden die von der eigenen Organisation vorgegebenen Sicherheitsrichtlinien auf einem Endgerät verletzt, müssen automatisiert Aktionen erfolgen. Dies können je nach Kritikalität folgende Aktionen sein:

- Information eines Administrators bei geringfügigen Verletzungen der Sicherheitsrichtlinien, z. B. unterbliebenes Update einer App
- Sperren des mobilen Endgerätes bis zur Wiederherstellung der Sicherheitsrichtlinie bei mittlerer Kritikalität, z. B. Installation unzulässiger Apps
- Löschen der organisationsinternen Daten bzw. Löschen aller Daten auf dem mobilen Endgerät bei besonders kritischen Verletzungen von Richtlinien, z. B. Erlangung von Root-Rechten bzw. Jailbreak
- Aktivieren einer Kill-Switch-Funktionalität z. B. nach Diebstahl, sodass das Gerät weder mit einer neuen SIM-Karte noch nach einer Neuinstallation des Betriebssystems betrieben werden kann.

M-TK-201 Rollenbasierte Zugriffsberechtigungen auf Objekte des mobilen Endgerätes

Der Zugriff auf Objekte des Endgerätes, d. h. Dienste, Funktionen, Anwendungen, Parameter und gespeicherte Daten, für die ein erhöhter Schutzbedarf besteht, muss durch Zugriffsrechte kontrolliert werden können. Der Zugriff auf ein solches Objekt darf nur für einen (gemäß seiner Rolle) autorisierten und gemäß Maßnahme M-TK-199 „Benutzerauthentisierung am mobilen Endgerät“ authentisierten Benutzer gestattet werden. Dabei muss zumindest zwischen der Rolle eines Administrators und der Rolle eines normalen Nutzers unterschieden werden. Ein feiner strukturierbares Berechtigungskonzept ist wünschenswert.

M-TK-202 Schutz des mobilen Endgerätes vor schadenstiftender Software

Für mobile Endgeräte, die für schadenstiftende Software (z. B. Viren, Würmer, Trojanische Pferde und Spyware) anfällig sind, ist der Einsatz einer entsprechenden Schutz-Software unumgänglich. Die entsprechende Kombination von Funktionen aus den Bereichen MDM (insbesondere Verwaltung der Apps durch einen Company App Store), Personal Firewall, Virenschutz und Host-basiertem Intrusion Prevention System (IPS) muss für das jeweilige System abgestimmt werden.

Hinweis: Eine entsprechende Schutz-Software ist nicht für alle mobilen Betriebssysteme verfügbar und ist teilweise mit Einschränkungen verbunden (z. B. hinsichtlich der umfassenden Möglichkeiten zur Erkennung von schadenstiftender Software).

M-TK-203 Deaktivierung der automatischen Rufannahme

Die automatische Rufannahme muss, sofern möglich, für Endgeräte, die Daten mit einem erhöhten Schutzbedarf verarbeiten, deaktiviert werden.

M-TK-204 Schutz vor unerwünschter Konfigurationsänderung über die GSM/UMTS-Funkschnittstelle

Mit Hilfe spezieller Kurznachrichten lassen sich Konfigurationseinstellungen an mobile Endgeräte übermitteln – sogenanntes Over the Air (OTA) Provisioning (auch Service-SMS genannt). OTA Provisioning erlaubt außerdem die Übertragung von Firmware an ein mobiles Endgerät (Firmware Over the Air, FOTA). Weiterhin unterstützen moderne SIM-Karten die Speicherung von Programmen, die per SMS auf die SIM-Karte übertragen werden können (als SIM-Toolkit bezeichnet).

Gegen den Empfang von OTA-Provisioning-SMS (und verwandter Techniken) sowie gegen SIM-Toolkit gibt es keine unmittelbaren Schutzmaßnahmen. Die Betriebssysteme der Endgeräte müssen die Manipulation von Konfigurationsdaten von außen durch den Netzbetreiber nur auf ausdrückliche Betätigung des Anwenders hin zulassen. Hier muss der Nutzer entsprechend informiert werden.

M-TK-205 Schutzmaßnahmen für das Herunterladen von Inhalten

Eine Verbindung über das Internet darf erst nach Bestätigung durch den Nutzer aufgebaut werden. Eine Ausnahme bilden geeignet authentisierte Computer, die dem Vertrauensbereich der lokalen IT-Infrastruktur (bzw. TK-Anlage) zugeordnet sind und zu denen eine verschlüsselte Verbindung aufgebaut wird.

Weiterhin muss das mobile Endgerät so konfiguriert werden, dass eine Bestätigung durch den Nutzer vor dem Herunterladen von Inhalten (inklusive MMS) erforderlich ist. Beim Zugriff auf aktive Inhalte gelten dabei allgemein die Schutzmaßnahmen der IT-Grundschutz-Kataloge.

Beim Zugriff auf Inhalte mit erhöhtem Schutzbedarf muss darauf geachtet werden, dass eine Absicherung gemäß den in Kapitel 6 auf den jeweiligen Anwendungstyp zutreffenden Maßnahmen verwendet wird.

M-TK-206 Prozess zur Behandlung des Verlusts eines mobilen Endgerätes

Werden auf mobilen Endgeräten vertrauenswürdige Daten gespeichert, muss ein Prozess zur Behandlung des Verlusts eines mobilen Endgerätes implementiert werden, der den Umgang mit diesen Daten bei Beeinträchtigung von Vertraulichkeit und Integrität regelt. Dies beinhaltet beispielsweise, dass Zugangsberechtigungen gesperrt werden und Zertifikate sowie Passwörter sofort zurückgezogen werden.

9.3.2.2 Wireless LAN

Für WLAN-Endgeräte, z. B. Notebook oder Tablet mit Softphone, gelten allgemein die in Kapitel 4.3.2 gelisteten Maßnahmen.

Es gelten außerdem auch für WLAN-Endgeräte die in Kapitel 9.3.2.1 spezifizierten Sicherheitsmaßnahmen, sofern diese sich sinngemäß auf WLAN-Endgeräte anwenden lassen.

9.3.2.3 DECT

Es gelten sinngemäß - sofern anwendbar - auch für DECT-Endgeräte die in Kapitel 9.3.2.1 spezifizierten Sicherheitsmaßnahmen.

M-TK-207 Einsatz von DECT-Endgeräten mit verbesserter DECT-konformer Verschlüsselung

Zur Authentisierung ist DSAA2 und zur Verschlüsselung der Daten auf der Luftschnittstelle ist DSC2 einzusetzen. Um die Verschlüsselung einsetzen zu können, müssen beide Geräte (FP und PP) DSC2 unterstützen. Das gleiche gilt für DSAA2 bei der Authentisierung. Es ist erforderlich,

dass bei beiden Endgeräten die Verschlüsselung automatisch aktiviert ist. Wenn eines der beiden Geräte die Methoden nicht unterstützt, sollte die Kommunikation unmittelbar von dem anderen Endgerät unterbrochen werden. Die Verschlüsselung sollte möglichst früh in der Kommunikation aktiv werden.

Die Endgeräte müssen einen regelmäßigen erneuten Schlüsselaustausch während einer laufenden Kommunikation (Re-keying) unterstützen. Das Intervall hierzu sollte bei mindestens 60 Sekunden liegen.

Die Dauer des Pairing eines FP, d.h. die automatische Erkennung und Konfiguration eines Endgerätes, darf 120 Sekunden nicht überschreiten. Anschließend muss der Pairing-Modus verlassen werden. Ein FP darf nicht automatisch nach dem Anschalten in den Pairing-Modus wechseln. Der Wechsel in den Pairing-Modus sollte stets aktiv vom Benutzer oder Administrator veranlasst werden.

M-TK-208 Einsatz von DECT-Endgeräten mit zusätzlicher Verschlüsselung

Bei erhöhtem Schutzbedarf sollten die eingesetzten Geräte neben der DECT-Standard-verschlüsselung möglichst zusätzlich eine Ende-zu-Ende-Verschlüsselung zwischen DECT-Endgeräten oder zwischen DECT-Endgeräten und einer an gesicherter Stelle im Festnetz installierten Verschlüsselungsbox unterstützen. Die Schlüssellänge muss mindestens 128 Bit betragen. Als zugrunde liegendes Verschlüsselungsverfahren kommt AES in Frage. Ein sicheres, möglichst dynamisches Schlüsselmanagement, z. B. basierend auf Zertifikaten oder dem Diffie-Hellman-Verfahren, muss unterstützt werden. Der Einsatz von Pre-Shared Keys ist nur bei einer geringen Anzahl von Endgeräten sinnvoll.

Die Endgeräte sollten so konfiguriert werden können, dass die zusätzliche Verschlüsselung grundsätzlich aktiviert ist. Wenn die zusätzliche Verschlüsselung bei Bedarf aktiviert wird, muss ein eindeutiger Hinweis den Benutzer auf den Fall aufmerksam machen, dass die zusätzliche Verschlüsselung für ein Gespräch nicht aktiviert ist (siehe auch Maßnahme M-TK-49 „Warnung bei unsicheren Einstellungen“). Für den Nutzer muss die zusätzliche Verschlüsselung ohne Aufwand aktivierbar sein, d. h. per Knopfdruck oder einem vergleichbar einfachen Schritt.

9.3.2.4 Bluetooth

Es gelten sinngemäß - sofern anwendbar - auch für Bluetooth-Endgeräte die in Kapitel 9.3.2.1 spezifizierten Sicherheitsmaßnahmen.

M-TK-209 Sichere Konfiguration und Verwendung des Bluetooth-Adapters

Da bei Bluetooth die Absicherung der Kommunikation nicht erzwungen wird, liegt die Verantwortung für den Einsatz von Sicherheitsmechanismen beim Nutzer. Die sichere Konfiguration und der umsichtige Umgang mit der Technik sind also wesentliche Elemente. Für die Verwendung eines Bluetooth-Adapters sind folgende Einstellungen zu beachten:

- Die Bluetooth-Schnittstellen der Geräte sollten bei Nichtbenutzung deaktiviert werden.
- Bluetooth-Geräte sollten möglichst wenig „offen“ konfiguriert werden. Es sind nach Möglichkeit die Betriebsmodi non-discoverable, non-connectable und non-pairable einzustellen.
- Verwendung starker PINs: Die Komplexität der PIN ist ein entscheidendes Element der Absicherung von Bluetooth. Die PIN muss mit maximal möglicher Komplexität gewählt werden. Eine PIN sollte also eine möglichst zufällige Folge maximal möglicher Länge (möglichst 128 Bit, mindestens aber 64 Bit) aus dem gerätespezifisch verwendbaren Zeichenvorrat sein.
- Authentisierung und Verschlüsselung: Der Adapter ist so zu konfigurieren, dass generell eine Authentisierung beim Verbindungsaufbau durchgeführt wird und die Kommunikation verschlüsselt wird. Zu beachten ist dabei, dass die Länge des Schlüssels

(maximal 128 Bit und minimal nur 8 Bit) zwischen den Geräten ausgehandelt wird und normalerweise der Nutzer hier keinen direkten Einfluss nehmen kann. Daher ist im Vorfeld der Nutzung sicherzustellen, dass die verwendeten Geräte tatsächlich die maximale mögliche Schlüssellänge von 128 Bit nutzen.

Verwendung semi-permanenter Verbindungsschlüssel[37]: Wird bei einem solchen Paar zu einem unerwarteten Zeitpunkt vom Benutzer eine PIN-Eingabe verlangt, sollte dieser nach Möglichkeit darauf verzichten, bis er sich in abhörsicherer Umgebung befindet. Dies erfordert eine entsprechende Einweisung des Nutzers.

Das Pairing darf nur mit vertrauenswürdigen Geräten, die im Vorfeld entsprechend den in dieser Maßnahme beschriebenen Vorgaben geprüft wurden, erfolgen.

Bei Verlust/Diebstahl eines mobilen (bzw. stationären) Gerätes müssen alle zugehörigen Verbindungsschlüssel in den verbliebenen Geräten gelöscht werden.

M-TK-210 Einsatz von Bluetooth-Endgeräten mit zusätzlicher Verschlüsselung

Für den erhöhtem Schutzbedarf müssen die eingesetzten Geräte neben der Bluetooth-Standardverschlüsselung einen weiteren Verschlüsselungsmechanismus unterstützen, der zusätzlich aktiviert werden kann. Ein Grund hierzu liegt in der vergleichsweise schwachen Verschlüsselung von Bluetooth.

Die effektive Schlüssellänge sollte mindestens 128 Bit betragen. Als Verschlüsselungsverfahren kommt AES in Frage. Dabei ist auch der Einsatz von Mechanismen wie IPsec (siehe Anhang, Kapitel 13.3.4.3) und TLS/SSL (siehe Anhang, Kapitel 13.3.3 und Kapitel 13.3.4.4) möglich.

Die Endgeräte müssen so konfiguriert werden können, dass die zusätzliche Verschlüsselung grundsätzlich aktiviert ist. Wenn die zusätzliche Verschlüsselung nur bei Bedarf aktiviert wird, muss ein eindeutiger Hinweis den Benutzer auf den Fall aufmerksam machen, dass die zusätzliche Verschlüsselung für ein Gespräch nicht aktiviert ist (siehe auch Maßnahme M-TK-49 „Warnung bei unsicheren Einstellungen“). Für den Nutzer muss die zusätzliche Verschlüsselung ohne Aufwand aktivierbar sein, d. h. per Knopfdruck oder einem vergleichbar einfachen Schritt.

9.3.3 Netzwerk

In diesem Kapitel werden für die einzelnen betrachteten mobilen und drahtlosen Systeme die für das Netzwerk relevanten Sicherheitsmaßnahmen erarbeitet:

- Mobilfunk und Fixed Mobile Convergence, siehe Kapitel 9.3.3.1
- Wireless LAN (WLAN), siehe Kapitel 9.3.3.2
- DECT, siehe Kapitel 9.3.3.3
- Bluetooth, siehe Kapitel 9.3.3.4

9.3.3.1 Mobilfunk und Fixed Mobile Convergence

M-TK-211 Berücksichtigung der Sicherheit bei der Vertragsgestaltung mit einem Dienstanbieter

Durch die Integration mobiler und organisationsinterner Telekommunikation ist die Grenze zwischen internen und externen Dienstleistungen manchmal nur schwer zu ziehen. Es ist daher besonders wichtig, die aus einem erhöhten Schutzbedarf resultierenden Anforderungen in Verträgen mit Dienstanbietern angemessen zu berücksichtigen. Dies beinhaltet neben den Festlegungen zur Verfügbarkeit auch Vereinbarungen zur Absicherung von Kundendaten

37 Die Nutzung temporärer Schlüssel erfordert eine Schlüsselaushandlung pro Verbindung. Hier ist das System vergleichsweise verwundbar und diese Phase ist in der Vergangenheit immer wieder zu Angriffen ausgenutzt worden. Daher wird bewusst zu semi-permanenten Schlüsseln geraten!

sowie Informationspflichten des Dienstanbieters bei Sicherheitsvorfällen. Außerdem sind Regelungen zur Überwachung der Umsetzung der Vereinbarungen zu treffen.

Bei der Auswahl eines Dienstanbieters ist eine Einschätzung der Vertrauenswürdigkeit gemäß Maßnahme M-TK-245 „Nachweis der Vertrauenswürdigkeit des Dienstanbieters“ zu empfehlen.

9.3.3.2 Wireless LAN

M-TK-212 Trennung von LAN- und WLAN-Verkehr im kabelbasierten Netz

LAN und WLAN müssen durch ein Sicherheitselement mit VoIP-tauglicher Firewall- und ggf. Intrusion-Prevention-Funktion entkoppelt werden. Dabei muss der Verkehr der WLAN-Endgeräte vom kabelbasierten Netz so getrennt werden, dass ein Zugriff auf eine Ressource in der kabelbasierten LAN-Infrastruktur nur über das Sicherheitselement möglich ist.

Diese Trennung kann auf logische Weise durch VLAN - ggf. in Verbindung mit einer Trennung auf Layer 3 durch Access Control Lists (ACL) bzw. Virtual Routing and Forwarding (VRF) - oder wie in einem Controller-basierten WLAN-Design durch IP-Tunnel erfolgen. Bei einem Controller-basierten Design kann bei entsprechend hohem Schutzbedarf der LAN-Infrastruktur weiterhin in Betracht gezogen werden, die Access Points über ein separates Netz anzubinden, über das ausschließlich WLAN-Controller erreichbar sind. Im Einzelfall kann auch eine physische Netztrennung von LAN und WLAN durch Verwendung eigener aktiver Komponenten für das WLAN angemessen sein.

Bei Nutzung eines Controller-basierten Designs muss bei einem erhöhten Schutzbedarf eine gegenseitige Authentisierung von Access Points und WLAN-Controller erfolgen und die Übertragung zwischen Access Points und WLAN-Controller möglichst verschlüsselt werden.

M-TK-213 Absicherung des LAN-Zugangs für Access Points

Der Ethernet-Anschluss eines Access Point an das kabelbasierte LAN muss bei einem erhöhten Schutzbedarf abgesichert werden, da ein Angreifer an dieser Schnittstelle einerseits versuchen kann, den WLAN-Verkehr zu belauschen und andererseits auf Infrastruktur-Ressourcen zuzugreifen. Hierzu ist eine auf den jeweiligen Schutzbedarf abgestimmte Kombination folgender Maßnahmen umzusetzen:

- Sofern technisch möglich, können Access Points mit einem IEEE 802.1X Supplicant ausgestattet werden und IEEE 802.1X auf den entsprechenden Ports am Access Switch aktiviert werden. Die Access Points erhalten auf diese Weise erst nach erfolgreicher Authentisierung einen LAN-Zugang.
- Bei einem Controller-basierten Design kann Port Security auf den entsprechenden Ports des Access Switch konfiguriert werden und der Port an die MAC-Adresse des Access Point gebunden werden.
- Die Anbringung von Access Points sollte so durchgeführt werden, dass Access Points möglichst unsichtbar montiert und gegen einen unberechtigten Zugriff geschützt sind (beispielsweise durch eine Montage oberhalb einer Zwischendecke).

M-TK-214 Berücksichtigung der Anforderungen einer Sprachübertragung bei der Planung der Funkzellen

Funkzellen müssen in ihrer Ausdehnung und ihrer Überlappung so geplant werden, dass die WLAN-Ausleuchtung den Anforderungen einer Sprachübertragung hinsichtlich Mobilität und Verfügbarkeit gerecht wird.

9.3.3.3 DECT

M-TK-215 Absicherung bei Anschluss von Radio Fixed Parts an ein LAN

Sofern Radio Fixed Parts verwendet werden, die über eine Ethernet-Schnittstelle an eine VoIP-Infrastruktur angebunden sind, muss der Zugriff auf Komponenten und Geräte im LAN kontrolliert werden. Hierzu ist analog zu der für WLAN beschriebenen Maßnahme M-TK-212 „Trennung von LAN- und WLAN-Verkehr im kabelbasierten Netz“ eine Trennung zwischen dem Netz, über das Fixed Parts angeschlossen werden, und dem Rest der LAN-Infrastruktur zu schaffen. Weiterhin muss analog zu Maßnahme M-TK-213 „Absicherung des LAN-Zugangs für Access Points“ der LAN-Zugang für Radio Fixed Parts abgesichert werden.

9.3.3.4 Bluetooth

M-TK-216 Absicherung von Bluetooth Access Points bei Anschluss an ein LAN

Werden Bluetooth Access Points über eine Ethernet-Schnittstelle an eine VoIP-Infrastruktur angebunden, muss der Zugriff auf Komponenten und Geräte im LAN kontrolliert werden. Hierzu ist analog zu der für WLAN beschriebenen Maßnahme M-TK-212 „Trennung von LAN- und WLAN-Verkehr im kabelbasierten Netz“ eine Trennung zwischen dem Netz, über das Bluetooth Access Points angeschlossen werden, und dem Rest der LAN-Infrastruktur zu schaffen. Weiterhin muss analog zu Maßnahme M-TK-213 „Absicherung des LAN-Zugangs für Access Points“ der LAN-Zugang für Bluetooth Access Points abgesichert werden.

9.3.4 Netz- und Systemmanagement

In diesem Kapitel werden für die einzelnen betrachteten mobilen und drahtlosen Systeme die für das Netz- und Systemmanagement relevanten Sicherheitsmaßnahmen erarbeitet:

- Mobilfunk und Fixed Mobile Convergence, siehe Kapitel 9.3.4.1
- Wireless LAN (WLAN), siehe Kapitel 9.3.4.2
- DECT, siehe Kapitel 9.3.4.3
- Bluetooth, siehe Kapitel 9.3.4.4

9.3.4.1 Mobilfunk und Fixed Mobile Convergence

M-TK-217 Fernadministration der mobilen Endgeräte durch ein Mobile Device Management

Bei erhöhtem Schutzbedarf müssen mobile Endgeräte zentral mit einem Mobile Device Management über GSM/UMTS/LTE verwaltet werden können, das folgende Funktionen realisiert:

- Inventarisierung, Rollout und Fernkonfiguration
- Systemmanagement und Endgeräteüberwachung
- Fernwartung und Support

Details hierzu finden sich in Kapitel 9.1.3. Dabei ist insbesondere darauf zu achten, dass die Vorgehensweise bei Verlust eines Endgerätes auch organisatorisch geregelt ist.

M-TK-218 Regelmäßige, möglichst automatische Sicherung von Daten und Konfiguration mobiler Endgeräte

Neben dem Verlust der Vertraulichkeit von Daten ist auch der tatsächliche Verlust von Daten kritisch für Organisationen. Daher sollte die dezentrale Datenhaltung vermieden werden.

Wenn eine Datenhaltung auf dem mobilen Endgerät nicht vermieden werden kann, muss das mobile Endgerät in das zentrale Datensicherungskonzept der Organisation integriert werden. Dies gilt zumindest für Daten mit erhöhtem Schutzbedarf hinsichtlich Verfügbarkeit.

Hierzu sollte idealerweise ein Mobile Device Management genutzt werden. Ansonsten muss eine regelmäßige Sicherung über organisatorische Richtlinien gewährleistet werden.

Die Endgerätekonfiguration sollte, um einen reibungslosen Betrieb sicherzustellen, ebenfalls gesichert werden. Neben der Möglichkeit zum lokalen Backup sollte diese idealerweise von zentraler Stelle erneut auf das Endgerät eingespielt werden können.

M-TK-219 Einschränkung der Apps

Überflüssige Berechtigungen für Apps sind nach dem „Need-to-Know-Prinzip“ möglichst zu entziehen.

Applikationskonfigurationen sollten durch eine Vorkonfiguration der Applikationen, z. B. für den Zugriff auf die Organisationsinfrastruktur, über eine MDM-Lösung vorgegeben werden. Durch vorgegebene Konfigurationen lassen sich Bedienfehler seitens des Anwenders und die Gefahr z. B. durch Phishing-Attacken verringern.

Hinweis: Eine Festschreibung der Konfiguration ist jedoch für diverse mobile Betriebssysteme nicht möglich, sodass die bewusste Manipulation von Konfigurationen nicht unterbunden werden kann.

Eine zentrale Software-Verteilung sollte möglichst (z. B. über ein MDM-System) eingesetzt werden. Dabei sollte zumindest ein Whitelisting-Ansatz in Kombination mit der Bereitstellung vorkonfigurierter Apps erfolgen.

Um einen Whitelisting- bzw. Blacklisting-Ansatz wirksam umzusetzen, dürfen die Apps ausschließlich über einen Company App Store bezogen werden. Der direkte Zugriff auf nicht organisationseigene App Stores muss unterbunden werden.

M-TK-220 Überwachung der Endgeräte hinsichtlich Anomalien

Ein Monitoring von mobilen Endgeräten sollte über MDM-Agenten auf dem mobilen Endgerät realisiert werden. Neben betriebsrelevanten Faktoren, wie Alter und Zustand des Endgerätes, ist das Logging von sicherheitsrelevanten Vorfällen wichtiger Bestandteil einer MDM-Lösung.

Hierzu gehören beispielsweise

- mehrfache Falscheingaben von Kennwörtern, die auf eine Brute-Force-Attacke hindeuten,
- Versuche auf dem Endgerät Root-Rechte zu erlangen oder einen Jailbreak durchzuführen oder
- Verlust/Diebstahl eines Endgerätes.

Diese Maßnahme wird typischerweise in Kombination mit M-TK-200 „Automatische Handlungen bei Verletzung von Sicherheitsrichtlinien auf mobilen Endgeräten“ eingesetzt.

9.3.4.2 Wireless LAN

Es gelten sinngemäß - sofern anwendbar - auch für WLAN-Endgeräte die in Kapitel 9.3.4.1 spezifizierten Sicherheitsmaßnahmen.

M-TK-221 Kontinuierliche Überwachung der Luftschnittstelle

Die Luftschnittstelle muss über ein geeignetes Werkzeug zumindest an allen kritischen Stellen des mit WLAN versorgten Gebiets überwacht werden (siehe Abbildung 65).

Die Überwachung beinhaltet unter anderem die regelmäßige Prüfung aller Funkkanäle bei 2,4 GHz bzw. bei 5 GHz, die Messung von Leistungsparametern inklusive der Feststellung der Qualität, mit der andere WLAN-Stationen (insbesondere andere Access Points) empfangen werden, sowie die Analyse der Übertragungen hinsichtlich Fehlern oder Angriffsmustern.

Hierzu sollte das WLAN-Management auch eine Funktion zur Lokalisierung von WLAN-Geräten (insbesondere von fremden Access Points) unterstützen.

Dabei muss beachtet werden, dass der Einsatz einer solchen Überwachungsfunktion auf den produktiv genutzten Access Points die Leistung des WLAN und insbesondere die Sprachübertragung spürbar beeinträchtigen kann[38].

Meldungen zu Fehlern und zu sicherheitsrelevanten Ereignissen sollten an eine zentrale Fehlerkonsole geschickt werden. Hier können SNMP Traps sowie Syslog-Meldungen (siehe [IETF RFC5424-2009] und [BSI LogMon-2009]) genutzt werden.

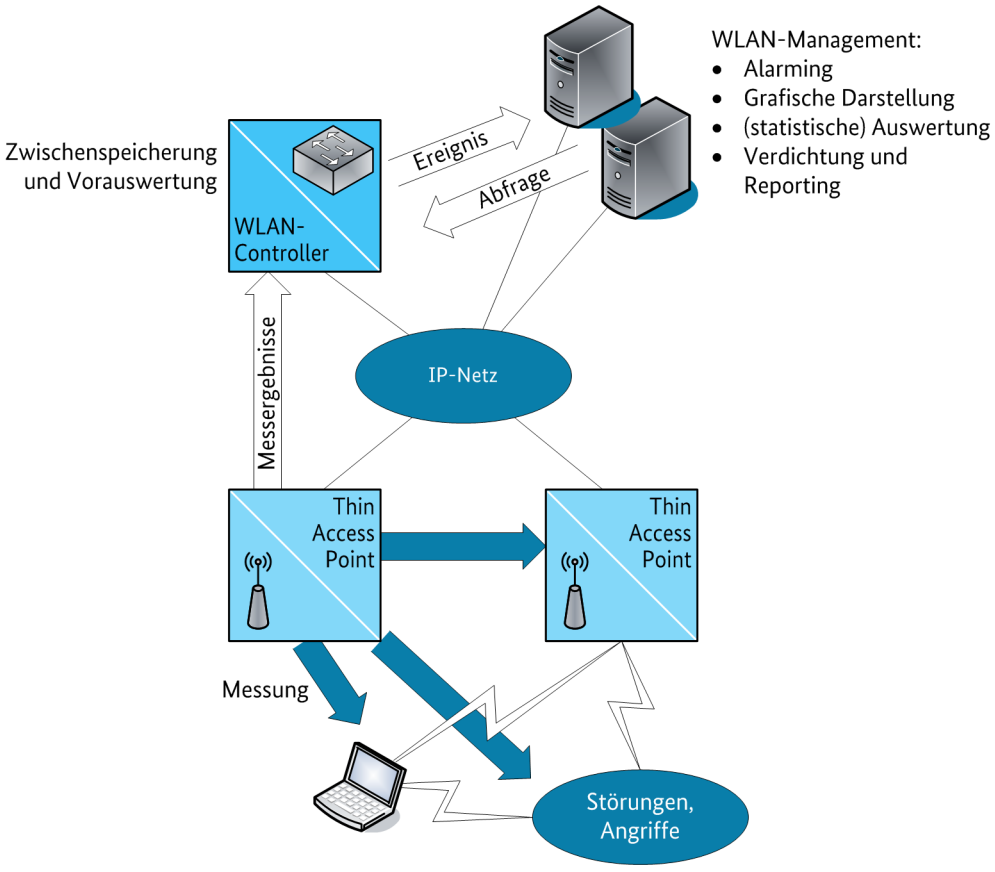


Abbildung 65: Überwachung der Luftschnittstelle durch Access Points in einem Controller-basierten WLAN-Design

38 Hierzu schaltet ein Access Point regelmäßig vom Normalbetrieb für eine gewisse Zeitspanne in einen Messbetrieb um. Während dieses Messbetriebs kann der Access Point keine Nutzdaten mehr transportieren und es kommt zu entsprechenden Verzögerungen (ggf. sogar zu Verlusten) bei der Übertragung von Sprachdaten. Häufigkeit und Dauer des Messbetriebs können herstellerspezifisch konfiguriert werden. Es gibt auch Lösungen, welche den Messbetrieb durch eine eigene Zusatz-Hardware in den Access Points realisieren. Bei solchen Lösungen kommt es nicht zu Beeinträchtigungen der Datenübertragung durch Messungen. Grundsätzlich können auch zusätzliche Access Points installiert werden, die eine reine Überwachungsfunktion für die produktiv genutzten Access Points haben.

M-TK-222 Kontinuierliche Überwachung der WLAN-Infrastruktur

Die Netzelemente der WLAN-Infrastruktur (insbesondere Access Points, WLAN-Controller und RADIUS-Server) müssen kontinuierlich hinsichtlich ihrer Verfügbarkeit überwacht werden. Meldungen zu Fehlern und zu sicherheitsrelevanten Ereignissen sollten an eine zentrale Fehlerkonsole geschickt werden. Hier können SNMP Traps sowie Syslog-Meldungen genutzt werden.

M-TK-223 Fernadministration der WLAN-Endgeräte

WLAN-Endgeräte sollten bei einem erhöhten Schutzbedarf zentral über das WLAN verwaltet werden können. Dabei sollte die Konfiguration des Gerätes (insbesondere die Sicherheitseinstellungen) geprüft und möglichst auch den Vorgaben entsprechend angepasst werden können. Zumindest sollte die Möglichkeit bestehen, ein Endgerät zu sperren und alle relevanten Daten zu löschen. Diese Fernadministration darf nur über eine sichere Kommunikationsverbindung (d. h. abgesichert durch eine angemessene Authentisierung und Verschlüsselung, siehe Maßnahme M-TK-78 „Sichere Administration von Endgeräten“) erfolgen.

Hierzu kann auch ein Mobile Device Management gemäß Kapitel 9.1.3 eingesetzt werden.

9.3.4.3 DECT

Es gelten sinngemäß - sofern anwendbar - auch für DECT-Endgeräte die in Kapitel 9.3.4.1 spezifizierten Sicherheitsmaßnahmen.

M-TK-224 Protokollierung des Einsatzes zusätzlicher Verschlüsselung

Für den erhöhten Schutzbedarf sollte in den Verbindungsdaten aufgezeichnet werden, ob ein Gespräch gemäß Maßnahme M-TK-208 „Einsatz von DECT-Endgeräten mit zusätzlicher Verschlüsselung“ zusätzlich verschlüsselt wurde oder nicht. Diese Maßnahme dient der Ursachenforschung bei einem Sicherheitsvorfall. Es besteht hierbei ein potenzieller Zielkonflikt mit dem Datenschutz, der eine entsprechende Sorgfalt in Speicherung und Auswertung der Verbindungsdaten erfordert.

M-TK-225 Verzicht auf den Einsatz von DECT bei erhöhtem Schutzbedarf

Bei erhöhtem Schutzbedarf (insbesondere falls Maßnahme M-TK-208 „Einsatz von DECT-Endgeräten mit zusätzlicher Verschlüsselung“ nicht umgesetzt werden kann) ist der Verzicht auf den Einsatz von DECT eine Option, die in Betracht gezogen werden muss.

9.3.4.4 Bluetooth

Es gelten sinngemäß - sofern anwendbar - auch für Bluetooth-Endgeräte die in Kapitel 9.3.4.1 spezifizierten Sicherheitsmaßnahmen.

M-TK-226 Verzicht auf den Einsatz von Bluetooth bei erhöhtem Schutzbedarf

Bei erhöhtem Schutzbedarf (insbesondere falls Maßnahme M-TK-210 „Einsatz von Bluetooth-Endgeräten mit zusätzlicher Verschlüsselung“ nicht umgesetzt werden kann) ist der Verzicht auf den Einsatz von Bluetooth eine Option, die in Betracht gezogen werden muss.

9.4 Zusammenfassung

Bis vor wenigen Jahren war die Telefonie die wesentliche Anwendung für die Anbindung mobiler Endgeräte an eine TK-Anlage. Dies hat sich durch die Verbreitung von Smartphones und Tablets inzwischen verändert. Smartphones und Tablets verfügen über leistungsfähige Mobilfunk- und WLAN-Technologien und greifen mit diesen sowohl auf organisationsinterne TK-Lösungen als auch auf das Internet zu. Lauschangriffe, Datenabfluss, Datenverlust und Bewegungsprofile bilden daher die zentralen Gefährdungen bei der Integration mobiler Endgeräte in die TK-Infrastruktur einer Organisation. Somit sind bei der Anbindung mobiler Endgeräte unter anderem die folgenden Angriffspunkte zu berücksichtigen:

- Unzureichend abgesicherte Kommunikationsschnittstellen und -strecken

  Dies betrifft mit GSM/UMTS/LTE, WLAN, Bluetooth und DECT alle mobilen und drahtlosen Kommunikationsmöglichkeiten eines mobilen Endgerätes. Bei Mobilfunknetzen wie GSM/UMTS/LTE kommt hinzu, dass ein Verlust der Vertraulichkeit grundsätzlich auch in der Infrastruktur eines Mobilfunkbetreibers erfolgen kann. Dies kann durch unzureichend gesicherte Kommunikationsstrecken (z. B. ungesicherten Richtfunk) oder interne Angriffe verursacht werden. Da die Mobilfunknetze jedoch teilweise außerhalb des Verantwortungsbereichs des TK-Anlagenbetreibers liegen, muss diese Gefährdung zumindest teilweise akzeptiert werden.

- Unzureichende Absicherung des mobilen Endgerätes

  Lauschattacken, Datenabfluss, Datenverlust und Bewegungsprofile sind insbesondere durch Schwachstellen im mobilen Betriebssystem, schadenstiftende Apps und speziell durch zu hohe Berechtigungen für Apps möglich. Außerdem ist schadenstiftende Software (Trojaner, Viren und Würmer) eine stetig steigende Bedrohung.

- Unzureichende Trennung privater und dienstlicher Daten auf dem mobilen Endgerät

  Mobile Endgeräte werden nicht selten sowohl dienstlich als auch privat genutzt. Kritisch ist dabei eine unzureichende Trennung privater und dienstlicher Daten, da zunächst dienstliche Daten über die private Nutzung abfließen könnten. Außerdem besteht durch die Korrelation privater und dienstlicher Informationen ein wesentlich größeres kumuliertes Gefährdungspotenzial.

Die Erarbeitung einer Sicherheitskonzeption für die Anbindung mobiler Endgeräte umfasst neben den generell zu ergreifenden Maßnahmen (siehe Kapitel 10) die folgenden Aspekte.

Sicherheitsmaßnahmen auf Ebene der Server und Anwendungen

Bei Kommunikation zwischen Server und mobilem Endgerät muss eine Authentisierung zwischen den Kommunikationspartnern stattfinden. Dies gilt auch für die Kommunikation zwischen mobilen Endgeräten. Außerdem sollte eine konsequente Ende-zu-Ende-Verschlüsselung der gesamten Kommunikation, d. h. inklusive der Sprachkommunikation, erfolgen.

Durch den Einsatz von Server-based Computing kann eine Speicherung organisationsinterner Daten auf mobilen Endgeräten vermieden werden.

Sicherheitsmaßnahmen auf Ebene der Endgeräte

Auf Ebene der Endgeräte stellt der Nutzer ein erhebliches Sicherheitsrisiko dar. Die Nutzungsrechte auf dem Endgerät müssen daher erheblich eingeschränkt werden. Der Nutzer darf keine Berechtigungen auf einem mobilen Endgerät haben, die bei leichtfertiger Verwendung das Auftreten der Gefährdungen erheblich wahrscheinlicher machen, z. B. durch Installation von Apps, Änderungen von Parametern usw.

Weiterhin muss die dienstliche Verwendung von Produkten aus dem Consumer-Bereich eingeschränkt werden, da Consumer-Produkte (Endgeräte-Hardware, mobile Betriebssysteme und Apps) einerseits oft Sicherheitsmaßnahmen erschweren oder sogar unmöglich machen und andererseits - meist bedingt durch die kurzen Produktzyklen in diesem Marktsegment - häufig erhebliche Schwachstellen aufweisen.

Falls es notwendig ist, dienstlich Daten auf dem Endgerät zu speichern, so ist eine Kapselung dienstlicher Daten durch Container- und Virtualisierungstechniken mit zusätzlicher Verschlüsselung notwendig.

Bei erhöhtem Schutzbedarf hinsichtlich der Vertraulichkeit sollten außerdem abhörsichere Mobiltelefone verwendet werden.

Sicherheitsmaßnahmen auf Ebene des Netzwerks

Auf Netzwerkebene muss eine sichere Anbindung mobiler Endgeräte durch konsequente Kontrolle der Kommunikation an zentralen Sicherheits-Gateways erfolgen, die möglichst eine Entkopplung der IP-Kommunikation beinhaltet.

Es muss sowohl eine Absicherung der Luftschnittstelle wie beispielsweise bei WLAN und DECT erfolgen als auch sichergestellt werden, dass die Kommunikation in der kabelbasierten Infrastruktur keine Sicherheitslücken aufweist. Bei DECT kommt erschwerend hinzu, dass mit den bestehenden Mitteln des DECT-Standards die Kommunikation auf der Luftschnittstelle nur unzureichend abgesichert werden kann. Generell muss bei der Verwendung von drahtlosen Techniken berücksichtigt werden, dass die Verfügbarkeit solcher Systeme stets geringer als bei kabelgebunden Systemen ist.

Netz- und Systemmanagement

Zur Vermeidung von Angriffen auf mobile Endgräte oder auf die TK-Anlage unter Nutzung von Schwachstellen in den Endgeräten ist eine Härtung der mobilen Endgeräte, des Systemmanagements inkl. Software-Verteilung und eine Erzwingung entsprechender Richtlinien durch ein zentrales Mobile Device Management (MDM) notwendig.

Weiterhin muss eine Überwachung mobiler Endgeräte hinsichtlich Anomalien und Richtlinienverletzung, speziell Erlangung unberechtigter Rechte, insbesondere Root-Rechte bzw. Jailbreak, erfolgen und es sind automatisierte Aktionen bei Feststellung von Anomalien und Richtlinien-Verletzung, z. B. Löschung (engl. Wipe) von (dienstlichen) Daten, Apps oder des kompletten Endgerätes festzulegen.

Abbildung 66 zeigt zusammenfassend die grundsätzliche Vorgehensweise bei der Absicherung von mobilen Endgeräten, insbesondere von Smartphones und Tablets, und macht deutlich, dass manche Maßnahmen nur dann ergriffen werden müssen, wenn andere Maßnahmen nicht ausreichend umgesetzt werden können.

Die Abbildung verdeutlicht die im Text zuvor beschriebenen grundsätzlichen Schritte und zur Absicherung der Integration mobiler Endgeräte in Form eines Flussdiagramms. Neben den zwingend vorzunehmenden Maßnahmen wie z. B. Härtung von zentralen Komponenten visualisiert das Flussdiagramm essentielle Maßnahmen, z. B. den Einsatz von Server-based Computing, Mobile Device Management oder eines Company App Store, sowie Ausweichmaßnahmen wie z. B. den Einsatz von Virtualisierungs- und Container-Technik auf dem mobilen Endgerät, falls Server-based Computing nicht möglich ist.

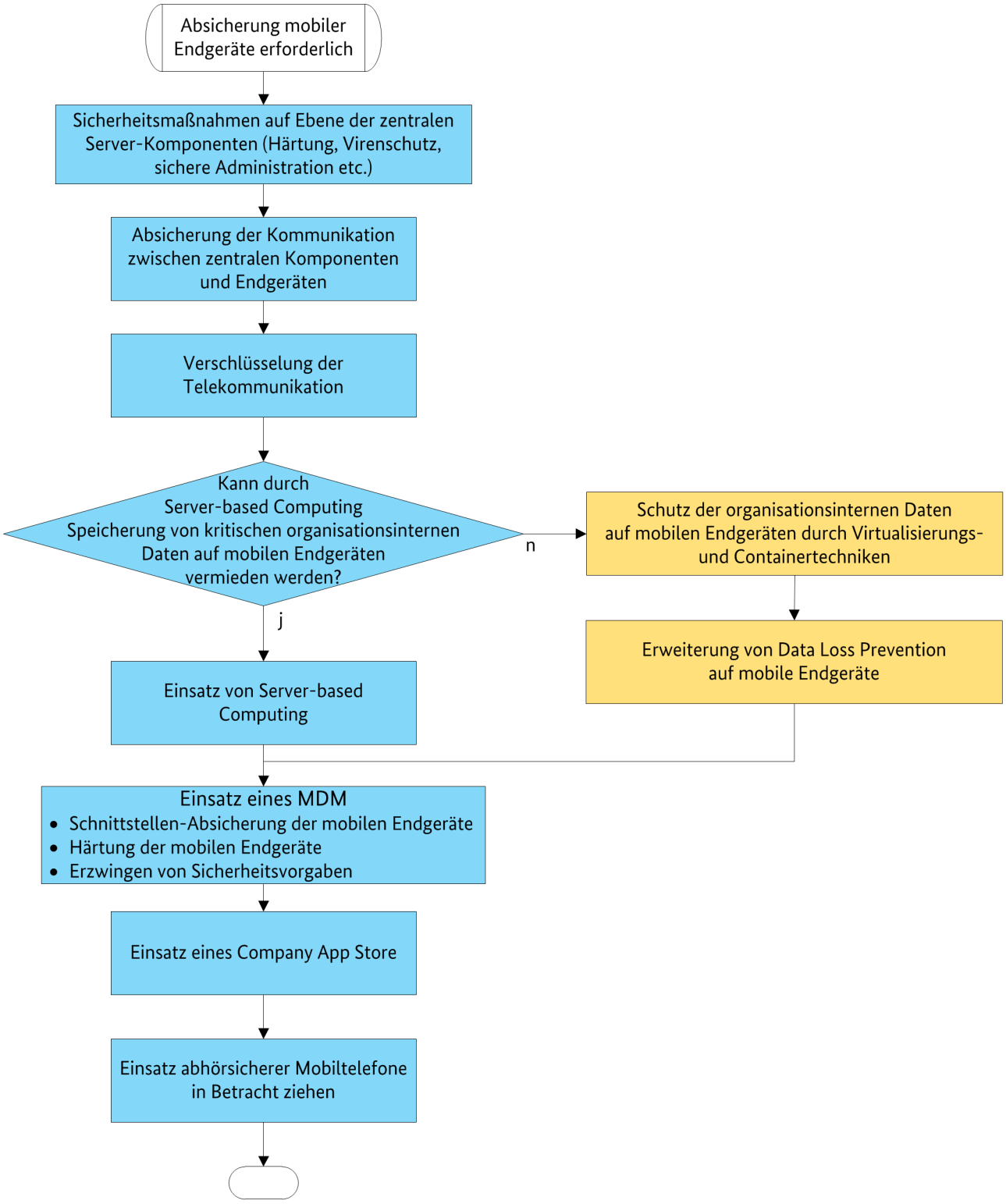


Abbildung 66: Grundsätzliche Vorgehensweise bei der Absicherung von mobilen Endgeräten

10 Generell zu ergreifende Sicherheitsmaßnahmen

In diesem Kapitel werden systemübergreifende Aspekte beschrieben, die für die betrachteten Telekommunikationssysteme gleichermaßen gelten. Dies beinhaltet die folgenden Punkte:

- Auslegung der passiven Netzinfrastruktur bei erhöhtem Schutzbedarf, siehe Kapitel 10.1
- Absicherung von Servern des Telekommunikationssystems, siehe Kapitel 10.2
- Sicheres Netz- und Systemmanagement, siehe Kapitel 10.3
- Aspekte des Datenschutzes, siehe Kapitel 10.4
- Auswahl von Dienstanbietern, siehe Kapitel 10.5
- Notfallvorsorge, siehe Kapitel 10.6
- Organisatorische Maßnahmen, siehe Kapitel 10.7

10.1 Auslegung der passiven Netzinfrastruktur bei erhöhtem Schutzbedarf

Im Falle eines erhöhten Schutzbedarfs muss auch die Auslegung der passiven Netzinfrastruktur (Verkabelung, Rangierfelder usw.) mit besonderer Sorgfalt hinsichtlich der Verhinderung unbefugten Zugangs zum Netzwerk (Vertraulichkeit und Integrität von Telefonie-Kommunikation) und der Minimierung des Angriffsrisikos für die genutzten Kabelstrecken (Verfügbarkeit) realisiert werden.

Ergänzend zum Baustein B 2.12 „IT-Verkabelung“ der IT-Grundschutz-Kataloge ist die folgende Maßnahme herauszuheben:

M-TK-227 Sichere Kabelführung

In dieser Maßnahme werden keine TK-spezifischen Aspekte erläutert, sondern allgemeine Hinweise zur sicheren Verlegung von Kabeln gegeben. Sichere Kabelführung bedeutet die Minimierung von versehentlicher oder vorsätzlicher Beschädigung von Kabelinstallationen sowie von Eingriffen in die Verkabelung zur Schaffung von Abhörmöglichkeiten.

Für erhöhten Schutzbedarf bei der Verkabelung sollten ergänzend zu Maßnahme M 5.5 „Schadensmindernde Kabelführung“ der IT-Grundschutz-Kataloge die folgenden Aspekte realisiert werden:

- Grundsätzlich sollte die Zahl der Stellen, an denen verlegte Kabel zugänglich sind, auf das betriebsnotwendige Maß beschränkt werden.
- Kabelstrecken und Anschlussdosen sollten nicht öffentlich zugänglich sein.

  Insbesondere bei Backbone-Kabeln und Sekundärverkabelung sollte auf die Einhaltung dieser Maßnahme geachtet werden. Im Falle von öffentlich frequentierten Bereichen sollten die Kabel über abgehängten Decken, unter Doppelböden, in unzugänglichen Bereichen usw. verlegt werden.
- Zugänge zu Kabelkanälen müssen verschlossen werden, um Manipulationen an den Kabeln zu erschweren.
- Nicht genutzte Anschlussdosen sollten nicht rangiert sein, da ansonsten die Gefahr besteht, dass ein Unbefugter Zugang zum Netzwerk erhält.

  Der Rangierzustand der Dosen sollte konsequent dokumentiert werden, um immer eine aktuelle Übersicht der möglichen Zugänge zum Netzwerk vorliegen zu haben.

- Kabelwege sind durch gezielte Maßnahmen gegen Beschädigung durch Brand zu schützen (Brandabschottung).

10.2 Absicherung von Servern des Telekommunikationssystems

Ein Server muss unabhängig von seinem Einsatzbereich in einem Telekommunikationssystem angemessen geschützt werden. Allgemein sind hierzu die jeweils zutreffenden Maßnahmen der Bausteine B 3.101 „Allgemeiner Server“ bis B 3.109 „Windows Server 2008“ der IT-Grundschutz-Kataloge umzusetzen. Insbesondere wird auf folgende Maßnahmen hingewiesen.

M-TK-228 Produktauswahl von TK-Lösungen unter Berücksichtigung von Sicherheitsaspekten

Viele TK-Dienste, integrierte Applikationen und Endgeräte lassen sich durch eine umsichtige Planung und entsprechende technische Maßnahmen hinreichend absichern. Steht der Sensibilität der Daten jedoch nur ein schwacher realisierbarer Schutz gegenüber, so muss dies bei der Auswahl einer TK-Lösung berücksichtigt und im Zweifelsfall auf die Nutzung der entsprechenden Anwendung verzichtet werden.

Folgende Aspekte sind dabei hinsichtlich eines erhöhten Schutzbedarfs besonders hervorzuheben:

- Telefonie-Server basieren oft auf Standardbetriebssystemen mit den einschlägig bekannten Sicherheitsschwächen und -lücken.
- Die Nutzung von IP-Telefone und insbesondere von mobilen Endgeräte können das Sicherheitsniveau des IP-Netzes bzw. der VoIP-Gesamtlösung reduzieren. Um dies zu vermeiden, sind Möglichkeiten zur gezielten Konfiguration der Telefone gemäß Sicherheitsgesichtspunkten notwendig.

Im Sinne dieser Gesichtspunkte werden über eine gezielte Produktauswahl die Voraussetzungen für ein hohes Sicherheitsniveau der TK-Lösung geschaffen. Folgende Punkte sind dabei zu beachten:

- Auswahl des Betriebssystems des Telefonie-Servers unter Sicherheitsaspekten

  Bei einem für erhöhten Schutzbedarf geeigneten Produkt muss es möglich sein, das System durch gezielte Konfiguration auf ein Minimalsystem zu reduzieren, bei dem nur die konkret benötigten Funktionalitäten aktiviert sind. Nach Möglichkeit sind Betriebssysteme zu wählen, die nicht bevorzugtes Ziel für schadenstiftende Software sind.

- Eine für das Produkt bzw. eine für die im Produkt eingesetzte Plattform vorliegende Sicherheitszertifizierung ist allgemein positiv zu bewerten und wird für den erhöhten Schutzbedarf gefordert.

  Dabei ist darauf zu achten, dass die Zertifizierung eine Basis hat, die eine geeignete Vergleichbarkeit bzw. Bewertbarkeit des mit dem Zertifikat konstatierten Sicherheits-potenzials gewährleistet. Optimal ist eine Zertifizierung nach Common Criteria. Ein rein herstellereigenes Prüfschema ist unzulänglich für eine ausreichende Aussagekraft des Zertifikats.

  Bei erhöhtem Schutzbedarf sollte die Vertrauensstufe EAL4[39] oder besser EAL4+ gemäß Common-Criteria-Definition erreicht werden[40].

Stehen nach Funktionalitäten ansonsten vergleichbar geeignete Produktalternativen für die geplante TK-Lösung zur Verfügung, so sollte dieser Aspekt gezielt als Auswahlkriterium herangezogen werden.

39 Die Common-Criteria-Spezifikation sieht verschiedene Vertrauenswürdigkeitsstufen (Evaluation Assurance Level) EAL1 (niedrigste Stufe) bis EAL 7 (höchste Stufe) vor, die mit einem Produkt erreicht werden können.

40 Die Vorgänger der Common Criteria sehen ebenfalls verschiedene Stufen der Vertrauenswürdigkeit vor, hier sollte eine äquivalente Stufe erreicht werden.

M-TK-229 Härtung von Servern des Telekommunikationssystems

Server des Telekommunikationssystems basieren oft auf Standardbetriebssystemen mit den einschlägig bekannten Sicherheitsschwächen und -lücken. Diese Systeme sind durch eine Härtung ergänzend zu M 4.237 „Sichere Grundkonfiguration eines IT-Systems“ der IT-Grundschutz-Kataloge abzusichern, die die folgenden Prüf- bzw. Aktionspunkte umfasst:

- Nicht benötigte Administrationsschnittstellen müssen deaktiviert werden, z. B. Deaktivierung der Webschnittstelle, wenn die Administration nur über ein Command Line Interface erfolgen soll.
- Jeder nicht benötigte IP-Service und Netzdienst auf einem Server des TK-Systems ist zu deaktivieren, um zu vermeiden, dass Sicherheitsschwachstellen dieser Dienste ausgenutzt werden können.
- Zur Prüfung, ob ein Server Sicherheitsschwachstellen aufweist, sollten Security-Scanner eingesetzt werden, die den Server von innen und außen (über das Netz) überprüfen.
- Zur Prüfung von Systemdateien und anderen kritischen, jedoch keinen schnellen Änderungen unterliegenden Dateien und Verzeichnissen sollten prüfsummenbildende Programme eingesetzt werden, die die Integrität der Dateien sicherstellen.
- Sicherheits-Patches für das Betriebssystem der Server des Telekommunikationssystems und den darauf verwendeten Programmen müssen getestet und anschließend so schnell wie möglich installiert werden.

Wenn Linux als Betriebssystem eingesetzt wird, so müssen unter anderem die folgenden Punkte beachtet werden:

- Durchführung einer Minimalinstallation bzw. Deinstallation nicht benötigter Pakete
- Deaktivierung nicht benötigter Dienste, z. B. Network File System (NFS), Server Message Block (SMB), X Window System, remote copy (rcp), remote login (rlogin) und remote execution (rexec)
- Minimierung der Zugangsprivilegien für Dateien und Verzeichnisse

Eine manuelle und automatische Log-Auswertung ist zwingender Bestandteil der Sicherheitsmechanismen auf den Systemen.

Weitere Einzelmaßnahmen, die zur Härtung beitragen, sind in Maßnahme M-TK-235 „Schutz vor schadenstiftender Software für die Server der TK-Lösung“ zu finden.

Eine wichtige Grundlage zur effektiven Härtung ist die Vertrauenswürdigkeit der verwendeten Server-Plattform bzw. des Server-Betriebssystems. Hierzu sollte eine Zertifizierung nach Common Criteria vorliegen. Bei erhöhtem Schutzbedarf sollte die Vertrauensstufe EAL4 oder besser EAL4+ erreicht werden (siehe [CCRA CC-2012]).

M-TK-230 Spezielle Absicherung von virtualisierten TK-Servern

Werden die Komponenten der TK-Lösung als virtuelle Systeme eingerichtet, so sollten bei erhöhtem Schutzbedarf hinsichtlich Integrität und Vertraulichkeit die Virtualisierungs-plattform und virtualisierten TK-Server durch geeignete Maßnahmen angemessen abgesichert werden. Über die Maßnahmen in Baustein B 3.304 „Virtualisierung“ der BSI IT-Grundschutz-Kataloge hinausgehend sind hier folgende Punkte zu nennen:

- Trennung von sicheren und unsicheren virtuellen Maschinen (VMs) bzw. VMs für Server mit normalem und erhöhten Schutzbedarf auf dedizierte Hosts
- Feste Zuweisung von ausreichenden Ressourcen für die TK-bezogenen VMs
- Besondere Härtung der Virtualisierungsplattform
- Umfassende Kapselung der TK-bezogenen VMs

- Reduzierung der Kommunikation bzw. Schnittstellen der TK-bezogenen VM zu anderen VMs und Systemkomponenten auf das benötigte Minimum
- Getrennter Management-Zugang für die Administration / Überwachung der TK-bezogenen VMs

M-TK-231 Einschränkung und Kontrolle von Berechtigungen für die Administration eines Servers des Telekommunikationssystems

Ergänzend zu Maßnahme M 4.237 „Sichere Grundkonfiguration eines IT-Systems“ der IT-Grundschutz-Kataloge müssen die folgenden Punkte beachtet werden:

- Administrationskonten müssen personalisiert sein, um eine Zuordnung von Tätigkeit und Administrator sicherzustellen. Gruppen- oder Funktionskonten sind möglichst zu vermeiden.
- Administrationskonten dürfen nur so viele Rechte erhalten, wie zum Arbeiten benötigt werden. Dabei sollte eine gezielte Unterscheidung zwischen den Zugriffsberechtigungen „Lesen und Schreiben“ und „nur Lesen“ vorgenommen werden.
- Hierzu ist ein Berechtigungskonzept zu erstellen, das rollenbasierte Berechtigungsprofile zu verschiedenen Administrationsfunktionen spezifiziert. Dabei können beispielsweise unterschiedliche Berechtigungen für einen internen Administrator mit Vollzugriff und einen externen Wartungspartner mit eingeschränkten Administrationsrechten für die Remote-Wartung festgelegt werden.
- Das Berechtigungskonzept sollte möglichst hierarchisch aufgebaut werden. Über die höchste Berechtigungsebene müssen alle Funktionen zugreifbar sein; die zugreifbaren Funktionen der darunter liegenden Ebenen werden durch die höchste Berechtigungsebene zugewiesen.

M-TK-232 Einschränkung und Kontrolle des Zugangs zu einem Server des Telekommunikationssystems

Ergänzend zu Maßnahme M 4.239 „Sicherer Betrieb eines Servers“ der IT-Grundschutz-Kataloge müssen die folgenden Punkte beachtet werden:

- Der Zugriff auf Management-Funktionen muss für alle Administrationsschnittstellen durch eine angemessene Authentisierung abgesichert werden. Die Authentisierung muss mindestens über Nutzername und Passwort erfolgen, wobei eine entsprechende Passwortrichtlinie konsequent umzusetzen ist. Für den erhöhten Schutzbedarf kann der Einsatz stärkerer Authentisierungsmechanismen (z. B. Zertifikate in Verbindung mit Smartcards) in Betracht gezogen werden. Wenn die Telefonie und IT aus strategischer Sicht zusammenwachsen sollen, wird aus der Sicherheitsperspektive empfohlen, diesen Weg auch für die Datenhaltung konsequent umzusetzen. Hierzu sollte eine Integration der Telefonie in den vorhandenen organisationsweiten Verzeichnisdienst (Corporate Directory Service) vorgenommen werden.
- Wenn die zulässige Anzahl fehlgeschlagener Authentisierungsversuche überschritten wird, sollte das entsprechende Konto für eine bestimmte Zeit gesperrt werden.

Es dürfen ausschließlich sicherere Protokolle - Secure Shell (SSHv2), HTTPS, Secure Copy (SCP), Simple Network Management Protocol (SNMPv3) für den administrativen Zugriff auf das System verwendet werden.

Nach einer bestimmten Zeit der Inaktivität sollten Administrationssitzungen automatisch geschlossen werden.

Für den erhöhten Schutzbedarf gelten folgende zusätzliche Einzelmaßnahmen:

- Über die durchgeführten Administrationstätigkeiten muss eine nicht manipulierbare Logbuchdatei (je Berechtigungsebene) erstellt und nach Eingabe des Passworts der

entsprechenden Ebene ausgegeben werden können. Zusätzlich sollten die Logdateien ausgedruckt und sicher verwahrt werden.

- Die Benutzung von Remote-Zugängen sollte so weit möglich eingeschränkt werden. Weiterhin ist ein direkter Remote-Zugriff zur Administration des Servers zu vermeiden. Stattdessen sollte eine Middleware wie z. B. ein Terminal-Server oder Proxy-Server eingesetzt werden. Die Lösung muss außerdem sicherstellen, dass alle Aktivitäten während einer Administrationssitzung protokolliert werden können.

M-TK-233 Physische Sicherheit der Server der Telekommunikationslösung

Der Zugang zu zentralen TK-Komponenten ist physisch zu schützen, indem solche Komponenten in abgeschlossenen Technikräumen oder Server-Räumen mit Zugangskontrolle installiert werden.

Im Falle erhöhten Schutzbedarfs sind die Maßnahmen in den Bausteinen B 2.4. „Serverraum“, B 2.6 „Raum für technische Infrastruktur“, B 2.7 „Schutzschränke“ und B 2.9 „Rechenzentrum“ besonders konsequent umzusetzen, insbesondere

- Unterbringung in abschließbaren Schränken statt in (insbesondere bei Servern üblicheren) offenen Racks und Verwendung spezieller Schließsysteme für diese Schränke.
- Um Sabotage zu verhindern, sollte als Zugangskontrollmechanismus bei erhöhtem Schutzbedarf eine elektronische Zugangskontrolle mit Protokollierung installiert werden. Bevorzugt sollte ein System verwendet werden, welches eine starke Authentisierung, z. B. mittels Chipkarte, unterstützt.
- Im Server-Raum sollte zudem eine Videoüberwachung installiert sein.

Eine konsequente Auslegung des physischen Zugangsschutzes erhöht die Kosten und den Aufwand gegenüber einfacheren Formen zum Teil deutlich, sodass sie im Sinne der Verhältnismäßigkeit dem erhöhten Schutzbedarf vorbehalten sein sollte.

Um eine möglichst hohe Verfügbarkeit sicherzustellen, sollten redundante zentrale Komponenten der TK-Lösung an zwei örtlich getrennten Standorten betrieben werden. Diese Standorte müssen so ausgewählt sein, dass jeweils ein entsprechender Schutz vor Wasser- und Feuerschäden sowie Überspannung gewährleistet ist.

M-TK-234 Berücksichtigung der Server der TK-Lösung im Datensicherungskonzept der Organisation

Wurde ein Sicherheitsvorfall bei einem Server des Telekommunikationssystems entdeckt, so kommt den Möglichkeiten einer effizienten Wiederherstellung der vollen Verfügbarkeit und Integrität eine zentrale Bedeutung zu. In jedem Fall muss mit Hilfe der getroffenen Vorkehrungen der aktuelle Zustand vor Eintreten eines Notfalls für alle Teilsysteme der TK-Lösung wiederhergestellt werden. Ein wesentliches Element stellen hier Backups mit einer Datensicherung sowie Sicherungen der Systemzustände dar. Basis hierfür sind die in Baustein B 1.4 „Datensicherungskonzept“ aufgeführten Maßnahmen, die um die folgenden wesentlichen Punkte ergänzt werden:

- Konfigurationen und Anwendungsdaten müssen gesichert werden. Hierzu muss ein entsprechendes Konzept erstellt werden und mit den allgemeinen Konzepten der Datensicherung für Server und Netzkomponenten abgestimmt werden.
- Im Fall von Appliances weichen die einsetzbaren Datensicherungsmöglichkeiten und -werkzeuge häufig von den Standardlösungen zur Datensicherung ab. Hierzu muss ein geeignetes Konzept zur Integration von Appliances in die Datensicherung erstellt und umgesetzt werden.

  Beispiel: Systemkonfiguration und sonstige Daten werden bei einer Appliance, z. B. einem PSTN-Gateway einer VoIP-Lösung, automatisch in eine Archivdatei überführt. Diese Archivdatei kann dann auf einem Server gespeichert werden, der wiederum dem allgemeinen Datensicherungskonzept unterliegt.

- Für die Sicherung von Systeminstallationen und Systemkonfigurationen können Images, Snapshots, Software- und Konfigurationssicherung via Datensicherungswerkzeug oder Kombinationen aus solchen Ansätzen eingesetzt werden. Für die gewählten Ansätze bzgl. Systeminstallationen und -konfigurationen ist durch entsprechende Regelungen zum Change-Prozess sicherzustellen, dass nach jeder Änderung an (Teil-)Systemen eine geeignete Aktualisierung erfolgt. Dabei sind die Aktualisierungen miteinander kombinierter Sicherungsformen so zu gestalten, dass der Aufwand für den Sicherungsvorgang vertretbar bleibt, ohne jedoch die Zeit für eine grundlegende Systemwiederherstellung dadurch signifikant zu verlängern.

  Beispiel: Wird für ein System mit einer Kombination aus Image und automatischer Nachinstallation von Patches gearbeitet, so kann eine Reihe von Patch-Vorgängen übersichtlichen Ausmaßes erfolgen, ehe ein neues Image erstellt wird.

- Wichtig ist, dass für die Sicherung von Anwendungsdaten eine Planung der Sicherungszeitpunkte und Formen durchgeführt wird, die den Anforderungen bzgl. eines maximal tolerablen Datenverlusts gerecht wird. Die entsprechenden Festlegungen sind in einen Gesamt-Datensicherungsplan des zentralen IT-Bereichs aufzunehmen.

M-TK-235 Schutz vor schadenstiftender Software für die Server der TK-Lösung

Alle Infektionswege für die Ausbreitung von Viren und sonstiger schadenstiftender Software sind auch auf Servern des Telekommunikationssystems zu kontrollieren. Dazu gehören Datenträger, Mail-Services usw.

Zum Schutz vor Malware, z. B. vor Viren, Würmern und Trojanern, sollten die Server des Telekommunikationssystems die Maßnahmen gemäß Baustein B 1.6 „Schutz vor Schadprogrammen“ der IT-Grundschutz-Kataloge umsetzen.

M-TK-236 Einbindung der Server der TK-Lösung in das Patch-Management der Organisation

Die Aktualisierung von Software insbesondere zwecks Schließen von Sicherheitslücken erfordert die ständige Verfolgung der entsprechenden Meldungen und Hinweise. Grundsätzlich sind hierfür die Maßnahmen des Bausteins B 1.14 „Patch- und Änderungsmanagement“ der IT-Grundschutz-Kataloge zu beachten.

Die Möglichkeiten zur Automatisierung des Patch-Managements sind unterschiedlich, abhängig von der Betriebssystem-Basis der konkret verwendeten Produkte und der vorhandenen Verteilungslösungen wie z. B. Windows Server Update Services (WSUS).

Die Netzelemente eines Telekommunikationssystems können eine heterogene Umgebung bilden, die aus verschiedenen Plattformen bzw. Betriebssystemen oder Betriebssystem-Versionen und unterschiedlichen Anwendungen (oft von verschiedenen Herstellern stammend) zusammengesetzt ist. Die Dauer von vorbereitenden Tests und die potenziellen Stabilitätsrisiken bei Einspielen neuer Patches müssen gegenüber dem Zugewinn an Sicherheit abgewogen werden.

Hier ist eine besondere Abstimmung des Patch-Managements erforderlich. Ein Patch einer Komponente kann Auswirkungen auf die Funktion anderer Komponenten haben. Im schlimmsten Fall kommt es zu einem Dienstausfall des gesamten Telekommunikations-systems.

Besonders zu beachten ist dabei die Abstimmung im Vorfeld: Eine Änderung der Software eines Elements des Telekommunikationssysteme (z. B. einer UCC-Applikation) muss im Vorfeld mit den verantwortlichen Betreibern anderer (Teil-)Systeme, zu denen Schnittstellen bestehen, abgestimmt werden. Hierzu müssen entsprechend formalisierte Prozesse eingerichtet werden.

10.3 Sicheres Netz- und Systemmanagement

Typischerweise werden auch die TK-Komponenten in ein zentrales Netz- und Systemmanagement eingebunden. Diese Integration muss entsprechend dem erhöhten Schutzbedarf hinsichtlich Integrität und Vertraulichkeit angemessen geschützt werden. Allgemein sind hierzu die jeweils zutreffenden Maßnahmen in Baustein B 4.2 „Netz- und Systemmanagement“ der IT-Grundschutz-Kataloge umzusetzen. Insbesondere wird auf folgende Maßnahmen hingewiesen.

M-TK-237 Sichere Konfiguration des Netzwerk-Management-Protokolls

Auch modernen TK-Lösungen weisen nicht selten Schwächen bei der Absicherung des Netzwerk-Management-Protokolls auf. Als Standardprotokoll für das Netzmanagement gilt das Simple Network Management Protocol (SNMP), welches in den RFCs 3411 bis 3418[41] beschrieben wird. SNMP liegt derzeit in drei verschiedenen Versionen vor, wobei die beiden älteren SNMP-Versionen keine starke Authentisierung und Verschlüsselung unterstützen. In der dritten Version des SNMP-Protokolls (SNMPv3) wurden diese Schwächen beseitigt und ein ausreichender Schutz zur Wahrung der Vertraulichkeit und Integrität implementiert. Aus diesem Grund sollte möglichst SNMPv3 benutzt werden.

Falls SNMP generell nicht zur Konfiguration oder zum Netzmanagement der Geräte benötigt wird, sollte es auf den Geräten deaktiviert werden.

Kann auf eine Nutzung von SNMPv1 oder SNMPv2 nicht verzichtet werden, so sind zumindest grundlegende Maßnahmen wie die Einschränkung der zugriffsberechtigten IP-Adressen und die Verwendung von abgeschotteten Management-Subnetzen zu ergreifen. Um zu verhindern, dass nicht jeder Nutzer per SNMP auf die Netzwerk-Komponenten zugreifen kann, können ACLs verwendet werden, die den Zugriff mittels SNMP beschränken. Des Weiteren können ACLs zur Limitierung des Zugriffs auf Management-Stationen implementiert werden.

SNMP unterscheidet zwischen Lese- und Schreib-Zugriffen. Um einen möglichst hohen Schutz sicherzustellen, sollten bei Nutzung von SNMPv1 oder SNMPv2 ausschließlich Lese-Zugriffe erlaubt werden.

Alle sicherheitsrelevanten Vorfälle eines Servers der TK-Lösung sollten zur Sicherung und Auswertung verschlüsselt auf einen gehärteten Syslog-Server übertragen werden. Bei erhöhtem Schutzbedarf sollte der Syslog-Server nur von autorisierten Servern Log-Nachrichten akzeptieren.

Zur Authentisierung der Management-Station sollte ein RADIUS-Server verwendet werden.

Zur Administration muss so weit wie möglich auf Telnet verzichtet werden, da Telnet keine Verschlüsselung bietet. Stattdessen sollte SSHv2 eingesetzt werden.

M-TK-238 Überwachung der Komponenten des Telekommunikationssystems

Die Komponenten des Telekommunikationssystems (z. B. Server und Gateways) müssen kontinuierlich zentral überwacht werden. Dies beinhaltet zunächst die Überwachung der Verfügbarkeit der Komponenten. Dies kann durch regelmäßige Anfragen über die Kommunikationsschnittstellen der Komponenten (z. B. per SNMP-basierten Polling oder per Ping) erfolgen. Die Polling-Intervalle müssen im Einzelfall festgelegt werden und richten sich nach der geforderten Verfügbarkeit der Dienste des Telekommunikationssystems.

Weiterhin sollten die Komponenten so konfiguriert werden, dass bei Fehlersituationen und bei Überschreiten von (anwendungsabhängigen) Schwellwerten ein Alarm zu einer zentralen Fehlerkonsole geschickt wird. Hier können SNMP Traps sowie Syslog-Meldungen genutzt werden.

41 Siehe [IETF RFC3411-2002], [IETF RFC3412-2002], [IETF RFC3413-2002], [IETF RFC3414-2002], [IETF RFC3415-2002], [IETF RFC3416-2002], [IETF RFC3417-2002], [IETF RFC3418-2002]

Bei einem erhöhten Schutzbedarf sollte die Überwachung auf die Verfügbarkeit der notwendigen Dienste erweitert werden. Dabei kann beispielsweise überwacht werden, ob auf einer Komponente gewisse Prozesse laufen und ob ein Dienst auf eine Anfrage reagiert.

M-TK-239 Erweiterung von Penetrationstests auf die verwendeten TK-Technologien

Penetrationstests müssen insbesondere bei erhöhtem Schutzbedarf auch für die verwendeten TK-Technologien so erweitert werden, dass sie auch die spezifischen Schwachstellen von VoIP-, UCC- und sonstigen TK-Systemen erkennen können. Gegebenenfalls sind auch zielgerichtete Penetrationstests für die verwendete Technologie zu entwickeln. Beispielsweise sind beim Einsatz von Voice over IP (VoIP) und Unified Communications and Collaboration (UCC) technologiebedingt spezifische Schwachstellen möglich, etwa bei der Signalisierung durch Session Initiation Protocol (SIP), die durch Angreifer ausgenutzt werden können. Zur Erkennung solcher Schwachstellen sind in einem gewissen Umfang Werkzeuge verfügbar, die im Zusammenhang mit bestehenden oder neu entwickelten Penetrationstests angewendet werden können.

M-TK-240 Ergänzung der Überwachung um Honeypots für die verwendeten TK-Technologien

Als Honeypot wird ein spezieller Server bezeichnet, der die Dienste von anderen Servern simuliert und so Angreifer vom eigentlichen Ziel hin zum Honeypot ablenken soll, um Angriffe ins Leere laufen zu lassen und sie zu analysieren. Auf Honeypots werden hierzu Angriffsversuche protokolliert sowie gegebenenfalls ein Alarm ausgelöst, sodass eine Auswertung dieser Daten zur Identifikation von Schwachstellen wesentlich beiträgt.

Zur gezielten Analyse von Schwachstellen kann entweder die bestehende Lösung ergänzt oder es können speziell auf VoIP- und UCC-Technologien zielgerichtete Honeypots in die IT-Systeme integriert werden.

M-TK-241 Erweiterung des Verwundbarkeits-Managements für die verwendeten TK-Technologien

In den jeweiligen Prozessen des Verwundbarkeits-Managements sind auf Ebene eines Computer Emergency Response Teams (CERT) die eingesetzten TK-Technologien zu berücksichtigen. Dies schließt beispielsweise die spezifischen Verwundbarkeiten von SIP und anderen Signalisierungsprotokollen mit ein. In diesem Zusammenhang ist der Einsatz von Security-Scannern, die Schwachstellen auch in der verwendeten TK-Technologie erkennen können, von besonderer Bedeutung. Zum Einsatz von Security-Scannern im Allgemeinen siehe auch M-TK-229 „Härtung von Servern des Telekommunikationssystems“. Es sind gegebenenfalls spezielle Produkte für VoIP, UCC und andere TK-Technologien einzusetzen.

10.4 Datenschutz

Insbesondere im Bereich von TK-Lösungen werden häufig Daten verarbeitet und gespeichert, die besonderen Anforderungen an Integrität und Vertraulichkeit unterliegen oder sogar als personenbezogene Daten besonderen gesetzlichen Bestimmungen unterliegen. Insbesondere werden auf den Telefonie-Servern personenbezogene Daten verarbeitet und gespeichert, die entsprechend vor einem unberechtigten Zugriff geschützt werden müssen. Basis für einen erhöhten Schutzbedarf sind die Maßnahmen in Baustein B 1.5 „Datenschutz“ der IT-Grundschutz-Kataloge, die für TK-Lösungen durch die folgenden Maßnahmen ergänzt bzw. detailliert werden.

M-TK-242 Schutz von Verbindungsdaten

Die für Abrechnung und Gebührenerfassung zu ermittelnden Daten werden aus den sogenannten Call Detail Records (CDRs, auch als Call Data Records bezeichnet) extrahiert. In diesen Datensätzen werden Verbindungsdaten wie z. B. Quelle, Ziel und die Dauer des Gesprächs gespeichert.

Für die dabei erfassten personenbezogenen Daten gelten besondere Schutzanforderungen, die sich unmittelbar aus den anwendbaren Gesetzen und Regelungen beispielsweise zum

Datenschutz – insbesondere das Bundesdatenschutzgesetz (BDSG) sowie die Datenschutzgesetze der Länder – und aus dem Telekommunikationsgesetz ergeben.

Speicherung, Übertragung, Auswertung, Archivierung und Verarbeitung personenbezogener Daten müssen den gesetzlichen Richtlinien zum Datenschutz entsprechen. Hierzu dienen folgende Maßnahmen:

- Damit keine Person einen alleinigen Zugang zu Verbindungsdaten erhält, kann eine technische Durchsetzung des Vier-Augen-Prinzips eingerichtet werden.
- Eigene Zuordnung zu einem einzelnen Anschluss kann durch Anonymisierung der letzten 3 Ziffern einer Telefonnummer in den Aufzeichnungen verhindert werden.

Bei als privat markierten Gesprächen müssen in Aufzeichnungen und Auswertungen von CDRs alle Telefonnummern anonymisiert werden.

M-TK-243 Nutzung von speziell abgesicherten Räumlichkeiten

Besteht bei Gesprächen oder Datenkommunikation ein erhöhter Schutzbedarf hinsichtlich Vertraulichkeit, so sollte derartige Kommunikation in dedizierten Räumen erfolgen, die speziell gegen Abgreifen von Informationen geschützt werden (Abhörsicherung, Sichtschutz, Zutrittsschutz, regelmäßige Überprüfung auf Abhörwanzen usw.).

Als Beispiel ist hier ein abhörsicherer, nicht von außen einsehbarer Besprechungsraum für geheime Konferenzen zu nennen.

M-TK-244 Sichere Außerbetriebnahme von Komponenten des Telekommunikationssystems

Auf den Komponenten von Telekommunikationssystemen fallen während des Betriebs personenbezogene Daten an, beispielsweise Verbindungsdaten, die zur Gebührenabrechnung benötigt werden. Gespeichert werden diese Daten auf den eingebauten Datenträgern, z. B. Auf einer Festplatte, dieser Systeme.

Bei der Außerbetriebnahme dieser Komponenten ist darauf zu achten, dass die Datenträger, auf denen personenbezogenen Daten gespeichert werden, sicher entsorgt werden. Sicher entsorgen bedeutet, dass die Datenträger entweder physisch durch Zerstörung unlesbar gemacht werden oder das die Daten auf dem Datenträger so gelöscht werden, dass eine Rekonstruktion der Daten nicht möglich ist.

10.5 Auswahl von Dienstanbietern

Bei einem erhöhten Schutzbedarf sollte beim Einkauf von Telekommunikationsdienstleistungen generell der Baustein B 1.11 „Outsourcing“ der IT-Grundschutz-Kataloge angewendet werden. Dabei ist die Einschätzung der Vertrauenswürdigkeit eines Dienstanbieters ein wichtiges Element.

M-TK-245 Nachweis der Vertrauenswürdigkeit des Dienstanbieters

Durch eine Zertifizierung beispielsweise nach ISO 27001 auf Basis von IT-Grundschutz kann ein Dienstanbieter dokumentieren, dass er (für die zertifizierten Bereiche) ein Sicherheitsmanagement in einer gewissen Tiefe umsetzt. Eine solche Zertifizierung oder ein vergleichbarer Nachweis kann bei der Auswahl des Dienstanbieters zur Einschätzung von dessen Vertrauenswürdigkeit herangezogen werden. Ein Dienstanbieter könnte beispielsweise einem Kunden Informationen über die eingesetzten Mechanismen zum Schutz der Kundendaten geben und in einem gewissen Rahmen dem Kunden einen Einblick in die Umsetzung dieser Maßnahmen gewähren.

10.6 Notfallvorsorge

M-TK-246 Notfallvorsorge für alle Teilsysteme der TK-Lösung

Telefonie gehört in jeder Organisation zu den wichtigsten IT-Diensten. Ein vollständiger Ausfall ist nicht hinzunehmen. Dies wird für den normalen Schutzbedarf in Baustein B 1.3 „Notfallmanagement“ und für VoIP bereits im Baustein B 4.7 „VoIP“ der BSI IT-Grundschutz-Kataloge in Maßnahme M 6.100 „Erstellung eines Notfallplans für den Ausfall von VoIP“ adressiert. Für den erhöhten Schutzbedarf werden die folgenden Aspekte der Notfallvorsorge besonders betont:

- Mindestens das Absetzen von Notrufen muss jederzeit möglich sein.
- Bei schadenstiftenden Ereignissen, die im IT-Bereich zu Ausfällen mit Notfallausmaß führen können, müssen während der Notfallbehandlung Telefonate mit Externen geführt werden können (z. B. Support-Firmen).
- Die Erreichbarkeit für Kunden oder Partner per Telefon ist wichtig für die Akzeptanz der angebotenen Leistungen, insbesondere bei Kontaktcentern und Händlersystemen.

In vielen Fällen umfasst aus solchen Gründen ein erhöhter Schutzbedarf für TK-Lösungen insbesondere einen erhöhten Schutzbedarf bzgl. Verfügbarkeit. Einer geeigneten Notfallvorsorge für TK-Lösungen über den B 1.3 „Notfallmanagement“ hinaus kommt daher für die Prozesse der Organisation eine hohe Bedeutung zu.

Eine angemessene Notfallvorsorge für TK-Lösungen setzt sich dabei aus verschiedenen Komponenten zusammen:

- Durchführung von Maßnahmen zur Vorbereitung einer schnellen Wiederherstellung von Systemkomponenten

  Hier sind, wie in Maßnahme M-TK-234 „Berücksichtigung der Server der TK-Lösung im Datensicherungskonzept der Organisation“ beschrieben, je nach Elementen der TK-Gesamtlösung unterschiedliche Lösungen zu prüfen und aktuell zu halten.

  Für alle so getroffenen Vorkehrungen zur schnellen Systemwiederherstellung ist in regelmäßigen Abständen zu prüfen, ob diese auch tatsächlich als Basis für eine Systemwiederherstellung funktionsfähig sind. Typische Prüfungen dieser Art sind z. B.:

  - Prüfung von Datenträgern mit System- oder Datensicherungen auf Lesbarkeit
  - Prüfung von Images auf Lauffähigkeit nach Probeinstallation auf Testsystemen oder vergleichbarer Ersatz-Hardware.

  Durchgeführte Tests und Testergebnisse sind zu dokumentieren.

- Festlegung von Sofortmaßnahmen für typische Schadenssituationen

  Eine typische Sofortmaßnahme dieser Art kann darin bestehen, für Notfälle festgelegte Sperrungen des Zugangs zur Telefonie für das Gros der Apparate zu aktivieren, und so die Nutzung der verbliebenen Anlagenkapazitäten auf festgelegte, im Notfall wichtige Arbeitsplätze zu konzentrieren.

  Weitere typische Sofortmaßnahmen ergeben sich für Sicherheitsvorfälle im Bereich der TK-Lösung, deren Ausbreitung verhindert werden soll, z. B. Abkopplung eines stark gestörten TK-Systems vom produktiven Netz bei Virenbefall als erkannter Ursache.

- Vorbereitung von Notbetriebsformen

  Zu bevorzugen sind separate Anschlüsse an das PSTN, parallel zur Systemlösung. Solche Anschlüsse sichern die Möglichkeit, Notrufe und Erreichbarkeit auch dann zu gewährleisten, wenn die Gesamtlösung grundlegend gestört sein sollte. Bei der Planung dieser Notbetriebsform ist darauf zu achten, dass hierfür ausreichende Direktanschlüsse

geschaffen werden, um an allen notwendigen Stellen eines betrachteten Standorts Notrufmöglichkeiten und Notarbeitsplätze zu erhalten. Beispiele hierfür sind Alarmzentrale, Werksarzt oder vorgesehener Raum für Krisenstab.

Eine weitere Notbetriebslösung kann darin bestehen, dass zum Tätigen oder Entgegennehmen wichtiger Anrufe sowie zur Koordination der Notfallbehandlung Mobiltelefone an ausgewählte Nutzer ausgegeben werden. Diese Nutzer müssen im Rahmen der Notfallvorsorge festgelegt werden. Diese Festlegungen sind in einem Notfallplan zur TK-Lösung zu dokumentieren, zusammen mit einer Vorschrift, wie der Prozess zur Verteilung der Mobiltelefone verläuft und über welche Kontakte er anzustoßen ist. Als Lösung für Notruftelefone ist diese Notbetriebsform allerdings eher ungeeignet, da die Verfügbarkeit von Mobilfunknetzen phasenweise deutlich unter der des PSTN-Festnetzes liegt.

- Festlegen und Bereithalten von Basis-Hardware für Ausweichlösungen

  Für bestimmte Elemente der TK-Gesamtlösung kann es sinnvoll sein, eine unvorhergesehen lange Wartezeit auf eine gleichwertige Ersatz-Hardware zu überbrücken. Hierzu wird auf einer Ausweich-Hardware eine Installation betriebsfertig gemacht, die der vom Notfall betroffenen Teillösung funktional gleichwertig ist. Im Vergleich zum Normalbetriebszustand weist eine solche Ausweichlösung häufig Nachteile bzgl. Performance und Redundanz auf. Typische Beispiele als Ausweichbasis sind (ressourcenschwächere) Testsysteme oder als Ausweichplattform für verschiedenste Systeme vorgehaltene Ersatz-Hardware. Sofern TK-Teilsysteme in Form virtueller Systeme realisiert sind, kann eine Ausweichlösung auch darin bestehen, eine für andere IT-Systeme vorhandene Virtualisierungsbasis als vorübergehendes Gastsystem zu nutzen.

  Alle Ausweichlösungen haben gemeinsam, dass mit ihrer Hilfe nicht der Normalbetriebszustand erreicht wird, d. h. die Ausweichinstallation kann nicht dauerhaft bestehen bleiben.

  In einem Notfallplan zur TK-Lösung ist festzuhalten, welche Ausweichlösungen in Frage kommen und mit Hilfe welcher Schritte die jeweilige Ausweichlösung herbeigeführt wird.

- Festlegungen zur Wiederanlaufreihenfolge

  Hier ist zum einen die Bestimmung einer geeigneten Wiederanlaufreihenfolge innerhalb der Komponenten des TK-Gesamtsystems zu leisten. Je grundlegender die Funktionalität eines Teilsystems für die Möglichkeit zum Telefonieren ist, umso früher sollte ein solches Teilsystem wiederhergestellt oder zumindest durch eine funktionsgleiche Ausweichlösung überbrückt sein.

  Insofern sind zunächst alle Teilsysteme bzw. Teilfunktionen der TK-Lösung wieder herzustellen, die notwendig sind, damit Nutzer überhaupt Zugang zur Telefonie erhalten und Telefongespräche führen können. Erst danach folgen Mehrwertdienste bzw. UCC-Applikationen. Für diese ist eine Wiederanlaufreihenfolge nach den folgenden Kriterien zu entscheiden:

  - technische Abhängigkeiten solcher Dienste untereinander
  - Bedeutung für die Geschäftsprozesse der Organisation
  - Umfang des von ihrer Verfügbarkeit profitierenden Nutzerkreises

  Die TK-Lösung darf jedoch nicht isoliert betrachtet werden. Da sie gemeinsam mit anderen IT-Nutzungsformen dieselbe Netzwerkinfrastruktur verwendet und zum Teil auch dieselben Kommunikations-Basisdienste wie DNS nutzt, muss die TK-Lösung mit ihren Komponenten in eine übergeordnete Wiederanlaufplanung eingeordnet werden.

  Dabei hat sich in der Praxis gezeigt, dass IT-Gesamtlösungen zu komplex sind, um alle möglichen Ausfallszenarien vorbereitend durchzuspielen und hierfür geeignete Wiederanlauffestlegungen zu treffen. Vielmehr ist eine fallweise Bestimmung über Prioritätsklassen zu empfehlen: Alle IT-Systeme, auch die TK-Komponenten, werden im

nächsten Schritt der geeigneten Prioritätsklasse zugeordnet. Die Wiederherstellung wird grundsätzlich in Reihenfolge der Prioritätsklassen gesteuert (Priorisierung der Wiederherstellungsmaßnahmen). Sind mehrere Systeme der gleichen Klasse betroffen, so kann parallel an deren Wiederherstellung gearbeitet werden, soweit keine Ressourcenkonflikte entstehen. Bei Ressourcenkonflikten, z. B. bei Zuständigkeit der gleichen Personen für betroffene Systeme gleicher Priorität, werden flexibel je nach Lage durch leitendes Personal der IT (als Notfallteam) Reihenfolgeentscheidungen getroffen.

Alle Festlegungen, die im konkreten Notfall zur Bestimmung der Wiederanlaufreihenfolge führen, sind im Rahmen der Notfallvorsorge vorbereitend zu dokumentieren (Notfallhandbuch der IT bzw. Notfallplan TK-Lösung).

- Abschluss von Support-Verträgen inklusive Notfall-Konditionen

  Während typische Wartungsverträge sich auf das Incident Management konzentrieren, müssen für den Notfall besondere Vereinbarungen getroffen werden. Notfallszenarien können größere Systemschäden beinhalten, die über das im Incident typische Ausmaß an benötigter Ersatz-Hardware hinausgehen. Hier muss für Kernsysteme der VoIP-Lösung eine Notfall-spezifische Vertragskomponente erwogen werden, die eine Express-Lieferung von Ersatz-Hardware für alle solchen Kernsysteme beinhaltet. Werden solche Vereinbarungen inklusive der im Notfall notwendigen kurzen Lieferzeiten getroffen, so ist dies mit einer entsprechenden Vorhaltung von Hardware beim Support-Unternehmen verbunden und erhöht entsprechend die Vertragsgebühren. Alternativ kann in bestimmtem Umfang eine eigene Reserveteilhaltung für solche wichtigen Komponenten erwogen werden, mit Unterbringung möglichst fern von den durch sie zu ersetzenden produktiven Komponenten.

  Ebenfalls Teil eines Support-Vertrags, der auch im Notfall greift, ist die Option auf Unterstützung durch externen 3rd-Level-Support. Entsprechende vertragliche Festlegungen stellen sicher, dass bei Bedarf kurzfristig auf entsprechend kompetentes Personal des Externen zurückgegriffen werden kann und nicht erst Verhandlungen über die Konditionen erfolgen müssen.

- Erstellung eines Notfallplans für alle Komponenten der TK-Lösung

  Soweit sie nicht aus einem übergeordneten Notfallhandbuch oder ähnlichen Business-Continuity-relevanten Dokumenten hervorgehen, sind alle für die Notfallbehandlung zur TK-Lösung relevanten Festlegungen in einem solchen Notfallplan festzuhalten. Dieser nennt alle vorbereiteten bzw. vorbereitend festgelegten Sofortmaßnahmen, Ausweichlösungen, Notbetriebsformen und Schritte zu deren Einleitung sowie typische Schritte auf dem Weg zur Wiederherstellung des Normalbetriebs. Ebenfalls enthalten sind notwendige Kontaktinformationen für den Notfall, Festlegungen bzgl. Zuständigkeiten für die Einleitung/Durchführung von Maßnahmen und besondere Meldepflichten in Notfällen bzgl. der TK-Lösung.

- Durchführung von Notfallübungen

  Gerade für die TK-Lösung ist die sichere Beherrschung notwendiger Notfallmaßnahmen von hoher Bedeutung. Angesichts der hohen Wichtigkeit der Telefonierfähigkeit bzw. der Bedeutung der TK-Lösung für die Geschäftsprozesse der Organisation gerade auch im Notfall darf keine wertvolle Zeit durch Unsicherheiten verloren werden. Entsprechend sind typische Maßnahmen regelmäßig einzuüben. Sofern dies nicht im Rahmen regelmäßig im Betriebsalltag wiederkehrender Tätigkeiten erfolgt (z. B. Installation zusätzlicher Geräte mit Hilfe von Images), muss ein Einüben in Form von Notfallübungen erfolgen.

10.7 Organisatorische Maßnahmen

Bei einem erhöhten Schutzbedarf der TK-Lösung kommt den Anwendern und Administratoren eine besondere Bedeutung bei der effektiven Umsetzung der spezifizierten Maßnahmen zu. Generell sollte der Baustein B 1.2 „Personal“ der IT-Grundschutz-Kataloge angewendet werden, ergänzend sind die folgenden Maßnahmen besonders zu beachten:

M-TK-247 Sensibilisierung der Anwender von TK-Diensten hinsichtlich Sicherheitsaspekten

Mit dem Einsatz von TK-Diensten insbesondere bei Nutzung durch mobile Endgeräte gehen vielfältige Gefährdungen einher, die durch den bewussten Umgang der Anwender mit Applikationen und Endgeräten vermieden oder abgemildert werden können. Hierzu gehört insbesondere die Bedienung und die Konfiguration der Endgeräte. Beispiele sind:

- Die Nutzer insbesondere von mobilen Endgeräten müssen trainiert werden, sodass sie für eine Kommunikation erkennen, ob diese verschlüsselt oder unverschlüsselt erfolgt.
- Der Abfluss sensibler Daten über Webkonferenzen kann vermieden werden, wenn dem Anwender die Möglichkeit zu Screenshots auf der Gegenseite bewusst gemacht wird und somit besonderes Augenmerk auf die Vertrauenswürdigkeit des Kommunikationspartners gelenkt wird. Das Wecken des Sicherheitsbewusstseins und die Erläuterung von Gefährdungen sollte Bestandteil der Schulungsprogramme für Anwender und Systemadministratoren sein.

M-TK-248 Schulung der Anwender von TK-Diensten zu Sicherheits- und Datenschutzaspekten

Die Bedienung von TK-Diensten ist in den vergangenen Jahren bedeutend leichter geworden. Andererseits ist die Zahl der in der Praxis eingesetzten Applikationen und Dienste sowie die Vielfalt der Endgeräte erheblich gewachsen. Diese Situation kann dazu führen, dass Benutzer überfordert sind, Dienste und Endgeräte nicht ihrer Bestimmung entsprechend nutzen oder fehlerhaft bedienen und sich möglicher Sicherheitsrisiken nicht bewusst sind. Hierdurch können die Vertraulichkeit und die Verfügbarkeit gefährdet sein.

Mitarbeiter müssen daher im sicheren Umgang mit den zur Verfügung stehenden Kommunikationsmedien, Applikationen und Endgeräten entsprechend geschult werden.

Besonderes Augenmerk ist auf den Umgang mit der Bearbeitung von personenbezogenen Daten und anderen schützenswerten Informationen zu richten. Dies gilt insbesondere für Agenten und Supervisoren in Kontaktcentern und Händlersystemen, aber auch für Administratoren der entsprechenden Speichersysteme. Supervisoren müssen zudem über die Regelungen zur Wahrung der Privatsphäre der Mitarbeiter informiert werden, da ihnen im Rahmen des Quality Monitoring erhebliche Eingriffe in die Privatsphäre des Agenten ermöglicht werden (z. B. Abhören von Gesprächen).

M-TK-249 Schulung der Administratoren von TK-Lösungen

TK-Systeme und integrierte Applikationen sowie die Einbindung der Endgeräte können nicht isoliert betrachtet werden. Änderungen an einem Teilsystem (z. B. die Einrichtung einer Fernwartungsmöglichkeit) können sicherheitsrelevante Auswirkungen auf andere Teilsysteme oder sogar auf das komplexe Gesamtsystem haben. Es ist daher erforderlich, die Administratoren der jeweiligen Teilsysteme zu den Wechselwirkungen mit dem Gesamtsystem zu schulen und auf mögliche Sicherheitsrisiken hinzuweisen. Dies gilt auch dann, wenn der jeweilige Administrator nur mit der Betreuung eines Teilsystems befasst ist.

10.8 Zusammenfassung

Es gibt Sicherheitsmaßnahmen, welche systemübergreifend erfüllt sein müssen, um ein angemessenes Sicherheitsniveau des Telekommunikationssystems zu erreichen. Diese vorgestellten systemübergreifenden Maßnahmen sind als generische Maßnahmen zu betrachten. Sie müssen an das System, in welchem sie umgesetzt werden sollen, angepasst und für dieses konkretisiert werden. Es werden insbesondere solche Maßnahmen betrachtet, welche für TK-Lösungen oft vernachlässigt werden, da sie bei der Betrachtung einzelner Systeme nicht direkt erkennbar sind.

Die Maßnahmen, welche für Telekommunikationssysteme mit erhöhtem Schutzbedarf erforderlich sind, setzten die Maßnahmen für normalen Schutzbedarf und deren Umsetzung voraus, welche in den IT-Grundschutz-Katalogen beschrieben werden. Die folgenden Maßnahmen sind für das gesamte Telekommunikationssystem relevant.

Auslegung der passiven Netzinfrastruktur

Bei der Auslegung der passiven Infrastruktur, welche beispielsweise die Verkabelung des Netzwerkes betrifft, muss das Risiko einer unzureichenden Verfügbarkeit minimiert werden und unbefugte Zugriffe verhindert werden.

In Ergänzung des IT-Grundschutz-Bausteins B 2.12 „IT-Verkabelung“ muss eine sichere Kabelführung erfolgen. So müssen Beschädigungen von Kabelinstallationen (versehentlich oder beabsichtigt) soweit möglich verhindert und Eingriffe in die Verkabelung mit dem Ziel des Abhörens unterbunden werden.

Absicherung von Servern des Telekommunikationssystems

Zusätzlich zu den Maßnahmen der IT-Grundschutz-Kataloge müssen Server eines Telekommunikationssystems mit erhöhten Sicherheitsanforderungen besonders geschützt werden. Server des TK-Systems müssen physisch geschützt werden, d. h. ihre Unterbringung erfolgt in abgeschlossenen Räumen mit Zugangskontrolle und Videoüberwachung.

Der zur Vermeidung von Sicherheitsvorfällen erforderliche Schutz geht über die Maßnahmen in IT-Grundschutz-Katalogen hinaus.

- Server, welche mit Standardbetriebssystemen betrieben werden, müssen ergänzend gehärtet und bekannte Schwachstellen zeitnah geschlossen werden.
- Bei der Aktualisierung des Systems ist zu beachten, dass Patches in einem Teilbereich des Systems Einfluss auf andere Teilbereiche haben können.
- Systeme sind durch entsprechende Konfiguration auf ein Minimalsystem zu reduzieren, nicht benötigte Netzdienste sind zu deaktivieren und mögliche Infektionswege müssen überwacht werden.
- Bei erhöhtem Schutzbedarf ist die Sicherheit eines Systems mittels Sicherheitszertifizierung nachzuweisen.
- Virtuelle Systeme mit erhöhtem Schutzbedarf bezüglich Integrität und Vertraulichkeit sind besonders zu härten und umfassend zu kapseln.
- Zur Sicherstellung einer effektiven Wiederherstellung der vollen Verfügbarkeit müssen Konfigurationen und Anwendungen gesichert werden. Die Sicherungen müssen stets aktuell gehalten werden. Die Art der Sicherung ist an den maximal tolerablen Datenverlust anzupassen.
- Der administrative Zugang zu Servern im Telekommunikationssystem muss weitestmöglich eingeschränkt werden. Zugriffe müssen personalisiert und authentifiziert erfolgen und in einer Logbuchdatei protokolliert werden.

Sicheres Netz- und Systemmanagement

Typischerweise sind Telekommunikationskomponenten in ein zentrales Netz- und Systemmanagement eingebunden. Unterliegen sie einem erhöhten Schutzbedarf müssen sie mittels geeignetem Netzwerk-Management-Protokoll geschützt werden. Das verwendete Protokoll muss einen ausreichenden Schutz zur Wahrung der Vertraulichkeit und Integrität bieten und eine Möglichkeit bieten sicherheitsrelevante Vorfälle zu sichern und auszuwerten.

In Hinblick auf die Verfügbarkeit der Komponenten müssen diese kontinuierlich zentral überwacht werden. Bei erhöhten Schutzbedarf ist die Überwachung auch auf notwendige Dienste zu erweitern. In Fehlersituationen soll ein Alarm zu einer zentralen Fehlerkonsole weitergeleitet werden.

Datenschutz

Bereiche, in denen personenbezogene Daten verarbeitet und gespeichert werden, unterliegen erhöhten Anforderungen bezüglich Integrität und Vertraulichkeit. Die Schutzmaßnahmen der IT-Grundschutz-Kataloge sind dann um die folgenden Maßnahmen zu erweitern.

- Keine Person darf alleinigen Zugang zu den Daten haben. Dies lässt sich zum Beispiel über das Vier-Augen-Prinzip realisieren.
- Eine Zuordnung zu einem einzelnen Anschluss soll durch (teilweise) Anonymisierung vermieden werden.
- Speichermedien, auf welchen sich personenbezogene Daten befinden, müssen sicher entsorgt werden, was beispielsweise durch physische Zerstörung oder nicht rekonstruierbare Löschung der Daten umgesetzt werden kann.

Werden Informationen mit erhöhtem Schutzbedarf hinsichtlich der Vertraulichkeit ausgetauscht, sollte eine derartige Kommunikation von speziell geschützten Räumen ausgehen.

Auswahl von Dienstanbietern

Bei Einkauf von Telekommunikationsdienstleistungen ist die Vertrauenswürdigkeit eines Dienstanbieters besonders zu berücksichtigen. Der Anbieter kann seine Vertrauenswürdigkeit beispielsweise über eine Zertifizierung nach ISO 27001 (oder ein vergleichbares Zertifikat) darlegen. Alternativ könnte der Dienstanbieter seinem Kunden auch eine entsprechende Prüfung der eigenen Vertrauenswürdigkeit (inkl. Untersuchung von Infrastruktur und Arbeitsprozessen) erlauben.

Notfallvorsorge

Die Notfallvorsorge soll verhindern, dass ein schadenstiftendes Ereignis zu einem vollständigen Ausfall der Telefonie führt. Bei einem erhöhten Schutzbedarf bezüglich Verfügbarkeit muss mindestens das Absetzten von Notrufen, das Führen von externen Telefonaten (z. B. zu Support-Firmen) und die Erreichbarkeit per Telefon sichergestellt werden. Eine angemessene Notfallvorsorge beinhaltet daher die folgenden Maßnahmen:

- Es müssen Vorbereitungen für eine schnelle Wiederherstellung von Systemkomponenten getroffen werden. Hierbei ist regelmäßig zu überprüfen, ob diese als Basis für eine Systemwiederherstellung funktionsfähig sind. Diese Maßnahmen sind zu dokumentieren.
- Es müssen Sofortmaßnahmen für typische Schadenssituationen festgelegt und Notbetriebsformen vorbereitet werden. Das Vorbereiten von Notbetriebsformen beinhalten das Festlegen erster Maßnahmen und das Bereithalten von Basis-Hardware.
- Die Wiederherstellungsreihenfolge des Systems muss festgelegt werden. In der Reihenfolge sollten Teilsysteme mit grundlegenden Funktionalitäten priorisiert werden.
- Die Sicherung von optionaler Unterstützung sollte im Rahmen von Support-Verträgen sichergestellt werden. Diese Verträge können bei Bedarf auch Regelungen zur Lieferung von Ersatz-Hardware beinhalten.

- Die Maßnahmen der Notfallvorsorge sind in einem Notfallplan festzuhalten. Der Notfallplan sollte auch Zuständigkeiten, notwendige Kontaktinformationen und Meldepflichten beinhalten.

Um sicher zu stellen, dass alle notwendigen Maßnahmen im Notfall sicher beherrscht werden, sind regelmäßig Notfallübungen durchzuführen. Diese Übungen müssen mindestens die Maßnahmen beinhalten, welche im Betriebsalltag nicht regelmäßig durchgeführt werden.

Organisatorische Maßnahmen

Bei einem erhöhten Schutzbedarf von TK-Lösungen müssen die Maßnahmen der IT-Grundschutz-Kataloge um Maßnahmen erweitert werden, welche insbesondere Anwender und Administratoren der TK-Lösungen betrifft:

- Anwender von Endgeräten müssen die Bedienung der Endgeräte und darauf installierten Applikation sicher beherrschen. Dazu gehört, dass der Anwender über ein angemessenes Sicherheitsbewusstsein verfügt, Bestimmungen von Applikationen kennt und deren Sicherheitsrisiken beurteilen kann. Diese Kenntnisse können beispielsweise über Schulungen vermittelt werden.
- Supervisoren z. B. in Kontaktcentern müssen Regelungen zur Wahrung der Privatsphäre von Mitarbeitern kennen und diese anwenden.
- Administratoren müssen Wechselwirkungen zwischen verschiedenen Anwendungen berücksichtigen, da Änderungen an einem Teilsystem sicherheitsrelevante Auswirkungen auf andere Systemteile oder das Gesamtsystem haben können.

11 Übersicht über Gefährdungen und Maßnahmen

Im Folgenden wird die Gesamtheit der erarbeiteten Gefährdungen und Sicherheitsmaßnahmen gelistet (siehe Kapitel 11.1). Ergänzt wird die Liste in Kapitel 11.2 durch die Zusammenstellung der referenzierten Bausteine, Gefährdungen und Sicherheitsmaßnahmen der BSI IT-Grundschutz-Kataloge (siehe [BSI GSK-2013]).

11.1 Spezifiziert in dieser Technische Leitlinie

11.1.1 Gefährdungen

Klassische Telekommunikationstechnik		**Spezifikation**
G-TK-1	Unzureichende oder fehlende Konzepte für die Wartung einer TK-Anlage	Seite 38
G-TK-2	Ungeeignete Aufstellung eines Wartungsapparats	Seite 38
G-TK-3	Unzureichende Passwort-Policy für einen administrativen Zugang	Seite 38
G-TK-4	Unzureichender Schutz personenbezogener Daten	Seite 38
G-TK-5	Verstöße gegen das Urheberrecht	Seite 39
G-TK-6	Unzureichende Prüfung der Identität von Kommunikationspartnern	Seite 39
G-TK-7	Funktionsstörung oder Ausfall der TK-Anlage durch Fehlkonfiguration	Seite 39
G-TK-8	Nachlässigkeiten bei der Verwendung eines PCs für die Administration einer TK-Anlage	Seite 39
G-TK-9	Software-Fehler	Seite 39
G-TK-10	Undokumentierte Funktionen	Seite 40
G-TK-11	Abhören von Verbindungen	Seite 40
G-TK-12	Manipulation der Signalisierung	Seite 40
G-TK-13	Abhören von Räumen	Seite 41
G-TK-14	Missbrauch von Wartungszugängen	Seite 41
G-TK-15	Gebührenbetrug	Seite 41
G-TK-16	Schadenstiftende Software auf Wartungs-PCs	Seite 41
G-TK-17	Verschleierte Identifizierung zwischen Gesprächsteilnehmern	Seite 42

Tabelle 3: Gefährdungen für Klassische Telekommunikationstechnik

Voice over IP		**Spezifikation**
G-TK-18	Ausfall der mitgenutzten IP-Infrastruktur	Seite 77
G-TK-19	Ausfall eines für VoIP mitgenutzten Weitverkehrsnetzes	Seite 77
G-TK-20	Unzureichende Regelungen für den Einsatz von VoIP	Seite 78
G-TK-21	Unzureichende Harmonisierung zwischen IT- und VoIP-Betrieb	Seite 78
G-TK-22	Fehlende, ungeeignete und inkompatible Betriebsmittel für VoIP	Seite 79
G-TK-23	Unzureichende Verwaltung und Kontrolle von Zugangs- und Zugriffsmöglichkeiten auf VoIP-Endgeräte	Seite 79
G-TK-24	Kein ordnungsgemäßer Benutzerwechsel für VoIP-Endgeräte	Seite 79
G-TK-25	Mangelhafte Behandlung der Archivierung von Sprachnachrichten und elektronischen Faxnachrichten	Seite 80
G-TK-26	Unzulängliche vertragliche Regelungen für externe Leistungen zur VoIP-Lösung	Seite 80

Voice over IP		**Spezifikation**
G-TK-27	Unzureichende Regelungen für das Ende der externen Dienstleistungen für eine VoIP-Lösung	Seite 80
G-TK-28	Unzureichende Regelungen für den IP-Anlagenanschluss mit dem ITSP	Seite 81
G-TK-29	Unzureichende oder fehlende Planung der Absicherung für die Erweiterung der Außenanbindung um eine VoIP-Komponente	Seite 81
G-TK-30	Unzureichende Kontrolle auf Kommunikationsstrecken bei standortübergreifender Kommunikation	Seite 81
G-TK-31	Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten der VoIP-Benutzer	Seite 81
G-TK-32	Unstrukturierte Datenhaltung durch VoIP-Nutzer	Seite 82
G-TK-33	Konfigurationsfehler und Bedienungsfehler bei VoIP-Lösungen	Seite 82
G-TK-34	Fehlerhafte Administration von Zugangs- und Zugriffsrechten zu VoIP-Installationen	Seite 82
G-TK-35	Denial-of-Service-Angriffe auf VoIP	Seite 84
G-TK-36	Abhören der VoIP-Kommunikation durch Schwachstellen in Netzwerkprotokollen	Seite 85
G-TK-37	Missbräuchlicher Zugriff auf VoIP-Geräte	Seite 87
G-TK-38	Übertragung von schadenstiftender Software über die IP-Kommunikation mit VoIP-Netzelementen des ITSP	Seite 87

Tabelle 4: Gefährdungen für VoIP

Hybrid-Anlagen		**Spezifikation**
G-TK-39	Unzureichende oder fehlende Kompetenzen für Planung und Betrieb einer Hybrid-Anlage	Seite 118
G-TK-40	Unzureichende organisatorische Struktur für den Betrieb einer Hybrid-Anlage	Seite 119
G-TK-41	Unzureichende oder fehlende Konzepte, Regelungen und Prozesse für das Management einer Hybrid-Anlage	Seite 119
G-TK-42	Unzureichend abgestimmte Konfigurationen und Sicherheitseinstellungen für ISDN und VoIP	Seite 119
G-TK-43	Gesamtverfügbarkeit bei Störung einer Komponente	Seite 119
G-TK-44	Fehlende oder unzureichende Integration der Management-Komponenten	Seite 120
G-TK-45	Übergreifende Wirkung eines Angriffs auf eine VoIP-Komponente	Seite 120

Tabelle 5: Gefährdungen für Hybrid-Anlagen

Unified Communications and Collaboration		**Spezifikation**
G-TK-46	Unzureichende oder fehlende Kompetenzen für Planung und Betrieb eines UCC-Systems	Seite 141
G-TK-47	Unzureichende Organisation des Betriebs eines UCC-Systems	Seite 141
G-TK-48	Ungeordnete Nutzung der Kommunikationsmöglichkeiten	Seite 141
G-TK-49	Unzureichende oder fehlende Konzepte, Regelungen und Prozesse für das Management eines UCC-Systems	Seite 141
G-TK-50	Nicht abgestimmte Konfigurationen und Sicherheitseinstellungen	Seite 142
G-TK-51	Zustellung von UM-Nachrichten an falsches Postfach durch Fehlkonfiguration	Seite 142
G-TK-52	Versehentliche Preisgabe von Informationen durch Verwendung von Video am Desktop	Seite 142
G-TK-53	Unbeabsichtigte Preisgabe vertraulicher Informationen durch Application Sharing und Desktop Sharing	Seite 142
G-TK-54	Fehlkonfiguration von Mehrfachsignalisierung und Weiterleitungen	Seite 143
G-TK-55	Zugriff auf Applikationen oder andere Ressourcen durch Freigabe der Steuerung	Seite 143
G-TK-56	Verlust der Verfügbarkeit bei Störung anderer Systemkomponenten	Seite 143

Unified Communications and Collaboration		Spezifikation
G-TK-57	Fehlfunktion von Mehrfachsignalisierung und Weiterleitungen	Seite 143
G-TK-58	Übergreifende Wirkung eines Angriffs auf ein UCC-System	Seite 144
G-TK-59	Unbefugte oder missbräuchliche Nutzung eines UCC-Systems	Seite 144
G-TK-60	Vertraulichkeitsverlust von in UCC-Systemen und integrierten Applikationen gespeicherten Daten	Seite 144
G-TK-61	Angriff auf die Trunk-Verbindungen zwischen UCC-Diensten	Seite 144
G-TK-62	Verlust der Vertraulichkeit durch Kompromittierung des UCC-Clients	Seite 144
G-TK-63	Leistungsüberwachung und Profilbildung durch Präsenzdienste	Seite 145
G-TK-64	Abfluss von Informationen via Instant Messaging	Seite 145
G-TK-65	Verbreitung von Malware, bösartiger Hyperlinks und Spam via Instant Messaging	Seite 145
G-TK-66	Ausspähen von IM-Konversationen	Seite 145
G-TK-67	Ungesicherte Aufzeichnung bzw. Protokollierung von Kommunikation	Seite 145
G-TK-68	Unberechtigter Zugriff auf Postfächer eines UM- oder Voicemail-Systems	Seite 145
G-TK-69	Denial-of-Service auf UM-Postfächer	Seite 146
G-TK-70	Denial-of-Service-Attacken auf UCC-Dienste	Seite 146
G-TK-71	Versenden gefälschter Faxe im Namen Dritter	Seite 147
G-TK-72	Ausspähen von Anwendern und Räumen mittels UCC-Client und Desktop-Video	Seite 148
G-TK-73	Leistungsüberwachung durch Zugriff auf Videokamera	Seite 148
G-TK-74	Abfluss von Daten und Informationen via Webkonferenz durch Screenshots oder Copy&Paste	Seite 148
G-TK-75	Vertraulichkeitsverlust durch Kompromittierung von Konferenzbrücken	Seite 148
G-TK-76	Vertraulichkeitsverlust durch Malware auf Endgeräten mit Softphone oder UCC-Client	Seite 148
G-TK-77	Manipulation von Mehrfachsignalisierung und Weiterleitungen	Seite 149

Tabelle 6: Gefährdungen für Unified Communications and Collaboration

Spezielle TK-Systeme		Spezifikation
Videokonferenz		
G-TK-78	Unzureichende Regelungen für den Einsatz von Videokonferenzen	Seite 173
G-TK-79	Unzureichende Planung von Videokonferenzsystemen	Seite 173
G-TK-80	Unzureichende Harmonisierung zwischen IT-, TK-Anlagen- und Videokonferenz-Betrieb	Seite 173
G-TK-81	Unzureichende Verwaltung und Kontrolle von Zugangs- und Zugriffsmöglichkeiten auf Video-Terminals	Seite 174
G-TK-82	Kein ordnungsgemäßer Benutzerwechsel für Video-Terminals	Seite 174
G-TK-83	Mangelhafte Behandlung der Archivierung von Videokonferenzen	Seite 174
G-TK-84	Unzureichende Prüfung der Identität von Kommunikationspartnern	Seite 174
G-TK-85	Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten der Videokonferenzbenutzer	Seite 174
G-TK-86	Konfigurationsfehler und Bedienungsfehler bei Videokonferenzlösungen	Seite 175
G-TK-87	Fehlerhafte Administration von Zugangs- und Zugriffsrechten zu Videokonferenz-Installationen	Seite 175
Kontaktcenter		
G-TK-88	Fehlkonfiguration des IVR-Systems	Seite 188
G-TK-89	Fehlkonfiguration des Kommunikationsroutings	Seite 188
G-TK-90	Entwenden von sensiblen und personenbezogenen Daten	Seite 189

Spezielle TK-Systeme		**Spezifikation**
G-TK-91	Manipulation von Anrufverteilung oder Dialer	Seite 189
G-TK-92	Attacken durch Missbrauch von Integration in öffentliche Webpräsenzen	Seite 189
G-TK-93	Störung der Betriebsabläufe durch Manipulation von Management-Systemen	Seite 189
Händlersysteme		
G-TK-94	Mangelnde Abstimmung zwischen IT/TK-Betrieb und Betrieb des Händlersystems	Seite 198
G-TK-95	Versehentliches Enthüllen von Informationen durch Händler	Seite 199
G-TK-96	Fehlkonfiguration des Händlersystems und mitgenutzter Systeme	Seite 199
G-TK-97	Abhören der Händlerkommunikation	Seite 199
G-TK-98	Manipulation der Händlerkommunikation	Seite 199
Alarmierungssysteme		
G-TK-99	Unzureichende Regelungen für den Einsatz von Alarmierungssystemen	Seite 210
G-TK-100	Unzureichende Regelungen mit Blick auf Einhaltung maßgeblicher Gesetze und Vorschriften für den Einsatz von Alarmierungssystemen	Seite 210
G-TK-101	Unzureichende Planung (der TK-Mitnutzung) von Alarmierungssystemen	Seite 210
G-TK-102	Unzureichende Kontrolle von Zugangs- und Zugriffsmöglichkeiten zu Elementen einer Alarmierungslösung	Seite 211
G-TK-103	Unzureichender Schutz personenbezogener Daten bei Verwendung durch eine Alarmierungslösung	Seite 212
G-TK-104	Unzureichende Prüfung der Identität von Kommunikationspartnern bei eingehenden Alarmen	Seite 212
G-TK-105	Ungeeigneter Umgang mit Nutzerzugängen und -ausstattung zu Alarmierungslösungen	Seite 212
G-TK-106	Ausfall der mitgenutzten TK-Infrastruktur	Seite 213
G-TK-107	Technisch bedingte Fehlalarme	Seite 213
G-TK-108	Denial-of-Service-Angriffe auf bzw. über Alarmierungssysteme	Seite 213
G-TK-109	Alarmierungssysteme als Ausgangspunkt für Angriffe auf TK-Lösungen	Seite 214

Tabelle 7: Gefährdungen für Spezielle TK-Systeme

Provider-basierte TK-Dienste		**Spezifikation**
Soziale Netzwerke und Soziale Medien		
G-TK-110	Mangelhafte Trennung zwischen privater und dienstlicher Nutzung	Seite 235
G-TK-111	Fehlende Richtlinien zum Umgang mit Sozialen Netzwerken und Medien	Seite 235
G-TK-112	Fehlende oder nicht ausreichende Vorabkontrolle der Außendarstellung über Soziale Netzwerke und Medien	Seite 235
G-TK-113	Mangelhafte Integration der Nutzung von Sozialen Netzwerken und Medien in etablierte Abläufe	Seite 235
G-TK-114	Mangelhafte Verwaltung der Zugriffsrechte für dienstliche Accounts in Sozialen Netzwerken oder Medien	Seite 236
G-TK-115	Keine Information der Mitarbeiter bei Preisgabe persönlicher Daten	Seite 236
G-TK-116	Fehlende oder unzureichende Regelungen bzgl. Nutzungsrechten einer Organisation an Daten in Sozialen Netzwerken und Medien	Seite 236
G-TK-117	Unzureichende Absicherung des Nutzeraccounts	Seite 237
G-TK-118	Unverschlüsselte Nutzung von Sozialen Netzwerken und Medien	Seite 237
G-TK-119	Fehlkonfiguration der Datenschutzeinstellungen	Seite 237
G-TK-120	Versehentliche, unautorisierte Preisgabe von schützenswerten Informationen	Seite 238

Provider-basierte TK-Dienste		**Spezifikation**
G-TK-121	Ungerechtfertigtes Vertrauen in Informationen und Absender	Seite 238
G-TK-122	Verletzung von Urheberrechten	Seite 238
G-TK-123	Preisgabe vertraulicher Informationen durch Client-Software	Seite 238
G-TK-124	Phishing und Betrug über Soziale Netzwerke und Medien	Seite 239
G-TK-125	Identitätsdiebstahl und Social Engineering in Sozialen Netzwerken und Medien	Seite 240
G-TK-126	Profilbildung und Tracking von Personen	Seite 240
G-TK-127	Rekonstruktion von internen Organisationsinformationen	Seite 240
G-TK-128	Herbeiführen eines Reputationsverlustes	Seite 240
G-TK-129	Behinderung der Kommunikation durch Manipulation von Kontaktdaten	Seite 240
Outsourcing, IP-Centrex, Cloud Computing und UC as a Service		
G-TK-130	Fehlende Regelungen und Mechanismen zur Trennung auf Multi-Mandanten-Plattformen	Seite 257
G-TK-131	Unzureichende Regelungen in Bezug auf Wartungsarbeiten	Seite 258
G-TK-132	Mangelnde Verfügbarkeit des Weitverkehrsnetzes beziehungsweise des Netzes zwischen Dienstleister und Organisation	Seite 258
G-TK-133	Versagen der Mechanismen zur Trennung auf Multi-Mandanten-Plattformen	Seite 258
G-TK-134	Abhören von Leitungen / Lauschangriff im Netz des Dienstleisters	Seite 259
G-TK-135	Abfluss von Daten aus dem Netz des Dienstleisters	Seite 259
G-TK-136	Manipulation und Verlust von Daten	Seite 259

Tabelle 8: Gefährdungen für Provider-basierte TK-Dienste

Einbindung Mobiler Endgeräte		**Spezifikation**
G-TK-137	Störung durch Blitzeinschlag	Seite 288
G-TK-138	Beeinträchtigung durch Großveranstaltungen	Seite 288
G-TK-139	Ausfall oder Störung eines öffentlichen Funknetzes	Seite 289
G-TK-140	Fehlende oder unzureichende Regelungen sowie unzureichende Kenntnis über Regelungen bei intelligenten mobilen Endgeräten	Seite 289
G-TK-141	Fehlendes oder unzureichendes Management sowie unzureichende Kontrolle der IT-Sicherheitsmaßnahmen	Seite 290
G-TK-142	Unzureichender Schutz vor unberechtigtem Zugriff auf Mobile Endgeräte und deren Daten	Seite 290
G-TK-143	Ungeordneter Weitergabe oder Außerbetriebnahme	Seite 290
G-TK-144	Unzureichendes Schlüsselmanagement bei Verschlüsselung	Seite 290
G-TK-145	Einschränkung durch unzureichende Kapazitäten des genutzten Datendienstes	Seite 291
G-TK-146	Unkontrollierter paralleler Aufbau von Kommunikationsverbindungen	Seite 291
G-TK-147	Unzureichende Planung für die Nutzung von VoIP, Video und UCC-Diensten	Seite 291
G-TK-148	Unzureichende Planung für den Einsatz in widrigen Umgebungsbedingungen	Seite 291
G-TK-149	Konfigurations- und Bedienungsfehler bei mobilen Endgeräten	Seite 292
G-TK-150	Verlust von Kontaktdaten und sonstigen gespeicherten Daten	Seite 292
G-TK-151	Unerwünschter Datenzugriff durch Apps auf mobilen Endgeräten	Seite 292
G-TK-152	Umfassende bzw. zielgerichtete missbräuchliche Überwachung mobiler Endgeräte und deren Nutzer	Seite 293
G-TK-153	Einschränkungen durch Malware	Seite 293

Tabelle 9: Gefährdungen für die Einbindung Mobiler Endgeräte

11.1.2 Maßnahmen

Klassische Telekommunikationstechnik		**Spezifikation**
M-TK-1	Sperrung nicht benötigter oder sicherheitskritischer Leistungsmerkmale	Seite 42
M-TK-2	Schaffung eines zusätzlichen TK-Ersatzanschlusses für Notrufe	Seite 43
M-TK-3	Katastrophenschaltung	Seite 44
M-TK-4	Erhöhter Zutrittsschutz	Seite 44
M-TK-5	Geeignete Aufstellung der TK-Anlage	Seite 45
M-TK-6	Sichere Ablage von Kontaktinformationen	Seite 45
M-TK-7	Sicherer Umgang mit Daten zur Anlagennutzung	Seite 45
M-TK-8	Absicherung eines LAN-Anschlusses der ISDN-basierten TK-Anlage	Seite 46
M-TK-9	Absicherung der Kommunikation über ein IAD	Seite 46
M-TK-10	Sperrung bestimmter Fax-Rufnummern	Seite 48
M-TK-11	Gesicherte Aufstellung der Faxlösung	Seite 48
M-TK-12	Verhinderung der Faxfunktionsnutzung bei ungeschützten Multifunktionsgeräten	Seite 49
M-TK-13	Sichere Nutzung von Faxgeräten und Multifunktionsgeräten mit Faxfunktion	Seite 49
M-TK-14	Sichere Aufbewahrung eingegangener Faxnachrichten	Seite 50
M-TK-15	Sicherung von Telefonie-Endgeräten in frei zugänglichen Räumen	Seite 50
M-TK-16	Einsatz sicherheitsintelligenter Endgeräte	Seite 51
M-TK-17	Aktivierung einer Warnung bei Nutzung unsicherer Merkmale	Seite 51
M-TK-18	Sicherer Umgang mit Schnittstellen am Telefonie-Endgerät	Seite 51
M-TK-19	Geschützte Übertragung von Sprachdaten	Seite 51
M-TK-20	Verzicht auf Einsatz von Wartungsapparaten	Seite 54
M-TK-21	Sperrung der Wartungsmöglichkeit per Wartungsapparat an der Anlage	Seite 54
M-TK-22	Gesicherte Übertragung der Sprachdaten zwischen Partnerstandorten durch Leitungsverschlüsselung	Seite 54
M-TK-23	Restriktive Einbindung externer Wartung	Seite 55
M-TK-24	Sichere Aufstellung von Administrationsendgeräten	Seite 56
M-TK-25	Sichere Konfiguration von Administrationsendgeräten	Seite 56
M-TK-26	Regelungen für sichere TK-Administration	Seite 57
M-TK-27	Sichere Konfiguration des Management-Zugangs zur TK-Anlage	Seite 57
M-TK-28	Protokollierung und regelmäßige Kontrolle von Fernwartungszugriffen	Seite 58
M-TK-29	Verfügbarkeitssicherung durch (automatisierte) Zustandsüberwachung	Seite 58
M-TK-30	Abschluss eines Support-Vertrags inklusive externer Beratungskompetenz	Seite 58

Tabelle 10: Maßnahmen für Klassische Telekommunikationstechnik

Voice over IP		**Spezifikation**
M-TK-31	Durchgängige Verschlüsselung des Medienstroms	Seite 88
M-TK-32	Durchgängige Verschlüsselung der Signalisierung	Seite 89
M-TK-33	Absicherung von VoIP bei der Verwendung von Thin Clients	Seite 90
M-TK-34	Authentisierung zwischen Endgeräten und Servern des VoIP-Systems	Seite 90
M-TK-35	Authentisierung zwischen Servern	Seite 90
M-TK-36	Redundanz der Telefonie-Server	Seite 90
M-TK-37	Redundanz der Server und Gateways, von denen die Funktion des Telefonie-Servers und des Telefonie-Dienstes unmittelbar abhängt	Seite 90
M-TK-38	Schaffung eines zusätzlichen PSTN-Ersatzanschlusses für Notrufe	Seite 90

Voice over IP		**Spezifikation**
M-TK-39	Automatische PSTN-Umschaltung für kleinere Außenstellen	Seite 91
M-TK-40	Absicherung von Telefonie-Daten im Verzeichnisdienst	Seite 91
M-TK-41	Verfügbarkeit kritischer Telefonie-Daten	Seite 91
M-TK-42	Einschränkungen von DNS für VoIP	Seite 91
M-TK-43	Einschränkung von ENUM	Seite 92
M-TK-44	Redundante Internetanbindung für den IP-Anlagenanschluss	Seite 92
M-TK-45	Zusätzlicher IP-Anlagenanschluss	Seite 92
M-TK-46	Zusätzlicher PSTN-Anschluss	Seite 92
M-TK-47	Verwendung eines Session Border Controller zur Absicherung eines IP-Anlagenanschlusses	Seite 92
M-TK-48	Sicherung von IP-Telefonen in unübersichtlichen Umgebungen	Seite 94
M-TK-49	Warnung bei unsicheren Einstellungen	Seite 94
M-TK-50	Prozess zur Behandlung des Verlusts eines VoIP-Endgerätes	Seite 94
M-TK-51	Absicherung der Firmware	Seite 94
M-TK-52	Absicherung von Konfigurationsdateien	Seite 94
M-TK-53	Sicherheit von Softphones	Seite 95
M-TK-54	Sichere Konfiguration von Ethernet-Ports für den PC-Anschluss an IP-Telefonen	Seite 95
M-TK-55	Sichere Konfiguration von IP und von IP-basierten Diensten	Seite 96
M-TK-56	Einschränkung des lokalen Zugriffs auf die Konfiguration des IP-Telefons	Seite 96
M-TK-57	Benutzerabhängige Berechtigungen	Seite 96
M-TK-58	Schutz von teilnehmerspezifischen Daten auf einem IP-Telefon	Seite 97
M-TK-59	Einschränkung von Internettelefonie auf dedizierte, gehärtete Endgeräte	Seite 97
M-TK-60	Sichere Konfiguration der Netzwerk-Komponenten	Seite 98
M-TK-61	Sicheres Routing	Seite 98
M-TK-62	Absicherung von Switch-Ports	Seite 98
M-TK-63	Quality of Service im Netzwerk	Seite 99
M-TK-64	Zugangskontrolle zum Netzwerk	Seite 99
M-TK-65	MAC Security im Anschlussbereich für Endgeräte	Seite 99
M-TK-66	VPN zur Kommunikation über eingeschränkt vertrauenswürdige Netze	Seite 100
M-TK-67	Netztrennung für VoIP	Seite 100
M-TK-68	Netztrennung zwischen IP-PBX und Session Border Controller	Seite 104
M-TK-69	Erkennung und Abwehr von DoS-Angriffen gegen VoIP und von SPIT durch IPS / IDS	Seite 105
M-TK-70	Angemessene Verfügbarkeit des LAN für die Verwendung von VoIP	Seite 106
M-TK-71	Angemessene Verfügbarkeit der vom VoIP-System genutzten Netzdienste	Seite 106
M-TK-72	Angemessene Verfügbarkeit der Stromversorgung für IP-Telefone	Seite 106
M-TK-73	Sichere Administration des Telefonie-Servers	Seite 107
M-TK-74	Sichere Administration von PSTN-Gateways	Seite 107
M-TK-75	Sichere Administration von Anwendungs- und Management-Servern	Seite 108
M-TK-76	Sichere Administration von Abrechnungs- und Gebührenerfassungssystemen	Seite 108
M-TK-77	Sichere Verwaltung von Teilnehmerprofilen	Seite 108
M-TK-78	Sichere Administration von Endgeräten	Seite 108
M-TK-79	Sichere Administration von Netzkomponenten	Seite 109
M-TK-80	Überwachung der Komponenten des VoIP-Systems	Seite 109
M-TK-81	Datensicherung für die Elemente des VoIP-Systems	Seite 109
M-TK-82	VoIP-Tauglichkeit der IP-Infrastruktur für einen IP-Anlagenanschluss	Seite 109

Voice over IP		**Spezifikation**
M-TK-83	Überwachung der VoIP-Anbindung zum ITSP	Seite 110
M-TK-84	Sichere Administration des Session Border Controller	Seite 110
M-TK-85	Notfallvorsorge für das VoIP-System	Seite 111
M-TK-86	Harmonisierung zwischen IT-Betrieb und VoIP-Anlagen-Betrieb	Seite 112

Tabelle 11: Maßnahmen für VoIP

Hybrid-Anlagen
- -

Tabelle 12: Maßnahmen für Hybrid-Anlagen

Unified Communications and Collaboration		**Spezifikation**
M-TK-87	Absicherung der E-Mail-Kommunikation eines UCC-Systems	Seite 149
M-TK-88	Absicherung des Sprachkanals zwischen TK-Anlage bzw. VoIP-Kommunikationssystem und UCC-Systemen	Seite 150
M-TK-89	Absicherung von CTI-Verbindungen und Schnittstellen zur Anwendungsintegration	Seite 151
M-TK-90	Absicherung der Kommunikation zwischen UCC-System und weiteren IT-Systemen	Seite 151
M-TK-91	Absicherung der Kommunikation zwischen UCC-System und Datenbank	Seite 152
M-TK-92	Schutz vor unberechtigtem Zugriff auf Datenbanksysteme	Seite 152
M-TK-93	Absicherung der Kommunikation eines Präsenzsystems	Seite 152
M-TK-94	Vermeidung der Speicherung von Präsenzinformationen	Seite 153
M-TK-95	Einschränkung der Sichtbarkeit von Präsenzinformationen	Seite 153
M-TK-96	Differenzierung der Sichtbarkeit von Präsenzinformationen	Seite 154
M-TK-97	Verhindern der Verbreitung von Malware und bösartigen Hyperlinks per Instant Messaging	Seite 154
M-TK-98	Vermeidung von Spam over Instant Messaging	Seite 154
M-TK-99	Verhinderung des Datenabflusses durch Data Loss Prevention	Seite 155
M-TK-100	Sicherung von Konferenzräumen	Seite 156
M-TK-101	Sicherer Umgang mit Gesprächs- und Konferenzaufzeichnungen	Seite 157
M-TK-102	Absicherung des telefonischen Zugriffs auf UCC-Anwendungen durch eine PIN	Seite 158
M-TK-103	Einschränkung der Zugriffsrechte	Seite 158
M-TK-104	Einschränkung von Weiterleitungszielen und gleichzeitiger Rufsignalisierung	Seite 159
M-TK-105	Deaktivierung der CTI-Funktion für Konferenztelefone	Seite 159
M-TK-106	Absicherung von UCC-Systemen auf Ebene der Endgeräte	Seite 159
M-TK-107	Möglichkeit zur individuellen Einstellung des Präsenzstatus bei Endgeräten	Seite 160
M-TK-108	Ständiges Einblenden der Teilnehmerliste auf den Endgeräten	Seite 160
M-TK-109	Verwenden von Kameras mit geeigneter Brennweite	Seite 160
M-TK-110	Signalisierung der Kameraaktivität und Verwendung von Kameraabdeckungen	Seite 160
M-TK-111	Richtliniengesteuerte Aktivierung/Deaktivierung von Kamera und Mikrofon	Seite 160
M-TK-112	Geeignete Standortwahl und Umgebungsgestaltung bei Einsatz von Desktop-Video	Seite 161
M-TK-113	Netztrennung zwischen UCC-Systemen und weiteren IT-Systemen	Seite 161
M-TK-114	Sichere Administration der Server für UCC-Systeme	Seite 163
M-TK-115	Absicherung der Management-Schnittstellen eines UCC-Systems	Seite 163
M-TK-116	Koordination der Planung und Administration von UCC-Diensten	Seite 163

Tabelle 13: Maßnahmen für Unified Communications and Collaboration

Spezielle TK-Systeme		Spezifikation
Videokonferenz		
M-TK-117	Absicherung der zentralen Komponenten des Videokonferenzsystems	Seite 176
M-TK-118	Durchgängige Verschlüsselung eines mit IP übertragenen Video-Medienstroms	Seite 176
M-TK-119	Durchgängige Verschlüsselung einer IP-basierten Video-Signalisierung	Seite 177
M-TK-120	Authentisierung zwischen Video-Terminals und zentralen Video-Systemen	Seite 177
M-TK-121	Sicheres Ressourcenmanagement für Videokonferenzen	Seite 177
M-TK-122	Einschränkung des lokalen Zugriffs auf die Konfiguration des Video-Terminals	Seite 177
M-TK-123	Automatische Annahme eines Video-Anrufs deaktivieren	Seite 178
M-TK-124	Deaktivierung / Ausschaltung des Video-Terminals	Seite 178
M-TK-125	Anzeige der aktuellen Teilnehmer und Benachrichtigung bei neu eintretenden Teilnehmern einer Videokonferenz	Seite 178
Kontaktcenter		
M-TK-126	Authentisierung am IVR-System	Seite 190
M-TK-127	Qualitätssicherung der Routing-Regeln	Seite 191
M-TK-128	Data Loss Prevention am Agentenarbeitsplatz	Seite 191
M-TK-129	Authentisierung des Zugriffs auf Kontaktcenter-Anwendungen	Seite 191
M-TK-130	Verhinderung des automatisierten Zugriffs auf Internet-Kontaktformulare	Seite 191
M-TK-131	Beschränkung des Netzzugriffs auf dedizierte Räumlichkeiten im Kontaktcenter	Seite 192
M-TK-132	Hochverfügbare Auslegung der Netzkomponenten und Systeme im Kontaktcenter	Seite 192
M-TK-133	Absicherung der Übergänge in öffentliche Netze	Seite 192
M-TK-134	Absicherung der Management-Schnittstellen	Seite 193
M-TK-135	Schulung von Kontaktcenter-Administratoren und Schichtleitern/Supervisoren	Seite 194
M-TK-136	Zutrittsbeschränkung für Kontaktcenter-Räumlichkeiten	Seite 194
Händlersysteme		
M-TK-137	Verwendung dedizierter Händlersysteme	Seite 200
M-TK-138	Festlegung dedizierter Gesprächskreise	Seite 200
M-TK-139	Vermeidung von Fehlbedienung durch intuitive Bedienkonzepte	Seite 201
Alarmierungssysteme		
M-TK-140	Schaffung geeigneter Umgebungsbedingungen für zentrale Elemente eines Alarmierungssystems	Seite 214
M-TK-141	Sichere Konfiguration zentraler Elemente einer Alarmierungslösung	Seite 215
M-TK-142	Absicherung der Anbindung von Alarmierungssystemen an TK-Infrastrukturen	Seite 216
M-TK-143	Verstärkte Absicherung der von Alarmierungssystemen mitgenutzten TK-Installationen	Seite 217
M-TK-144	Ausstattung und Anbringung der Endpunkte unter Berücksichtigung von Sicherheitsaspekten	Seite 217
M-TK-145	Verbindliche Regelungen für den Umgang mit Endpunkten zu Alarmierungssystemen	Seite 218
M-TK-146	Absicherung der Kommunikation zwischen Elementen eines Alarmierungssystems	Seite 218
M-TK-147	Automatisierte Überwachung der Komponenten von Alarmierungssystemen	Seite 219
M-TK-148	Erhöhte Frequenz gezielter Sicht- und Zustandsprüfungen	Seite 219
M-TK-149	Schulung der Administratoren bzw. des Betriebspersonals von Alarmierungssystemen	Seite 219
M-TK-150	Bedarfsgerechte Notfallplanung und -vorsorge für Kopplung von Alarmierungssystemen und TK-Lösungen	Seite 220
M-TK-151	Erarbeitung sicherheitsrelevanter Regelungen für den Einsatz von Alarmierungssystemen	Seite 220

Spezielle TK-Systeme		Spezifikation
M-TK-152	Erstellung einer Konzeption zur integrierten Nutzung von Alarmierungssystem und TK-Lösungen	Seite 222
M-TK-153	Produktauswahl von Alarmierungssystemlösungen unter Sicherheitsgesichtspunkten	Seite 222
M-TK-154	Einweisung, Schulung und Sensibilisierung der Nutzer von Alarmierungssystemen	Seite 222

Tabelle 14: Maßnahmen für Spezielle TK-Systeme

Provider-basierte TK-Dienste		Spezifikation
Soziale Netzwerke und Soziale Medien		
M-TK-155	Berechtigungskonzept zur Steuerung der Freigabe des Präsenzstatus	Seite 241
M-TK-156	Berechtigungskonzept und technische Umsetzung für externe Kommunikation mit Sozialen Netzwerken und Medien	Seite 241
M-TK-157	Kanalisierung des Zugriffs auf dienstliche Accounts in Sozialen Netzwerken und Medien über Portallösung	Seite 241
M-TK-158	Dokumentation der Zugriffe und Aktivitäten bei Nutzung von Sozialen Netzwerken und Medien	Seite 242
M-TK-159	Vermeiden der bidirektionalen Kontaktsynchronisation mit Sozialen Netzwerken und Medien	Seite 242
M-TK-160	Host-basiertes Data Loss Prevention (DLP) bei Nutzung von Sozialen Netzwerken und Medien	Seite 243
M-TK-161	Netzwerk-basiertes Data Loss Prevention (DLP) bei Nutzung Sozialer Netzwerke und Medien	Seite 243
M-TK-162	Verhinderung oder Einschränkung der Nutzung von Sozialen Netzwerken und Medien am Netzübergang	Seite 243
M-TK-163	Netztechnische Isolation von Clients und Infrastrukturteilen mit Zugriff auf Soziale Netzwerke und Medien	Seite 244
M-TK-164	Sichere Administration der Server-Systeme und Gateways zur Anbindung an Soziale Netzwerke und Medien	Seite 244
M-TK-165	Schulung der Administratoren für den Zugang zu Sozialen Netzwerken und Medien	Seite 245
M-TK-166	Klärung und rechtsverbindliche Regelung juristischer Aspekte zur Nutzung Sozialer Netzwerke und Medien im dienstlichen Kontext	Seite 245
M-TK-167	Geeignete Einbindung der Nutzung von Sozialen Netzwerken und Medien in etablierte Prozesse	Seite 246
M-TK-168	Transparente und durchsetzbare Regelungen zur Nutzung Sozialer Netzwerke und Medien im dienstlichen Kontext	Seite 247
M-TK-169	Gezielte Trennung von dienstlichem und privatem Gebrauch von Sozialen Netzwerken und Medien	Seite 248
M-TK-170	Einschränkung oder Verbot der Privatnutzung von Sozialen Netzwerken und Medien am Arbeitsplatz	Seite 249
M-TK-171	Verbot der ungeschützten Übertragung vertraulicher Inhalte über Soziale Netzwerke und Medien	Seite 249
M-TK-172	Information und Schulung der Anwender bzgl. sicherer Nutzung von Sozialen Netzwerken und Medien	Seite 249
M-TK-173	Benennung von Ansprechpartnern	Seite 249
Outsourcing, IP-Centrex, Cloud Computing und UC as a Service		
M-TK-174	Konsequente Verschlüsselung bei Transport, Speicherung und Verarbeitung von Daten	Seite 260
M-TK-175	Härtung der Virtualisierungsplattform	Seite 261
M-TK-176	Einsatz von UC-fähigem Virenschutz	Seite 261

Provider-basierte TK-Dienste		Spezifikation
M-TK-177	Einsatz von Host-basierten DLP-Systemen bei Cloud-Nutzung	Seite 261
M-TK-178	Einsatz von Netzwerk-basierten DLP-Systemen bei Cloud-Nutzung	Seite 261
M-TK-179	Dem Schutzbedarf angepasste Überwachung der Dienste	Seite 261
M-TK-180	Regelmäßige Erstellung von Berichten und Informationspflicht bei Sicherheitsvorfällen	Seite 262
M-TK-181	Nachweis und Überprüfung der Vertrauenswürdigkeit des Dienstleisters	Seite 262
M-TK-182	Einsatz von sicherheitsüberprüftem Personal	Seite 262
M-TK-183	Regelmäßige Auditierung der Infrastruktur des Dienstleisters	Seite 262
M-TK-184	Festlegung des Speicherortes der Daten bei Outsourcing und Cloud-Nutzung	Seite 262
M-TK-185	Lesender Zugriff auf die vom Dienstleister bereitgestellten Komponenten	Seite 262

Tabelle 15: Maßnahmen für Provider-basierte TK-Dienste

Einbindung Mobiler Endgeräte		Spezifikation
Mobilfunk und Fixed Mobile Convergence		
M-TK-186	Gegenseitige Authentisierung von mobilen Endgeräten und einer zentralen Komponente der FMC- bzw. UCC-Lösung	Seite 294
M-TK-187	Schutz von Servern für mobile Endgeräte	Seite 294
M-TK-188	Verwendung einer Ende-zu-Ende-Verschlüsselung für die Telekommunikation	Seite 294
M-TK-189	Verschlüsselung von Nachrichten	Seite 295
M-TK-190	Einsatz von Server-based Computing	Seite 295
M-TK-194	Einsatz von abhörsicheren Mobiltelefonen	Seite 296
M-TK-195	Absicherung aller Kommunikationsschnittstellen des Endgerätes	Seite 296
M-TK-196	Schutz der organisationsinternen Daten auf einem mobilen Endgerät	Seite 297
M-TK-197	Erweiterung von Data Loss Prevention auf mobile Endgeräte	Seite 297
M-TK-198	Sperrung des mobilen Endgerätes für Nutzereingaben	Seite 297
M-TK-199	Benutzerauthentisierung am mobilen Endgerät	Seite 297
M-TK-200	Automatische Handlungen bei Verletzung von Sicherheitsrichtlinien auf mobilen Endgeräten	Seite 298
M-TK-201	Rollenbasierte Zugriffsberechtigungen auf Objekte des mobilen Endgerätes	Seite 298
M-TK-202	Schutz des mobilen Endgerätes vor schadenstiftender Software	Seite 298
M-TK-203	Deaktivierung der automatischen Rufannahme	Seite 299
M-TK-204	Schutz vor unerwünschter Konfigurationsänderung über die GSM/UMTS-Funkschnittstelle	Seite 299
M-TK-205	Schutzmaßnahmen für das Herunterladen von Inhalten	Seite 299
M-TK-206	Prozess zur Behandlung des Verlusts eines mobilen Endgerätes	Seite 299
M-TK-211	Berücksichtigung der Sicherheit bei der Vertragsgestaltung mit einem Dienstanbieter	Seite 301
M-TK-217	Fernadministration der mobilen Endgeräte durch ein Mobile Device Management	Seite 302
M-TK-218	Regelmäßige, möglichst automatische Sicherung von Daten und Konfiguration mobiler Endgeräte	Seite 302
M-TK-219	Einschränkung der Apps	Seite 304
M-TK-220	Überwachung der Endgeräte hinsichtlich Anomalien	Seite 304
Wireless LAN		
M-TK-191	Verschlüsselung, Integritätsschutz und Authentisierung auf der Luftschnittstelle	Seite 295
M-TK-192	Ende-zu-Ende-Verschlüsselung für Medienströme	Seite 295
M-TK-193	Absicherung Authentication-Server	Seite 296

Einbindung Mobiler Endgeräte		**Spezifikation**
M-TK-212	Trennung von LAN- und WLAN-Verkehr im kabelbasierten Netz	Seite 302
M-TK-213	Absicherung des LAN-Zugangs für Access Points	Seite 302
M-TK-214	Berücksichtigung der Anforderungen einer Sprachübertragung bei der Planung der Funkzellen	Seite 302
M-TK-221	Kontinuierliche Überwachung der Luftschnittstelle	Seite 305
M-TK-222	Kontinuierliche Überwachung der WLAN-Infrastruktur	Seite 306
M-TK-223	Fernadministration der WLAN-Endgeräte	Seite 306
DECT		
M-TK-207	Einsatz von DECT-Endgeräten mit verbesserter DECT-konformer Verschlüsselung	Seite 299
M-TK-208	Einsatz von DECT-Endgeräten mit zusätzlicher Verschlüsselung	Seite 300
M-TK-215	Absicherung bei Anschluss von Radio Fixed Parts an ein LAN	Seite 303
M-TK-224	Protokollierung des Einsatzes zusätzlicher Verschlüsselung	Seite 306
M-TK-225	Verzicht auf den Einsatz von DECT bei erhöhtem Schutzbedarf	Seite 306
Bluetooth		
M-TK-209	Sichere Konfiguration und Verwendung des Bluetooth-Adapters	Seite 300
M-TK-210	Einsatz von Bluetooth-Endgeräten mit zusätzlicher Verschlüsselung	Seite 301
M-TK-216	Absicherung von Bluetooth Access Points bei Anschluss an ein LAN	Seite 303
M-TK-226	Verzicht auf den Einsatz von Bluetooth bei erhöhtem Schutzbedarf	Seite 306

Tabelle 16: Maßnahmen für die Einbindung Mobiler Endgeräte

Generell zu ergreifende Sicherheitsmaßnahmen		Spezifikation
M-TK-227	Sichere Kabelführung	Seite 310
M-TK-228	Produktauswahl von TK-Lösungen unter Berücksichtigung von Sicherheitsaspekten	Seite 311
M-TK-229	Härtung von Servern des Telekommunikationssystems	Seite 312
M-TK-230	Spezielle Absicherung von virtualisierten TK-Servern	Seite 312
M-TK-231	Einschränkung und Kontrolle von Berechtigungen für die Administration eines Servers des Telekommunikationssystems	Seite 313
M-TK-232	Einschränkung und Kontrolle des Zugangs zu einem Server des Telekommunikationssystems	Seite 313
M-TK-233	Physische Sicherheit der Server der Telekommunikationslösung	Seite 314
M-TK-234	Berücksichtigung der Server der TK-Lösung im Datensicherungskonzept der Organisation	Seite 314
M-TK-235	Schutz vor schadenstiftender Software für die Server der TK-Lösung	Seite 315
M-TK-236	Einbindung der Server der TK-Lösung in das Patch-Management der Organisation	Seite 315
M-TK-237	Sichere Konfiguration des Netzwerk-Management-Protokolls	Seite 316
M-TK-238	Überwachung der Komponenten des Telekommunikationssystems	Seite 316
M-TK-239	Erweiterung von Penetrationstests auf die verwendeten TK-Technologien	Seite 317
M-TK-240	Ergänzung der Überwachung um Honeypots für die verwendeten TK-Technologien	Seite 317
M-TK-241	Erweiterung des Verwundbarkeits-Managements für die verwendeten TK-Technologien	Seite 317
M-TK-242	Schutz von Verbindungsdaten	Seite 317
M-TK-243	Nutzung von speziell abgesicherten Räumlichkeiten	Seite 318
M-TK-244	Sichere Außerbetriebnahme von Komponenten des Telekommunikationssystems	Seite 318
M-TK-245	Nachweis der Vertrauenswürdigkeit des Dienstanbieters	Seite 318
M-TK-246	Notfallvorsorge für alle Teilsysteme der TK-Lösung	Seite 319
M-TK-247	Sensibilisierung der Anwender von TK-Diensten hinsichtlich Sicherheitsaspekten	Seite 322
M-TK-248	Schulung der Anwender von TK-Diensten zu Sicherheits- und Datenschutzaspekten	Seite 322
M-TK-249	Schulung der Administratoren von TK-Lösungen	Seite 322

Tabelle 17: Generell zu ergreifende Sicherheitsmaßnahmen

11.2 Referenziert aus den BSI IT-Grundschutz-Katalogen

11.2.1 Bausteine

Nr.	Titel
B 1.2	„Personal“
B 1.3	„Notfallmanagement“
B 1.4	„Datensicherungskonzept“
B 1.5	„Datenschutz“
B 1.6	„Schutz vor Schadprogrammen“
B 1.11	„Outsourcing“
B 1.14	„Patch- und Änderungsmanagement“
B 2.4	„Serverraum“
B 2.6	„Raum für technische Infrastruktur“
B 2.7	„Schutzschränke“
B 2.9	„Rechenzentrum“
B 2.11	„Besprechungs-, Veranstaltungs- und Schulungsräume“
B 2.12	„IT-Verkabelung“
B 3.101	„Allgemeiner Server“
...	...
B 3.109	„Windows Server 2008“
B 3.301	„Sicherheits-Gateway (Firewall)“
B 3.302	„Router und Switches“
B 3.304	„Virtualisierung“
B 3.401	„TK-Anlage“
B 3.404	„Mobiltelefon“
B 3.405	„PDA“
B 4.2	„Netz- und Systemmanagement“
B 4.6	„WLAN“
B 4.7	„VoIP“
B 4.8	„Bluetooth“
B 5.19	„Internet-Nutzung
B 5.21	„Webanwendungen“

Tabelle 18: Referenzierte Bausteine

11.2.2 Gefährdungen

Nr.	Titel
G 2	„Organisatorische Mängel“ (Gefährdungskatalog)
G 3	„Menschliche Fehlhandlungen“ (Gefährdungskatalog)
G 5	„Vorsätzliche Handlungen“ (Gefährdungskatalog)
G 1.17	„Ausfall oder Störung eines Funknetzes“
G 2.1	„Fehlende oder unzureichende Regelungen“
G 2.2	„Unzureichende Kenntnis über Regelungen“
G 2.4	„Unzureichende Kontrolle der Sicherheitsmaßnahmen“
G 2.6	„Unbefugter Zutritt zu schutzbedürftigen Räumen“
G 2.7	„Unerlaubte Ausübung von Rechten“
G 2.28	„Verstöße gegen das Urheberrecht“
G 2.54	„Vertraulichkeitsverlust durch Restinformationen“
G 2.61	„Unberechtigte Sammlung personenbezogener Daten“
G 2.66	„Unzureichendes Sicherheitsmanagement“
G 2.84	„Unzulängliche vertragliche Regelungen mit einem externen Dienstleister“
G 2.87	„Verwendung unsicherer Protokolle in öffentlichen Netzen“
G 2.96	„Veraltete oder falsche Informationen in einem Webangebot“
G 2.103	„Unzureichende Schulung der Mitarbeiter“
G 2.105	„Verstoß gegen gesetzliche Regelungen und vertragliche Vereinbarungen“
G 2.117	„ Fehlende oder unzureichende Planung des WLAN-Einsatzes“
G 2.162	„Fehlende Zulässigkeit der Verarbeitung personenbezogener Daten“
G 2.163	„Nichteinhaltung der Zweckbindung bei der Verarbeitung personenbezogener Daten“
G 2.164	„Überschreitung des Erforderlichkeitsgrundsatzes bei der Verarbeitung personenbezogener Daten“
G 2.165	„Fehlende oder unzureichende Datenvermeidung und Datensparsamkeit bei der Verarbeitung personenbezogener Daten“
G 2.166	„Verletzung des Datengeheimnisses bei der Verarbeitung personenbezogener Daten“
G 2.167	„Fehlende oder nicht ausreichende Vorabkontrolle“
G 2.168	„Gefährdung der Rechte Betroffener bei der Verarbeitung personenbezogener Daten“
G 2.169	„Fehlende oder unzureichende Absicherung der Datenverarbeitung im Auftrag bei der Verarbeitung personenbezogener Daten“
G 2.170	„Fehlende Transparenz für den Betroffenen und die Datenschutz-Kontrollinstanzen“
G 2.171	„Gefährdung vorgegebener Kontrollziele bei der Verarbeitung personenbezogener Daten“
G 2.172	„Fehlende oder unzureichende Absicherung der Verarbeitung personenbezogener Daten im Ausland“
G 2.173	„Unzulässige automatisierten Einzelfallentscheidungen oder Abrufe bei der Verarbeitung personenbezogener Daten“
G 2.174	„Fehlende oder unzureichende Datenschutzkontrolle“
G 3.3	„Nichtbeachtung von Sicherheitsmaßnahmen“
G 3.7	„Ausfall der TK-Anlage durch Fehlbedienung“
G 3.13	„Weitergabe falscher oder interner Informationen“
G 3.16	„Fehlerhafte Administration von Zugangs- und Zugriffsrechten“
G 3.37	„Unproduktive Suchzeiten“
G 3.38	„Konfigurations- und Bedienungsfehler“
G 3.43	„Ungeeigneter Umgang mit Passwörtern“

Nr.	Titel
G 3.44	„Sorglosigkeit im Umgang mit Informationen“
G 3.45	„Unzureichende Identifikationsprüfung von Kommunikationspartnern“
G 3.105	„Ungenehmigte Nutzung von externen Dienstleistungen“
G 3.107	„Rufschädigung“
G 4.52	„Datenverlust bei mobilem Einsatz“
G 4.56	„Ausfall der VoIP-Architektur“
G 4.57	„Störungen beim Einsatz von VoIP über VPNs“
G 4.58	„Schwachstellen beim Einsatz von VoIP-Endgeräten“
G 4.59	„Nicht-Erreichbarkeit von VoIP durch NAT“
G 5.2	„Manipulation an Informationen oder Software“
G 5.7	„Abhören von Leitungen“
G 5.11	„Vertraulichkeitsverlust von in TK-Anlagen gespeicherten Daten“
G 5.12	„Abhören von Telefongesprächen und Datenübertragungen“
G 5.13	„Abhören von Räumen über TK-Endgeräte“
G 5.14	„Gebührenbetrug“
G 5.18	„Systematisches Ausprobieren von Passwörtern“
G 5.19	„Missbrauch von Benutzerrechten“
G 5.22	„Diebstahl bei mobiler Nutzung des IT-Systems“
G 5.25	„Maskerade“
G 5.30	„Unbefugte Nutzung eines Faxgerätes oder eines Fax-Servers“
G 5.31	„Unbefugtes Lesen von Faxsendungen“
G 5.32	„Auswertung von Restinformationen in Faxgeräten und Fax-Servern“
G 5.33	„Vortäuschen eines falschen Absenders bei Faxsendungen“
G 5.34	„Absichtliches Umprogrammieren der Zieltasten eines Faxgerätes“
G 5.35	„Überlastung durch Faxsendungen“
G 5.42	„Social Engineering“
G 5.64	„Manipulation an Daten oder Software bei Datenbanksystemen“
G 5.71	„Vertraulichkeitsverlust schützenswerter Informationen“
G 5.72	„Missbräuchliche Groupware-Nutzung“
G 5.73	„Vortäuschen eines falschen Absenders“
G 5.85	„Integritätsverlust schützenswerter Informationen“
G 5.90	„Manipulation von Adressbüchern und Verteillisten“
G 5.104	„Ausspähen von Informationen“
G 5.112	„Manipulation von ARP-Tabellen“
G 5.134	„Fehlende Identifizierung zwischen Gesprächsteilnehmern“
G 5.135	„SPIT und Vishing“
G 5.136	„Missbrauch frei zugänglicher Telefonanschlüsse“
G 5.143	„Man-in-the-Middle-Angriff“
G 5.157	„Phishing und Pharming“
G 5.158	„Missbrauch sozialer Netzwerke“
G 5.172	„Umgehung der Autorisierung bei Webanwendungen“

Tabelle 19: Referenzierte Gefährdungen

11.2.3 Maßnahmen

Nr.	Titel
M 2.11	„Regelungen des Passwortgebrauchs“
M 2.277	„Funktionsweise eines Switches“
M 2.374	„Umfang der Verschlüsselung von VoIP“
M 4.204	„Sichere Administration von Routern und Switches“
M 4.237	„Sichere Grundkonfiguration eines IT-Systems“
M 4.239	„Sicherer Betrieb eines Servers“
M 5.5	„Schadensmindernde Kabelführung“
M 5.56	„Sicherer Betrieb eines Mailservers“
M 5.57	„Sichere Konfiguration der Mail-Clients“
M 5.108	„Kryptographische Absicherung von E-Mail“
M 5.109	„Einsatz eines E-Mail-Scanners auf dem Mail-Server“
M 5.108	„Kryptographische Absicherung von Groupware bzw. E-Mail“
M 5.109	"Einsatz eines E-Mail-Scanners auf dem Mailserver"
M 5.116	"Integration eines E-Mail-Servers in ein Sicherheits-Gateway"
M 5.134	„Sichere Signalisierung bei VoIP“
M 5.135	„Sicherer Medientransport mit SRTP“
M 5.136	„Dienstgüte und Netzmanagement bei VoIP“
M 5.153	„Planung des Netzes für virtuelle Infrastrukturen“
M 5.155	„Datenschutz-Aspekte bei der Internet-Nutzung“
M 5.156	„Sichere Nutzung von Twitter“
M 5.157	„Sichere Nutzung von sozialen Netzwerken“
M 6.100	„Erstellung eines Notfallplans für den Ausfall von VoIP“
M 6.101	„Datensicherung bei VoIP“

Tabelle 20: Referenzierte Maßnahmen

12 Ausblick

Moderne Telekommunikationssysteme sind durch eine weitgehende Integration in die IT-Landschaft geprägt. Treibende Kräfte sind die Nutzung IP-basierter TK-Anwendungen und -Dienste sowie die Netzkonvergenz mit IP als anwendungs- und dienstübergreifendem Träger. Auf dieser Basis ermöglicht Unified Communications & Collaboration (UCC) als Plattform den einheitlichen Zugriff auf Telekommunikations-, Datenaustausch- und Informationsdienste. Dies hat schon heute zu einer hohen Dynamik in der Entwicklung neuer Anwendungen im Telekommunikationsbereich geführt, die künftig noch deutlich zunehmen wird. Die Nutzung von Videokonferenzen, Präsenzdiensten und Instant Messaging ist beispielsweise für diverse Organisationen schon heute ein selbstverständliches Element der Telekommunikation und entsprechend in Arbeitsmethoden und Geschäftsprozesse integriert. Dies zeigt sich speziell im Bereich der Kontaktcenter, welche die gesamte Palette von UCC bis hin zu Sozialen Netzwerken und Sozialen Medien nutzen.

Ausgehend von der in der Vergangenheit etablierten ISDN-basierten TK-Anlagentechnik bewegt sich die Evolution der Telekommunikation seit geraumer Zeit mit einem inzwischen rasantem Tempo in diese Richtung. Aus der Perspektive des Endnutzers gibt es für die Telekommunikation künftig keinen Unterschied mehr zwischen TK-Geräten („Telefonen“) und IT-Geräten („PCs“). Die Integration von TK und IT spiegelt sich auch im Netzwerk und den zentralen Komponenten wider, wie sich z. B. auch im Bereich von Alarmierungssystemen und Händlersystemen zeigt. Sprach- und Datennetze wachsen zusammen, sowohl in der Technik als auch auf Betriebsebene.

In dieser Entwicklung der Telekommunikation nimmt die mobile Kommunikation insbesondere über Mobilfunknetze und WLAN eine herausragende Rolle ein. Dabei wird der drahtgebundene Zugang zu TK-Diensten zwar nicht vollständig verdrängt werden, jedoch wird es zu einem massiven Bedeutungsverlust kommen. TK-Dienste und Anwendungen werden immer stärker eine Domäne mobiler Endgeräte. Dies wird auch durch die inzwischen hohe verfügbare Bandbreite ermöglicht, die bereits heute im WLAN und im Mobilfunk in naher Zukunft im Gigabit-Bereich liegt. Smartphones und Tablets haben zusammen mit UCC die Sicht auf die Telekommunikation in der IT fundamental geändert. Jederzeit an jedem Ort auf jede benötigte Information zugreifen zu können hat ein Potenzial, dessen Grenze längst noch nicht erreicht ist. Dies wird verstärkt durch die Ergänzung um ein ortsspezifisches Dienstangebot bis hin zur Integration von Augmented Reality (erweiterte Sicht auf die Realität) in Anwendungen. Dieses Potenzial ist jedoch mit erheblichen Sicherheitsproblemen verbunden.

Erschwerend kommt gerade bei Smartphones und Tablets vermehrt die Freigabe der privaten Nutzung bis hin zur dienstlichen Nutzung privater Endgeräte (Bring Your Own Device, BYOD) hinzu. Eine Trennung privater und dienstlicher Nutzung (mobiler) Endgeräte ist immer weniger zeitgemäß (und in der Praxis immer weniger erzwingbar). Sicherheitsmaßnahmen werden also auch weiterhin organisatorische Regelungen, den Einsatz von Mobile Device Management (MDM) sowie Virtualisierungs- und Containertechniken zur Trennung dienstlicher und privater Daten umfassen.

Die Absicherung der modernen Telekommunikation muss daher insgesamt ganzheitlich system- und anwendungsübergreifend erfolgen. Eine Konzentration beispielsweise auf Sicherheitsmaßnahmen auf Ebene des Netzwerks (z. B. Einsatz von Firewalls) und auf die Härtung der beteiligten IT-Systeme reicht nicht aus. Ein umfassender Schutz erfordert Kontrolle und Schutz auf Ebene der Datenflüsse, insbesondere Medienstrom und Signalisierung, und der beteiligten Anwendungen. Da moderne TK-Anwendungen hoch komplexe Systeme sind, ist Informationssicherheit daher als zentraler Bestandteil der Architektur der TK-Anlagen und der TK-Anwendungen zu sehen. Hier sind sowohl Entwickler als auch Integratoren und Betreiber einer TK-Landschaft gleichermaßen in der Pflicht.

Eine effektive Informationssicherheit ist dabei grundsätzlich in der eigenen Infrastruktur möglich, denn hier kann eine umfassende Kontrolle realisiert werden. Outsourcing bedeutet dagegen Kontrollverlust verbunden mit entsprechenden Sicherheitsrisiken. Dies gilt speziell auch für Cloud Computing. Dabei muss natürlich zwischen Private Cloud und Public Cloud unterschieden werden, da in der Private Cloud die Dienste und Anwendungen über die eigene Infrastruktur („On Premises“) angeboten werden.

Spätestens bei der Hybrid Cloud und insbesondere bei der Virtual Private Cloud verwischen die Grenzen jedoch wieder und die Sicherheitskonzepte müssen dies sehr genau berücksichtigen.

Da immer mehr TK-Anwendungen in den Bereichen VoIP, UCC und mobile Endgeräte über die Public Cloud angeboten werden, ist es immer schwerer, sich auf die eigene IT-Infrastruktur zurückzuziehen und manchmal unmöglich, wie z. B. die App-Store-Konzepte der Hersteller zeigen. Es fehlen jedoch Best-Practice-Ansätze und insbesondere international anerkannte Standards zur Absicherung der Nutzung der Public Cloud und zur Absicherung der Public Cloud selbst. Außerdem stecken wichtige Techniken, die eine sichere Verarbeitung der Daten in der Public Cloud erlauben, z. B. homomorphe Verschlüsselung, noch in den Kinderschuhen. Forschung, Entwicklung und Standardisierung haben hier vermutlich noch einen weiten Weg vor sich.

Als Endpunkt der Telekommunikation war und ist der Mensch ein besonders schwer in den Griff zu bekommendes Element in der Informationssicherheit. Nun hat er in dieser Rolle Gesellschaft bekommen: die autonom agierende und kommunizierende Maschine. Schon jetzt ist spürbar, dass das Internet of Things eine immer größere Rolle einnehmen wird. Wir werden uns daran gewöhnen müssen, das immer mehr Dinge in unserer Umgebung eine Internet-Anbindung haben und Telekommunikationsdienste nutzen. Besonders deutlich wird diese Entwicklung im Automobilbereich. Moderne Autos nutzen z. B. WLAN, Bluetooth sowie Mobilfunk und sind über das Internet mit dem Fahrer, dem Hersteller und der sonstigen Umgebung vernetzt. Das autonom fahrende Auto ist kein Science Fiction mehr. Im Internet of Things sind Sicherheitsvorfälle mit ungeahntem Ausmaß vorstellbar. Die Informationssicherheit muss hier von Anfang an zentrales Element in der Gestaltung von Systemen im Internet of Things sein und dies beinhaltet insbesondere auch die Absicherung der Telekommunikation.

13 Anhang

In diesem Anhang werden die Grundlagen der verwendeten Technologien vertieft beschrieben:

- Die Grundlagen zu VoIP-Techniken werden in Kapitel 13.1 dargestellt.
- Ergänzende Ausführungen zu UCC und zur Anwendungsintegration finden sich in Kapitel 13.2.
- Eine Beschreibung der netzbasierten Sicherheitsmechanismen erfolgt in Kapitel 13.3.

13.1 Grundlagen zu VoIP-Techniken

13.1.1 Übertragung von Signalisierungsdaten

Zur Übertragung der Signalisierungsnachrichten werden unterschiedliche Protokolle eingesetzt. Zu nennen sind hier insbesondere die folgenden Protokolle, die an dieser Stelle kurz beschrieben werden:

- Session Initiation Protocol (SIP)
- H.323
- Media Gateway Control Protocol (Megaco)
- Inter-Asterisk eXchange (IAX)

Darüber hinaus wird das Verfahren Telephone Number Mapping (ENUM) beschrieben, das die Übersetzung von Telefonnummern in DNS-Namen (Domain Name System) und umgekehrt realisiert und über das die für die Signalisierung benötigten Informationen verwaltet werden können.

13.1.1.1 Session Initiation Protocol

Das Session Initiation Protocol (SIP) wurde von der Internet Engineering Task Force (IETF) entwickelt (siehe [IETF RFC3261-2002]) und lehnt sich an das Hypertext Transfer Protocol (HTTP) an, besitzt jedoch keinen unmittelbaren Anwendungsbezug hierzu. SIP wird verwendet, um die erforderlichen Informationen für den Aufbau und die Steuerung einer Sitzung (also etwa eines Telefongesprächs) auszutauschen. Die für eine Sprachübertragung nötigen Details wie unterstützte Sprach-Codecs werden mittels des Session Description Protocol (SDP) innerhalb der SIP-Protokolldateneinheit ausgehandelt.

In Abbildung 67 ist die grundsätzliche SIP-Architektur vereinfacht dargestellt. Wesentliche Elemente sind dabei zunächst der User Agent (UA) und der SIP-Proxy. Zur Teilnehmerlokalisierung wird der SIP-Proxy durch weitere SIP-Server unterstützt (SIP-Registrar-Server und SIP-Redirect-Server).

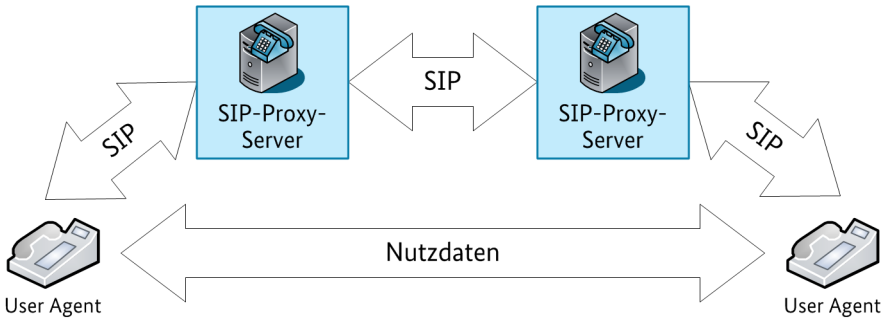


Abbildung 67: Vereinfachte SIP-Architektur

User Agents stellen die Endpunkte der SIP-Signalisierung dar. Ein User Agent ist zunächst der entsprechende Dienst im Endgerät, welcher die SIP-Funktionalität bietet. Gateways zu anderen Netzen wie ISDN haben ebenfalls einen UA implementiert. Üblicherweise wird ein User Agent, welcher eine Verbindung initiiert, User-Agent-Client (UAC) und das entsprechende Ziel User-Agent-Server (UAS) genannt.

Neben den User Agents beinhaltet eine SIP-Architektur in der Regel mindestens einen SIP-Proxy. Beim Aufbau einer Session schickt der anrufende User Agent die SIP-Signalisierungspakete an seinen SIP-Proxy. Die SIP-Anfrage wird dann an den SIP-Proxy des angerufenen User Agent weitergeleitet, welcher einen eingehenden Anruf signalisiert. Die Weiterleitung muss nicht direkt an den Proxy des User Agent gerichtet sein, sondern kann auch über mehrere Hops, d. h. zwischengeschaltete Proxies, erfolgen. Im Falle vieler Hops kann dadurch beim Verbindungsaufbau eine spürbare Verzögerung entstehen (auch SIP-Trapezoid genannt).

Um herauszufinden, an wen die Signalisierungsnachrichten für eine Sitzung weiterzuleiten sind, wendet sich ein SIP-Proxy an einen sogenannten SIP-Registrar-Server. SIP-Endgeräte müssen sich, um erreichbar zu sein, an einem SIP-Registrar-Server registrieren, der seinerseits die Informationen zur Registrierung an eine Datenbank (Location Service) weitergibt. Falls der angerufene Teilnehmer nicht am selben Registrar-Server wie der Anrufende angemeldet ist, muss der Aufenthaltsort erst bestimmt werden. Dies geschieht durch eine Anfrage an den zuständigen SIP-Proxy oder SIP-Redirect-Server, welche wiederum den Location Service nutzen, um den aktuellen Aufenthaltsorts des Teilnehmers zu ermitteln.

SIP-Proxy, SIP-Registrar-Server und SIP-Redirect-Server sind logische Funktionen, die auch auf einer gemeinsamen Hardware implementiert werden können.

Über die SIP-Nachrichten handeln die User Agents die Modalitäten für ihre Session aus. Dabei kommunizieren die User Agents meist nicht direkt, sondern über die SIP-Proxies. Der Austausch der eigentlichen Nutzdaten (z. B. die Sprachkommunikation oder der Medientransfer) erfolgt dann ohne zwischengeschaltete Proxies direkt zwischen den User Agents.

SIP ist nicht auf Sprachübertragung beschränkt, sondern kann auch für andere Dienste, z. B. für Videokonferenzen oder Instant Messaging, verwendet werden.

SIP kann sowohl das User Datagram Protocol (UDP) als auch das Transmission Control Protocol (TCP) für die Übertragung nutzen. Bei der Verwendung von UDP wird die Neuübertragung bei Paketverlust durch SIP geregelt.

13.1.1.2 H.323

H.323 wurde zunächst 1996 von der ITU-T verabschiedet und war das erste Signalisierungsprotokoll für VoIP. Eine aktualisierte Form ist seit 2006 verfügbar (siehe [ITU H.323-2009]). Es referenziert diverse Unterprotokolle, z. B. für die Rufsignalisierung (siehe [ITU H.225-2009]), für die Sicherheit (siehe [ITU H.235-2005]), für das Öffnen und Schließen von Kanälen zur Medienübertragung (siehe [ITU H.245-2011]) und für den Faxversand (siehe [ITU T.38-2010]).

Abbildung 68 zeigt die Architektur eines H.323-Systems, das aus folgenden Komponenten besteht:

- Unter einem Terminal sind alle Arten von Endgeräten zu verstehen, die eine einzelne Verbindung terminieren, z. B. Telefone, Mailbox-Systeme, Videosysteme oder auch Softphones. Damit deckt der Begriff Terminal alle Systeme ab, die zur Kommunikation zwischen Teilnehmern eingesetzt werden.
- Ein Gateway realisiert den Übergangspunkt von einer H.323-Architektur in andere Netze (PSTN), beispielsweise ISDN. Prinzipiell ist die Funktion des Gateways also die Konvertierung der Nachrichten zwischen verschiedenen Formaten. Diese Konvertierung ist nicht auf Signalisierungsnachrichten beschränkt, sondern übersetzt auch zwischen verschiedenen Audio- und Video-Codecs.
- Multipoint Control Units (MCUs) sind Endpunkte, welche dem Management und der Verwaltung von Konferenzschaltungen zwischen drei oder mehr Terminals oder Gateways dienen.
- Ein Gatekeeper realisiert die Zugangskontrolle von H.323-Terminals zu einem H.323-Netzwerk. Dazu werden Registration-, Admission- und Status-Nachrichten (Registration, Admission and Status, RAS)

verwendet. Darüber hinaus realisiert der Gatekeeper das Bandbreitenmanagement, d. h. er verwaltet und bearbeitet die Bedürfnisse der Terminals bezüglich Bandbreite und teilt sie diesen zu. Eine weitere Aufgabe ist das Abbilden von H.323-Identitäten (beispielsweise nutzer@example.com) auf E.164-Rufnummern (etwa +491234567890, siehe [ITU E.164-2010]) und umgekehrt. Anrufverwaltung ist ebenfalls ein wesentlicher Bestandteil der Gatekeeper-Funktionalität. Damit ist der Gatekeeper das zentrale Element eines H.323-Systems.

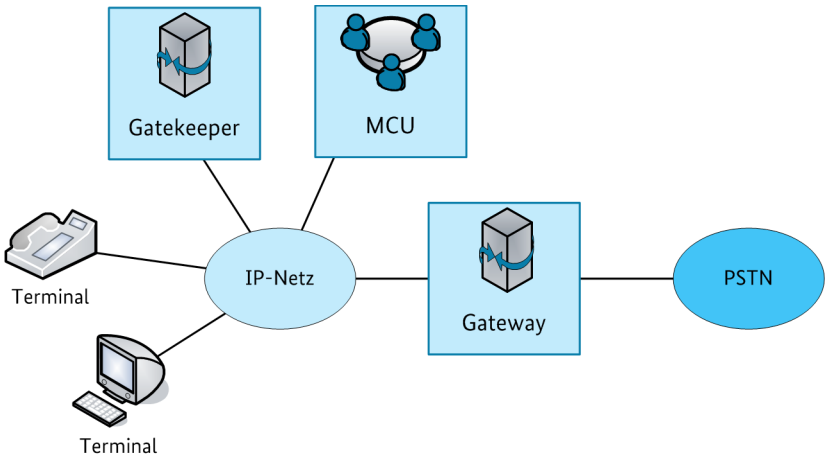


Abbildung 68: Architektur von H.323

Die Signalisierung nach H.323 umfasst mehrere Phasen:

- Im ersten Schritt erfolgt über den RAS-Kanal in Form von H.225-Nachrichten ein Anmeldevorgang: Die Terminals senden hierzu zunächst einen Register Request (RRQ) an den Gatekeeper. Bei erfolgreicher Registrierung antwortet dieser mit einer Nachricht vom Typ Register Confirmation (RCF), andernfalls versendet der Gatekeeper ein Registration Reject (RRJ). Die Kommunikation während der Registrierung findet über UDP statt.
- Anschließend wird über H.225 ein Steuerkanal für die weitere Signalisierung (üblicherweise über TCP) aufgebaut.
- Danach handeln die Teilnehmer über H.245 innerhalb des Steuerkanals ihre Fähigkeiten zur Sprach- und Videoübertragung aus.

Eine Übertragung von H.323-RAS-Nachrichten kann auch auf Basis des Transportkanals für die Anrufsignalisierung (H.225.0) erfolgen. Das im ITU-T-Standard H.460.17 spezifizierte Verfahren reduziert die Anzahl der benötigten TCP-Verbindungen und eignet sich somit zur Vermeidung von Problematiken bei der Überwindung von NAT (siehe [ITU H.460.17-2005]).

Die Nutzdaten werden üblicherweise über RTP versendet (siehe Kapitel 4.1.4 und 13.1.2)

13.1.1.3 Media Gateway Control Protocol (Megaco und MGCP)

Das Media Gateway Control Protocol (Megaco und MGCP) ist ein von ITU-T unter der Empfehlung [ITU H.248-2013] veröffentlichtes Protokoll zur Steuerung von dezentralen Media Gateways (MGWs) über einen Media Gateway Controller (MGC)[42]. Megaco/H.248 ging als Erweiterung aus dem ebenfalls Media Gateway Control Protocol genannten, aber MGCP abgekürzten, [IETF RFC3435-2003] hervor und stellt eine Kooperation zwischen der ITU-T und der IETF dar.

Das Prinzip von Megaco/H.248 ist in Abbildung 69 im Zusammenspiel mit SIP gezeigt. Aus Gründen des besseren Verständnisses sind in der Abbildung das Signalisierungs-Gateway (Signalling Gateway) und das

42 Ursprünglich wurde das Protokoll auch in RFC 3525 spezifiziert. Dieser RFC ist aber inzwischen als „Historic“ klassifiziert, da alle Inhalte in H.248 erfasst sind.

MGW getrennt dargestellt. Eine physische Trennung ist jedoch keine Voraussetzung. Es kann auch eine rein logische Trennung zwischen den Gateways vorgenommen werden.

Ruft ein VoIP-Endpunkt, hier als SIP-UA dargestellt, einen Teilnehmer in einem anderen Netz (z. B. dem öffentlichen Netz, PSTN) an, signalisiert er dies seinem SIP-Proxy. Der Proxy leitet die Anfrage zum MGC weiter. Der MGC hat jetzt zwei Aufgaben:

- Zum einem setzt der MGC die Signalisierungsdaten des SIP-Pakets in das im PSTN verwendete Signalisierungssystem Nr. 7 (SS7) um.
- Zum anderen muss der MGC die Parameter für die Nutzdatenübertragung zwischen MGW und UA koordinieren.

Die nach SS7 übersetzten SIP-Nachrichten leitet der MGC via SS7 over IP an das zuständige Signalisierungs-Gateway weiter, welches die SS7-Nachricht in das PSTN überträgt. Im MGW werden dann auf Basis der Angaben des MGC entsprechende Ressourcen zwischen PSTN und IP-Netz geschaltet, d. h. die Nutzdatenübertragung zwischen den Endgeräten in PSTN und IP-Netz findet statt.

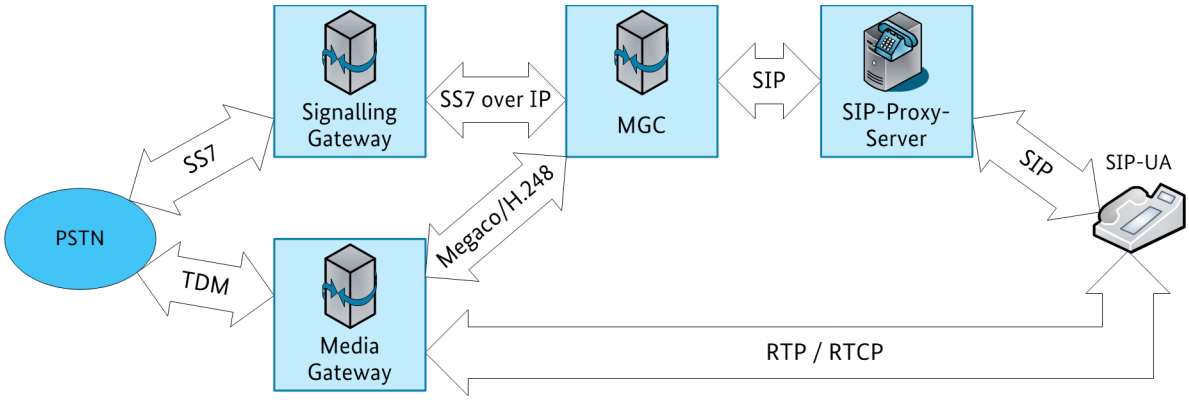


Abbildung 69: Illustration des Funktionsprinzips von Megaco/H.248

13.1.1.4 Inter-Asterisk eXchange (IAX)

Das Protokoll Inter-Asterisk eXchange (IAX) wurde zunächst für die Verbindung zwischen Asterisk-Servern zur Übertragung von Signalisierungs- und Sprachdaten spezifiziert. Inzwischen wird es auch für die Kommunikation zwischen Endgeräten und Asterisk-Servern verwendet. IAX ist in Version 2 in RFC 5456 spezifiziert (siehe [IETF RFC5456-2010]).

IAX wurde so spezifiziert, dass bei der Übertragung ohne Probleme auch NAT verwendet werden kann (z. B. in Form eines NAT Traversal Gateway als Komponente einer Firewall). Zur Unterstützung von NAT sind bei IAX daher keine zusätzlichen Mechanismen auf Ebene eines NAT Traversal Gateways oder Protokolle wie STUN, TURN oder ICE erforderlich.

IAX unterstützt eine Verschlüsselung der Kommunikation mit AES und 128 Bit Schlüssellänge. Die Schlüssel werden pro Sitzung, d. h. pro Anruf, aus einer Zufallszahl und einem gemeinsamen Passwort über einen MD5 Digest (Message Digest Algorithm 5) abgeleitet.

13.1.1.5 E.164 Telephone Number Mapping (ENUM)

Das E.164 Telephone Number Mapping (ENUM) ist in [IETF RFC6116-2011] und [IETF RFC6117-2011] spezifiziert und verwaltet auf Basis des Domain Name System (DNS) die Zuordnung von herkömmlichen Telefonnummern nach E.164 der ITU-T-Empfehlung [ITU E.164-2010] zu Internetadressen (Uniform Resource Identifier, URI). Als Toplevel-Domain wurde arpa, als Subdomain e164 gewählt.

Auch wenn ENUM hauptsächlich im Zusammenhang mit VoIP verwendet wird, ist ENUM nicht auf VoIP beschränkt, sondern ermöglicht, dass unter einer Adresse – der Telefonnummer – beliebige Kontaktdaten hinterlegt sind. Neben den Adressen für Festnetzanschluss, Fax, mobiles Endgerät oder Anrufbeantworter

können theoretisch beliebige Informationen hinterlegt werden. Die Internet Assigned Numbers Authority (IANA) verwaltet diese Einträge. Mögliche ENUM-Kontaktdaten sind z. B.:

- E-Mail
- Instant Messaging
- Webseite
- SMS / MMS / EMS (via PSTN oder E-Mail)
- Visitenkarte (vCard)

Die Anwendung bzw. das Endgerät entscheidet letztendlich, welche Daten verwendet werden.

Der Nutzen für die Telefonie soll anhand eines Beispiels verdeutlicht werden, bei dem eine gewählte Telefonnummer in die entsprechende ENUM-Domain übersetzt wird:

1. Wahl der Telefonnummer durch den Benutzer: +49123456789
2. Entfernen aller Zeichen, die keine Ziffer darstellen: 49123456789
3. Einfügen von Punkten zwischen den Ziffern: 4.9.1.2.3.4.5.6.7.8.9
4. Umkehrung der Reihenfolge: 9.8.7.6.5.4.3.2.1.9.4
5. Anhängen der Domain-Suffixe: 9.8.7.6.5.4.3.2.1.9.4.e164.arpa
6. Nachdem die E.164-Nummer entsprechend umgewandelt ist, durchsucht der ENUM-Client (z. B. ein Gateway oder ein Endgerät) die Domain 9.8.7.6.5.4.3.2.1.9.4.e164.arpa nach DNS NAPTR Resource Records (RR)[43]. Diese NAPTR-Einträge enthalten Regeln für die Umschreibung und Auflösung der Anfrage, welche schließlich die Ziel-URI ergeben.

Der so ermittelte URI kann jetzt im Rahmen der Signalisierung als Zieladresse des fernen UA verwendet werden.

13.1.2 Übertragung der Nutzdaten

Das Real-Time Transport Protocol (RTP) dient der Übertragung echtzeitsensitiver Daten für Unicast- und Multicast-Anwendungen (siehe [IETF RFC3550-2003]). Vornehmlich wird RTP für die Übertragung von Medienströmen in Form von Sprach- und Videodaten eingesetzt. RTP setzt auf dem User Datagram Protocol (UDP) auf. Im Gegensatz zu anderen Anwendungsprotokollen, die UDP verwenden, z. B. RADIUS, werden bei RTP-Sitzungen im Fall von Paketverlusten Daten nicht erneut übertragen. Stattdessen werden Datenverluste und damit verbundene Qualitätsschwankungen bewusst in Kauf genommen, um zu verhindern, dass Delay und Jitter durch wiederholtes Senden der Pakete erhöht werden.

RTP-Pakete enthalten eine Sequenznummer, um evtl. Datenverlust im Empfänger detektieren zu können. Zur Wahrung der Synchronität enthalten RTP-Pakete einen Zeitstempel auf Basis eines Grundtaktes in Sender und Empfänger. Dabei bezieht sich dieser Zeitstempel auf den Moment, an welchem das erste Byte der RTP-Payload generiert wurde. Über diesen Zeitstempel lässt sich neben Synchronisation auch der Jitter ermitteln.

RTP besitzt keine Mechanismen, um dem Sender über empfangene Daten und evtl. Verluste sowie über die Qualität der Übertragung (Jitter) Bericht zu erstatten. Darum wurde als Zusatzprotokoll zum RTP das RTP Control Protocol (RTCP) entwickelt. Es dient der Rückmeldung und Aushandlung von Übertragungs-parametern. Teilnehmer geben sich über RTCP periodisch Rückmeldung über die Qualität der empfangenen Daten, um eine flexible Anpassung des Datenstroms an die Netzqualität zu ermöglichen. Um die Bandbreite für RTP nicht durch Verwendung von RTCP einzuschränken, regulieren die Stationen auch die Frequenz der RTCP-Datenpakete.

43 NAPTR ist eine Abkürzung für Naming Authority Pointer und bezeichnet einen gemäß [IETF RFC3404-2002] festgelegten DNS-Eintrag, der unter anderem die Prioritäten der URIs festlegt.

13.1.3 Sicherheitsmechanismen in VoIP

In diesem Kapitel werden die Möglichkeiten der Absicherung von VoIP auf der Vermittlungsschicht (Network Layer) und höher beschrieben:

- Sicherer Medientransport
  - Secure Real-Time Transport Protocol (SRTP, siehe Kapitel 13.1.3.1).
  - Weitere Verfahren wie IPsec[44] und allgemein VPN-Techniken (siehe Kapitel 13.1.3.2).
- Sichere Signalisierung
  - Transport Layer Security (TLS, siehe Kapitel 13.1.3.3) oder auf der Vermittlungsschicht über IPsec
  - Absicherung der Signalisierungsprotokolle für SIP (siehe Kapitel 13.1.3.4)
  - Absicherung der Signalisierungsprotokolle für H.323 (siehe Kapitel 13.1.3.5)

Grundlage der hier beschriebenen Verfahren sind Verschlüsselungsalgorithmen, die für den Schutz der Vertraulichkeit und Integrität von Informationsströmen dienen. Als Verschlüsselungsverfahren kommt im Zusammenhang mit VoIP häufig der Advanced Encryption Standard (AES) zum Einsatz. Auf die Darstellung der Details der Verschlüsselungsalgorithmen wird an dieser Stelle verzichtet und auf die einschlägige Literatur zu Kryptografie verwiesen.

Eine detaillierte Darstellung der Sicherheitsmechanismen für VoIP-Systeme findet sich in der VoIPSEC-Studie des BSI (siehe [BSI VoIPSec-2005]).

13.1.3.1 Secure Real-Time Transport Protocol (SRTP)

Da bei RTP und RTCP die Daten im Klartext übertragen werden, kann die Kommunikation durch Mitschneiden der Nachrichten mitgehört werden. Daneben kann aber auch der Inhalt gezielt gefälscht werden oder durch Manipulation der Steuerinformationen ein Denial of Service (DoS) erreicht werden.

Zur Erhöhung der Sicherheit beim Real-Time Transport Protocol wurde daher das Secure Real-Time Transport Protocol (SRTP) entwickelt und im [IETF RFC3711-2004] der IETF spezifiziert.

SRTP bietet kryptografischen Schutz sowohl für RTP als auch für RTCP hinsichtlich Vertraulichkeit, Authentizität und Integrität. Weiterhin bietet SRTP einen Schutz gegen Replay-Angriffe. Ein Replay-Angriff liegt zum Beispiel dann vor, wenn ein Angreifer die Audioinformationen der Ansage einer Mailbox aufzeichnet und später abspielt, um dem Anrufenden vorzutäuschen, dass eine Kommunikation mit einer bestimmten Mailbox vorliegt.

SRTP verwendet ein symmetrisches Verschlüsselungsverfahren mit einer Schlüssellänge von mindestens 128 Bit, das auf AES basiert. Die Verwendung von AES mit Schlüssellängen 192 Bit und 256 Bit ist in [IETF RFC6188-2011] beschrieben.

Das Schlüsselmaterial, der sogenannte Master Key, muss beiden Kommunikationspartnern bekannt sein. Aus dem Master Key werden die eigentlichen Sitzungsschlüssel abgeleitet. Zur Erzeugung und Verwaltung der Master Keys ist ein Schlüsselmanagement notwendig. SRTP legt einen solchen Mechanismus nicht fest, sodass hier ergänzende Verfahren zum Tragen kommen. Die Schlüsselverwaltung für SRTP kann über einen spezifischen Mechanismus (s. u.) oder alternativ im Rahmen der Signalisierung (siehe Kapitel 13.1.3.4 und 13.1.3.5) erfolgen.

Ein speziell für das Schlüsselmanagement bei einer Echtzeit-Multimedia-Kommunikation entwickeltes Verfahren ist Multimedia Internet KEYing (MIKEY), welches in [IETF RFC3830-2004] spezifiziert ist. Über MIKEY kann ein gemeinsamer Schlüssel basierend auf einem Pre-Shared Key (PSK), über Diffie-Hellman oder über eine Public Key Infrastructure (PKI) vereinbart werden. MIKEY ist dabei unabhängig vom Signalisierungsprotokoll. Für VoIP besteht der Anwendungsbereich von MIKEY in der Aushandlung von Sicherheitsparametern und des Master Key für SRTP. Dabei können an einem Endgerät unterschiedliche Schlüssel für verschiedene, simultane Sitzungen vereinbart werden. Für Konferenzschaltungen gestattet

44 Bei IPv6 sind die in IPsec spezifizierten Mechanismen ein fester Bestandteil des Standardumfangs von IPv6.

MIKEY auch die gemeinsame Verwendung eines Master Key. MIKEY hat eine vergleichsweise geringe Akzeptanz bei den Herstellern erzielt.

Ein alternatives Verfahren, das sehr weite Verbreitung gefunden hat, wird als Session Description Protocol Security Descriptions for Media Streams (SDES) bezeichnet. Dieses SIP-basierte Verfahren wird in Abschnitt 13.1.3.4.3 beschrieben. Ein weiteres Verfahren zur Herstellung eines Sicherheitskontextes, der für das dynamische Schlüsselmanagement genutzt werden kann, steht mit dem DTLS-basierten DTLS-SRTP gemäß RFC 5764 (siehe [IETF RFC5764-2010] zur Verfügung. Es gewinnt aufgrund von Vorteilen beim Schlüsseltausch zunehmend an Verbreitung.

Die mit SRTP spezifizierte Sicherheitsarchitektur deckt sowohl Unicast- als auch Multicast-Applikationen ab. Da die Verschlüsselung und die Vertrauensbeziehung Ende-zu-Ende-Charakter haben, ist sie insbesondere für heterogene Netzumgebungen, z. B. für Mischungen aus drahtgebundenen und drahtlosen Netzen, geeignet.

Bei der Verwendung von SRTP wird der RTP-Header nicht verschlüsselt. Die unverschlüsselte Übertragung der RTP-Header dient zum Beispiel dazu, dass die Verwendung neuer Schlüssel im RTP-Paket vermerkt wird (Re-Keying). SRTP verfügt über kein Re-Keying, bietet jedoch Ansätze und Parameter, welche von einem ergänzenden Verfahren zum Schlüsselmanagement genutzt werden können.

13.1.3.2 IP Security (IPsec)

IP Security (IPsec) wurde 1998 mit dem Ziel entwickelt, die sicherheitstechnisch relevanten Schwächen des Internet Protocol (IP Version 4) zu beheben. IPsec realisiert eine Ergänzung zu IP und ist daher unabhängig von der Anwendung und dem verwendeten Transportprotokoll. Für eine IP-Kommunikation sichert IPsec Vertraulichkeit, Authentizität und Integrität zu. Die Verschlüsselung der Daten geschieht manchmal noch mit 3DES, jedoch ist der Einsatz aktueller Verfahren wie AES zu bevorzugen. Weitere Informationen zu IPsec können Kapitel 13.3.4.3 entnommen werden.

Der in Abbildung 70 dargestellte Ansatz zeigt einen IPsec-Tunnel zwischen einem Endgerät mit SIP-UA und einem VPN-Gateway. Damit ist das Endgerät über diesen Tunnel gesichert in das vertrauenswürdige Netz, z. B. ein Firmennetz, eingebunden. Über den Tunnel ist neben anderen Anwendungen auch die SIP-Kommunikation vor Angriffen aus dem nicht vertrauenswürdigen Netz, z. B. dem Internet, geschützt.

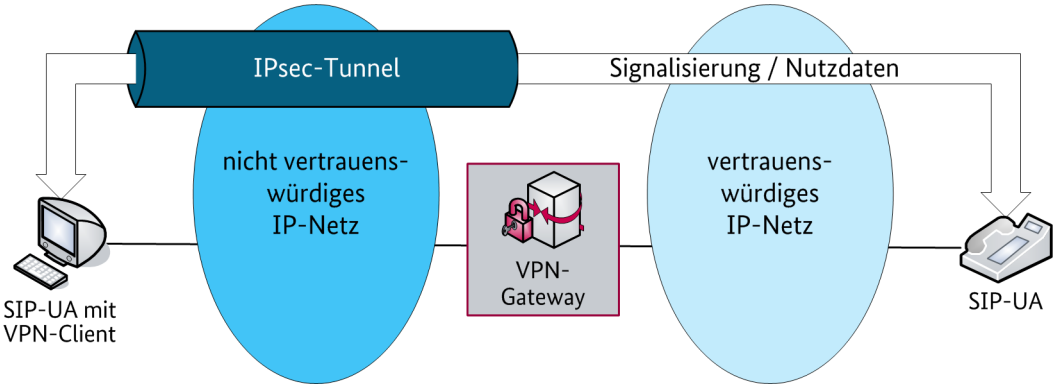


Abbildung 70: Anbindung von Endgeräten über ein VPN

IPsec kann darüber hinaus zur Verbindung von zwei vertrauenswürdigen IP-Netzen über ein dazwischenliegendes nicht vertrauenswürdiges IP-Netz genutzt werden (siehe Abbildung 71). Ein solches Szenario für den Einsatz von IPsec ist die Kopplung von TK-Netzen über eine IP-Verbindung. Die Media-Gateways bauen dafür über das nicht vertrauenswürdige IP-Netz einen Tunnel auf, über welchen die Sprach-Kommunikation abgewickelt wird.

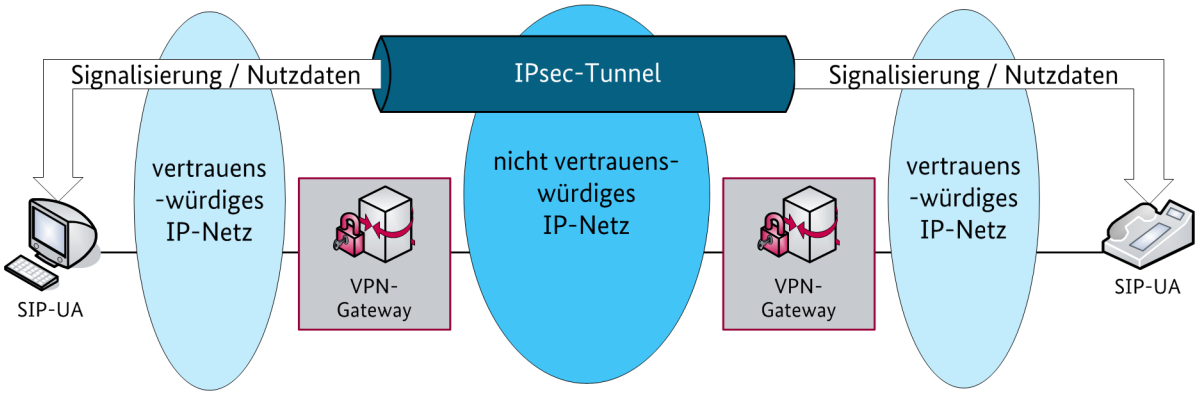


Abbildung 71: Verbindung von Netzen über ein VPN

13.1.3.3 Transport Layer Security (TLS)

Transport Layer Security (TLS) ist die standardisierte Version des unter Secure Socket Layer (SSL) bekannten Verfahrens (siehe [IETF RFC5246-2008]). Die Sicherheitsmechanismen bei TLS umfassen sowohl Verschlüsselung als auch Authentisierung. TLS setzt auf der verbindungsorientierten Kommunikation der Schicht 4 auf, d. h. TLS verwendet TCP.

Für die Anwendung von TLS bei der Absicherung einer VoIP-Kommunikation (primär für die Signalisierung) wäre aber der Schutz einer verbindungslosen Kommunikation von Interesse. Hierzu gibt es Datagram TLS (DTLS), eine Adaptierung von TLS, die UDP verwendet, siehe [IETF RFC6347-2012]. DTLS ist in der Praxis noch nicht geläufig. Wenn die VoIP-Signalisierung über TLS abgesichert werden soll, wird meist über TCP übertragen.

Für die Authentisierung einer TLS-Sitzung werden Zertifikate verwendet. Dies erfordert insbesondere für die Endgeräte eine entsprechende Zertifikatsverwaltung im Rahmen einer Public Key Infrastructure (PKI). Dabei ist es notwendig, dass zwischen den Zertifizierungsstellen (Certificate Authorities, CAs), welche die Zertifikate der beteiligten Kommunikationspartner signiert und ausgestellt haben, ein Vertrauensverhältnis besteht. Dieses Vertrauensverhältnis kann über Zwischeninstanzen etabliert werden, was den Aufbau einer Vertrauenskette erfordert.

Der TLS-Ansatz wird auch in der IP-Telefonie (insbesondere für SIP) verwendet. Damit wird zum Beispiel die Authentisierung zwischen IP-Telefonen und Telefonie-Servern realisiert und das Schlüssel-management für die Ende-zu-Ende-Verschlüsselung des Nutzdatentransports abgesichert. Eine detailliertere Beschreibung von TLS mit Hinweisen zur sicheren Nutzung findet sich in Kapitel 13.3.3.

13.1.3.4 SIP-Sicherheitsmechanismen

SIP bietet als textbasiertes Signalisierungsprotokoll eine große Angriffsfläche für Attacken und erfordert daher entsprechende Sicherheitsmechanismen.

13.1.3.4.1 Absicherung auf Transportebene

Die Sprachdaten werden zur Optimierung der Übertragungszeit meist direkt von einem Endgerät zum anderen übertragen. Die SIP-Signalisierung erfolgt dagegen ggf. auch über Zwischeninstanzen wie z. B. Proxies bei Providern. Für diese in Abbildung 72 gezeigten Szenarien kann eine Verschlüsselung von SIP-Nachrichten von SIP-Instanz zu SIP-Instanz (Hop-by-Hop) erfolgen. Dies setzt voraus, dass die einzelnen Zwischeninstanzen vertrauenswürdig sind.

Bemerkung: Wie in Kapitel 13.1.3.4.2 erläutert, ermöglicht SIP grundsätzlich auch eine Ende-zu-Ende-Absicherung mittels Secure Multipurpose Internet Message Extensions (S/MIME), jedoch ist diese Variante mit gewissen Nachteilen verbunden und in der Praxis kaum anzutreffen.

Daher basiert die Absicherung von SIP in der Regel wie bei HTTP auf TLS (siehe Kapitel 13.1.3.3). Zur Aktivierung von TLS wird bei HTTP „https:“ statt „http:“ verwendet. Analog wird bei SIP „sips:“ statt „sip:“ in der Adressierung benutzt. Während die ungesicherte Variante von SIP in der Regel auf UDP basiert, setzt die gesicherte SIP-Variante, d. h. TLS, grundsätzlich auf TCP auf. Wie in Kapitel 13.1.3.3 erläutert, setzt die Nutzung von TLS voraus, dass die Kommunikationspartner einer gemeinsamen Instanz vertrauen bzw. über weitere Zwischeninstanzen eine Vertrauenskette aufbauen. Zum Beispiel baut der UA eines Endgerätes eine Vertrauensbeziehung mit dem Outbound-Proxy[45] des eigenen Unternehmens bzw. der eigenen Behörde auf, welcher wiederum Vertrauensbeziehungen mit anderen Instanzen eingeht usw. Alle am Verbindungsaufbau beteiligten Instanzen speichern bei einer sicheren Signalisierung Statusinformationen zu jeder SIP-Kommunikation, was die Skalierbarkeit des Verfahrens einschränkt.

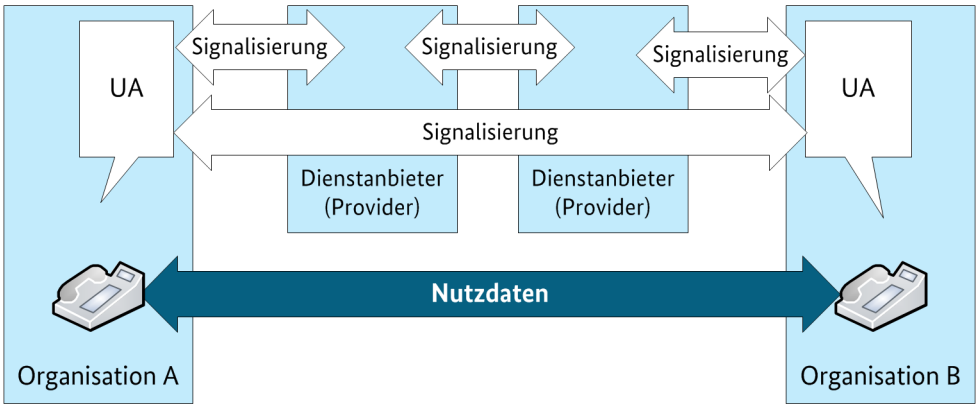


Abbildung 72: Signalisierung über Zwischeninstanzen

13.1.3.4.2 Absicherung auf Anwendungsebene

Das Verfahren Secure Multipurpose Internet Message Extensions (S/MIME) wurde ursprünglich von den Laboratorien der RSA Security Inc. entwickelt, um eine sichere Ende-zu-Ende-Übertragung von Nachrichten, insbesondere E-Mails, zu ermöglichen. Mittlerweile hat die IETF die Standardisierung von S/MIME übernommen und in diesem Zusammenhang unter anderem [IETF RFC5750-2010], [IETF RFC5751-2010] und [IETF RFC5652-2009] veröffentlicht.

Der Einsatz von S/MIME ist jedoch nicht auf die Absicherung von E-Mails beschränkt, sondern kann für jegliche Kommunikation verwendet werden, in der MIME genutzt wird, z. B. für Instant Messaging oder SIP. S/MIME ermöglicht damit im Unterschied zur Hop-by-Hop-Absicherung, wie sie bei TLS erfolgt, eine sichere Ende-zu-Ende-Signalisierung.

Allgemein dient der Standard MIME (Multipurpose Internet Mail Extensions) der Kodierung von Nachrichten. Insbesondere bei E-Mails dient MIME der Kodierung von binären Daten bzw. Zeichen, die nicht im US-ASCII-Zeichensatz vorhanden sind. Um welche Daten es sich im kodierten Teil handelt, wird durch den MIME-Typ bzw. Content Type angegeben, z. B. „text“ für Textdateien, „multipart“ für mehrteilige Daten oder „application“ für applikationsspezifische Inhalte. Die sichere Übertragung der Nachrichten mit den Zielen Vertraulichkeit und Integrität wird bei S/MIME durch eine Verschlüsselung und Signatur der MIME-kodierten Daten erreicht. S/MIME nutzt hierfür eine Public-Key-Infrastruktur mit Zertifikaten nach ITU-T-Standard X.509 in Version 3 (siehe [ITU X.509-2012]).

Im Rahmen des SIP-Protokolls nach [IETF RFC3261-2002] wird der Body einer SIP-Nachricht MIME-kodiert übertragen und ermöglicht damit eine optionale Absicherung mittels S/MIME. Bei der Verschlüsselung von Signalisierungsinformationen, die Ende-zu-Ende (Peer-to-Peer) übertragen werden, muss beachtet werden, dass zwischengeschaltete Proxies auf diese Informationen aus dem SIP-Paket nicht

45 Der Outbound-Proxy ist derjenige Proxy-Server, an den ein UA einen ausgehenden Anruf signalisiert. Die Adresse des Outbound-Proxy kann manuell auf dem UA konfiguriert oder durch einen DHCP-Server zugewiesen werden. Andere Methoden zur Auffindung (Discovery) des Outbound-Proxy sind grundsätzlich auch möglich.

mehr zugreifen können. Um die Zustellung der SIP-Nachrichten zu gewährleisten, müssen also bestimmte Header-Felder (z. B. die SIP-Routing-Information) im Klartext übertragen werden.

Weitere Header-Felder und der SDP-Body können hingegen durch S/MIME geschützt werden. Die Konsequenz ist, dass Netzelemente, welche zwischen den beiden Teilnehmern agieren, z. B. Firewalls, SBCs (Session Border Controller) oder SIP-Proxies, nicht länger auf den Inhalt der SIP-Nachrichten zugreifen können. Insbesondere Firewalls mit VoIP-Applikationsintelligenz sind dadurch nicht mehr in der Lage, dynamisch RTP-Ports für die Nutzdaten zu öffnen.

S/MIME bietet für SIP zwei Modi:

- Nur die Payload der SIP-Nachricht wird verschlüsselt und/oder signiert.
- Die gesamte SIP-Nachricht wird erneut MIME-kodiert und als Payload einer neuen SIP-Nachricht versendet und damit getunnelt. Für SIP und S/MIME im Tunnelmodus wird der Inhalt der inneren SIP-Nachricht mit dem MIME-Typ „message/sip“ gekennzeichnet und bis auf die erforderlichen Felder zur Weiterleitung der Nachricht durch S/MIME geschützt.

Der Einsatz von S/MIME ermöglicht unter anderem den sicheren Austausch von Schlüsselmaterial für SRTP.

Da S/MIME auf X.509-Zertifikaten basiert, gelten allgemein die Hinweise aus Kapitel 13.3.3 zur Verwendung von Zertifikaten. Im Gegensatz zu den Geräte- bzw. Server-spezifischen Zertifikaten bei TLS werden die Zertifikate bei S/MIME auf den jeweiligen Benutzer ausgestellt. Entsprechend ist bei der Validierung der Zertifikate nicht der Hostname zu verifizieren, sondern der Benutzer in Form seiner öffentlichen SIP bzw. SIPS-URI (z. B. nutzer@example.com).

Aufgrund der fehlenden Herstellerunterstützung ist der Einsatz von S/MIME im Zusammenhang mit SIP derzeit noch nicht relevant.

13.1.3.4.3 SIP-basiertes Schlüsselmanagement für SRTP

Das Schlüsselmanagement für SRTP kann über SIP durch die Nutzung eines im Session Description Protocol (SDP) vorgesehenen Schlüsselfelds erfolgen. SDP wurde in der SIP-Architektur zunächst nur für die Beschreibung von Session-Merkmalen wie Audio- und Videomerkmalen eingesetzt. Unter der Bezeichnung SDES wurde es in [IETF RFC4568-2006] jedoch um die Aushandlung von Security Suites[46], Schlüsseln und anderen Sicherheitsparametern erweitert. Für den Transport von Schlüsselmaterial mittels SDES müssen die SDP-Informationen ihrerseits verschlüsselt übertragen werden. Dies kann durch Absicherung der SIP-Signalisierung über TLS (siehe Kapitel 13.1.3.4.1) oder S/MIME (siehe Kapitel 13.1.3.4.2) erfolgen.

13.1.3.4.4 Authentisierung zum Aufbau einer SIP-Sitzung

Unabhängig von einer etwaigen Nutzung von TLS zur Absicherung der Signalisierung kann zwischen den SIP-Elementen eine Authentisierung zum Aufbau der SIP-Sitzung erfolgen.

In der SIP-Authentisierungsarchitektur nach [IETF RFC3261-2002] wird die Übertragung von Kennwörtern im Klartext (HTTP Basic) ausdrücklich abgelehnt. Die Methode zur Authentisierung, SIP Digest Authentication, basiert auf HTTP Digest Authentication. Die Authentisierung der Proxies erfolgt dabei analog zur Authentisierung der Endgeräte, d. h. mittels HTTP Digest Authentication. Verschiedene Proxies entlang des Signalisierungspfads können jeweils eine separate Authentisierung fordern.

Proxies, die eine Authentisierung fordern, weisen nicht-authentisierte Client-Requests mit dem Return-Code „407 Proxy Auth required“ ab. Innerhalb des SIP-Headers fügt der Proxy hierbei ein weiteres Header-Feld, den sogenannten „Proxy Authenticate Header“, ein. Dann sendet der Client, d. h. der UA, den Request erneut, diesmal jedoch mit Authentisierungsinformationen in dem zusätzlichen Feld „Proxy Authorization“:

46 Der Begriff Security Suite kann am ehesten mit Sicherheitspaket übersetzt werden. Eine Security Suite vereinigt verschiedene Sicherheitsverfahren (beispielsweise zur Verschlüsselung, Integritätsprüfung und Authentisierung).

- Innerhalb des im empfangenen 407-Code enthaltenen Proxy Authenticate Header findet der UA einen zufälligen Wert, die sogenannte Challenge. Aus dieser Challenge bildet der UA dann mit seinem Nutzernamen und seinem Passwort einen Hash-Wert entsprechend der angegebenen Authentisierungsmethode, beispielsweise MD5.
- Daraufhin schickt der UA einen erneuten INVITE-Request an den Proxy, der einen Proxy Authorization Header mit dem errechneten Hash-Wert enthält.

Abbildung 73 zeigt ein Beispiel für mehrere Authentisierungsschritte während des Rufaufbaus. Hier wird neben der Proxy-Autorisierung auch die Autorisierung am angerufenen Teilnehmer verdeutlicht.

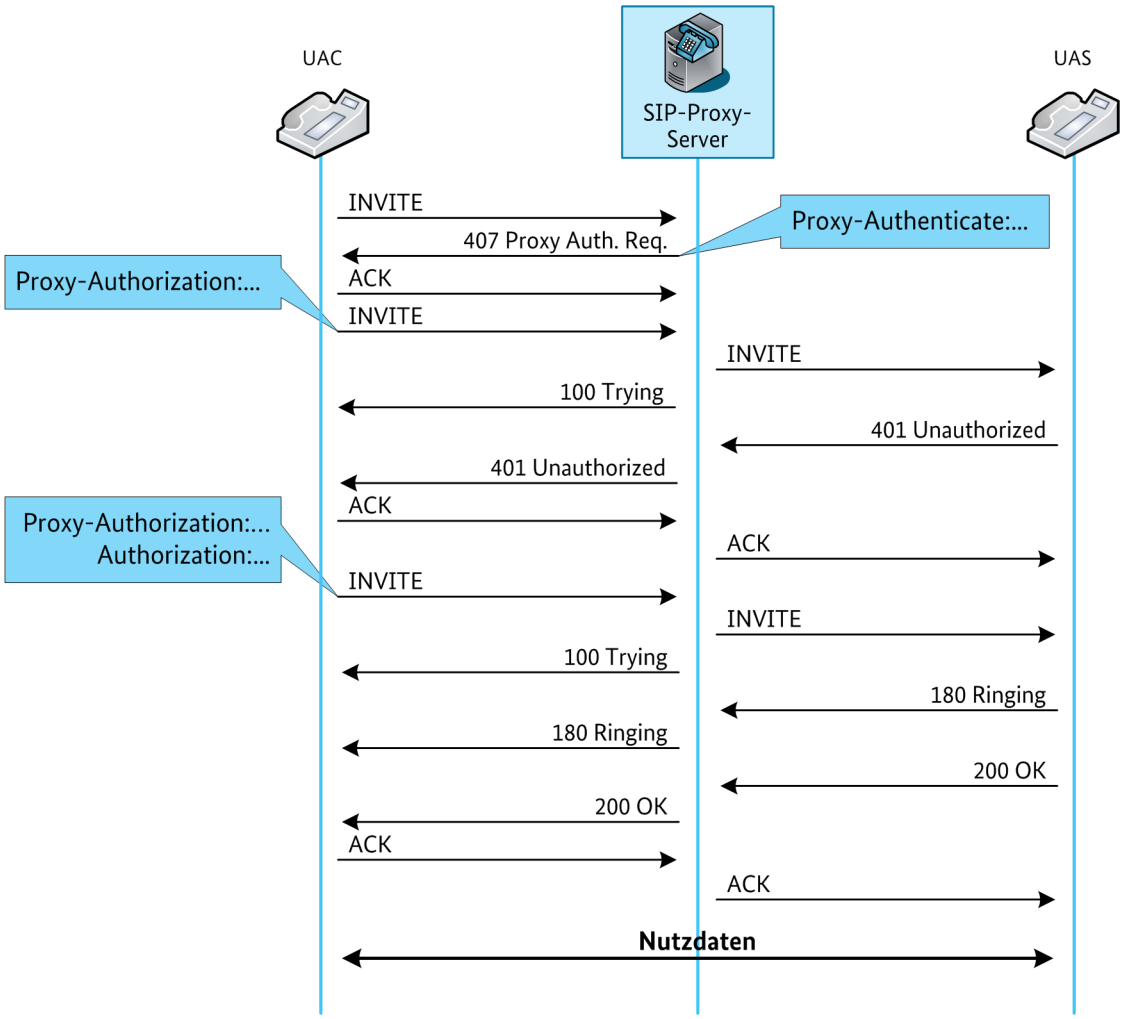


Abbildung 73: Ablauf eines Rufaufbaus mit mehrfacher Authentisierung entlang des Signalisierungspfads

In dem in der Abbildung 73 dargestellten Beispiel baut der UAC die Sitzung auf. Dazu sendet er eine INVITE-Nachricht an seinen SIP-Proxy. Dieser antwortet mit der Meldung „407 Proxy Authentication Required“, um dem UAC mitzuteilen, dass für die Nutzung der Dienste des Proxy-Systems eine Authentisierung erforderlich ist.

Das Endgerät übermittelt eine erneute INVITE-Message mit einem „Proxy-Authorization“-Header. Dieser Header enthält die Antwort auf die vom Proxy mit der 407-Nachricht versandten Challenge. Im Falle einer erfolgreichen Authentisierung durch den Proxy leitet dieser die INVITE-Nachricht an den UAS des angerufenen Endgerätes weiter.

Fordert dieser auch eine Authentisierung vom Client („401 Unauthorized“), wird die INVITE-Nachricht nochmals vom Initiator (UAC) via SIP-Proxy zum Partner (UAS) geschickt, diesmal zusätzlich mit der Authentisierungsinformation für das angerufene Endgerät. Somit trägt die dritte INVITE-Nachricht zwei

Header, einen mit den für die Nutzung der Proxy-Dienste erforderlichen Informationen und einen mit den vom anderen Endgerät angeforderten Authentisierungsinformationen. Sind beide Authentisierungsinformationen gültig, wird die INVITE-Methode vom anderen SIP-Partner akzeptiert und die Verbindung kommt zustande.

Fordern mehrere Proxies entlang des Signalisierungspfads eine Authentisierung vom Endgerät, so müssen die beschriebenen Schritte mehrfach ausgeführt werden. Der Client muss je Authentisierungsschritt ein INVITE-Paket mit den entsprechenden Authentisierungsinformationen generieren und versenden.

Die SIP Digest Authentication ist optional und kann für verschiedene SIP-Methoden, wie REGISTER und INVITE, genutzt werden. Da die SIP Digest Authentication selektiv von der jeweiligen Implementierung für einzelne SIP-Methoden angefordert werden muss und nicht die gesamte Signalisierung automatisch abgesichert wird, entsteht eine nicht unerhebliche Komplexität und es bleibt das Risiko, dass Teile der Signalisierung ohne Authentisierung durchgeführt werden. Weiterhin sind für die Zusicherung von Vertraulichkeit und Integrität der Signalisierungsinformationen weitergehende Mechanismen erforderlich. Aus diesen Gründen hat sich in der Praxis die Verwendung von TLS zur Absicherung von SIP durchgesetzt.

13.1.3.4.5 Teilnehmer-Identifikation

Analog zur ISDN-basierten Telekommunikation unterstützt SIP Funktionen zur Anzeige der Identität von Teilnehmern bzw. zur Unterdrückung dieser Anzeige. Hierzu ist bei SIP ein zusätzliches Protokollfeld (ein sogenannter Extension Header) namens Remote Party Identification (RPID) vorgesehen, das differenziert nach User, Subscriber und Terminal die Identitätsinformationen übertragen kann.

Signierte Informationen im RPID-Feld können genutzt werden, um die authentisierte Identifizierung des Initiators sicherzustellen. Dazu muss eine Vertrauenskette zwischen den involvierten SIP-Instanzen zur Bestätigung der Authentisierung genutzt werden. Die zwischengeschaltete SIP-Instanz authentisiert dabei den Anrufer und fügt eine signierte RPID hinzu (eine fehlgeschlagene Authentisierung wird auch angezeigt).

Der Initiator der Session kann ein bestimmtes Vertraulichkeitsniveau fordern, sodass die Nachricht nur dann an einen anderen Vertrauensbereich weitergeleitet wird, wenn die angeforderte Vertraulichkeit garantiert ist.

13.1.3.5 Sicherheitsmechanismen in H.323

In einer H.323-Umgebung ist der wichtigste Sicherheitsstandard H.235 „Security and Encryption for H-Series (H.323 and other H.245-based) Multimedia Terminals“. H.235 beschreibt Mechanismen in folgenden Bereichen:

- Verschlüsselung von Audio- und Video-Daten (AV), die über RTP übertragen werden
- Sicherheitsmechanismen für die Kommunikation zwischen dem Endgerät und dem Gatekeeper (Registration, Admission and Status, RAS) und Sicherheitsmechanismen während des Verbindungsaufbaus entsprechend der Spezifikation H.225
- Aushandlung der Sicherheitsfähigkeiten (Security Capabilities) über H.245

Die Ziele des ITU-Standards H.235 sind Authentisierung, Integrität und Vertraulichkeit bei Punkt-zu-Punkt- und Mehrpunkt-Konferenzen, die H.245 als Protokoll zur Aushandlung der Fähigkeiten der Endgeräte nutzen. In H.235 werden keine Vorschriften gemacht, welche Verschlüsselungsverfahren unterstützt werden müssen, d. h. es können verschiedene Verschlüsselungsverfahren und Schlüssellängen genutzt werden. Es wird empfohlen, dass Endgeräte so viele Verfahren wie möglich unterstützen können, um Interoperabilitätsproblemen begegnen zu können. Weiterhin können bestimmte Verschlüsselungsverfahren auf den Transport, andere auf die Signalisierung angewandt werden.

Grundlegend für H.235 ist die Annahme, dass die Bedrohungen nicht über die Endgeräte, sondern aus dem Netz kommen. Endgeräte selbst werden als vertrauenswürdig und somit auch als ausreichend geschützt eingestuft.

13.1.3.5.1 Schutz von Registrierung, Autorisierung und Signalisierung

Zur Absicherung von RAS zwischen Endpunkt und Gatekeeper kommt üblicherweise TLS oder IPsec zum Einsatz (siehe Kapitel 13.1.3.3 und Kapitel 13.1.3.2). Für den Verbindungsaufbau über H.225 zwischen zwei Endpunkten wird ebenfalls TLS oder IPsec genutzt.

Innerhalb der nach H.225 aufgebauten Verbindung können die Endgeräte ihre Fähigkeiten über H.245 aufeinander abstimmen. Dabei werden auch der zu verwendende Sicherheitsmechanismus und die zugehörigen Sitzungsschlüssel vereinbart. Die Sitzungsschlüssel können auch während der Sitzung neu ausgehandelt werden.

13.1.3.5.2 Authentisierung

Die Authentisierung bei H.235 kann mittels Pre-Shared Key (PSK) oder durch den Austausch von Zertifikaten implementiert werden. H.235 beschreibt das Protokoll für den Austausch der Authentisierungsinformation sowohl für eine beidseitige als auch für eine einseitige Authentisierung und lässt Varianten für die Authentisierungsprozedur und -kriterien zu.

Zertifikate belegen zum Beispiel, dass der Kommunikationspartner im Besitz des zu einem öffentlichen Schlüssel passenden privaten Schlüssels ist. Eine erforderliche Richtlinie, wie mit von einer bestimmten Instanz signierten Zertifikaten umgegangen wird, d. h. akzeptieren oder ablehnen, ist jedoch kein Bestandteil von H.235, sondern dem Betreiber der Geräte überlassen. Die Akzeptanz oder Ablehnung von Zertifikaten kann automatisiert oder manuell durchgeführt werden, analog zu Zertifikaten im World Wide Web.

Als weitere Option kann die Authentisierung im Rahmen eines separaten Sicherheitsprotokolls wie TLS oder IPsec durchgeführt werden.

13.1.3.5.3 Schlüsselmanagement

Zur Vereinbarung der Schlüssel für die Verschlüsselung des Datentransports kann ein verschlüsselter H.245-Kanal ausgehandelt werden. Es ist auch möglich, H.245 unverschlüsselt zu nutzen und die Sitzungsschlüssel über ein separates Schlüsselmanagementverfahren auszutauschen. Jede Instanz, die einen verschlüsselten Kanal terminiert, wird als vertrauenswürdig und geschützt eingestuft, z. B. eine MCU oder ein Gateway. Falls die Vertrauensbeziehung nicht a priori besteht, muss jede als vertrauenswürdig zu behandelnde Instanz im Übertragungspfad authentisiert werden (analog zu SIP).

Falls es keine gemeinsamen Sicherheitsfähigkeiten gibt, kann das angerufene Endgerät die Annahme des Anrufs verweigern. Die Authentisierung des H.245-Kanals erfolgt vor dem Austausch jeglicher Fähigkeiten der Endgeräte.

Bei Mehrpunktkonferenzen handelt die MCU mit jedem Teilnehmer die Sicherheit separat aus.

Für das Schlüsselmanagement nach H.235 werden sogenannte dynamische Payload Types unter RTP eingesetzt. Während herkömmliche Payload Types Angaben über die Art der Payload, also Audio oder Video, sowie über verwendeten Code beinhalten, werden dynamische Payload Types von den Endpunkten vereinbart. Bei H.235 wird nach jeder Aushandlung eines neuen Sitzungsschlüssels (Re-Keying) ein neuer dynamischer Payload Type vereinbart. Hierzu wird das Master-Slave-Prinzip angewendet. Dabei gibt der Master sowohl den Payload Type als auch den Sitzungsschlüssel über H.245 vor.

H.235 sieht zwei Varianten des Schlüsselmanagements vor:

- Falls der Gatekeeper die unter H.235 vorgesehenen Sicherheitsmechanismen nicht unterstützt, erfolgt nur die Phase Registration, Admission and Status (RAS) über den Gatekeeper. Alle anderen Phasen folgen direkt (Peer-to-Peer) unter Umgehung des Gatekeepers. Dieser Ablauf ist in Abbildung 74 dargestellt. Das Problem bei diesem Ansatz besteht darin, dass die fehlende Unterstützung der Sicherheitsmechanismen durch den Gatekeeper das Schlüsselmanagement bei einem Einsatz vieler Endgeräte erschwert.

- Bei einer gegebenen H.235-Unterstützung durch den Gatekeeper erfolgen alle Phasen der Signalisierung über den Gatekeeper, wie in Abbildung 75 dargestellt. Lediglich die Nutzdatenübertragung erfolgt direkt zwischen den Endgeräten ohne Einbindung des Gatekeeper. Dabei kann der Gatekeeper auch das zentrale Schlüsselmanagement übernehmen.

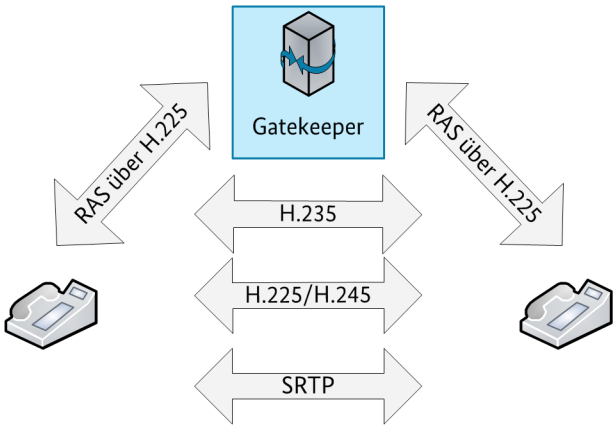


Abbildung 74: H.235 zwischen den Endpunkten

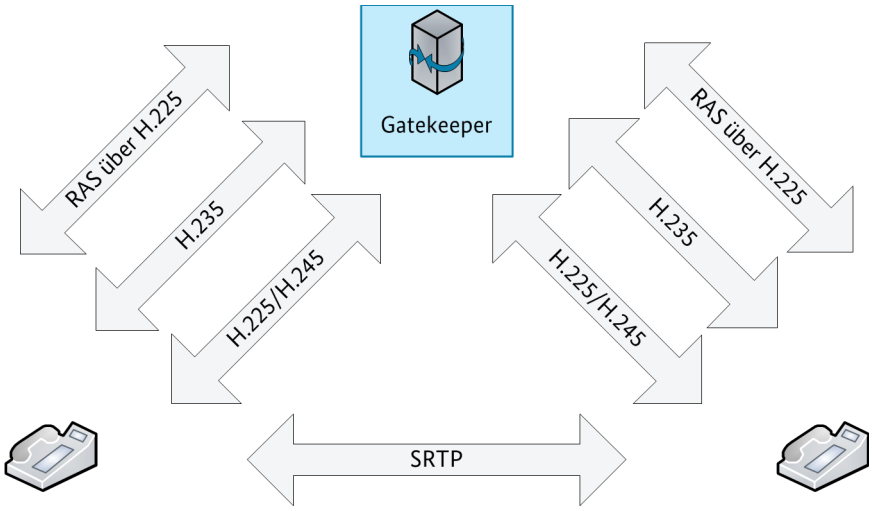


Abbildung 75: H.235 zentral über den Gatekeeper

13.2 Grundlagen zu UCC und Anwendungsintegration

13.2.1 Präsenzdienste und Instant Messaging

13.2.1.1 Session Initiation Protocol and Presence Leveraging Extensions (SIP/SIMPLE)

Das Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE) ist ein auf SIP basierendes Protokoll, das Erweiterungen im Bereich Instant Messaging und Präsenzinformationen bereitstellt. SIMPLE ist ein offener Standard, der in [IETF RFC3428-2002] und [IETF RFC3856-2004] definiert wurde. Zum Versand von Instant Messages werden die folgenden zwei Modi definiert: der Page Mode sowie der Session Mode. Beim Page Mode werden Nachrichten über das SIP-Protokoll als Parameter übermittelt. Die so übermittelten Nachrichten sind lediglich Peer-to-Peer-Nachrichten, es wird also keine Sitzung ausgehandelt. Im Session Mode hingegen werden die Nachrichten als zu übertragender Medienstrom interpretiert und mit Hilfe des Message Session Relay Protocols (MSRP) übertragen. MSRP ist in [IETF RFC4975-2007] und [IETF RFC4976-2007] definiert.

Präsenzinformationen werden im SIP/SIMPLE über die Rich Presence Extensions to the Presence Information Data Format (RPID) zur Verfügung gestellt, siehe hierzu [IETF RFC4480-2006]. Der Präsenzstatus eines Nutzers wird anhand des RPID durch verschiedene Attribute dargestellt. Über das Attribut „activities“ kann beispielsweise die aktuelle Tätigkeit vermittelt werden. Hier sind eine Vielzahl von vordefinierten Ausprägungen möglich, beispielhaft seien hier „busy“, „vacation“ und „away“ genannt. Zusätzlich kann eine Freitext-Notiz hinterlegt werden. Der Status kann einerseits durch den Nutzer selbst, andererseits aber auch automatisch (z. B. über eine Kalender-Integration) verwaltet werden.

Bevor nun ein Nutzer A die Präsenzinformationen eines anderen Nutzers B erhalten kann, muss dies vom Nutzer B autorisiert werden. Hierzu können entsprechende Regeln definiert werden, unter welchen Umständen anderen Nutzern die geforderten Informationen zugänglich gemacht werden. Details hierzu können in RFC 5025 nachgelesen werden (siehe [IETF RFC5025-2007]).

SIP/SIMPLE stellt außerdem verschiedene Sicherheitsmechanismen zur Verfügung. So kann beispielsweise die Kommunikation per Ende-zu-Ende-Verschlüsselung abgesichert werden, wodurch die gesendeten Informationen ausschließlich dem vorgesehenen Empfänger zugänglich gemacht werden.

13.2.1.2 eXtensible Messaging and Presence Protocol (XMPP)

Das eXtensible Messaging and Presence Protocol (XMPP) ist basierend auf dem XML-Standard ebenfalls ein offener Standard zum Austausch von Präsenzinformationen und zum Versand von Instant Messages. XMPP ist in mehreren RFCs spezifiziert: [IETF RFC6120-2011], [IETF RFC6121-2011], [IETF RFC6122-2011], [IETF RFC3922-2004] und [IETF RFC3923-2004].

Insbesondere die folgenden Funktionen werden von XMPP bzw. den verfügbaren Erweiterungen bereitgestellt: Versand von Instant Messages, Austausch von Präsenzinformationen sowie Verwaltung einer Kontaktliste. Durch das erweiterbare Design kann XMPP ebenfalls der Signalisierung von Sprach- und Videoübertragungen, dem Dateitransfer sowie vielen weiteren Applikationen dienen. Die Kommunikation zwischen den Gesprächspartnern ist in der Regel Server-basiert, was eine Protokollierung und Aufzeichnung der abgehaltenen Sitzungen ebenso wie die Kommunikation über Vertrauensgrenzen hinweg erlaubt.

Die Informationen werden im XMPP-Standard in kleinen Datenpaketen („XML stanza“ genannt) übertragen. Standardmäßig gibt es drei Arten von XML stanzas, message, presence und IQ (kurz für Info/Query), die wie folgt definiert sind:

- Das message stanza liefert Nachrichten nach dem Push-Prinzip an den genannten Adressaten aus.
- Beim Einsatz des presence stanza werden die Präsenzinformationen in Form von Freitext-Nachrichten in der Regel an alle Nutzer gesendet, die diesen Nutzer abonniert haben. Dabei muss jedoch der Nutzer, von dem Präsenzinformationen verlangt werden, dieses Abonnement im Vorfeld manuell oder über eine Automatisierung bestätigen.
- Die IQ stanzas basieren, ähnlich wie das Hypertext Transfer Protocol HTTP, auf dem Frage-Antwort-Prinzip.

Zur Absicherung der über XMPP geführten Kommunikation können die einzelnen Wege - also Client-zu-Server, Server-zu-Server sowie Client-zu-Client - mittels SSL/TLS verschlüsselt werden. Dabei ist eine Ende-zu-Ende-Verschlüsselung in jedem Fall einer Kombination aus Client-zu-Server- und Server-zu-Server-Verschlüsselung vorzuziehen, da im zweiten Fall die Daten an den beteiligten Servern zunächst entschlüsselt und anschließend wieder verschlüsselt werden. Hingegen werden bei einer Ende-zu-Ende-Verschlüsselung die Daten erst vom Ziel-Client entschlüsselt.

13.2.2 Computer Telephony Integration (CTI) und Anwendungsintegration

Zur Kopplung von Computer und Telefon bzw. von CTI-Server und TK-Anlage wurden eine Reihe von Protokollen und Application Programming Interfaces (APIs) entwickelt, deren bekannteste Vertreter in Tabelle 21 zusammengefasst sind.

Abkürzung	Name	Einsatzgebiet
CSTA	Computer Supported Telecommunications Applications	ISO-standardisiertes Anwendungsprotokoll für Einzel- und Mehrplatzlösungen
TAPI	Telephony Application Programming Interface	Programmierschnittstelle für Windows-basierte Rechner; ermöglicht Einzel- und Mehrplatzlösungen
TSAPI	Telephony Server API	Programmierschnittstelle für Novell Netware; ermöglicht Mehrplatzlösungen
JTAPI	Java Telephony API	Java-basierte Programmierschnittstelle für Einzel- und Mehrplatzlösungen

Tabelle 21: Wichtige CTI-Programmierschnittstellen und -Protokolle

Abbildung 76 zeigt am typischen Aufbau einer Mehrplatzlösung, wo die im Folgenden beschriebenen Protokolle eingesetzt werden. Die in der Abbildung gezeigte Anbindung über eine CTI-Middleware ist nur dann erforderlich, wenn die TK-Anlage nicht über die verbreiteten CTI-Schnittstellen verfügt.

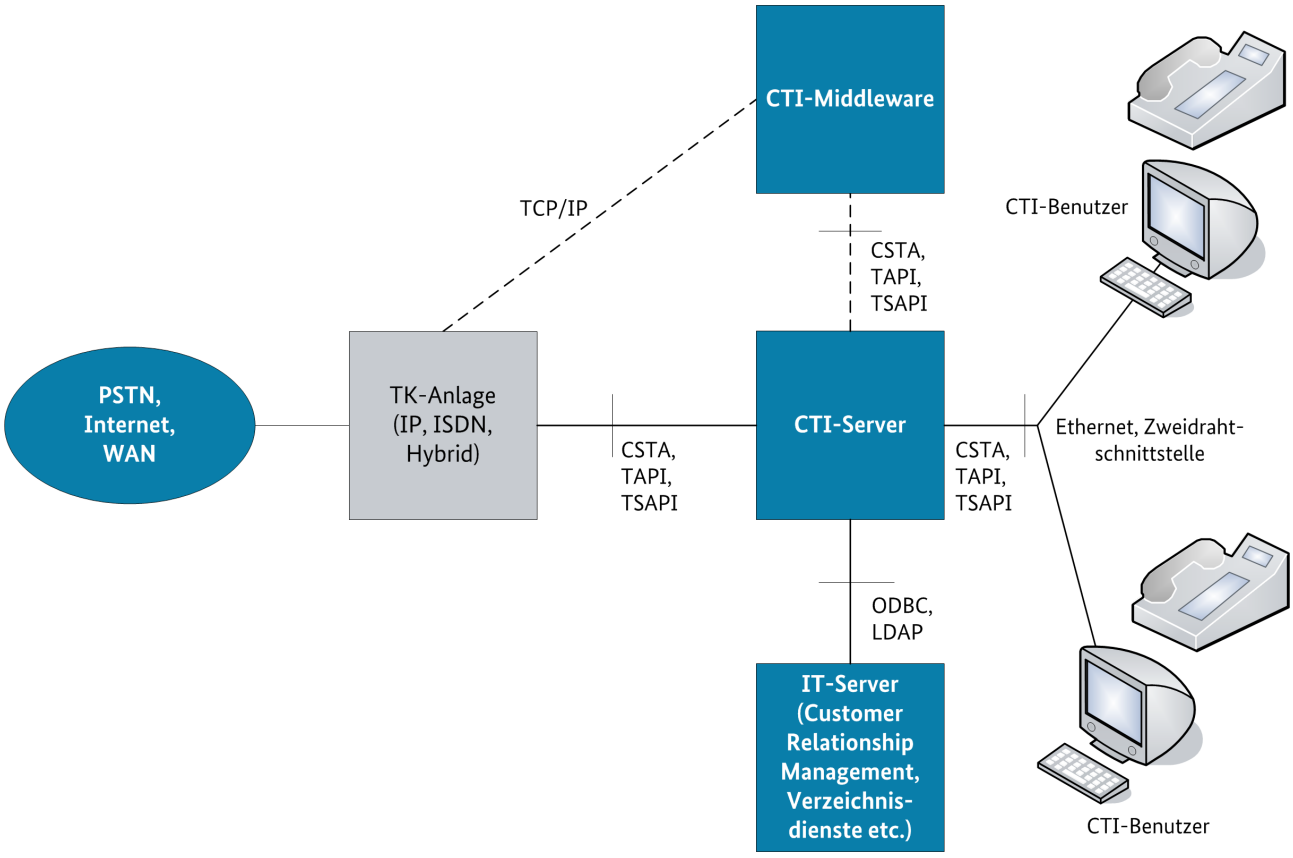


Abbildung 76: Typischer Aufbau einer Mehrplatzlösung mit Integration in ein IT-System

13.2.2.1 Computer Supported Telecommunications Applications (CSTA)

Im Gegensatz zu TAPI, TSAPI und JTAPI ist CSTA keine API, sondern ein Protokoll der Anwendungsschicht. Die ISO-Standards für CSTA spezifizieren die unterstützte Funktionalität sowie die zugehörigen Daten (siehe [ISO 18051-2012] und [ISO 18052-2012]). Die Funktionalität umfasst dabei u. a. die Verbindungskontrolle, die Endgerätekontrolle, die Überwachung von Endgeräten und Verbindungen sowie die Abrechnung von Verbindungsdaten. CSTA unterstützt sowohl Einzel- als auch Mehrplatzlösungen. Die Spezifikation gibt keine Mechanismen für den Transport von CSTA-Nachrichten vor, d. h. insbesondere, dass die Vertraulichkeit und Integrität der Daten, ähnlich wie bei den beschriebenen APIs, von den jeweiligen Herstellern der CTI-Server und TK-Anlagen abhängt.

13.2.2.2 Telephony Application Programming Interface (TAPI)

TAPI bietet Entwicklern von Windows-basierten CTI-Anwendungen eine generische Schnittstelle zur Nutzung von Telefoniediensten in Einzel- und Mehrplatzszenarien. Die Spezifikation umfasst Funktionen zur Abfrage und Steuerung von Telefonen, Verbindungen und Konferenzschaltungen sowie zur Behandlung von Kontaktcenter-spezifischen Aufgaben, wie zum Beispiel der Abfrage des Agentenstatus. Mithilfe dieses Funktionssatzes können von der einfachen Modemsteuerung bis hin zu komplexen Kontaktcenter-Anwendungen eine Vielzahl von CTI-Applikationen implementiert werden. Da TAPI nur eine Programmierschnittstelle darstellt, benötigt ein lauffähiges Programm einen sogenannten Internet Telephony Service Provider (ITSP). Dies ist eine Art Treiberprogramm, das die Funktionsaufrufe der CTI-Anwendung in Kommandos für das zu steuernde Gerät umsetzt. Dieses Treiberprogramm wird in der Regel vom Hersteller der TK-Anlage bzw. des zu steuernden Gerätes bereitgestellt, da praktisch jeder Hersteller sein eigenes Protokoll zur Verbindungskontrolle implementiert und diese proprietären Schnittstellen in der Regel auch nicht veröffentlicht werden. Ohne zusätzliche Maßnahmen ist die Vertraulichkeit und

Integrität der Daten, die über eine solche CTI-Verbindung transportiert werden, damit abhängig vom Hersteller bzw. vom Produkt. Eine ungesicherte CTI-Verbindung erlaubt u. a. das Mitlesen von Anrufdaten und sogar die Steuerung eines fremden Telefons, z. B. zur Initiierung eines Anrufs.

13.2.2.3 Telephony Server API (TSAPI) und Java Telephony API (JTAPI)

Vergleichbar mit TAPI stellen TSAPI und JTAPI ebenfalls Programmierschnittstellen bereit, die über spezielle Treiberkomponenten Funktionsaufrufe auf herstellerspezifische Protokolle umsetzen. Unterschiede zu TAPI bestehen hauptsächlich im angebotenen Funktionsumfang sowie im Einsatzgebiet. Unter anderem bietet TSAPI keine Unterstützung für First Party Call Control, da es primär für den Einsatz in Kontaktcenter-Umgebungen entwickelt wurde. JTAPI hingegen unterstützt sowohl Einzel- als auch Mehrplatzlösungen, wobei die CTI-Applikationen die Programmiersprache Java verwenden müssen. Da diese Schnittstellen wie TAPI einen Treiber benötigen, der die Kommunikation mit der TK-Anlage übernimmt, ist die Sicherheit der CTI-Verbindung auch hier herstellerabhängig.

13.2.2.4 Integration von Datenbanken und Verzeichnisdiensten

Zwei wichtige Schnittstellen für die Anbindung an IT-Systeme sind das Lightweight Directory Access Protocol (LDAP) und Open DataBase Connectivity (ODBC). Sie dienen der Anbindung von Verzeichnis-diensten und Datenbanken im Allgemeinen. Diese Art der Kopplung ist gerade bei UCC-Systemen sehr häufig vorzufinden, da Anwenderdaten und Adressinformationen aus einem Organisationsverzeichnis und einem Customer Relationship Management (CRM) in ein einheitliches Telefonbuch integriert oder Agentenarbeitsplätze in Kontaktcentern mit Kundendatenbanken und anderen IT-Systemen verbunden werden sollen. Beispielsweise kann über eine automatische Anruferidentifikation der passende Datensatz mit Kundendaten, Anrufhistorie, Vertragsdaten usw. aus einer Datenbank auf den Bildschirm gebracht werden. Die Anbindungen an solche Datenbanken erfolgt in der Regel über standardisierte Protokolle wie das bereits genannte LDAP bzw. über APIs wie ODBC. LDAP erlaubt die Abfrage und die Modifikation von Informationen eines Verzeichnisdienstes. ODBC ist eine standardisierte Datenbankschnittstelle, die SQL als Datenbanksprache verwendet. ODBC bietet also – vergleichbar mit TAPI – eine Programmierschnittstelle (API), die es einem Programmierer erlaubt, seine Anwendung relativ unabhängig vom verwendeten Datenbankmanagementsystem (DBMS) zu entwickeln, wenn dafür ein ODBC-Treiber existiert.

Ohne zusätzliche Maßnahmen ist die Vertraulichkeit und Integrität der Daten, die über eine ODBC-Verbindung transportiert werden, abhängig vom Hersteller des DBMS bzw. vom konkreten Produkt. LDAP hingegen sieht den Einsatz von TLS und SSL zur Authentisierung und Verschlüsselung vor.

Es sollte beachtet werden, dass ein spezifisches CTI-System noch eine Reihe weiterer Schnittstellen bieten kann, die hier nicht aufgeführt wurden. Beispiele hierfür sind die Verwendung des Protokolls SOAP[47], mit dessen Hilfe Daten zwischen Systemen ausgetauscht und entfernte Prozeduraufrufe (Remote Procedure Calls, RPCs) durchgeführt werden können, sowie Administrations-Schnittstellen. Es ist daher im Einzelfall mit dem Hersteller eines Systems zu klären, welche Schnittstellen vorhanden sind, welche für den Betrieb unter den gegebenen Anforderungen benötigt werden und welche gegebenenfalls deaktiviert werden können.

47 SOAP stand ursprünglich für Simple Object Access Protocol. Inzwischen wird der Begriff SOAP aber als Eigenname verwendet und steht nicht mehr für eine Abkürzung. SOAP ist ein Protokoll zum Austausch XML-basierter Nachrichten, über das insbesondere auch die Funktion eines Remote Procedure Call (RPC) realisiert werden kann. Die Extensible Markup Language (XML) ist eine vom World Wide Web Consortium (W3C) spezifizierte Auszeichnungssprache, die der formalen textuellen Beschreibung und Darstellung hierarchisch strukturierter Daten dient.

13.3 Grundlagen netzbasierter Sicherheitsmechanismen

In diesem Anhang werden spezielle technische Aspekte vertieft, die für die Absicherung von Telekommunikationssystemen eine besondere Rolle spielen:

- Kapitel 13.3.1 beschreibt Techniken für den Aufbau von Sicherheitszonen in einem Netzwerk.
- Kapitel 13.3.2 beschreibt die Port-basierte Authentisierung im LAN mit IEEE 802.1X.
- Kapitel 13.3.3 liefert Hinweise für die Verwendung von SSL/TLS.
- Kapitel 13.3.4 führt in die wesentlichen VPN-Techniken ein.

13.3.1 Techniken für den Aufbau von Sicherheitszonen

Allgemein stellt eine Sicherheitszone eine Gruppe von Endgeräten bzw. Servern dar, die aus Sicherheitsgründen von anderen Endgeräten bzw. Servern separiert wird und deren Kommunikation mit Endgeräten bzw. Servern außerhalb der Sicherheitszone kontrolliert werden soll.

Die Trennung einer Sicherheitszone von ihrer Umgebung erfolgt meist auf Ebene des Netzwerks. Hierfür wird der Übergang von und zu einer Sicherheitszone über eine Firewall gefiltert. Innerhalb einer Sicherheitszone wird die Kommunikation nicht eingeschränkt.

Abhängig von der Größe der einzurichtenden Sicherheitszone kommen typischerweise die folgenden Alternativen zur Realisierung einer Sicherheitszone in Betracht:

- Die zentralen Systeme einer Sicherheitszone können dabei zunächst einem einzelnen VLAN, d. h. IP-Subnetz, zugeordnet werden.

  Hierbei übernimmt die erste Layer-3-Komponente das Routing der Daten zu Kommunikationszielen außerhalb der eigenen Sicherheitszone. Dies ist typischerweise ein Layer-3-Switch (L3-Switch), der jedoch per Default alle Pakete automatisch zum Zielnetz weiterleitet. Soll dies vermieden werden, so muss ein entsprechender Filtermechanismus beispielsweise einer Firewall genutzt werden (siehe Abbildung 77).

  Sind auch Endgeräte Teil einer Sicherheitszone, muss die Firewall als erste Layer-3-Komponente im Kommunikationsweg alle Funktionen des Default Gateway für die Endgeräte übernehmen. Insbesondere ist hier ein DHCP-Relay einzurichten, das die DHCP-Pakete an die zentralen DHCP-Server weiterleitet. Hier tauchen in der Praxis häufig Probleme auf, da solche Funktionalitäten nicht zu den originären Aufgaben einer Firewall gehören.

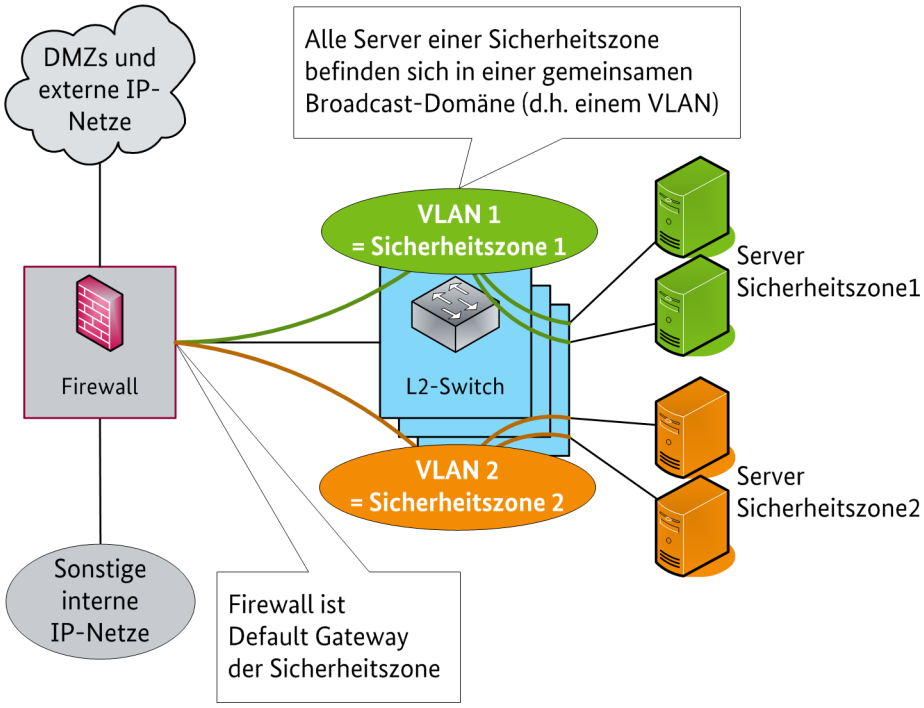


Abbildung 77: Aufbau von Sicherheitszonen mit VLAN

- Wenn mehrere VLANs, Layer-2-Switches (L2-Switches) bzw. IP-Subnetze einer Sicherheitszone zugeordnet werden sollen, muss die Netztrennung auf Layer 3 realisiert werden.

  In diesem Fall liegt immer eine Routing-Instanz innerhalb der Sicherheitszone, z. B. ein eigener L3-Switch im Fall einer physischen Trennung. Bei einer logischen Trennung kann mit virtuellen Routing-Instanzen über Virtual Routing and Forwarding (VRF) gearbeitet werden.

  Die Kombination aus VLANs und VRF-Instanzen ist eine in LANs übliche Technik zur logischen Trennung von Nutzergruppen (Best-Practice-Ansatz). VLANs realisieren hierbei eine logische Netztrennung auf Layer 2, die auf virtualisierten Layer-3-Komponenten via Virtual Routing and Forwarding (VRF) pro Sicherheitszone (Mandantengruppe) geroutet bzw. terminiert werden (siehe Abbildung 78).

  Eine Sicherheitszone erhält dabei eine eigene virtuelle Routing-Instanz (VRF-Instanz) auf jedem physischen Router bzw. Layer-3-Switch innerhalb der Sicherheitszone. Mehrere VRF-Instanzen einer Sicherheitszone sind typischerweise per VLAN miteinander vernetzt, um auf einer gemeinsamen Hardware verschiedene virtuelle Layer-3-Netze zu schaffen.

  Umfasst eine Sicherheitszone mehrere Layer-3-Switches, so werden die VLAN-Informationen der Sicherheitszone zwischen den Layer-3-Switches via VLAN-Tagging übertragen.

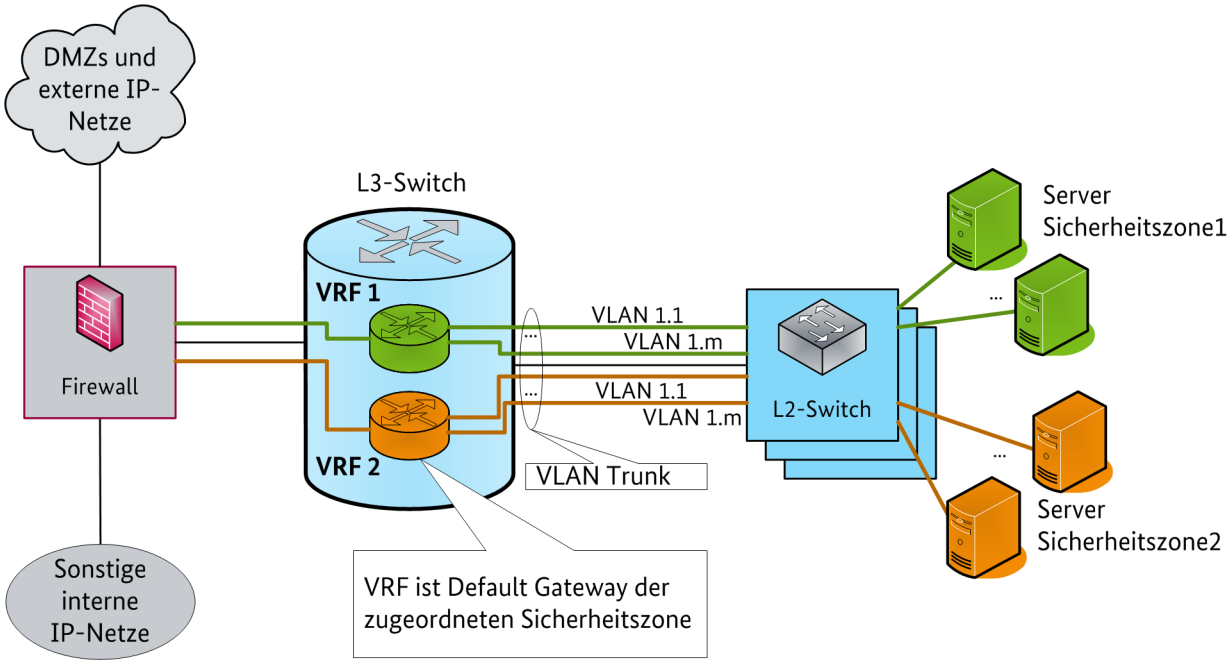


Abbildung 78: Aufbau von Sicherheitszonen mit VRF

Dieser Best-Practice-Ansatz mit VLANs und VRF-Instanzen wird beispielsweise auch durch die BSI IT-Grundschutz-Kataloge (siehe [BSI GSK-2013]) gestützt. Insbesondere können hier die für VLAN geltende

- Maßnahme M 2.277 „Funktionsweise eines Switches“ und
- Maßnahme M 5.153 „Planung des Netzes für virtuelle Infrastrukturen“

angewendet werden, die sich sinngemäß auf die Verwendung von VRF unmittelbar übertragen lassen. Somit ist die Realisierung von VLANs und VRF-Instanzen - flankiert durch zusätzliche Sicherheits-maßnahmen - zulässig, ebenso wie die Trennung von Nutzergruppen in virtualisierten Umgebungen. Für die virtualisierte Vernetzung kann auf etablierte Technik zurückgegriffen werden, die den individuellen Gegebenheiten einer Organisation angepasst werden kann.

Durch die beschriebenen Techniken für den Aufbau von Sicherheitszonen werden die meisten Nachteile alternativer Lösungen wie z. B. Sicherheitszonen auf Basis von MPLS oder MacSec behoben, insbesondere:

- Die Technik bedingt aufgrund der umfassenden Produktunterstützung und langjährigen Einsatzerfahrungen in der Regel weder ein Redesign des Netzes noch zusätzliche Investitionskosten für eine Organisation.
- Endgeräte innerhalb der Sicherheitszone können diese Zonen-VRF als Default Gateway nutzen. Die Layer-3-Komponenten sind für diesen Anwendungsfall konzipiert, sodass insbesondere Zusatzdienste wie DHCP-Relay stabil verfügbar sind.
- Die Layer-3-Komponenten realisieren das dynamische Routing meist in Hardware, sodass keinerlei Performance-Engpässe zu erwarten sind.
- Die Konfiguration und Administration von virtualisierten Netzkomponenten (Switches, Firewalls) unterscheidet sich meist nicht von den physischen Komponenten.
- Die Komplexität und der Betriebsaufwand für die beschriebene Lösung sind vergleichsweise gering, lediglich bei häufig hinzukommenden Mandanten/Sicherheitszonen muss eine Neukonfiguration vorgenommen werden.

13.3.2 Port-basierte Authentisierung im LAN mit IEEE 802.1X

Der Standard IEEE 802.1X (siehe [IEEE 802.1X-2010]) spezifiziert eine Methode zur Port-basierten Netzwerkzugangskontrolle für Ethernet nach IEEE 802.3 und WLAN nach IEEE 802.11. IEEE 802.1X definiert verschiedene Rollen der beteiligten Netzelemente (siehe Abbildung 79):

- Der Supplicant ist eine Software-Komponente im Endgerät (Client), die den Netzwerkzugang anfordert. Der Supplicant kann Bestandteil des Betriebssystems sein (sogenannter Native Supplicant).
- Das Gerät, das den Netzwerkzugang herstellt und eine Schnittstelle für die Authentisierung anbietet, heißt Authenticator. Im LAN liegt diese Funktion typischerweise in dem Switch, an den das Endgerät unmittelbar angeschlossen ist. Im WLAN wird diese Funktion vom Access Point bzw. WLAN-Controller wahrgenommen.
- Der Authentication-Server ist das Gerät, welches den eigentlichen Authentisierungsdienst bereitstellt. Der Authentication-Server ist typischerweise ein RADIUS-Server, jedoch legt der Standard IEEE 802.1X das Protokoll für den Authentication-Server nicht zwingend fest (siehe [IETF RFC2865-2000]).

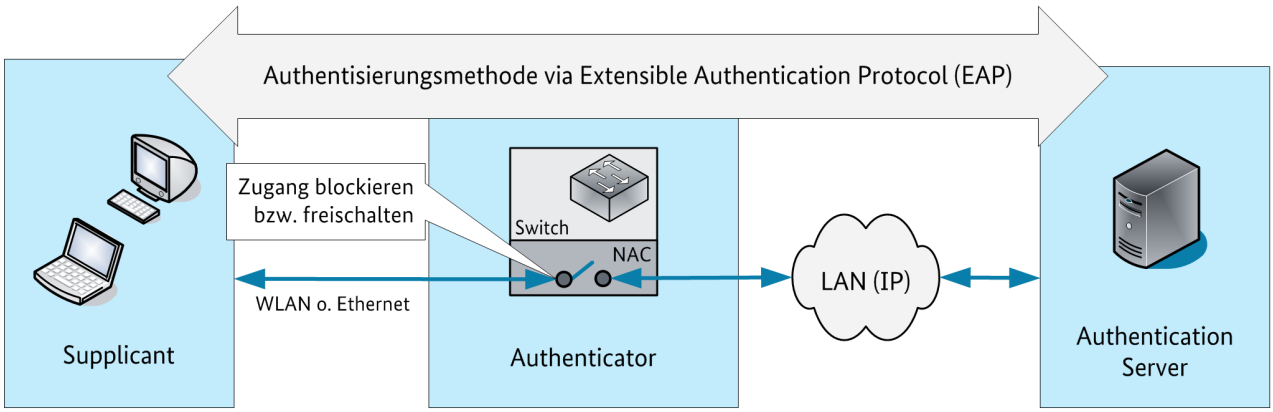


Abbildung 79: Rollen in IEEE 802.1X

Der Austausch der Authentisierungsinformationen geschieht über das Extensible Authentication Protocol (EAP, siehe [IETF RFC3748-2004] und [IETF RFC3579-2003]). Dabei erfolgt die Kommunikation über die LAN- bzw. WLAN-Schnittstelle zwischen Supplicant und Authenticator mit der Variante EAP over LAN (EAPOL). EAPOL gestattet die Übertragung von EAP-Nachrichten auf Layer 2. Auf diese Weise wird eine Authentisierung am Netzzugangspunkt ermöglicht, bevor eine Kommunikation auf IP-Ebene und höheren Protokollebenen stattfindet. Die Kommunikation zwischen Authenticator und Authentication-Server geschieht meist RADIUS-basiert, wobei die EAP-Nachrichten als RADIUS-Attribute übertragen werden. Für die Verwaltung der Daten der Geräte oder Nutzer, die sich mit IEEE 802.1X authentisieren, wird oft ein Verzeichnisdienst (Directory Service) wie z. B. LDAP verwendet, der vom RADIUS-Server angesprochen wird. Abbildung 80 zeigt die genutzten Protokolle im Überblick.

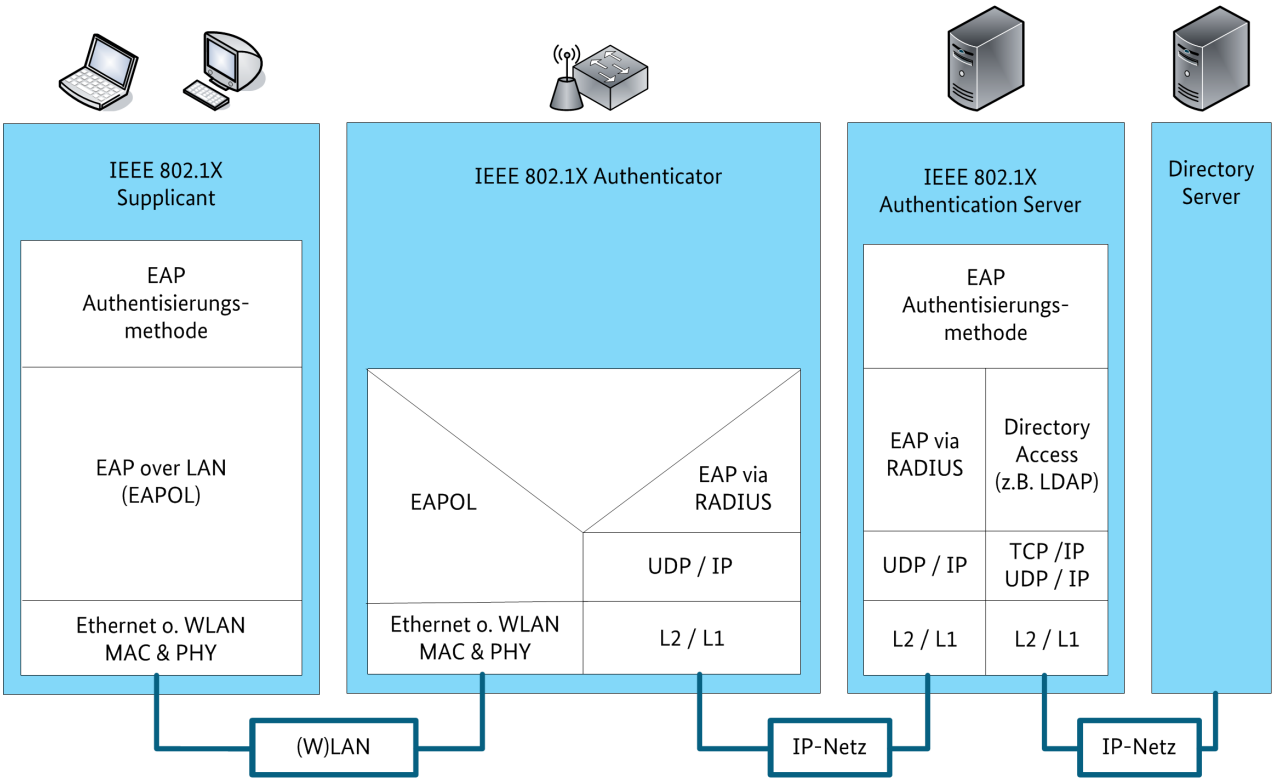


Abbildung 80: Protokolle in IEEE 802.1X

13.3.2.1 Authentisierungsmethoden

EAP ist modular und liefert einen Rahmen, in den die eigentlichen Authentisierungsverfahren, die sogenannten EAP-Methoden, eingebettet werden können. Damit EAP-Methoden für die Anwendung im WLAN geeignet sind, müssen sie zusätzlich auch die Möglichkeit der Erzeugung und Verteilung von Schlüsselmaterial für die in IEEE 802.11i spezifizierten Mechanismen bieten. Es gibt eine ganze Reihe von EAP-Methoden (siehe [IEEE 802.11-2012]).

Eine Auswahl der für die Absicherung von LAN und WLAN relevanten EAP-Methoden wird im Folgenden kurz beschrieben:

- EAP-TLS (siehe [IETF RFC5216-2008])

  Diese EAP-Methode basiert auf der Authentisierung gemäß Transport Layer Security (TLS). Es wird eine beidseitige Authentisierung anhand von X.509-Zertifikaten durchgeführt. Das bedeutet, dass eine Infrastruktur zur Verteilung und Verwaltung der Zertifikate (Ausstellung, Rückruf, Erneuerung usw.) benötigt wird.

  Bei EAP-TLS sendet der jeweils zu authentisierende Kommunikationspartner ein Zertifikat, das seinen öffentlichen Schlüssel enthält. Außerdem sendet er eine mit seinem privaten Schlüssel gebildete Signatur, sodass der Empfänger durch Anwendung des öffentlichen Schlüssels auf diese Signatur die Authentizität des Senders feststellen kann.

- EAP-TTLS (siehe [IETF RFC5281-2008])

  Bei EAP-TTLS (Tunneled TLS) wird die unter EAP-TLS beschriebene Methode nur zur Authentisierung des Servers genutzt. Anschließend wird ein TLS-Tunnel zwischen Server und Client aufgebaut, in dem dann geschützt die Authentisierung des Clients durch andere Methoden erfolgt, z. B. über Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) oder Microsoft Challenge Handshake Authentication Protocol (MSCHAP).

- PEAP (IETF Internet Draft)

  PEAP (Protected EAP) funktioniert ähnlich wie EAP-TTLS, es dürfen allerdings im Tunnelinneren nur EAP-Methoden zur Authentisierung des Clients angewendet werden. Ein Beispiel ist die Kombination von PEAP mit der EAP-Methode EAP-MSCHAPv2, die auf der oft bei Windows-Clients genutzten PPP-Authentisierungsmethode MSCHAPv2 basiert. Über EAP-MSCHAPv2 können die für eine Domänenanmeldung üblichen Abfragen von Nutzername und Passwort geschehen, sodass diese Methode gut zur Benutzerverwaltung in Windows-Lösungen passt.

EAP-TLS erreicht durch die direkte gegenseitige Authentisierung von Server und Client im Vergleich zu den anderen Verfahren ein höheres Sicherheitsniveau. Weiterhin ist EAP-TLS als RFC vergleichsweise solide spezifiziert.

13.3.2.2 Trennung von Nutzergruppen

Über IEEE 802.1X, genauer gesagt über das letzte RADIUS-Paket einer Authentisierungssequenz, kann ein VLAN Identifier (VID) vom RADIUS-Server an den Authenticator übertragen werden. Im kabelbasierten LAN setzt dann der Switch den Port, über den die Authentisierungssequenz erfolgt ist, in das entsprechende VLAN. Im WLAN wird vom Access Point bzw. vom WLAN-Controller die Kommunikation mit dem WLAN-Client, der sich authentisiert hat, dem vom RADIUS-Server angegebenen VLAN zugeordnet.

Der VID kann in der Konfiguration des RADIUS-Server pro Nutzergruppe festgelegt werden. Auf diese Weise können beispielsweise IP-Telefone dynamisch einem anderen Port zugewiesen werden als PCs, auch wenn sich beide Gerätetypen per IEEE 802.1X authentisieren würden.

Alternativ können zur Trennung von Nutzergruppen auch unterschiedliche ACLs auf den Access Switches oder Access Point bzw. WLAN-Controller genutzt werden. In Abhängigkeit der Authentisierung, d. h. Gruppenzugehörigkeit und Authentisierungsergebnis, wird dem Port eine passende ACL dynamisch zugewiesen. Nach erfolgreicher Authentisierung wird die zunächst angewendete Default-Policy-ACL durch eine der angemeldeten Gerätegruppe entsprechenden ACL ersetzt.

13.3.2.3 Multiuser-Authentisierung

Der Standard IEEE 802.1X geht explizit davon aus, dass an einem Ethernet-Port, an dem eine Authentisierung per IEEE 802.1X erfolgen soll, genau ein Gerät mit einer Supplicant-Funktion angeschlossen wird.

Die simultane Authentisierung mehrerer Geräte an einem Port knüpft der Standard an den Aufbau sicherer Kanäle und verweist auf WLAN nach IEEE 802.11i. Hier wird nach erfolgreicher Authentisierung zwischen einem WLAN-Client und einem Access Point ein dedizierter verschlüsselter Kanal etabliert, der damit einer logischen Punkt-zu-Punkt-Verbindung entspricht. Die Authentisierung mehrerer Supplicants über einen Hub oder einen Mini-Switch an einem einzelnen Port wird im Standard nicht spezifiziert.

Kaskadierter Anschluss von PCs und IP-Telefonen

Dies ist beim Einsatz von IP-Telefonen zu beachten, da diese Telefone oft mit einem eingebauten Ethernet Switch ausgestattet sind, über den ein PC unmittelbar an das IP-Telefon angeschlossen werden kann. Auf diese Weise spart man Ethernet-Anschlussdosen. Manche Hersteller gestatten die simultane Authentisierung von IP-Telefon und PC an einem Port des Access Switches (auch als Multiuser-Authentisierung bezeichnet). Dies ist aber keine im Standard IEEE 802.1X vorgesehene Betriebsart und stellt eine herstellerspezifische Lösung dar.

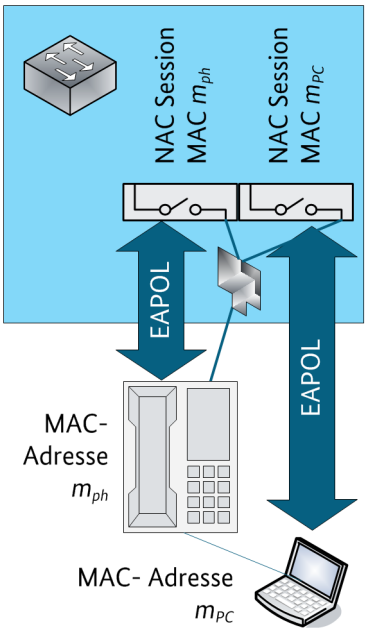


Abbildung 81: Simultane Authentisierung mehrerer Endgeräte an einem Netzwerk-Port

Weiterhin erlaubt der Standard IEEE 802.1X nicht die Übertragung von EAPOL über Pakete mit VLAN-Tag gemäß IEEE 802.1Q (siehe [IEEE 802.1Q-2011]). Diese Funktion wäre aber erforderlich, wenn der Kommunikationsverkehr eines IP-Telefon und eines an das IP-Telefon angeschlossenen PCs über unterschiedliche VLANs getrennt werden soll. Manche Hersteller unterstützen speziell für diesen Zweck die Konfiguration von zwei VLANs an einem Access-Port: einem Voice-VLAN, das mit einem VLAN-Tag übertragen wird, und einem Daten-VLAN ohne VLAN-Tag. Für die Authentisierung des IP-Telefons muss dann IEEE 802.1X herstellerspezifisch angepasst werden.

IEEE 802.1X gestattet aber auch eine kaskadierte Authentisierung, bei der ein Switch sich bei einem anderen Switch authentisiert, d. h. einen Supplicant implementiert und sich andererseits wie gewohnt als Authenticator anderen Supplicants gegenüber verhält.

Virtuelle Maschinen auf Clients

Wenn Clients mit Virtuellen Maschinen (VMs) und virtuellen MAC-Adressen verwendet werden, können am Switch-Port, an dem das Endgerät angeschlossen ist, mehrere MAC-Adressen vorliegen, obwohl nur ein einzelnes physisches Gerät vorhanden ist. Aus dem Blickwinkel des Switches ist der Fall einer Multiuser-Authentisierung gegeben.

In diesem Fall muss für IEEE 802.1X eine spezielle, herstellerspezifische Konfiguration vorgenommen werden, bei der in vielen Fällen keine dynamische VLAN-Zuweisung per RADIUS möglich ist.

Weiterhin limitieren Switch-Hersteller aufgrund der Speicheranforderungen die maximale Anzahl der simultanen NAC-Sitzungen an einem Netzwerk-Port (z. B. auf 32 Sitzungen).

13.3.2.4 Mischbetrieb

Manche der verfügbaren IP-Telefone unterstützen noch kein IEEE 802.1X. Eine Zugangskontrolle zum LAN kann dann praktisch nur über die MAC-Adresse des IP-Telefons erfolgen (sogenannte MAC-Adress-Authentisierung). Dabei prüft der Access Switch, ob die MAC-Adresse bekannt ist und einem IP-Telefon zugeordnet werden kann. Ist die Prüfung positiv, werden Pakete von und zu der MAC-Adresse vom Switch weitergeleitet, d. h. das Gerät erhält einen Netzzugang.

Da jeder Ethernet- oder WLAN-Adapter mit einer beliebigen MAC-Adresse konfiguriert werden kann[48], bietet diese Methode der Authentisierung nur einen ausgesprochen geringen Schutz. Außerdem ist eine MAC-Adress-Authentisierung herstellerspezifisch. Viele Switches und praktisch alle Access Points und WLAN-Controller unterstützen eine RADIUS-basierte Authentisierung einer MAC-Adresse.

Sofern der Schutzbedarf es zulässt, kann in Kombination mit IEEE 802.1X die MAC-Adress-Authentisierung in der Migrationsphase für Geräte, die (noch) kein IEEE 802.1X unterstützen, eingesetzt werden. Dabei ist wesentlich, dass Geräte, die sich per MAC-Adresse authentisieren, einen eingeschränkten und kontrollierten Zugang erhalten. Weiterhin muss der Netzverkehr dieser Geräte von den Geräten, die sich per IEEE 802.1X authentisieren, getrennt werden.

Hierzu unterstützen viele Hersteller von Switches eine gestufte Authentisierung (siehe Abbildung 82), die eine einheitliche Port-Konfiguration gestattet. In der Regel versucht dabei ein Port zunächst ein angeschlossenes Gerät per IEEE 802.1X zu authentisieren. Ist die Authentisierung mit IEEE 802.1X erfolgreich, wird der Port einem VLAN für autorisierte Endgeräte zugeordnet. Antwortet das Gerät nicht, wird die MAC-Adresse geprüft. Ist die MAC-Adresse bekannt, wird der Port in ein anderes - mit einem eingeschränkten Zugang verbundenes - VLAN gesetzt. Ist die MAC-Adresse unbekannt, kann entweder die Kommunikation abgewiesen werden oder das Gerät kommt in ein isoliertes VLAN, über das z. B. ein Gastzugang ermöglicht werden kann.

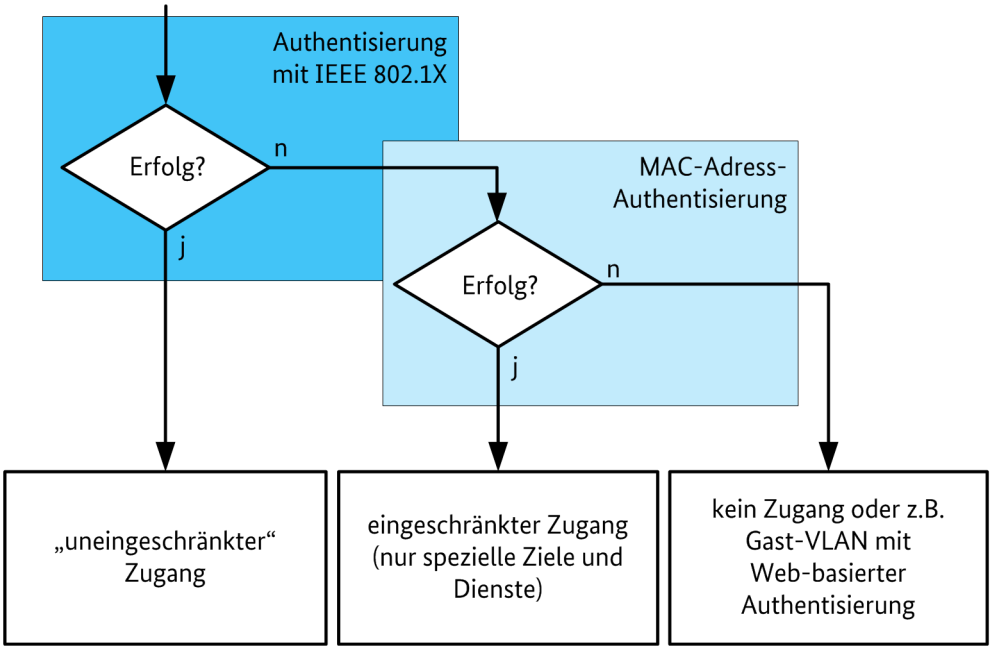


Abbildung 82: Mischbetrieb mit gestufter Authentisierung

13.3.2.5 Grundsätzliche Schwächen von IEEE 802.1X

Über IEEE 802.1X ist die Authentisierung eines Systems bzw. eines Nutzers am System möglich. Es erfolgt aber keine Authentisierung der über einen autorisierten Port übertragenen Pakete eines Endgerätes. Es findet insbesondere keine Prüfung statt, ob die Pakete auch tatsächlich von dem Gerät stammen, auf dem der Supplicant, der sich authentisiert hat, läuft.

Ein Angreifer könnte unter der MAC-Adresse eines authentisierten Supplicant einen Dialog mit der Infrastruktur führen, solange der Port autorisiert ist.

48 Jeder Adapter verfügt zwar über eine eindeutige in der Hardware festgelegte MAC-Adresse (sogenannte Burned-in Address), verwendet aber eine RAM-Kopie dieser Adresse, die durch einen Treiber-Befehl einfach mit einer anderen frei gewählten Adresse überschrieben werden kann.

Die Zusicherung von Vertraulichkeit und Integrität der über einen autorisierten Port übertragenen Pakete ist aber nicht Aufgabe eines Authentisierungsverfahrens wie IEEE 802.1X. Hierzu muss die Sicherheitsarchitektur um eine Komponente für Verschlüsselung und Integritätsprüfung erweitert werden. Für die verbindungslose Kommunikation in LAN/MAN werden diese Mechanismen in dem seit August 2006 verabschiedeten Standard IEEE 802.1AE beschrieben (siehe [IEEE 802.1AE-2006]). Für das hierzu notwendige Schlüsselmanagement und den Aufbau von Security Associations wurde in IEEE 802.1af als eine Erweiterung von IEEE 802.1X spezifiziert (siehe [IEEE 802.1X-2010]). IEEE 802.1X-2010 und IEEE 802.1AE bilden zusammen für das kabelbasierte LAN das konzeptionelle Pendant zur Absicherung von WLAN mit IEEE 802.11i (siehe Abbildung 83).

Daher muss aktuell für einen Einsatz von IEEE 802.1X das Restrisiko durch Schwächen in der Zusicherung von Vertraulichkeit und Integrität berücksichtigt werden. Für den normalen Schutzbedarf kann der Einsatz von IEEE 802.1X ausreichen. Für einen erhöhten Schutzbedarf sollten jedoch zusätzlich VPN-Mechanismen oder Verschlüsselung und Integritätsprüfung auf Anwendungsbasis oder (wenn verfügbar) IEEE 802.1AE genutzt werden.

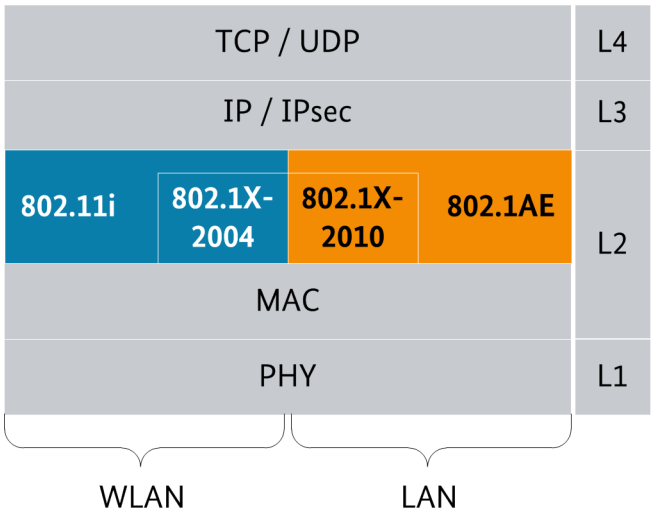


Abbildung 83: Absicherung der Kommunikation auf Layer 2

13.3.3 Hinweise für die Verwendung von SSL/TLS

Das ursprünglich von Netscape entwickelte Secure Sockets Layer (SSL) ist ein Protokoll für Datenübertragungen via TCP/IP, das die Vertraulichkeit und Integrität der Verbindung durch Verschlüsselung und Authentisierung absichert.

Die erste veröffentliche Version war SSL 2.0 im Jahr 1994. Aufgrund diverser Sicherheitslücken wurde 1996 eine verbesserte Version SSL 3.0 veröffentlicht, die als Grundlage für eine standardisierte Version von SSL diente: Transport Layer Security (TLS). TLS 1.0 wird dabei intern auch als SSL 3.1 bezeichnet.

Derzeit ist die TLS-Version 1.2 (siehe [IETF RFC5246-2008]) standardisiert.

TLS wird häufig im Bereich sicherer Webtransaktionen verwendet. TLS ist jedoch nicht auf Webtransaktionen und damit auf das HTTP-Protokoll beschränkt, da es im TCP/IP-Referenzmodell zwischen Transportschicht und den eigentlichen Anwendungen liegt (siehe Abbildung 84).

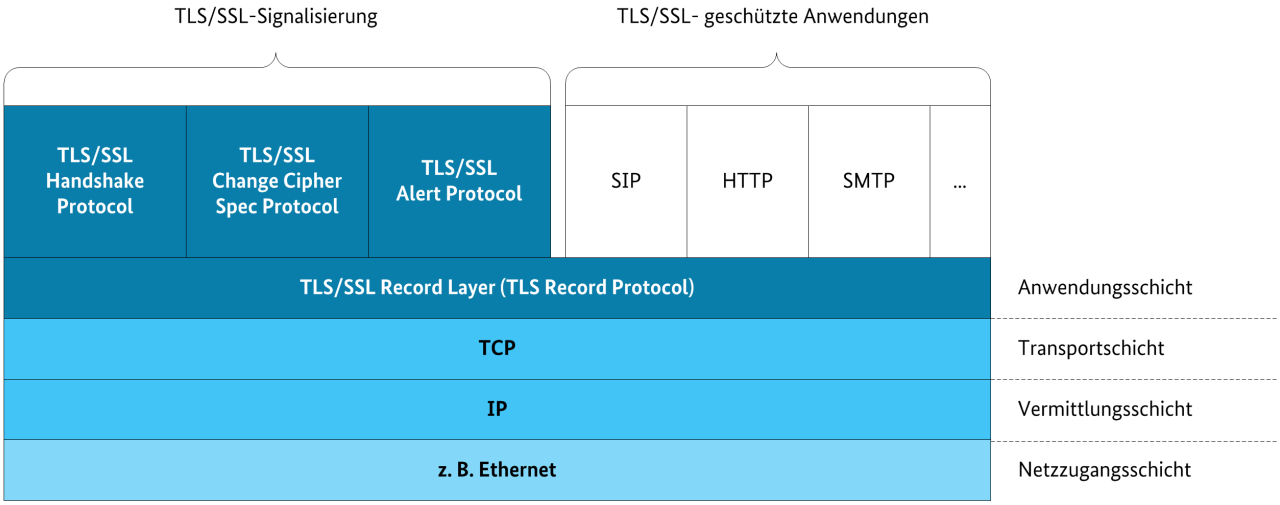


Abbildung 84: Einordnung von TLS/SSL in das TCP/IP-Referenzmodell

TLS wird zur Sicherung von TCP-Strömen verwendet. Seit April 2006 steht mit DTLS 1.2 (Datagram TLS, siehe [IETF RFC6347-2012]) auch eine standardisierte Variante für UDP zur Verfügung, die auf TLS 1.2 basiert. DTLS wird damit den Anforderungen im Bereich der Echtzeitkommunikation und insbesondere der IP-Telefonie gerecht, bei der eine minimale Verzögerung gefordert wird.

DTLS unterscheidet sich von TLS in den Bereichen, in denen sich der unzuverlässige UDP-Transport auswirkt. Dies beinhaltet unter anderem die folgenden Punkte:

- Durch die Möglichkeit von Neuübertragungen sorgt DTLS für die Zuverlässigkeit des initialen Handshake zur Authentisierung und zum Schlüsselaustausch. Bei TLS ist dies nicht notwendig, da bei Paketverlusten TCP automatisch für die Wiederholung sorgt.
- DTLS nummeriert die übertragenen Pakete, damit bei einem Paketverlust nicht auf eine Integritätsverletzung (wie es bei TLS der Fall wäre) geschlossen wird.

Nachfolgend werden Empfehlungen für den sicheren Umgang mit SSL/TLS gegeben. Dabei handelt es sich um allgemeine Empfehlungen, die je nach Anwendung und Schutzbedarf eine genauere Betrachtung erfordern.

13.3.3.1 Verwenden von TLS oder SSL

In der Regel unterstützen die Produkte unterschiedliche Versionen von SSL bzw. TLS. Neben dem aktuellen IETF-Standard TLS werden teilweise auch noch die von Netscape entwickelten Versionen SSL 2.0 und SSL 3.0 angeboten.

Aufgrund diverser Sicherheitslücken in den SSL-Versionen 2.0 und 3.0 wird dringend empfohlen, diese Versionen zu deaktivieren.

Microsoft hat die Lücken der SSL-Version 2.0 in ihrem proprietären Private Communications Technology (PCT) zwar behoben, allerdings gilt PCT als veraltet und ist zudem nicht weit verbreitet. Sofern Microsoft-Produkte zum Einsatz kommen, sollte darauf geachtet werden, dass PCT deaktiviert ist und alle relevanten Sicherheits-Updates eingespielt sind[49].

Aus den genannten Gründen wird der Einsatz von TLS in der jeweils aktuellen Version empfohlen. Aktuell wird TLS in der Version 1.2 von nahezu allen gängigen Browsern unterstützt, muss jedoch gegebenenfalls noch manuell aktiviert werden. Anders sieht es allerdings auf Anwendungsebene in Bezug auf TK- und UCC-Systeme aus, hier wird TLS 1.2 in den aktuellen Release-Ständen kaum bis gar nicht unterstützt. Einige Hersteller planen die Unterstützung für kommende Releases, jedoch ist damit nicht garantiert, dass auch eine Implementierung für die jetzigen Software-Stände per Update folgt.

49 Siehe http://www.kb.cert.org/vuls/id/586540

Gemäß der Technischen Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ des BSI (siehe [BSI TRKrypto-2013]) sollte wenn möglich TLS 1.2 verwendet werden. Hierbei ist jedoch die in TLS 1.2 eingeführte TLS Compression zu deaktivieren, da sonst ein Angriff durch den sogenannten CRIME Exploit (Compression Ratio Info-leak Made Easy) möglich ist. Sofern TLS 1.2 nicht verfügbar ist, können die älteren Versionen in der Übergangszeit weiter genutzt werden, jedoch sind hier ältere und damit eventuell unsichere Kryptoalgorithmen zu vermeiden und gegebenenfalls zusätzliche Schutzmaßnahmen nötig.

Es ist grundsätzlich nie ausgeschlossen, dass durch Design- und Implementierungsfehler signifikante Sicherheitslücken entstehen, die auch qualitativ hochwertige Verfahren kompromittieren können. Ein Beispiel ist der Heartbleed-Bug, der durch einen Programmfehler in der Heartbeat-Erweiterung von OpenSSL das unautorisierte Auslesen von sensitiven Daten ermöglichte (siehe [BSI HBbug-2014]). Hierbei handelte es sich um einen im Grunde simplen Programmierfehler (sog. Buffer over-read, bei dem ein Angreifer über die Grenzen eines Puffers hinaus auf Daten zugreifen kann), der jedoch als GAU in der IT-Sicherheit angesehen werden kann: Der Heartbleed-Bug kompromittierte die sichere Datenübertragung, blieb zwei Jahre unentdeckt und hinterließ bei einem Angriff keine Spuren[50].

13.3.3.2 Technische Absicherung des privaten Schlüssels

Während der öffentliche Schlüssel keinen Sicherheitsanforderungen unterliegt, sind für den privaten Schlüssel angemessene Sicherheitsvorkehrungen zu treffen.

Neben der physischen Sicherung des Systems ist eine grundlegende Maßnahme auf Betriebssystemebene die Vergabe restriktiver Zugriffsrechte für den privaten Schlüssel. Diese sollten so eingestellt werden, dass ein unbefugtes Auslesen des Schlüssels verhindert wird.

Zusätzlich kann der private Schlüssel verschlüsselt abgelegt werden, sofern dies nicht automatisch durch die jeweilige Applikation geschieht. Der Zugriff auf den privaten Schlüssel kann in diesem Fall nur nach einer entsprechenden Authentisierung erfolgen. Sofern Passwörter für die Authentisierung verwendet werden, gelten die Regeln zum Passwortgebrauch der IT-Grundschutz-Kataloge des BSI.

In der Regel ist für die Authentisierung ein manuelles Eingreifen notwendig, sodass sich diese Maßnahme nicht für Umgebungen eignet, in denen ein automatisches Starten des Systems bzw. des Dienstes erforderlich ist.

Vorausgesetzt der private Schlüssel ist durch weitere Maßnahmen wie beispielsweise eine Verschlüsselung geschützt, kommt es im Fall einer Kompromittierung des Systems (z. B. eines Servers) nicht zwangsläufig zu einer Kompromittierung des Zertifikats. Allerdings muss beachtet werden, dass der Angreifer je nach Berechtigungsstufe im Betriebssystem den Zugriff auf den privaten Schlüssel anderweitig erlangen kann, direkt oder indirekt, beispielsweise durch das Auslesen des Arbeitsspeichers oder das Abfangen eines Passwortes durch einen Keylogger.

Aus Sicherheitsgründen ist es daher nach einer Kompromittierung des Systems notwendig, die mit dem System verbundenen Zertifikate schnellstmöglich widerrufen zu lassen.

13.3.3.3 Als sicher geltende Cipher-Suite

Für SSL/TLS stehen verschiedene Kombinationen aus Schlüsselaustauschverfahren, Verschlüsselungsmethode und Nachrichtenauthentisierung zur Verfügung. Diese ergeben zusammen die sogenannte Cipher-Suite. Aufgrund der eingesetzten kryptografischen Verfahren unterschieden sich diese in Bezug auf die gewährleistete Sicherheit.

50 Das U.S. Government Repository of Standards based Vulnerability Management Data führt den Heartbleed-Bug unter der Bezeichnung CVE-2012-0160 in seiner Datenbank (National Vulnerability Database, NVD), die als Quelle für Fehlererkennung mit Vulnerability-Analysis-Systemen dient (siehe [NIST NVD160-2014]).

Abbildung 85: Namenskonvention für die Bezeichnung der unterschiedlichen Cipher-Suites

Nachfolgend werden gemäß der Technischen Richtlinie TR-02102 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ des BSI (siehe [BSI TRKrypto-2013]) für die verschiedenen Komponenten – Schlüsselaustausch, Verschlüsselungsmethode und Nachrichtenauthentisierung – geeignete Algorithmen aufgeführt.

13.3.3.3.1 Schlüsselaustausch und Authentisierung

Für den Schlüsselaustausch eignen sich die folgenden Verfahren:

- RSA-Verfahren
- Diffie-Hellman-Verfahren (DH)
- Eliptic-Curve-Diffie-Hellman-Verfahren (ECDH)

Zur Authentisierung können ebenfalls verschiedene Verfahren genutzt werden, unter anderem RSA oder der Digital Signature Algorithm (DSA) aus dem zugehörigen Digital Signature Standard der US-Regierung. Dieser ist spezifiziert in FIPS 186, aktuell in der Version 186-4 (siehe [NIST FIPS186-2013]). Ferner kann auch die Übertragung auf elliptische Kurven des DSA, also der Elliptic Curve Digital Signature Algorithm (ECDSA) genutzt werden.

Eine Auflistung der empfohlenen Kombinationen ist in der Technischen Richtlinie TR-02102 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ des BSI (siehe [BSI TRKrypto-2013]) zu finden.

13.3.3.3.2 Verschlüsselungsmethode

Als Verschlüsselungsmethode hat sich aktuell der Advanced Encryption Standard (AES) durchgesetzt. In älteren Versionen der TLS waren noch weitere Methoden verfügbar:

- Triple Data Encryption Standard (3DES, auch als TDES bezeichnet)
- RC4 („Ron's Code 4“, 1987 von Ronald L. Rivest entwickelt)
- International Data Encryption Algorithm (IDEA)

Jedoch sind diese mittlerweile nicht mehr sicher und daher seit [IETF RFC5469-2009] nicht mehr für den Einsatz mit TLS 1.2 empfohlen. Des weiteren sollte auch beim Einsatz von TLS 1.0 oder TLS 1.1 auf die oben genannten Verfahren verzichtet werden und stattdessen der AES eingesetzt werden.

In Bezug auf die Schlüssellänge gilt bei AES folgende Empfehlung: mindestens 128 Bit. Wenn möglich, sollte die Schlüssellänge jedoch bei 192 oder 256 Bit liegen.

Die Integrität und Authentizität einer Nachricht wird über einen sogenannten (Keyed-)Hash Message Authentication Code (HMAC) sichergestellt. Der HMAC berechnet sich hierbei aus dem Hash-Wert der Verknüpfung eines geheimen Schlüssels mit einer Klartextnachricht.

Aktuell gelten die Hash-Funktionen des Secure Hash Algorithm (SHA) als sicher, jedoch mit folgenden Einschränkungen:

- SHA-1 kann noch übergangsweise genutzt werden, sollte aber möglichst durch SHA-2 ersetzt werden.
- Nach 2015 sollten nur noch SHA-256, SHA-384, SHA-512 oder SHA-512/256 eingesetzt werden.

Die empfohlenen Kombinationen der oben genannten Methoden (Schlüsselaustausch, Verschlüsselung und Hash-Funktion können der Technischen Richtlinie TR-02102 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ des BSI (siehe [BSI TRKrypto-2013]) entnommen werden und werden daher hier nicht zusätzlich aufgelistet.

13.3.3.4 Validieren des Zertifikats

Bei der Verwendung von Zertifikaten sollte deren Korrektheit überprüft werden. Allgemein sind dabei folgende Punkte zu beachten:

- Der im Zertifikat genannte Name sollte mit dem DNS-Namen des Servers (allgemein des Gerätes) übereinstimmen, mit dem eine SSL/TLS-Verbindung hergestellt werden soll.
- Die Abfrage von Zertifikatssperrlisten (engl. Certificate Revocation List, CRL), d. h. Listen widerrufener Zertifikate, sollte möglichst genutzt werden. Diese Sperrlisten können entweder statisch oder dynamisch zur Verfügung stehen (z. B. via LDAP oder HTTP). Sofern das Online Certificate Status Protocol (OCSP) unterstützt wird, ist dieses den Sperrlisten vorzuziehen, da die Abfragen in Echtzeit erfolgen und zusätzlich gefälschte von nicht gesperrten Zertifikaten unterschieden werden können. OCSP kann auch mit herkömmlichen Sperrlisten nach CRL-Standard kombiniert werden.
- Das Ablaufdatum der Zertifikate sollte bei jeder Verwendung überprüft werden. Dies gilt auch für die Zertifikatskette einschließlich des Wurzelzertifikats (engl. Root Certificate). Abgelaufene Zertifikate gelten dabei als nicht länger vertrauenswürdig und ein Verbindungsaufbau sollte dementsprechend nicht durchgeführt werden. Das Ablaufdatum kann durch entsprechende Netzwerküberwachungs-dienste automatisiert überwacht werden. Vor Ablauf des Zertifikats kann entsprechend eine Benachrichtigung erfolgen, sodass eine frühzeitige Erneuerung beantragt werden kann.

13.3.3.5 Beidseitige Authentisierung

Im Regelfall wird eine SSL/TLS-basierte Authentisierung nur einseitig durchgeführt, d. h. der Server authentisiert sich gegenüber dem Client. Für den erhöhten Schutzbedarf und bei Server-zu-Server-Verbindungen sollte jedoch eine beidseitige Authentisierung erfolgen, auch bekannt unter dem Namen Mutual TLS (MTLS).

13.3.3.6 Nicht benötigte Root-Zertifikate

Aufgrund der besonderen Vertrauensstellung zu einer Zertifizierungsstelle innerhalb einer PKI sollten nur die benötigten Root-Zertifikate eingebunden werden, alle weiteren Root-Zertifikate sollte man entfernen. Wird zu einem späteren Zeitpunkt ein solches Zertifikat benötigt, kann dieses entsprechend importiert werden. Hierfür sind die Hinweise bezüglich des Imports von Zertifikaten zu beachten.

13.3.3.7 Zertifikatsimport

Für den Import der Zertifikate gilt es insbesondere den Fingerabdruck (engl. Fingerprint) sorgfältig zu prüfen, da dieser die Korrektheit des Zertifikats sicherstellen soll. In der Praxis finden sich häufig zwei Fingerabdrücke, die mit unterschiedlichen Hash-Funktionen gebildet werden; üblich sind ein SHA-1- und ein MD5-Fingerabdruck.

Der Fingerabdruck sollte dabei über einen anderen Kanal als das Zertifikat übertragen werden, um Manipulationsversuche zu verhindern. Dabei wird empfohlen, dass der Kanal durch kryptografische Verfahren gesichert ist (Beispiel: PGP-verschlüsselte E-Mail).

13.3.4 VPN-Techniken

13.3.4.1 Begriffsklärung

Der Begriff des Virtual Private Network (VPN) deutet bereits auf die wesentlichen Eigenschaften eines VPN hin: VPN sind privat und virtuell.

„Privat“ bedeutet in diesem Zusammenhang, dass ein solches Netzwerk von anderen Netzen durch geeignete technische Maßnahmen separiert ist. Somit können Kommunikationsverbindungen auf der Basis von VPN-Techniken in der gleichen Weise genutzt werden wie eigene, exklusiv genutzte physikalische Leitungen wie z. B. Fest- oder Wählverbindungen. In derartigen privaten Netzen kann eine völlig unabhängige Administration des Netzes erfolgen; so kann z. B. die Netzadresse selbst gewählt und deren Struktur ohne weitere Rücksprache mit den Betreibern anderer Netze festgelegt werden.

Gleichzeitig ist dieses private Netz jedoch nur „virtuell“ vorhanden, da die zugrunde liegende physikalische Netzinfrastruktur in Wirklichkeit nicht exklusiv, sondern von mehreren solchen Netzen gemeinsam genutzt wird.

VPN werden zur Abbildung verschiedener Szenarien genutzt, die sich lediglich durch die zu nutzenden Endpunkte der VPN-Verbindung unterscheiden (siehe Abbildung 86):

- Site-to-Site-VPN

  Ein Site-to-Site-VPN verbindet zwei LANs über ein unsicheres Trägernetzwerk miteinander, beispielsweise kann so eine sichere LAN-ähnliche Verbindung zwischen einer Außenstelle einer Organisation und der Hauptstelle geschaffen werden.

- End-to-Site-VPN oder Client-to-Site-VPN

  Häufigster Einsatzfall für End-to-Site-VPNs ist die sichere Anbindung von Mitarbeitern im Home-Office und von mobilen Nutzern, die aus fremden Gastumgebungen (Hotel-WLAN, Flughafen-Hotspot usw.) auf vernetzte interne Angebote einer Organisation zugreifen sollen.

- End-to-End-VPN oder Host-to-Host-VPN

  Mittels End-to-End-VPN bauen zwei Endgeräte direkt miteinander eine VPN-Verbindung auf. Ein typischer Einsatzfall ist die sichere Verbindung von zwei Servern über ein unsicheres Trägernetzwerk.

Diese unterschiedlichen VPN-Szenarien können mit den im Folgenden beschriebenen Techniken realisiert werden:

- IPsec-basierte VPN (kurz IPsec-VPN) setzen das Vorhandensein einer zugrunde liegenden Netzinfrastruktur auf Basis des Internet Protocol (IP) voraus. Diese reale Netzinfrastruktur dient als Trägernetz für alle darauf abgebildeten virtuellen Netze. Die bereits erwähnte Abschottung solcher VPNs gegeneinander erfolgt dabei durch Verwendung von Tunnel-Verfahren.
- TLS-basierte VPN (kurz TLS-VPN, ursprünglich SSL-VPN) nutzen als zugrunde liegende Infrastruktur grundsätzlich das Internet. Die das VPN bildenden Tunnel werden auf der Basis eines Standard-Browsers realisiert und je nach zu nutzender Applikation durch Plug-ins ergänzt.

Wesentliche Vorteile von VPNs sind Synergien bei der Nutzung des Trägernetzes und insbesondere die Möglichkeit, durch Verwendung entsprechender Tunnelverfahren ansonsten im Trägernetz nicht vorhandene Sicherheitsmechanismen bereitzustellen.

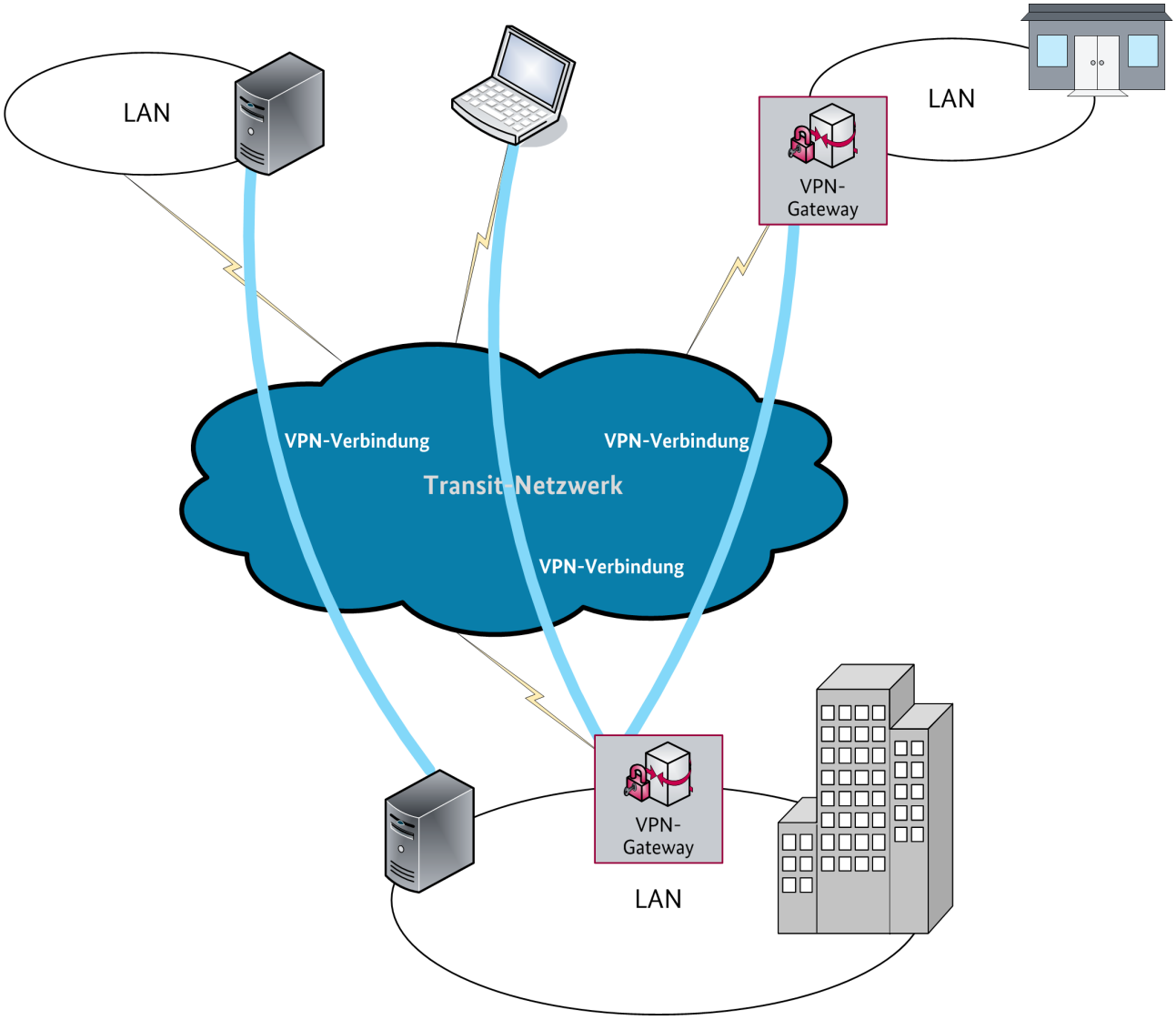


Abbildung 86: VPN-Szenarien

13.3.4.2 Tunneling

13.3.4.2.1 Tunnel-Prinzip

Tunneling beschreibt eine Methode, Daten eines Netzprotokolls A mit Hilfe eines anderen Netzprotokolls B durch ein Netzwerk zu transportieren. Dabei bildet das Datenpaket des Protokolls A die Nutzlast (engl. Payload) des Protokolls B, d. h. der Datenteil des Protokolls B enthält das vollständige Paket des Protokolls A. Aus Sicht von an diesem Vorgang unbeteiligten Komponenten, die auf Basis des Netzprotokolls B arbeiten, ist der Tunnelanfang der Absender und das Tunnelende der Empfänger dieses Pakets.

Das Grundprinzip ist in Abbildung 87 illustriert. Das Datenpaket des Protokolls A, d. h. die Payload wird innerhalb des Tunnels in ein Paket des Protokolls B gekapselt.

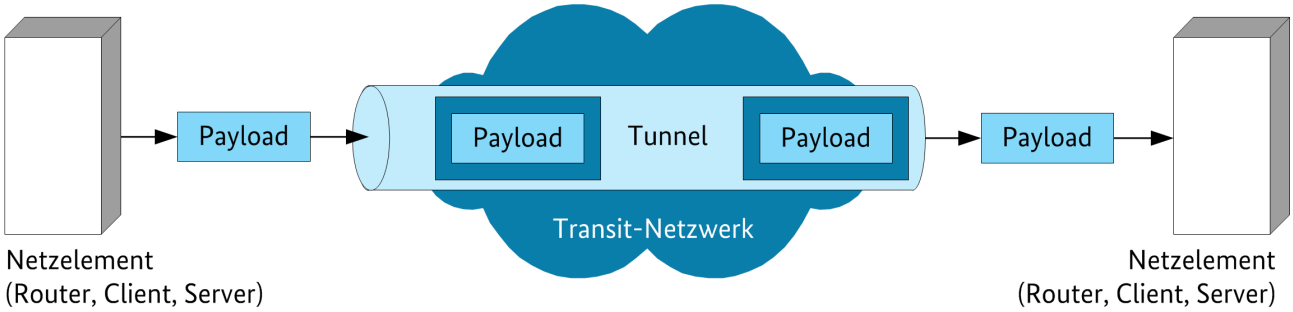


Abbildung 87: Prinzip des Tunneling

Folgender Ablauf ist allen Tunnelverfahren gemeinsam:

Die Netzsysteme TA (Tunnelanfang) und TE (Tunnelende) unterstützen sowohl Protokoll A als auch Protokoll B. TA ist so konfiguriert, dass Datenpakete des Protokolls A für bestimmte Ziele durch einen Protokoll-B-Tunnel zu TE transportiert werden. Empfängt TA ein zu tunnelndes Paket, so erzeugt das Netzsystem ein Paket des Protokolls B mit TA als Absender, TE als Empfänger und dem ursprünglichen Paket als Datenteil; dieses Paket wird auf Basis des Protokolls B zu TE transportiert. TE entfernt alle hinzugefügten Header und sendet das wiederhergestellte Paket des Protokolls A an das ursprüngliche Ziel.

Dieser Tunneling-Mechanismus funktioniert auch mehrmals hintereinander, d. h. es sind auch ineinander geschachtelte Tunnel möglich.

Für VPNs in IP-basierten Umgebungen stellt sich das Verfahren wie folgt dar:

Die Datenpakete des lokalen Netzprotokolls (IP, Payload) werden am Tunnelanfang (z. B. TA = dezentrales VPN-Gateway) verschlüsselt und in IP-Pakete, die im Trägernetz geroutet werden können, eingepackt. Am Tunnelende (z. B. TE = zentrales VPN-Gateway) werden die Protokoll-Header des Trägernetzes entfernt und die Payload entschlüsselt. Danach wird das originale Datenpaket jenseits des Tunnels weitergeleitet.

13.3.4.2.2 Tunnel-Protokolle

Grundsätzlich kommen verschiedene Tunnelprotokolle in Frage, die alle weit verbreitet bzw. sogar standardisiert sind, sodass von einer hohen Produkt-Kompatibilität ausgegangen werden kann. Sie unterscheiden sich allerdings insbesondere hinsichtlich der unterstützten Sicherheits-Funktionalitäten, was einen Einsatz in einer Umgebung mit erhöhtem Schutzbedarf beeinflusst:

- GRE (Generic Routing Encapsulation)
- L2TP (Layer 2 Tunneling Protocol)

  In Umgebungen mit erhöhten Sicherheitsanforderungen kommen GRE und L2TP als alleinige Protokolle nicht in Frage, da diese Protokolle keine Verschlüsselung unterstützen (siehe Kapitel 13.3.4.5.2).
- PPTP (Point-to-Point Tunneling Protocol)

  PPTP bietet zwar einen Schutz der Kommunikation durch Verschlüsselung, allerdings sind immer wieder Implementierungs-Schwächen aufgedeckt worden, sodass auch aktuelle Varianten für Umgebungen mit erhöhtem Schutzbedarf nur mit zusätzlichen Sicherheitsmaßnahmen eingesetzt werden sollten (siehe Kapitel 13.3.4.5.2).
- IPsec-Tunnel-Modus (Internet Protocol Security, kurz IPsec)

  IPsec ist seit etlichen Jahren spezifiziert und im praktischen Einsatz. Es bietet zum jetzigen Zeitpunkt die besten Voraussetzungen für sichere Kommunikation mit höchstem Kompatibilitätsgrad (siehe [IETF RFC4301-2005] sowie ergänzende Updates).

Das Verfahren L2TP over IPsec (kurz L2TP/IPsec), das in RFC 3193 spezifiziert wird, verwendet einen speziellen Ansatz. Hier wird ein L2TP-Tunnel verwendet, der zusätzlich durch IPsec (im Transportmodus) abgesichert wird (siehe [IETF RFC3193-2001]).

- TLS-Tunneling

  Transport Layer Security (TLS, ursprünglich Secure Sockets Layer, SSL) ist als Sicherheitsprotokoll seit einigen Jahren bekannt und im Einsatz zur Absicherung von Internetverbindungen, z. B. Onlinebanking. Es bietet für ein End-to-Site-Szenario gute Voraussetzungen für eine VPN-Anbindung ohne Abhängigkeit von einer bestimmten Client-Software.

13.3.4.3 IPsec-VPN

13.3.4.3.1 Funktionsweise von IPsec

IPsec bietet zwei Mechanismen zum Schutz der Ende-zu-Ende-Kommunikation in unsicheren IP-Netzen (meist das Internet):

- Eine Integritätsprüfung für IP-Pakete verhindert die Manipulation oder Fälschung von IP-Paketen durch Unberechtigte.
- Die Verschlüsselung des Paketinhalts verhindert das Ausspähen von Daten.
- Die Sicherheitsmechanismen werden durch zwei spezielle Paket-Header realisiert bzw. kontrolliert:
  - Der Authentication Header (AH) sichert durch eine kryptografische Prüfsumme die Integrität des Pakets (siehe [IETF RFC4302-2005]).
  - Encapsulating Security Payload (ESP) steuert über die darin enthaltenen Informationen die korrekte Entschlüsselung der kryptografisch geschützten Payload (siehe [IETF RFC4303-2005]).

Beide Header können entweder einzeln oder auch kombiniert angewandt werden, wobei man zwischen Tunnelmodus und Transportmodus unterscheidet.

Der Tunnelmodus arbeitet nach dem in Kapitel 13.3.4.2 beschriebenen Prinzip (siehe Abbildung 88).

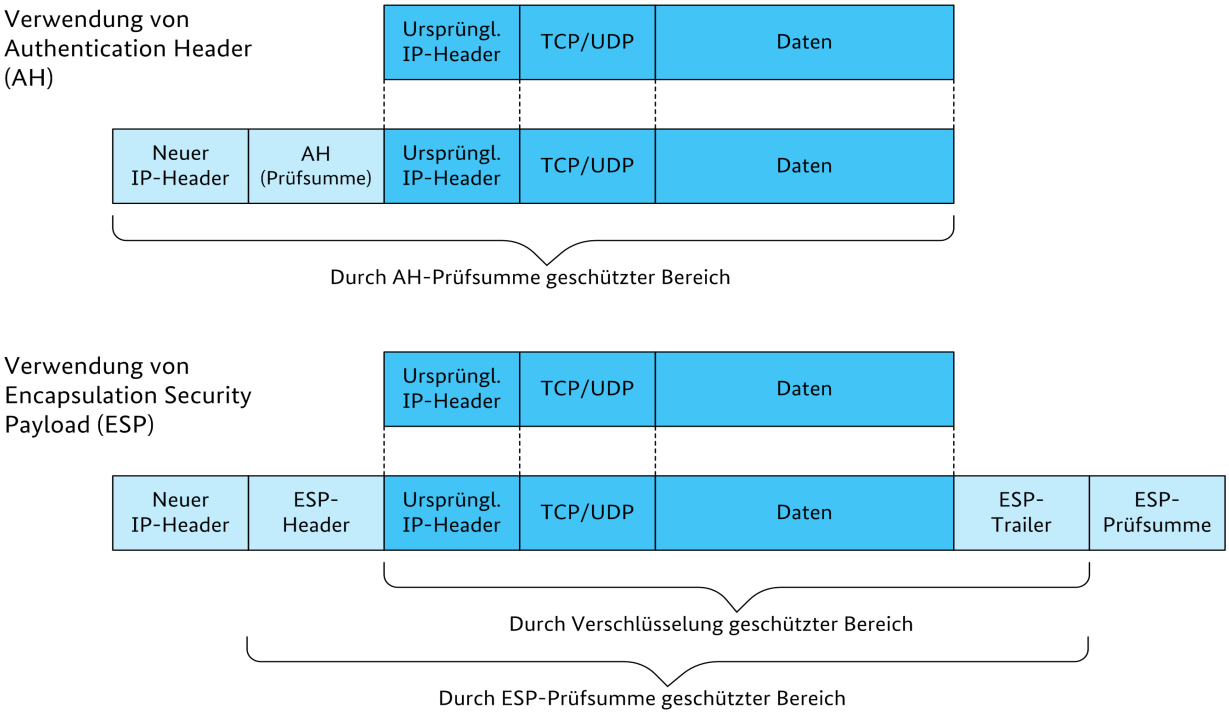


Abbildung 88: IPsec im Tunnelmodus

Im Transportmodus werden bei ESP lediglich die Daten und Header der Transport-Schicht geschützt. Es erfolgt keine Kapselung der IP-Header, sondern der IPsec-Header wird hinter dem originären IP-Header in das Original-Datagramm eingefügt (siehe Abbildung 89). Dieser Modus ist für die Absicherung von Peer-to-Peer-Kommunikationsverbindungen konzipiert und eignet sich wegen der Notwendigkeit trägernetzkonforme Adressen zu verwenden nur dann zum Aufbau von VPNs, wenn er mit einem Tunnel-Protokoll (z. B. L2TP) kombiniert wird.

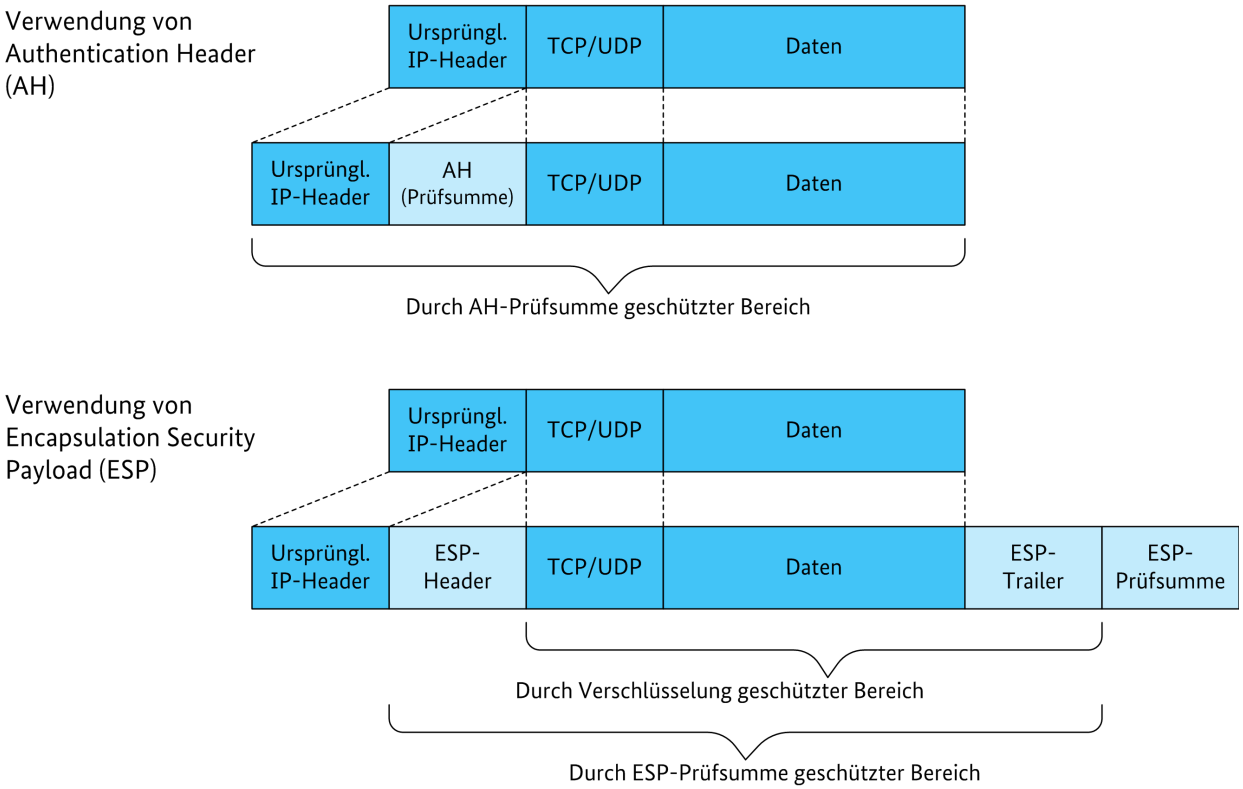


Abbildung 89: IPsec im Transportmodus

Die zum Einsatz der kryptografischen Verfahren, auf denen die Schutzwirkung der IPsec-Mechanismen beruht, notwendigen Parameter (welcher Algorithmus, welche Schlüssel etc.) werden entweder bei der Konfiguration der beteiligten Kommunikationssysteme festgelegt oder aber zwischen den Beteiligten über ein geeignetes Protokoll ausgehandelt. Hier kommt in aller Regel IKE (Internet Key Exchange) – eine pragmatische Teilmenge vom ISAKMP (Internet Security Association and Key Management Protocol) – zum Einsatz, welches derzeit in der Version 2 spezifiziert ist (siehe [IETF RFC5996-2010]).

13.3.4.3.2 Grenzen und Probleme bei IPsec

IPsec hat sich heute weitestgehend durchgesetzt, insbesondere zur Bildung von Site-to-Site-VPNs existieren keine nennenswerten Alternativen. Dennoch hat IPsec derzeit noch Einschränkungen, auch bei der Bildung von Site-to-Site-VPN. Die wesentliche Aspekte, die im Zusammenhang mit dem Einsatz von IPsec bzw. IPsec-basierten VPN-Lösungen zu beachten sind, werden im Folgenden kurz dargelegt.

Site-to-Site-VPN

Wenn Mitarbeiter aus vielen Standorten oder Außenstellen direkt miteinander telefonieren können sollen, müsste ein vollvermaschtes Site-to-Site-VPN aufgebaut werden. Der Eigenbetrieb eines solchen VPN mit den Mitteln von IPsec ist sehr aufwendig, da die Anzahl der aufzubauenden Security Associations (SAs) von quadratischer Komplexität ist, d. h. wahrscheinlich resultieren hohe Betriebskosten und ggf. auch massive technische Probleme (siehe Abbildung 90).

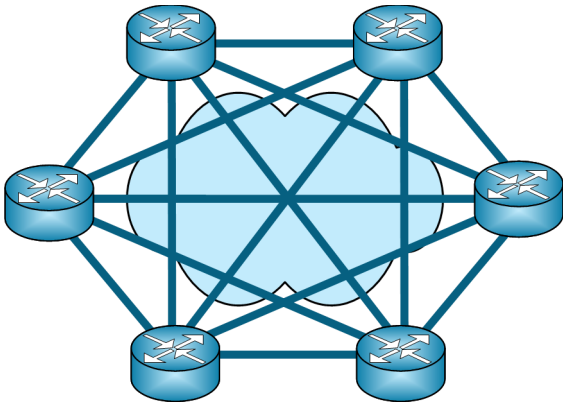


Abbildung 90: Quadratische Komplexität bei einem vollvermaschten Site-to-Site-VPN

Zur Vereinfachung des Schlüsselmanagements zur Verwaltung der SAs können allerdings auch herstellerspezifische Lösungen in Betracht gezogen werden. Ein Beispiel ist Cisco Group Encrypted Transport VPN (GET-VPN), das auf Basis einer Group-SA (siehe [IETF RFC6407-2011]) das Schlüsselmanagement für eine Gruppe von VPN-Endpunkten realisiert.

Der Aufbau eines Site-to-Site-VPN in Eigenregie wird nur für ein Hub-and-Spoke-Szenario empfohlen. Dies setzt allerdings entsprechendes Routing über das WAN voraus.

Benutzer-Authentisierung

IPsec unterstützt per se keine benutzerbezogene Identitätsüberprüfung. Im Fall einer transparenten Site-to-Site-Kopplung über zwei VPN-Gateways wird eine Benutzer-Authentisierung in aller Regel nicht benötigt. Eine solche Kopplung entspricht letztlich einer herkömmlichen WAN-Verbindung, die im Normalfall auch transparent Übertragungsdienste zur Verfügung stellt. Eine eventuell gewünschte zusätzliche Steuerung im Sinne einer benutzerbezogenen Autorisierung kann in solchen Fällen z. B. durch Einsatz von Firewall-Technik erreicht werden.

Häufig wird ein VPN hingegen zur Realisierung einer RAS-Lösung eingesetzt, d. h. als End-to-Site-VPN genutzt, oder zur Realisierung von Szenarien wie z. B. zur Absicherung von WLANs, bei denen generell auch bei transparentem Netzzugriff eine Prüfung der Nutzeridentität vorgesehen ist. Für derartige VPN-Szenarien gelten dann die gleichen Anforderungen an die Stärke der Benutzerauthentisierung wie beim klassischen Dial-In. Hier muss die in IPsec nicht unmittelbar verfügbare Benutzerauthentisierung über zusätzliche Maßnahmen erreicht werden. Im Wesentlichen bestehen folgende Möglichkeiten, eine Identifizierung des jenseitigen Benutzers zu gewährleisten:

- Verwendung von Zertifikaten zur Systemidentifizierung und Bindung dieser Zertifikate an einen Benutzer, z. B. mittels Smartcard, auf der das Zertifikat abgelegt ist
- Durchführung einer, in der Regel proprietären, Authentisierung im Rahmen des Tunnelaufbaus, d. h. während der IKE-Phase. Beispielsweise kann im Schutz des IKE-Tunnels eine Nutzername/Password-Abfrage durch das VPN-Gateway durchgeführt werden.
- Einsatz von geschachtelten Tunneln, bei denen ein Tunnelmechanismus Benutzerauthentisierung unterstützt, z. B. L2TP over IPsec
- Nachgelagerte Authentisierung an einer Firewall. Hierbei wird der Tunnel wird auf der Basis der Systemidentifikation etabliert, aber eine nachgelagerte Firewall verlangt im Rahmen der Autorisierung eine Authentisierung auf Benutzerebene.

Einsatz von NAT

Network Address Translation (NAT) hat in der Vergangenheit ein großes Problem beim Einsatz von VPN-Mechanismen auf IPsec-Basis dargestellt. Der Hauptgrund hierfür war, dass der Authentication Header, der die Integrität der übertragenen Pakete sicherstellt, die IP-Adressen des Pakets in die Prüfsummenberechnung einbezieht. Eine nachträgliche Manipulation einer der originalen Adressen führt somit beim

Empfänger des IPsec-Pakets zu einer negativen Prüfsummenverifikation und damit zum Verwerfen des empfangenen Pakets.

Mit NAT Traversal (NAT-T) wurde ein Verfahren entwickelt, das die wesentlichen praxisrelevanten Probleme löst. NAT-T ist seit Anfang 2005 spezifiziert und in vielen Netzwerken im Einsatz (siehe [IETF RFC3947-2005] und [IETF RFC3948-2005]).

Ideal wäre eine Möglichkeit zum Einsatz von IPsec ohne NAT-Problematik. Hier ist allerdings mit IPv4 angesichts der zum verbreiteten NAT-Einsatz führenden Adressknappheit keine Lösung zu erwarten. Mit Einführung von IPv6 verändert sich die Ausgangslage an dieser Stelle deutlich (siehe auch 13.3.4.3.5).

13.3.4.3.3 Funktionsweise von L2TP over IPsec

Das Layer 2 Tunneling Protocol (L2TP) stellt eine Weiterentwicklung des Point-to-Point Tunneling Protocol (PPTP) dar. L2TP kapselt die Payload in PPP-Frames, die wiederum auf UDP-Basis in IP-Pakete verpackt werden. Da PPP die Basis des Protokolls darstellt, bietet L2TP – anders als IPsec – eingebaute Verfahren zur Benutzerauthentisierung sowie zur Datenkompression. Eine Verschlüsselung ist optional definiert, wird jedoch in der Praxis kaum verwendet. Stattdessen wendet u. a. die in Windows-Betriebssystemen eingebaute VPN-Lösung zur Client-Anbindung L2TP over IPsec (L2TP/IPsec) an (siehe [IETF RFC3193-2001]).

Bei L2TP/IPsec wird zunächst eine IPsec-geschützte Kommunikationsbeziehung zwischen Client und VPN-Server etabliert. Diese verwendet ESP im Transportmodus (siehe Abbildung 89). Im Schutze dieser Verschlüsselung erfolgt dann der Aufbau des L2TP-Tunnels, über den sowohl die Netzkonfiguration (IP-Adresszuweisung) als auch der Datentransport erfolgt. Hierdurch wird eine zweistufige Authentisierung erreicht:

- Im ersten Schritt authentisieren sich die Computer beim Aufbau der IPsec-Verbindung.
- Im zweiten Schritt authentisieren sich die Benutzer beim Aufbau des L2TP-Tunnels.

Für die Geräte-Authentisierung kommen üblicherweise X.509-Zertifikate und für die Benutzer-Authentisierung beliebige PPP-Authentisierungsprotokolle zum Einsatz. Da bei entsprechender Konfiguration zur Geräte-Authentisierung zwingend Zertifikate notwendig sind, wird aus Sicherheitssicht ein zusätzlicher Steuerungsmechanismus erforderlich: Durch die Entscheidung, welche Geräte ein entsprechendes Zertifikat erhalten, wird festgelegt, welche Geräte am VPN teilnehmen dürfen. Anders als beispielsweise im Falle von PPTP kann so verhindert werden, dass Benutzer mit beliebigen und womöglich unsicheren PCs VPN-Verbindungen ins Organisationsnetz aufbauen. Voraussetzung hierfür ist natürlich, dass die entsprechenden Zertifikate von Benutzern nicht auf andere Geräte übertragen werden können.

13.3.4.3.4 Authentisierung: IKEv2

IPsec-VPNs basieren auf einer gegenseitigen Authentisierung im Rahmen des Internet Key Exchange Protocols (IKE), das während des Aufbaus der IPsec-Verbindung abläuft. Dabei handelt es sich in der ursprünglichen IKE-Spezifikation (IKEv1) jedoch ausschließlich um eine Geräte-Authentisierung; die Authentisierung von Benutzern ist erst mit IKE Version 2 (IKEv2) vorgesehen.

Das Internet Key Exchange Protocol (IKE) ist das Standard-Verfahren zur gegenseitigen Authentisierung sowie zum Austausch und zur Bereitstellung von Security Associations in IPsec-Implementierungen. IKE handelt sowohl seine eigenen als auch die IPsec-SAs aus und verwaltet diese ebenso wie die dort spezifizierten Parametersätze. Der Schlüsselaustausch verwendet das Diffie-Hellman-Verfahren mit Authentisierung. Zur Authentisierung können entweder Pre-Shared-Keys oder ein Public-Key-Verfahren wie z. B. RSA verwendet werden. Die Authentisierung stellt dabei den Schutz der jeweiligen Identität gegen Spoofing-Attacken sicher.

IKEv2 wurde im Dezember 2005 als Nachfolger von IKEv1 verabschiedet und hat dieses Protokoll weitestgehend abgelöst (siehe [IETF RFC5996-2010]). Mit den in IKEv2 spezifizierten Mechanismen sollen einige Schwächen von IKEv1 behoben werden und die Implementierung von IPsec-Tunneln vereinfacht werden. Ein Update zu [IETF RFC5996-2010] bietet eine herstellerunabhängige Protokollspezifikation für hochverfügbare VPN-Infrastrukturlösungen (VPN-Gateway im Cluster-Betrieb).

Aufgrund der vielfältigen Änderungen im IKE-Protokoll ist die IKE Version 2 nicht rückwärtskompatibel zur IKE Version 1, jedoch soll ein Parallelbetrieb beider Versionen problemlos möglich sein.

Die wesentlichen Veränderungen im Vergleich zu IKEv1 sind:

- Verzicht auf verschiedene Phasen, IKEv2 nutzt lediglich eine Phase für alle auszutauschenden Daten.
- Die Anzahl der erforderlichen Nachrichten wurde von einer Mindestanzahl von neun auf lediglich vier Nachrichten zum Aushandeln der Sicherheitsparameter reduziert.
- Die Nutzung von NAT Traversal für entsprechende Szenarien ist in IKEv2 integraler Bestandteil der Spezifikation.
- Ein Erreichbarkeitstest (Dead Peer Detection, DPD) ist in IKEv2 ebenfalls direkt in die Spezifikation aufgenommen.
- Einführung eines standardisierten Feldes (Configuration Payload), um die Zuteilung einer virtuellen IP-Adresse sowie die Mitteilung von DNS- und WINS-Serveradressen zu realisieren. Dieser ersetzt den nicht standardisierten „Config Mode“, der bei vielen IKEv1-Implementierungen zum Einsatz kommt.
- Unterstützung eines hybriden Authentisierungsmodus in einem RAS-Szenario:
  - Authentisierung des zentralen VPN-Gateway mit einer durch ein Zertifikat beglaubigten RSA-Signatur
  - Authentisierung der Clients mit Pre-Shared Keys (PSKs)

    Hierdurch sollen Man-in-the-Middle-Szenarien nach potenziell erfolgreichem Wörterbuch- bzw. Brute-Force-Angriff auf den PSK ausgeschlossen werden.
- Übermittlung des Zertifikats lediglich durch Senden der Zertifikats-URL.
- Unterstützung von Client-Authentisierungsmechanismen wie RADIUS, SecurID usw. durch Nutzung des Extensible Authentication Protocol (EAP) mittels EAP Payload (Legacy Authentication; dies ersetzt die bisherigen proprietären Protokollerweiterungen wie z. B. XAUTH)
- Vereinfachte Nutzung in mobilen Szenarien, in denen häufig IP-Adressen und L2-Adressen gewechselt werden müssen, durch die Ergänzung von Mobility and Multihoming Protocol (MOBIKE); bei IKEv1 müssen alle SAs bei einem Adresswechsel neu ausgehandelt werden.
- Verwendung expliziter Traffic Selectors, die den von der auszuhandelnden IPsec-SA erfassten Datenverkehr nach Adressen bzw. Ports beschreiben – unter IKEv1 musste dies fest konfiguriert und zwingend bei beiden Partner identisch sein.

IKEv2 gewährleistet wie IKEv1 den Aufbau von IKE-SAs und IPsec-SAs – letztere werden nunmehr als Child-SAs bezeichnet – auf der Basis von Public-Key-Kryptoverfahren. Die IKE-SA und die erste IPsec-SA werden im Idealfall innerhalb von vier Nachrichten ausgehandelt. Weitere Child-SAs können mit jeweils weiteren zwei Nachrichten ausgehandelt werden.

13.3.4.3.5 IP Version 6

Die bislang verbreiteten IPsec-VPNs basieren typisch auf einer IPv4-Infrastruktur. Mit der Umstellung der zugrunde liegenden Infrastruktur auf IPv6 wird ein IPsec-VPN zu einem IPv6-VPN, d. h. ein IPv6-VPN ist am Tunnelanfang und am Tunnelende an ein natives IPv6-Interface angeschlossen. Für die Tunnelendpunkte werden somit IPv6-Adressen verwendet, welche als globaler IPv6-Adressen für die Verwendung in öffentlichen Netzen in erheblich größerem Umfang als unter IPv4 zur Verfügung stehen. Probleme durch Kombination von IPSec und NAT entfallen hier (siehe Kapitel 13.3.4.3.2).

Die für IPsec-VPNs erforderlichen Mechanismen sind bereits in der Spezifikation für IPv4 und IPv6 ausgelegt. IPsec wurde sogar zunächst ausschließlich als integraler Bestandteil von IPv6 definiert (AH und ESP als optionale IPv6-Header) und erst nachträglich für IPv4 nutzbar gemacht. Spezielle Mechanismen für die Einrichtung von IPv6-VPNs sind somit nicht erforderlich. Vielmehr kann die Unterstützung von AH- und ESP-Headern durch die IPv6-Software eines vernetzten Gerätes unmittelbar als Basis für IPSec-VPN-Produktlösungen dienen.

13.3.4.4 TLS-basierte VPNs (ursprünglich: SSL-VPN)

Auch wenn die aktuellen Protokollversionen als Transport Layer Security (TLS) spezifiziert sind, ist häufig noch der alte Begriff „SSL-VPN“ im Zusammenhang mit entsprechenden Implementierungen geläufig. Alternativ findet man auch die Bezeichnung TLS/SSL-VPN. TLS-basierte VPNs sollen – so der Tenor aller Hersteller – neben einer möglichst geringen Komplexität der Lösung vor allem den Vorzug haben, in den meisten Einsatzbereichen ohne spezielle Client-Software auszukommen. Dies vereinfacht den Ausrollvorgang erheblich, reduziert die notwendige Schulung von Benutzern auf ein Minimum und erhöht die Flexibilität hinsichtlich der Client-Auswahl. Die marktverfügbaren TLS-basierten VPNs gehen dazu von einem Terminal-Server-Ansatz aus, bei dem als Client ein Standard-Webbrowser zum Zugriff auf bestimmte Applikationen zum Einsatz kommt. Dieser Ansatz musste allerdings mit steigenden Ansprüchen an die Flexibilität der Nutzung erweitert werden, um z. B. File Sharing zu ermöglichen.

Neben diesem – kommerziell ausgerichteten – Ansatz existieren auch Open-Source-Projekte, die einen transparenten Netzzugriff, ähnlich wie bei IPsec-basierten VPN, unter Verwendung von Tunneln realisieren.

13.3.4.4.1 Kommerzielle Ansätze für TLS-basierte VPNs auf Browser-Basis

Produktspezifische Mechanismen existieren hier in großer Vielfalt. Die nachfolgende kurze Beschreibung der gängigsten technischen Ansätze für Browser-basierte SSL-VPN kann daher nur einen groben Überblick bieten.

Grundprinzip

Anders als IPsec-VPNs verwenden TLS-basierte VPN-Lösungen in ihrer Grundform keinen speziellen Client, sondern nutzen den bereits auf praktisch allen in Frage kommenden Endgeräten vorhandenen Webbrowser. Damit der Nutzer mit Hilfe eines Standard-Browsers über ein TLS-basiertes VPN zentrale Ressourcen nutzen kann, benötigen diese Ressourcen ein Web-Front-End – die jeweilige Anwendung muss „Web-enabled“ sein.

Ein Beispiel für eine solche Anwendung ist der OWA-Dienst (Outlook Web Access). OWA ist eine Anwendung, die unter Zuhilfenahme eines Web-Servers dem Browser als Web-Client einen Zugriff auf Exchange-Server ermöglicht. Dabei greift allerdings der Browser nicht direkt auf den Exchange-Server zu, sondern er übermittelt die Benutzer-Aktion (etwa Klicken des Send-Button) per HTTP/HTTPS an den OWA-Server, der dann entsprechend auf den Exchange-Server zugreift.

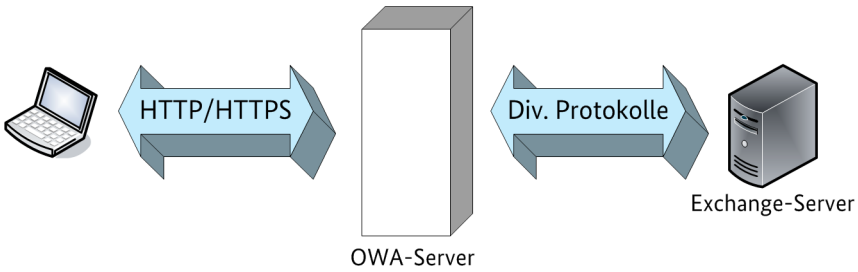


Abbildung 91: TLS-basiertes VPN für E-Mail mit Outlook Web Access

Bei diesem Beispiel dient der Browser also nur zur Visualisierung der Vorgänge[51], die eigentlich auf dem OWA-Server ablaufen. Es gibt grundsätzlich verschiedene Möglichkeiten, ein solches Web-Front-End bereitzustellen:

- Erweiterung des Anwendungs-Servers um eine solche Funktion
- Vorschaltung eines anwendungsspezifischen Gateways (wie beim OWA-Beispiel) auf Basis eines Web-Servers
- Vorschaltung eines Web-basierten Terminal-Servers, der für die gewünschten Applikationen entsprechende Front-Ends beinhalten muss

Um den eigentlichen Applikations-Server nicht zu überlasten (vor allem die Verschlüsselung bei TLS-basierter Kommunikation geht zu Lasten der Leistungsfähigkeit), empfehlen sich die beiden letztgenannten Ansätze. Ein weiterer Vorteil der Verwendung vorgelagerter Systeme ist die Möglichkeit, den Web-Access auch für solche Anwendungen bereitzustellen, bei denen der Server sich dafür prinzipbedingt eher schlecht oder auch gar nicht eignet. Darüber hinaus sind auch spezielle VPN-Gateways verfügbar, die die Absicherung von ansonsten nicht hinreichend „VPN-tauglichen“ Web-Applikationen, inkl. beliebiger Intranet-Anwendungen, übernehmen können und auch erweiterte Zugriffsmöglichkeiten für Applikationen bereitstellen, für die kein Web-basierter Zugriff verfügbar ist.

Erweiterungen

Nicht immer reichen die Standardmechanismen des Browsers aus, denn je nach Applikation benötigt der Browser eine Erweiterung seiner Möglichkeiten, die ihm allerdings zur Laufzeit mittels entsprechender Plug-ins (etwa in Form von Java-Applets oder ActiveX-Controls) verabreicht werden können.

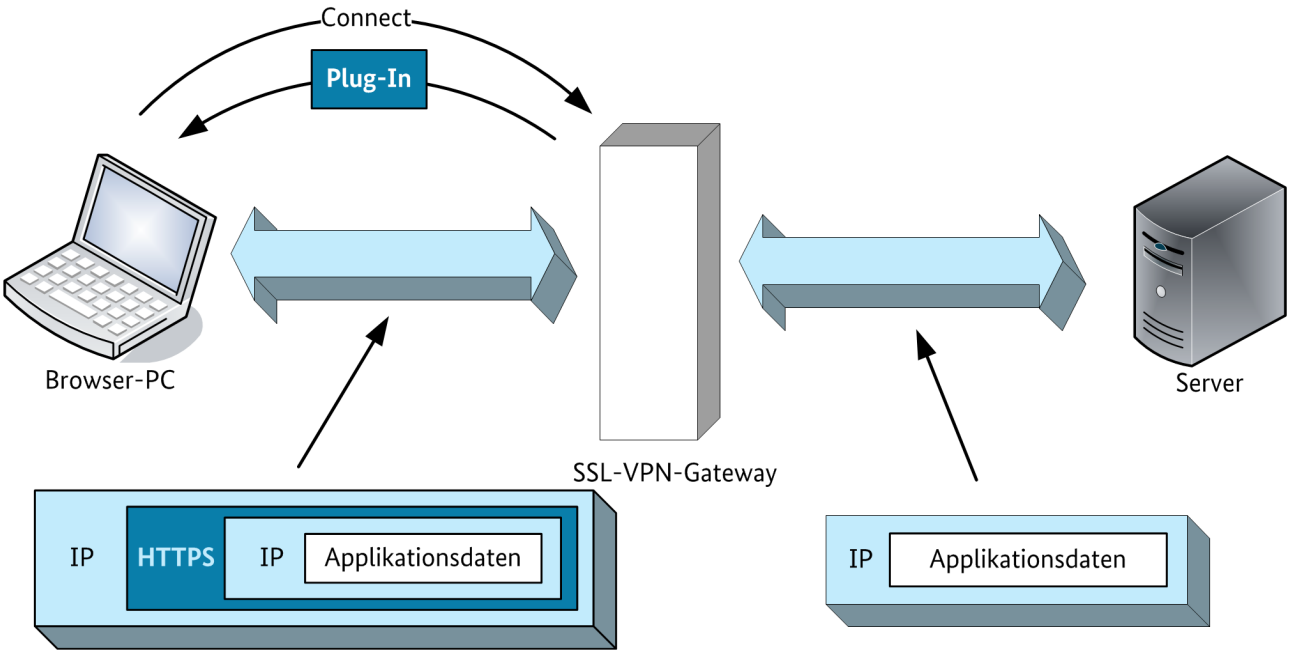


Abbildung 92: Erweiterter VPN-Zugriff mittels Plug-in

Üblicherweise verbindet sich hierfür der Nutzer zunächst mittels seines Browsers mit einem Webportal auf dem Gateway. Im ersten Schritt wird der Server über ein entsprechendes Zertifikat authentisiert und eine SSL-verschlüsselte HTTP-Verbindung aufgebaut. Durch diese Verbindung geschützt, wird im zweiten Schritt der Benutzer vom Portal aufgefordert, sich zu authentisieren – hier steht je nach Produkt eine Vielzahl verschiedener Authentisierungsmechanismen zur Verfügung. Nachdem die Authentisierung

51 Überhaupt ähneln TLS-basierte VPN-Lösungen sehr stark Terminal-Server-Ansätzen, nicht zuletzt deshalb funktionieren umgekehrt Terminal-Server ausgezeichnet auf der Basis von Browser-Clients.

erfolgreich abgeschlossen ist, erhält der Nutzer Zugriff auf alle Applikationen, die für den Nutzer freigegeben wurden, und kann diese herunterladen.

13.3.4.4.2 OpenVPN als Alternativansatz

OpenVPN ist ein Open-Source-Projekt und verfolgt einen technologisch anderen Ansatz als die bisher beschriebenen kommerziellen Lösungen.

Anders als die meisten Anbieter von TLS-VPN-Lösungen fokussiert OpenVPN nicht die Notwendigkeit eines speziellen Clients als Hauptproblem von IPsec-VPNs, sondern die Komplexität, die damit verbundenen Inkompatibilitäten und die technischen Probleme von IPsec.

Folgerichtig nutzt auch OpenVPN einen speziellen Client, der allerdings TLS als Schutzmechanismus nutzt und Kernel-nahe Systemmodifikationen vermeidet. Die damit verbundenen technischen und auch administrativen Probleme werden so vermieden.

Das Grundprinzip dieses Ansatzes ist die Verwendung virtueller Netzadapter, welche die zu übertragenden Bits aus dem Kernel Space des Systems in den sogenannten User Space transferieren, wo sie durch „beliebige“ Applikationen modifiziert werden können. Beim VPN-Ansatz erfolgt diese Modifikation in Form eines Verkapseln in UDP bzw. TCP und Sichern mittels TLS.

Da die entsprechende VPN-Applikation nicht im Kernel Space residiert, gestaltet sich die Installation erheblich konfliktärmer als bei IPsec, das zwangsläufig den IP-Stack selbst modifiziert. Ein weiterer Vorteil ist, dass die OpenVPN-Applikation mit anderen VPN-Mechanismen koexistieren kann – sogar mit einem IPsec-Client.

Bei der Einrichtung des OpenVPN wird der virtuelle Netzadapter wie ein normales Netz-Interface konfiguriert und als Routingpfad für das über das VPN erreichbare Netz eingerichtet.

Die von der jeweiligen Anwendung generierten Daten werden an das virtuelle Interface gesendet. Dieses wiederum übermittelt diese an die OpenVPN-Applikation, die die Kapselung und Absicherung vornimmt. Anschließend sendet die OpenVPN-Applikation das gekapselte Paket an die echte Netzwerkschnittstelle, die sie über das Netz überträgt. Auf der Empfängerseite läuft dieser Prozess in umgekehrter Reihenfolge ab.

Neben OpenVPN existieren noch diverse weitere ähnliche Projekte, die nach dem gleichen Prinzip arbeiten.

13.3.4.4.3 Authentisierung und Verschlüsselung bei TLS-basierten VPNs

HTTPS (Hypertext Transfer Protocol Secure) ist ein Protokoll zur Übertragung sensitiver, d. h. schützenswerter Informationen, über das Web. Es basiert auf HTTP, schützt jedoch die übertragenen Informationen mit Hilfe der TLS-Technologie (Transport Layer Security).

TLS ist als zusätzliches Protokoll zwischen TCP und HTTP angesiedelt (siehe Kapitel 13.3.3). Es leistet sowohl eine gegenseitige Authentisierung von Client und Server als auch den Schutz der Vertraulichkeit sowie der Integrität der übertragenen Daten durch kryptografische Verfahren. TLS verwendet wie praktisch alle aktuellen Verschlüsselungslösungen eine Hybridtechnik:

- Die Datenübertragung erfolgt auf der Basis eines zwischen Client und Server auszuhandelnden symmetrischen Kryptoalgorithmus (RC4, AES etc.)
- der dazu erforderliche symmetrische Schlüssel wird während der Verhandlungsphase unter Einsatz asymmetrischer Kryptoalgorithmen (RSA, DSA, DH etc.) zwischen den Kommunikationspartnern vereinbart. Während dieses Handshakes erfolgt gleichzeitig die (optional gegenseitige) Authentisierung.

Die Authentisierung ist üblicherweise mehrstufig implementiert. Den ersten Schritt stellt hierbei die Authentisierung des TLS-Servers durch den TLS-Client während des TLS-Handshake dar. Sofern der Benutzer ebenfalls über ein geeignetes Zertifikat verfügt, kann er optional in seiner Funktion als TLS-Client auf die gleiche Weise durch den TLS-Server authentisiert werden.

Der Server übermittelt sein Zertifikat an den Client, der dieses auf Gültigkeit überprüft, ein sogenanntes Pre-Master Secret kreiert und Public-Key-Mechanismen nutzt, um dieses Secret für den Server zu verschlüsseln und anschließend an diesen zu übermitteln. Auf diese Weise wird einerseits die Authentisierung des Servers, andererseits der Austausch eines Secret erreicht, welches im nächsten Schritt als Grundlage für den Aufbau einer verschlüsselten TLS-Verbindung genutzt wird. Voraussetzung hierfür ist, dass der Server über ein gültiges X.509-Zertifikat verfügt, dessen Aussteller der Client vertraut.

Statt die Benutzer-Authentisierung während des TLS-Handshake durchzuführen, wird diese üblicherweise in einer zweiten Stufe nachgeholt: beim Zugriff auf Ressourcen, beispielsweise auf das Webportal des VPN-Gateways. Hierbei können je nach Gateway-Produkt eine Vielzahl verschiedener Authentisierungsmerkmale eingesetzt werden, beispielsweise X.509-Zertifikate, AD-Benutzer und AD-Passwort; als Authentisierungsprotokoll wird häufig RADIUS eingesetzt.

Da der Entwickler der Browser-Software natürlich nicht im Vorfeld weiß, welche Ziele der Anwender mit seinem Browser ansteuern wird, besitzt dieser in der Regel Zertifikate der gängigen Certificate Authorities, denen er vertraut. Auf Windows-Rechnern sind hierzu CA-Zertifikate vieler öffentlicher Trustcenter (z. B. GeoTrust, VeriSign, D-Trust GmbH etc.) bereits im Lieferumfang des Betriebssystems enthalten. Kann der Server ein Zertifikat vorlegen, das von einer dieser CAs ausgestellt wurde, wird es vom Browser akzeptiert. Ansonsten muss der Browser, d. h. der Anwender, dem Server-Zertifikat ohne Beglaubigung vertrauen oder ggf. ein neues Zertifikat einer weiteren CA importieren.

Genauso wie beim IPsec-VPN gilt: Werden native Client-Applikationen in Kombination mit einem für die Applikation transparenten (in diesem Fall durch TLS geschützten) Tunnel genutzt, so finden weitere Authentisierungsvorgänge statt, die völlig unabhängig von den zuvor geschehenen sind. Welche Protokolle und Verfahren hierbei genutzt werden, ist wieder davon abhängig, welche Client-Typen auf welche Ressourcen zugreifen.

13.3.4.4.4 Grenzen und Probleme bei TLS/SSL

TLS/SSL hat sich heute als Alternative in bestimmten Einsatzbereichen durchgesetzt, insbesondere zur Bildung von Client-unabhängigen End-to-Site-VPNs. Dennoch haben auch die browserbasierten TLS/SSL-VPNs Einschränkungen, die insbesondere bei Nutzung von Fremdsystemen die Sicherheit des Netzwerkes gefährden:

- Da die Vertrauenswürdigkeit von Fremdsysteme nur unzureichend sicherzustellen ist, steigt die Gefahr sprunghaft an, dass ein Nutzer über ein solches Fremdsystem Malware ins eigene Netzwerk einschleust oder Angriffe ermöglicht.
- Eine aus Sicht eines VPN höchst sicherheitskritische Eigenschaft von Browsern ist das Caching geladener Informationen. Die Daten werden ausschließlich während ihres Transports über das Internet vor unbefugtem Zugriff geschützt.

Wird der Browser-Cache eines Clients in einem öffentlichen Bereich, z. B. einem Internet-Café, nicht zuverlässig geleert, kann der nachfolgende Anwender auf die angezeigten Inhalte ebenfalls zugreifen.

Ein sicherer Schutz gegen solche Angriffe ist ausschließlich die Bereitstellung eines vollständig gesäuberten Clients für jeden neuen Anwender.

- Auch die Sicherheitsprobleme, die durch einen zu sorglosen Umgang der Nutzer mit dem Fremdsystem bzw. den genutzten Daten resultieren, können nur durch die Bereinigung des Fremdsystems nach jeder Nutzung verhindert werden. Hierzu gehören insbesondere das unbeabsichtigte lokale Speichern von Daten oder auch das Nicht-Beenden von Browser-Sitzungen.
- TLS/SSL-VPNs gelten im Prinzip als „clientless“, da der zum Zugriff verwendete Browser bereits als Standard-Anwendung auf allen in Frage kommenden Client-Systemen vorinstalliert ist. Jedoch erfordern viele Applikationen den Einsatz zusätzlicher Plug-ins oder Applets, die zur Laufzeit auf den Client geladen werden. Die Nutzbarkeit dieser Applikationen bedingt dann jedoch entsprechend umfassende Rechte des Benutzers.

13.3.4.5 Abgrenzung: VPN-Techniken auf Layer 2

13.3.4.5.1 MPLS

Das Multiprotocol Label Switching (MPLS), eine Weiterentwicklung des Tag-Switching der Firma Cisco Systems, ist mittlerweile als Standard im Bereich der IP-Switching-Technologie für hochperformante Provider-Netzwerke etabliert (siehe [IETF RFC3031-2001]). Derzeit werden von allen großen Netzwerk-Providern (auch Carrier genannt) bevorzugt MPLS-basierte Produkte zum Aufbau von Weitverkehrsnetzen für Kunden angeboten – insbesondere im internationalen Bereich.

Wesentliche Eigenschaften von MPLS sind:

- Mandantenfähigkeit durch integrierte VPN-Mechanismen
- gute Skalierbarkeit
- QoS-Ansätze auf der Basis von Priorisierungsmechanismen
- eine weitestgehende Autokonfiguration durch Selbstlernmechanismen zur Verringerung des Administrationsaufwandes

MPLS-Netze basieren meist auf IP-Routernetzen. Für die verschiedenen Mandantennetze und Kommunikationsziele fügt MPLS Kennungen (sogenannte Label) in die zu transportierenden Datenpakete ein. Die Datenweiterleitung innerhalb einer MPLS-Struktur erfolgt dann ausschließlich auf der Basis dieser Label.

Bei MPLS werden dem Kunden durch einen Provider bzw. Carrier ein oder mehrere sogenannte MPLS Virtual Private Networks (MPLS-VPNs) bereitgestellt. Dabei muss beachtet werden, dass es sich bei einem MPLS-VPN zwar um ein virtuelles privates Netz handelt, jedoch anders als bei einem IPsec-VPN keine Verschlüsselung der Kommunikation ohne Zusatzinstrumente stattfindet. Innerhalb des MPLS-Netzes erfolgt die Trennung der verschiedenen MPLS-VPNs zwischen Layer 3 und Layer 2 durch virtuelle Routing-Instanzen (Virtual Routing and Forwarding, VRF) und durch ein sogenanntes Label, das als Zusatzinformation in den Paketen übertragen und einem MPLS-VPN zugeordnet wird. Die Datenweiterleitung innerhalb einer MPLS-Struktur erfolgt dann ausschließlich auf der Basis dieser Label. Somit wird pro Mandant ein eigenes virtuelles Netzwerk, d. h. VPN, eingerichtet. Das MPLS-Forwarding ist vollständig von den genutzten IP-Adressen innerhalb des MPLS-VPN entkoppelt. Darüber hinaus sind auch die IP-Adressstrukturen verschiedener MPLS-VPNs gegeneinander vollständig entkoppelt, sodass Überlappungen der Adressbereiche wie auch der Routing-Prozesse problemlos möglich sind. Am Übergang zu den Kundennetzen werden diese MPLS-VPNs dann auf dem Kunden bereitgestellten Routing-Instanzen terminiert. Mehrere Kunden bzw. mehrere MPLS-VPNs teilen sich also eine gemeinsame Infrastruktur, wie in Abbildung 93 dargestellt.

MPLS unterscheidet sich in wesentlichen Punkten von den in Kapitel 13.3.4.3 und 13.3.4.4 beschriebenen tunnelbasierten IPsec-VPNs:

- MPLS stellt dem Anwender QoS zur Verfügung, wenn auch nur in Ansätzen.
- Die Flexibilität beim VPN-Design ist bei MPLS erheblich eingeschränkt, da der Anwender sich in der Praxis analog zu klassischen Layer-2-VPNs an einen bestimmten Netzwerk-Provider und dessen Infrastruktur bindet.
- Die Sicherheit der Technologie ist analog zu den Layer-2-VPNs zu bewerten: In MPLS-Netzen ist wie oben schon gesagt keine Vertraulichkeit gegeben, da MPLS keinerlei Verschlüsselung und Authentisierung vorsieht. Maßnahmen zur Sicherung der Vertraulichkeit können teilweise durch den Provider bereitgestellt werden, jedoch begibt sich der Mandant damit in eine deutliche Abhängigkeit von einem Provider.

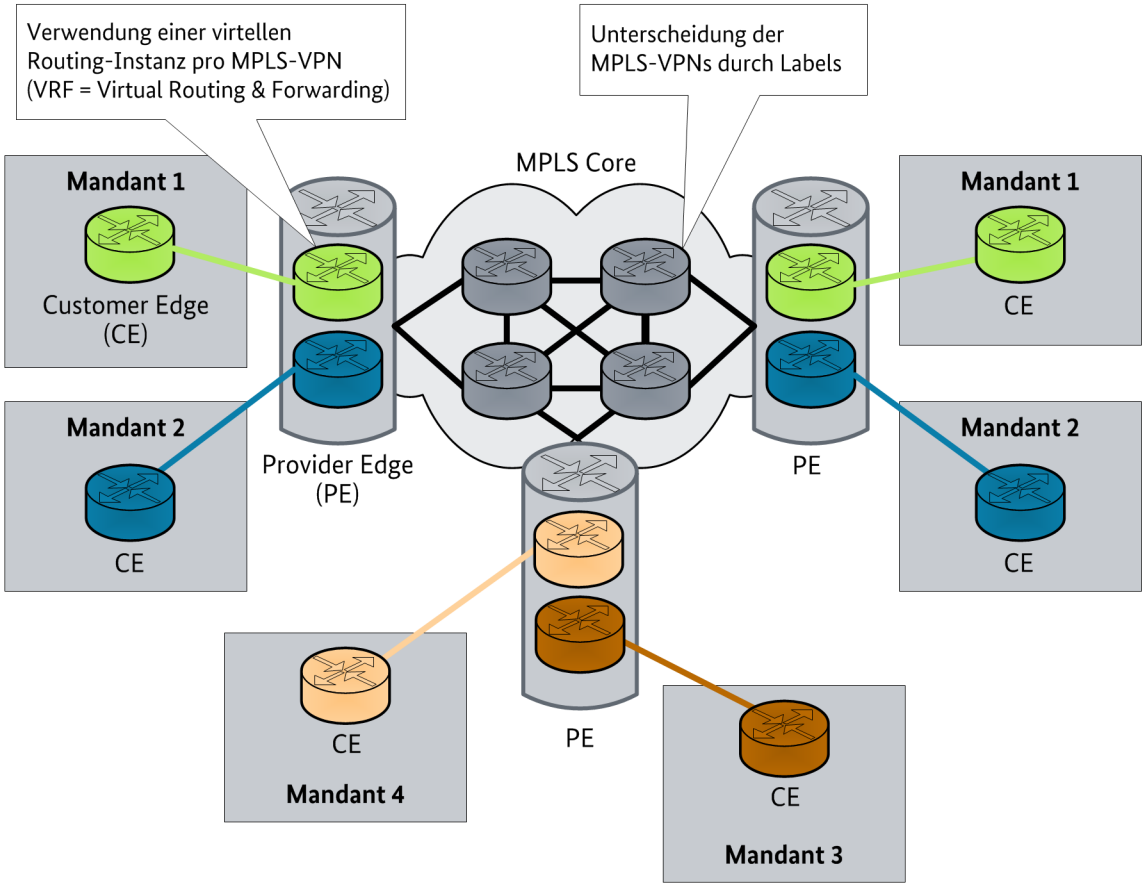


Abbildung 93: Mandantennetze in einer MPLS-Struktur

13.3.4.5.2 PPP-basierte VPNs

PPTP

Das Point-to-Point Tunneling Protocol (PPTP) wurde von Microsoft und einer Reihe anderer Herstellerfirmen entwickelt, um eine höhere Flexibilität für Dial-In-Lösungen zu erreichen.

PPTP erlaubt es, eine PPP-Verbindung (Point-to-Point Protocol) über den physikalischen Zugangspunkt in das Netzwerk hinein zu verlängern. Neben der so erreichten Flexibilisierung der Dial-In-Lösung erlaubt PPTP somit auch den Aufbau von VPNs, indem der mittels PPTP definierte Tunnel bis zum Client verlängert wird.

Das Protokoll kapselt PPP-Daten in IP-Datagramme unter Verwendung einer Variante der GRE, sodass als Transit-Netzwerke ausschließlich IP-basierte Netzwerk zum Einsatz kommen.

Die aus dem Mechanismus resultierende geschachtelte Paketstruktur ist in Abbildung 94 dargestellt. Man erkennt unmittelbar den mit dem Tunneling einhergehenden, aber auch kaum vermeidbaren Protokoll-Overhead, der sich jedoch durch Einsatz von Header-Compression-Mechanismen zumindest verringern lässt.

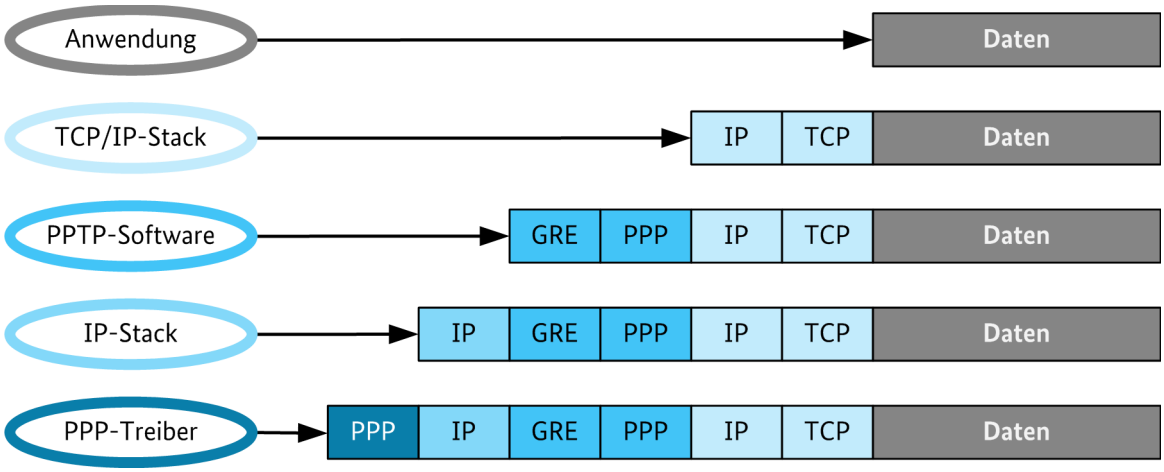


Abbildung 94: PPTP-Protokollarchitektur am Beispiel eines PPTP-Dial-In-Clients

PPTP unterscheidet sich in wesentlichen Punkten von den in Kapitel 13.3.4.3 und 13.3.4.4 beschriebenen tunnelbasierten IPsec-VPNs:

- Die zu übertragenen Daten, Payload genannt, können komprimiert und/oder verschlüsselt werden. PPTP verwendet zur Verschlüsselung ein proprietäres Verfahren, Microsoft Point-to-Point Encryption (MPPE), das sich aufgrund diverser Implementierungs-Schwächen als anfällig gegen kryptoanalytische Attacken erwiesen hat.

  Aufgrund dieser Schwächen kommt der Einsatz von PPTP für Bereiche mit erhöhten Sicherheitsanforderungen nicht in Betracht.

- Je Tunnel wird lediglich eine Kommunikationsverbindung unterstützt („Single Tunnel“), sodass für jede PPP-Verbindung, die über PPTP getunnelt werden soll, ein eigener PPTP-Tunnel aufgebaut werden muss.

  Diese Eigenschaft stellt in VPN-Szenarien, die Dial-In-Lösungen realisieren sollen, keine Einschränkung dar, da hier grundsätzlich für jede Kommunikationsbeziehung ein eigener Tunnel erforderlich ist.

L2TP

PPTP weist noch einige Einschränkungen auf, daher wurde ein weiteres Layer-2-Tunneling-Protokoll, das Layer 2 Tunneling Protocol (L2TP), definiert, das weit verbreitet ist (siehe [IETF RFC3931-2005])

L2TP kapselt die zum Transport der Payload verwendeten PPP-Frames nach Bedarf so, dass sie wahlweise über IP, X.25, Frame Relay oder Asynchronous Transfer Mode (ATM) versandt werden können. Die Kommunikationsbeziehung via L2TP, d. h. der Tunnel, kann dabei sowohl zwischen dem Dial-In-Router und dem L2TP-Server als auch zwischen dem Client und dem L2TP-Server aufgebaut werden.

Als Transitnetzwerk kommt jede der oben genannten Netzwerktechniken mit Unterstützung von Punkt-zu-Punkt-Verbindung in Frage. Falls über ein IP-Netz getunnelt wird (L2TP over IP), d. h. unter anderem ist auch den Aufbau von L2TP-Kommunikationstunneln über das Internet möglich, wird als Transportschicht-Protokoll UDP eingesetzt.

L2TP unterscheidet sich in wesentlichen Punkten von den in Kapitel 13.3.4.3 und 13.3.4.4 beschriebenen tunnelbasierten IPsec-VPNs:

- Die PPP-Payload kann wahlweise komprimiert und/oder verschlüsselt werden. Die zunächst spezifizierte Verschlüsselungsoption wird allerdings in der Praxis nicht genutzt.
- Stattdessen wird generell empfohlen, zur Verschlüsselung von L2TP-Kommunikation IPsec einzusetzen (siehe [IETF RFC3193-2001]). Dabei kann IPsec als Sicherungsmechanismus innerhalb von L2TP dienen. Alternativ kann aber auch ein L2TP-Tunnel innerhalb einer IPsec-geschützten Kommunikations-beziehung etabliert werden. Ein entsprechender Mechanismus wird auch als L2TP over IPsec bezeichnet (siehe Kapitel 13.3.4.3.3).
- Anders als PPTP benötigt L2TP im Prinzip nur einen Tunnel zwischen z. B. Dial-In-Router und L2TP-Server, da innerhalb dieses Tunnels Multiplexing genutzt werden kann.

Literaturverzeichnis

[ACM BeTe-2009] ACM Conference, M. Beck, E. Tews, „Practical attacks against WEP and WPA“, Proceedings of the second ACM conference on Wireless network security, Zürich, 2009, verfügbar unter http://dl.aircrack-ng.org/breakingwepandwpa.pdf

[BSI Bro314-2012] BSI, BSI-Bro12/314, „Eckpunktepapier – Sicherheitsempfehlungen für Cloud Computing Anbieter“, 2012, verfügbar unter https://www.bsi.bund.de

[BSI Bro321-2012] BSI, BSI-Bro12/321, „Sichere Netzübergreifende Sprachkommunikation (SNS)“, 2012, verfügbar unter https://www.bsi.bund.de/DE/Themen/weitereThemen/MobileSecurity/SNS/sns_node.html

[BSI BSIFB-2014] BSI, „BSI für Bürger - Sicherheit im Netz - Soziale Netze“, 2014, verfügbar unter https://www.bsi-fuer-buerger.de/BSIFB/DE/SicherheitImNetz/SozialeNetze/sozialeNetze_node.html

[BSI DrKoSi-2009] BSI, „Drahtlose Kommunikationssysteme und ihre Sicherheitsaspekte“, September 2009, verfügbar unter https://www.bsi.bund.de/DE/Publikationen/Broschueren/drahtloskom/index_htm.html

[BSI GSK-2013] BSI, „IT-Grundschutz-Kataloge“, September 2013, verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

[BSI HBbug-2014] BSI, „Heartbleed Bug: BSI sieht weiteren Handlungsbedarf“, 2014, verfügbar unter https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2014/Heartbleed_Bug_16042014.html

[BSI LogMon-2009] BSI, „Studie über die Nutzung von Log- und Monitoringdaten im Rahmen der IT-Frühwarnung und für einen sicheren IT-Betrieb“, März 2009, verfügbar unter https://www.bsi.bund.de/DE/Publikationen/publikationen_node.html

[BSI Mobil-2006] BSI, „Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen“, 2006, verfügbar unter https://www.bsi.bund.de/DE/Publikationen/Broschueren/mobile/index_htm.html

[BSI MPLS-2009] BSI, „Kurzstudie zu Gefährdungen und Maßnahmen beim Einsatz von MPLS“, Version 1.5, 2009, verfügbar unter https://www.bsi.bund.de

[BSI ÖMS-2008] BSI, „Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte“, Juli 2008, verfügbar unter https://www.bsi.bund.de/DE/Publikationen/Broschueren/oefms/index_htm.html

[BSI SiDECT-2012] BSI, Sicherheitshinweis: „Sicherheit von schnurlosen Telefonen nach DECT-Standard“, Februar 2012, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Sicherheitsberatung/Sicherheitshinweise/2012-02-14_Sicherheitshinweis_DECT_pdf.pdf?__blob=publicationFile

[BSI TRKrypto-2013] BSI, TR-02102 „Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, Januar 2013, verfügbar unter https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

[BSI TRWLAN-2005] BSI, „Technische Richtlinie Sicheres WLAN“, Teil 1 – 3, 2005, verfügbar unter SecuMedia Verlag

[BSI VoIPSec-2005] BSI, „VoIPSEC – Studie zur Sicherheit von Voice over Internet Protocol“, 2005, verfügbar unter http://www.bsi.de/literat/studien/VoIP/index.htm

[BSIG BTspec-2013] BSIG, „Specification of the Bluetooth System“, Version 4.1, Dezember 2013, verfügbar unter https://www.bluetooth.org/en-us/specification/adopted-specifications

[CCRA CC-2012] CCRA, Common Criteria, Version 3.1, Release 4, Part 1 - 3, September 2012, verfügbar unter http://www.commoncriteriaportal.org/cc

[DIN 14661] DIN, DIN 14661, „Feuerwehrwesen - Feuerwehr-Bedienfeld für Brandmeldeanlagen“, Februar 2011, verfügbar unter Beuth-Verlag

[DIN 14662] DIN, DIN 14662, „Feuerwehrwesen - Feuerwehr-Anzeigetableau für Brandmeldeanlagen“, Januar 2010, verfügbar unter Beuth-Verlag

[DIN 14675] DIN, DIN 14675, „Brandmeldeanlagen - Aufbau und Betrieb“, April 2012, verfügbar unter Beuth-Verlag

[DIN EN 54] DIN, DIN EN 54, „Brandmeldeanlagen“, Teil 1 bis 25, 1997 bis 2012, verfügbar unter Beuth-Verlag

[DIN VDE-0833] DIN, DIN VDE 0833, „Gefahrenmeldeanlagen für Brand, Einbruch und Überfall“, Teil 1 bis 4, 2007 bis 2009, verfügbar unter Beuth-Verlag

[ENISA CC-2009] ENISA, „Cloud Computing: Benefits, Risks and Recommendations for Information Security“, November 2009, verfügbar unter http://www.enisa.europa.eu/act/rm/files/deliverables/cloudcomputing-risk-Assessment/at_download/fullReport

[ENISA SmPh-2010] ENISA, „Smartphones: Information security risks, opportunities and recommendations for users“, Dezember 2010, verfügbar unter http://www.enisa.europa.eu/activities/identity-and-trust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-and-recommendations-for-users

[ETSI EN300175] ETSI, ETSI EN 300 175-1 bis 300 175-8, European Standard (Telecommunications Series), Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI), 2003 bis 2013, verfügbar unter http://www.etsi.org

[ETSI EN300444-2013] ETSI, ETSI EN 300 444, „Digital Enhanced Cordless Telecommunications (DECT); Generic Access Profile (GAP)“, Version 2.4.1, Juli 2013, verfügbar unter http://www.etsi.org

[ETSI EN301649-2012] ETSI, ETSI EN 301 649, „Digital Enhanced Cordless Telecommunications (DECT); DECT Packet Radio Service (DPRS)“, Version 2.2.1, Februar 2012, verfügbar unter http://www.etsi.org

[ETSI EN301650-2011] ETSI, ETSI EN 301 650, „Digital Enhanced Cordless Telecommunications (DECT); DECT Multimedia Access Profile (DMAP); Application Specific Access Profile (ASAP)“, Version 1.2.0, November 2011, verfügbar unter http://www.etsi.org

[ETSI ES282001-2009] ETSI, ETSI ES 282 001, „Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture“, ETSI Standard, Version 3.4.1, September 2009, verfügbar unter http://www.etsi.org

[ETSI TS102527] ETSI, ETSI TS 102 527 Part 1 bis 5, Digital Enhanced Cordless Telecommunications (DECT); New Generation DECT, 2007 bis 2014, verfügbar unter http://www.etsi.org

[ETSI TS103159-2014] ETSI, ETSI TS 103 159-1, „Digital Enhanced Cordless Telecommunications (DECT);Ultra Low Energy (ULE);Machine to Machine Communications;Part 1: Test Framework and Profile Test Specification (PTS)for Home Automation Network (phase 1)“, April 2014, verfügbar unter http://www.etsi.org

[ETSI TS133401-2010] ETSI, ETSI TS 133 401, „Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; 3GPP System Architecture Evolution (SAE); Security architecture (3GPP TS 33.401 version 8.7.0 Release 8)“, V8.7.0, April 2010, April 2010, verfügbar unter http://www.etsi.org

[ETSI TS187001-2011] ETSI, ETSI TS 187 001, „Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN SECurity (SEC); Requirements“, Version 3.7.1, März 2011, verfügbar unter http://www.etsi.org

[ETSI TS187003-2011] ETSI, ETSI TS 187 003, „Technical Specification Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture“, Version 3.4.1, März 2011, verfügbar unter http://www.etsi.org

[IEEE 802.11-2012] IEEE, Std 802.11, „Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications“, März 2012, verfügbar unter http://www.ieee.org

[IEEE 802.11ac-2013] IEEE, Draft Std 802.11ac, „Amd 4: Enhancements for Very High Throughput for operation in bands below 6GHz“, Version D7.0, September 2013, verfügbar unter http://www.ieee.org

[IEEE 802.11ad-2012] IEEE, Std 802.11ad, „Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 3: Enhancements for Very High Throughput in the 60 GHz Band“, Mai 2012, verfügbar unter http://www.ieee.org

[IEEE 802.1AE-2006] IEEE, Std 802.1AE, „Media Access Control (MAC) Security“, August 2006, verfügbar unter http://www.ieee.org

[IEEE 802.1Q-2011] IEEE, Std 802.1Q, „Virtual Bridged Local Area Networks“, August 2011, verfügbar unter http://www.ieee.org

[IEEE 802.1X-2010] IEEE, Std 802.1X, „Port-Based Network Access Control“, 2010, verfügbar unter http://www.ieee.org

[IEEE 802.3-2012] IEEE, Std 802.3-2012, „Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications“, 2012, verfügbar unter http://www.ieee.org

[IETF RFC2818-2000] IETF, RFC 2818, „HTTP Over TLS“, Mai 2000, verfügbar unter http://www.ietf.org/rfc/rfc2818.txt

[IETF RFC2865-2000] IETF, RFC 2865, „Remote Authentication Dial In User Service (RADIUS)“, Juni 2000, verfügbar unter http://www.ietf.org/rfc/rfc2865.txt

[IETF RFC3031-2001] IETF, RFC 3031, „Multiprotocol Label Switching Architecture“, Januar 2001, verfügbar unter http://www.ietf.org/rfc/rfc3031.txt

[IETF RFC3193-2001] IETF, RFC 3193, „Securing L2TP using IPsec“, November 2001, verfügbar unter http://www.ietf.org/rfc/rfc3193.txt

[IETF RFC3261-2002] IETF, RFC 3261, „SIP: Session Initiation Protocol“, Juni 2002, verfügbar unter http://www.ietf.org/rfc/rfc3261.txt

[IETF RFC3404-2002] IETF, RFC 3404, „Dynamic Delegation Discovery System (DDDS) Part Four: The Uniform Resource Identifiers (URI)“, Oktober 2002, verfügbar unter http://www.ietf.org/rfc/rfc3404.txt

[IETF RFC3411-2002] IETF, RFC 3411, „An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks“, Dezember 2002, verfügbar unter http://www.ietf.org/rfc/rfc3411.txt

[IETF RFC3412-2002] IETF, RFC 3412, „Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)“, Dezember 2002, verfügbar unter http://www.ietf.org/rfc/rfc3412.txt

[IETF RFC3413-2002] IETF, RFC 3413, „Simple Network Management Protocol (SNMP) Applications“, Dezember 2002, verfügbar unter http://www.ietf.org/rfc/rfc3413.txt

[IETF RFC3414-2002] IETF, RFC 3414, „User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)“, Dezember 2002, verfügbar unter http://www.ietf.org/rfc/rfc3414.txt

[IETF RFC3415-2002] IETF, RFC 3415, „View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)“, Dezember 2002, verfügbar unter http://www.ietf.org/rfc/rfc3415.txt

[IETF RFC3416-2002] IETF, RFC 3416, „Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)“, Dezember 2002, verfügbar unter http://www.ietf.org/rfc/rfc3416.txt

[IETF RFC3417-2002] IETF, RFC 3417, „Transport Mappings for the Simple Network Management Protocol (SNMP)“, Dezember 2002, verfügbar unter http://www.ietf.org/rfc/rfc3417.txt

[IETF RFC3418-2002] IETF, RFC 3418, „Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)“, Dezember 2002, verfügbar unter http://www.ietf.org/rfc/rfc3418.txt

[IETF RFC3428-2002] IETF, RFC 3428, „Session Initiation Protocol (SIP) Extension for Instant Messaging“, Dezember 2002, verfügbar unter http://www.ietf.org/rfc/rfc3428.txt

[IETF RFC3435-2003] IETF, RFC 3435, „Media Gateway Control Protocol (MGCP) Version 1.0“, Januar 2003, verfügbar unter http://www.ietf.org/rfc/rfc3435.txt

[IETF RFC3550-2003] IETF, RFC3550, „RTP: A Transport Protocol for Real-Time Applications“, Juli 2003, verfügbar unter http://www.ietf.org/rfc/rfc3550.txt

[IETF RFC3579-2003] IETF, RFC 3579, „RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP)“, September 2003, verfügbar unter http://www.ietf.org/rfc/rfc3579.txt

[IETF RFC3711-2004] IETF, RFC 3711, „The Secure Real-time Transport Protocol (SRTP)“, März 2004, verfügbar unter http://www.ietf.org/rfc/rfc3711.txt

[IETF RFC3748-2004] IETF, RFC 3748, „Extensible Authentication Protocol (EAP)“, Juni 2004, verfügbar unter http://www.ietf.org/rfc/rfc3748.txt

[IETF RFC3830-2004] IETF, RFC 3830, „MIKEY: Multimedia Internet KEYing“, August 2004, verfügbar unter http://www.ietf.org/rfc/rfc3830.txt

[IETF RFC3856-2004] IETF, RFC 3856, „A Presence Event Package for the Session Initiation Protocol (SIP)“, August 2004, verfügbar unter http://www.ietf.org/rfc/rfc3856.txt

[IETF RFC3922-2004] IETF, RFC 3922, „Mapping the Extensible Messaging and Presence Protocol (XMPP) to Common Presence and Instant Messaging (CPIM)“, Oktober 2004, verfügbar unter http://www.ietf.org/rfc/rfc3922.txt

[IETF RFC3923-2004] IETF, RFC 3923, „End-to-End Signing and Object Encryption for the Extensible Messaging and Presence Protocol (XMPP)“, Oktober 2004, verfügbar unter http://www.ietf.org/rfc/rfc3923.txt

[IETF RFC3931-2005] IETF, RFC 3931, „Layer Two Tunneling Protocol - Version 3 (L2TPv3)“, März 2005, verfügbar unter http://www.ietf.org/rfc/rfc3931.txt

[IETF RFC3947-2005] IETF, RFC 3947, „Negotiation of NAT-Traversal in the IKE“, Januar 2005, verfügbar unter http://www.ietf.org/rfc/rfc3947.txt

[IETF RFC3948-2005] IETF, RFC 3948, „UDP Encapsulation of IPsec ESP Packets“, Januar 2005, verfügbar unter http://www.ietf.org/rfc/rfc3948.txt

[IETF RFC4033-2005] IETF, RFC 4033, „DNS Security Introduction and Requirements“, März 2005, verfügbar unter http://www.ietf.org/rfc/rfc4033.txt

[IETF RFC4034-2005] IETF, RFC 4034, „Resource Records for the DNS Security Extensions“, März 2005, verfügbar unter

[IETF RFC4035-2005] IETF, RFC 4035, „Protocol Modifications for the DNS Security Extensions“, März 2005, verfügbar unter http://www.ietf.org/rfc/rfc4035.txt

[IETF RFC4301-2005] IETF, RFC 4301, „Security Architecture for the Internet Protocol“, Dezember 2005, verfügbar unter http://www.ietf.org/rfc/rfc4301.txt

[IETF RFC4302-2005] IETF, RFC 4302, „IP Authentication Header“, Dezember 2005, verfügbar unter http://www.ietf.org/rfc/rfc4302.txt

[IETF RFC4303-2005] IETF, RFC 4303, „IP Encapsulating Security Payload (ESP)“, Dezember 2005, verfügbar unter http://www.ietf.org/rfc/rfc4303.txt

[IETF RFC4480-2006] IETF, RFC 4480, „RPID: Rich Presence Extensions to the Presence Information Data Format (PIDF)“, Juli 2006, verfügbar unter http://www.ietf.org/rfc/rfc4480.txt

[IETF RFC4511-2006] IETF, RFC 4511, „Lightweight Directory Access Protocol (LDAP): The Protocol“, Juni 2006, verfügbar unter http://www.ietf.org/rfc/rfc4511.txt

[IETF RFC4568-2006] IETF, RFC 4568, „Session Description Protocol (SDP) Security Descriptions for Media Streams“, Juli 2006, verfügbar unter http://www.ietf.org/rfc/rfc4568.txt

[IETF RFC4975-2007] IETF, RFC 4975, „The Message Session Relay Protocol (MSRP)“, September 2007, verfügbar unter http://www.ietf.org/rfc/rfc4975.txt

[IETF RFC4976-2007] IETF, RFC 4976, „Relay Extensions for the Message Sessions Relay Protocol (MSRP)“, September 2007, verfügbar unter http://www.ietf.org/rfc/rfc4976.txt

[IETF RFC5025-2007] IETF, RFC 5025, „Presence Authorization Rules“, Dezember 2007, verfügbar unter http://www.ietf.org/rfc/rfc5025.txt

[IETF RFC5216-2008] IETF, RFC 5216, „The EAP-TLS Authentication Protocol“, März 2008, verfügbar unter http://www.ietf.org/rfc/rfc5216.txt

[IETF RFC5245-2010] IETF, RFC 5245, „Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols“, April 2010, verfügbar unter http://www.ietf.org/rfc/rfc5245.txt

[IETF RFC5246-2008] IETF, RFC 5246, „The Transport Layer Security (TLS) Protocol - Version 1.2“, August 2008, verfügbar unter http://www.ietf.org/rfc/rfc5246.txt

[IETF RFC5281-2008] IETF, RFC 5281, „Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol Version 0 (EAP-TTLSv0)“, August 2008, verfügbar unter http://www.ietf.org/rfc/rfc5281.txt

[IETF RFC5389-2008] IETF, RFC 5389, „Session Traversal Utilities for NAT (STUN)“, Oktober 2008, verfügbar unter http://www.ietf.org/rfc/rfc5389.txt

[IETF RFC5415-2009] IETF, RFC 5415, „Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification“, März 2009, verfügbar unter http://www.ietf.org/rfc/rfc5415.txt

[IETF RFC5424-2009] IETF, RFC 5424, „The Syslog Protocol“, März 2009, verfügbar unter http://www.ietf.org/rfc/rfc5424.txt

[IETF RFC5456-2010] IETF, RFC 5456, „IAX: Inter-Asterisk eXchange Version 2“, Februar 2010, verfügbar unter http://www.ietf.org/rfc/rfc5456.txt

[IETF RFC5469-2009] IETF, RFC 5469, „DES and IDEA Cipher Suites for Transport Layer Security (TLS)“, Februar 2009, verfügbar unter http://www.ietf.org/rfc/rfc5469.txt

[IETF RFC5652-2009] IETF, RFC 5652, „Cryptographic Message Syntax (CMS)“, September 2009, verfügbar unter http://www.ietf.org/rfc/rfc5652.txt

[IETF RFC5750-2010] IETF, RFC 5750, „Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Certificate Handling“, Januar 2010, verfügbar unter http://www.ietf.org/rfc/rfc5750.txt

[IETF RFC5751-2010] IETF, RFC 5751, „Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification“, Januar 2010, verfügbar unter http://www.ietf.org/rfc/rfc5751.txt

[IETF RFC5764-2010] IETF, RFC 5764 , „Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)“, Mai 2010, verfügbar unter http://www.ietf.org/rfc/rfc5764.txt

[IETF RFC5766-2010] IETF, RFC 5766, „Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)“, April 2010, verfügbar unter http://www.ietf.org/rfc/rfc6347.txt

[IETF RFC5996-2010] IETF, RFC 5996, „Internet Key Exchange Protocol Version 2 (IKEv2)“, September 2010, verfügbar unter http://www.ietf.org/rfc/rfc5996.txt

[IETF RFC6116-2011] IETF, RFC 6116, „The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)“, März 2011, verfügbar unter http://www.ietf.org/rfc/rfc6116.txt

[IETF RFC6117-2011] IETF, RFC 6117, „IANA Registration of Enumservices: Guide, Template, and IANA Considerations“, März 2011, verfügbar unter http://www.ietf.org/rfc/rfc6117.txt

[IETF RFC6120-2011] IETF, RFC 6120, „Extensible Messaging and Presence Protocol (XMPP): Core“, März 2011, verfügbar unter http://www.ietf.org/rfc/rfc6120.txt

[IETF RFC6121-2011] IETF, RFC 6121, „Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence“, März 2011, verfügbar unter http://www.ietf.org/rfc/rfc6121.txt

[IETF RFC6122-2011] IETF, RFC 6122, „Extensible Messaging and Presence Protocol (XMPP): Address Format“, März 2011, verfügbar unter http://www.ietf.org/rfc/rfc6122.txt

[IETF RFC6188-2011] IETF, RFC 6188, „The Use of AES-192 and AES-256 in Secure RTP“, März 2011, verfügbar unter http://www.ietf.org/rfc/rfc6188.txt

[IETF RFC6347-2012] IETF, RFC 6347, „Datagram Transport Layer Security Version 1.2“, Januar 2012, verfügbar unter http://www.ietf.org/rfc/rfc6347.txt

[IETF RFC6407-2011] IETF, RFC 6407, „The Group Domain of Interpretation“, Oktober 2011, verfügbar unter http://www.ietf.org/rfc/rfc6407.txt

[IETF RFC6562-2012] IETF, RFC 6562, „Guidelines for the Use of Variable Bit Rate Audio with Secure RTP“, März 2012, verfügbar unter http://www.ietf.org/rfc/rfc6562.txt

[ISO 18051-2012] ISO/IEC, ISO/IEC 18051, „Services for Computer Supported Telecommunications Applications (CSTA) Phase III“, September 2012, verfügbar unter Beuth-Verlag

[ISO 18052-2012] ISO/IEC, ISO/IEC 18052, „ASN.1 for Computer Supported Telecommunications Applications (CSTA) Phase III“, September 2012, verfügbar unter Beuth-Verlag

[ITU E.164-2010] ITU-T, E.164, „The international public telecommunication numbering plan“, November 2010, verfügbar unter http://www.itu.int/rec/T-REC-E.164-201011-I/en

[ITU H.225-2009] ITU-T, H.225.0, „Call signalling protocols and media stream packetization for packet-based multimedia communication systems“, Dezember 2009, verfügbar unter http://www.itu.int/rec/T-REC-H.225.0-200912-I/en

[ITU H.235-2005] ITU-T, H.235.0, „H.323 security: Framework for security in H series (H.323 and other H.245-based) multimedia systems“, September 2005, verfügbar unter http://www.itu.int/rec/T-REC-H.235.0-200509-I/en

[ITU H.245-2011] ITU-T, H.245, „Control protocol for multimedia communication“, Mai 2011, verfügbar unter http://www.itu.int/rec/T-REC-H.245-201105-I/en

[ITU H.248-2013] ITU-T, H.248.1, „Gateway control protocol: Version 3“, März 2013, verfügbar unter http://www.itu.int/rec/T-REC-H.248.1-201303-I/en

[ITU H.323-2009] ITU-T, H.323, „Packet-based multimedia communications systems“, Dezember 2009, verfügbar unter http://www.itu.int/rec/T-REC-H.323-200912-I/en

[ITU H.460.17-2005] ITU-T, H.460.17, „Using H.225.0 call signalling connection as transport for H.323 RAS messages“, September 2005, verfügbar unter http://www.itu.int/rec/T-REC-H.460.17-200509-I/en

[ITU T.38-2010] ITU-T, T.38, „Procedures for real-time Group 3 facsimile communication over IP networks“, September 2010, verfügbar unter http://www.itu.int/rec/T-REC-T.38-201009-I/en

[ITU X.509-2012] ITU-T, X.509, „Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks“, Oktober 2012, verfügbar unter http://www.itu.int/rec/T-REC-X.509-201210-P/en

[NIST FIPS186-2013] NIST, FIPS 186-4, „Digital Signature Standard (DSS)“, Juli 2013, verfügbar unter http://csrc.nist.gov/publications/PubsFIPS.html

[NIST NVD160-2014] NIST, NIST, National Vulnerability Data Base, „Vulnerability Summary for CVE-2014-0160“, 2014, verfügbar unter http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-0160

[NIST SP800145-2011] NIST, NIST Special Publication 800-145, „The NIST Definition of Cloud Computing“, September 2011, verfügbar unter http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[SIP TR-2011] SIP Forum, SIP-PBX / Service Provider Interoperability, „SIPconnect Technical Recommendation“, Version 1.1, März 2011, verfügbar unter http://www.sipforum.org

Abkürzungsverzeichnis

Ziffern

3DES	Triple DES (= TDES)
3GPP	3rd Generation Partnership Project

A

AAA	Authentication, Authorization & Accounting
ACD	Automatic Call Distribution
ACK	Acknowledge
ACL	Access Control List
ACM	Association for Computing Machinery
AD	(Microsoft) Active Directory
AES	Advanced Encryption Standard
AFH	(Bluetooth) Adaptive Frequency Hopping
AH	Authentication Header
ALG	Application Layer Gateway
AMIS	Audio Messaging Interchange Specification
API	Application Programming Interface
APN	Access Point Name
APNS	Apple Push Notification Service
App	(Smartphone) Application
ARP	Address Resolution Protocol
ASAP	Application Specific Access Profile
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
ATM	Asynchronous Transfer Mode
AuC	Authentication Center
AV	Audio und Video

B

B2B	Business-to-Business
B2C	Business-to-Customer
BCM	Business Continuity Management
BCP	Best Current Practice (IETF)
BDSG	Bundesdatenschutzgesetz
BMA	Brand-Melde-Anlage
BMZ	Brand-Melde-Zentrale
BPDU	STP Bridge Protocol Data Unit
BPI	Business Process Integration
BR	(Bluetooth) Basic Rate
BSC	(LTE) Base Station Controller
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Bluetooth Special Interest Group
BYOD	Bring Your Own Device

C

CA	Certificate Authority
CAC	Call Admission Control
CAPWAP	Control and Provisioning of Wireless Access Points
CAT-iq	(DECT) Cordless Advanced Technology – internet and quality
CBC	Cipher Block Chaining (DES)
CCITT	Comité Consultatif International de Télégraphique et Téléphonique
CCMP	Cipher Block Chaining Message Authentication Code Protocol
CCTV	Closed Circuit Television (Videoüberwachungsanlage)
CDR	Call Detail Record
CE	(MPLS) Customer Edge
CEBP	Communications Enabled Business Processes
CERT	Computer Emergency Response Teams
CHAP	Challenge Handshake Authentication Protocol
CI	Common Interface
CLIP	Calling Line Identification Presentation
CLIR	Calling Line Identification Restriction
CMS	Cryptographic Message Syntax
CPIM	Common Presence and Instant Messaging
CPU	Central Processing Unit
CRIME	Compression Ratio Info-leak Made Easy (Security Exploit)
CRL	Certificate Revocation List
CRM	Customer Relationship Management
CS	circuit-switched Services
CSMA/CD	Carrier Multiple Access/Collision Detection
CSP	Cloud Service Provider
CSTA	Computer Supported Telecommunications Applications
CTI	Computer Telephony Integration

D

DB	Datenbank (engl. Data Base)
DBMS	Datenbankmanagementsystem
DCOM	Distributed Component Object Model
DDNS	Dynamic Domain Name System
DECT	Digital Enhanced Cordless Telecommunications
DES	Data Encryption Standard
DFS	DECT Fixed System
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DIN	Deutsches Institut für Normung
DISA	Direct Inward System Access
DLP	Data Loss Prevention
DMAP	DECT Multimedia Access Profile
DMS	Dokumentenmanagementsystem
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions

DoD	Department of Defense
DoS	Denial of Service
DPD	(IKE) Dead Peer Detection
DPRS	DECT Packet Radio Service
DSA	Digital Signature Algorithm
DSAA	DECT Standard Authentication Algorithm
DSC	DECT Standard Cipher
DSS	Digital Signature Standard
DSS1	Digital Subscriber System No. 1
DTLS	Datagram TLS
DUN	(Bluetooth) Dialup Network Profile

E

E-Mail	Electronic Mail
E-UTRAN	(LTE) Evolved UMTS Terrestrial Radio Access Network
EAL	Evaluation Assurance Level (Common Criteria)
EAP	Extensible Authentication Protocol
EAP-MD5	Extensible Authentication Protocol - Message Digest Algorithm 5
EAP-MSCHAP	EAP Method Microsoft Challenge Handshake Authentication Protocol
EAP-TLS	EAP Method Transport Layer Security
EAP-TTLS	EAP Method Tunneled TLS
EAPOL	EAP over LAN
ECDH	Eliptic Curve Diffie Hellman-Verfahren
ECDSA	Elliptic Curve Digital Signature Algorithm
EDE	Encrypt Decrypt Encrypt
EDGE	Enhanced Data Rates for GSM Evolution
EDR	(Bluetooth) Enhanced Data Rate
EEA	Evolved Encryption Algorithm
EIR	(UMTS) Equipment Identity Register
EMS	Enhanced Messaging Service
EN	Europäische Norm
ENISA	European Network and Information Security Agency
eNodeB	(LTE) E-UTRAN Node B bzw. Evolved Node B
ENUM	E.164 Telephone Number Mapping
EPC	(LTE) Evolved Packet Core
ERM	Enterprise Resource Management
ES	(ETSI) European Standard
ESP	Encapsulated Security Payloads
ETB	Elektronische Telefonbücher
ETSI	European Telecommunications Standards Institute

F

FAT	Feuerwehr-Anzeigetableau
FBF	Feuerwehr-Bedienfeld
FCR	(ACD) First Call Resolution
FIPS	(NIST) Federal Information Processing Standard
FIT	Feuerwehr-Informations-Tableau
FMC	Fixed Mobile Convergence

FOTA	Firmware Over the Air
FP	(DECT) Fixed Part
FTP	File Transfer Protocol
FTPS	FTP over SSL

G

GAP	(DECT) Generic Access Profile
Gbit/s	Gigabit/Sekunde
GEA	GPRS Encryption Algorithm
GEMA	Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte
GERAN	GSM EDGE Radio Access Network
GET-VPN	(Cisco) Group Encrypted Transport VPN
GGSN	(UMTS) Gateway GPRS Support Node
GHz	GigaHertz
GMSC	(UMTS) Gateway MSC
GPRS	General Packet Radio Service
GPS	Global Positioning System
GRE	Generic Routing Encapsulation
GSK	(BSI IT-) Grundschutz-Kataloge
GSM	Global System for Mobile Communications
GW	Gateway

H

HD	High Definition
HLR	(UMTS) Home Location Register
HMAC	(Keyed-)Hash Message Authentication Code
HPLMN	Home Public Land Mobile Network
HSDPA	High Speed Downlink Packet Access
HSPA	High Speed Packet Access
HSS	(LTE) Home Subscriber Server
HSUPA	High Speed Uplink Packet Access
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over TLS / HTTP Secure

I

IaaS	Infrastructure as a Service
IAD	Integrated Access Device
IANA	Internet Assigned Numbers Authority
IAX	Inter-Asterisk eXchange
ICA	Independent Computing Architecture
ICE	Interactive Connectivity Establishment
ICMP	Internet Control Message Protocol
ID	Identity
IDEA	International Data Encryption Algorithm
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers

IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IKE-SA	IKE – Security Association
IM	Instant Messaging
IMAP	Internet Message Access Protocol
IMS	IP Multimedia Subsystem
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IP-PBX	Internet Protocol - Private Branch eXchange
IPcomp	(Internet Protocol) Payload Compression Protocol
IPS	Intrusion Prevention System
IPsec	IP Security
IPv4	Internet Protocol, Version 4
IPv6	Internet Protocol, Version 6
IQ	Info/Query
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISM-Band	Industrial, Scientific, and Medical Band
ISO	International Standards Organization
ISP	Internet Service Provider
IT	Information Technology
ITSP	Internet Telephony Service Provider
ITU	International Telecommunication Union (Internationale Fernmeldeunion)
ITU-T	ITU - Telecommunication Standardization Sector
IVR	Interactive Voice Response
IWU	(DECT) Interworking Unit

J

JTAPI	Java Telephony API

K

kbit/s	Kilobit/Sekunde

L

L2/L3	(OSI) Layer 2 / Layer 3
L2TP	Layer 2 Tunneling Protocol
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LE	(Bluetooth) Low Energy
LED	Light-Emitting Diode
LLC	Logical Link Control
LLDP-MED	Link Layer Discovery Protocol - Media Endpoint Discovery
LTE	Long Term Evolution

M

MAC	Media Access Control
MACsec	MAC Security
MAN	Metropolitan Area Network
MAPI-RPC	Messaging Application Programming Interface Remote Procedure Call

Mbit/s	Megabit/Sekunde
MCU	Multipoint Control Unit
MD5	Message-Digest Algorithm 5
MDM	Mobile Device Management
ME	Mobile Equipment
Megaco	Media Gateway Control Protocol
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MGW	Media Gateway
MHz	MegaHertz
MIB	Management Information Base
MIKEY	Multimedia Internet KEYing
MIME	Multipurpose Internet Message Extensions
MitM	Man in the Middle
MME	(LTE) Mobility Management Entity
MMS	Multimedia Messaging Service
MOBIKE	(IKE) Mobility and Multihoming Protocol
MOS	Mean Opinion Score
MPLS	Multiprotocol Label Switching
MPPE	Microsoft Point-to-Point Encryption
MSC	(UMTS) Mobile Switching Center
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSRP	Message Session Relay Protocol
mTAN	mobile TAN
MTLS	Mutual TLS

N

NAC	Network Access Control
NAPTR	Naming Authority Pointer
NAT	Network Address Translation
NAT-T	NAT Traversal
NFS	Network File System
NG DECT	New Generation DECT
NGN	Next Generation Network(s)
NIC	Network Interface Controller
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol (TCP/IP)

O

OCSP	Online Certificate Status Protocol
ODBC	Open DataBase Connectivity
ONS	One Number Service
OSI	Open Systems Interconnection
OTA	Over the Air (Provisioning)
OTP	One-Time-Password
OWA	Outlook Web Access

P

PaaS	Platform as a Service
PAP	Password Authentication Protocol
PBX	Private Branch eXchange
PC	Personal Computer
PCRF	(LTE) Policy&Charging Rules Function
PCT	Private Communications Technology
PDA	Personal Digital Assistant
PDF	Portable Document File
PDN	Packet Data Network
PE	(MPLS) Provider Edge
PEAP	Protected EAP
PEP	Personaleinsatzplanung
PGP	Pretty Good Privacy
PHY	Physical Layer
PIDF	Presence Information Data Format
PIM	Personal Information Manager
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
PoE	Power over Ethernet
PP	(DECT) Portable Parts
PPP	Point-to-Point Protocol
PPTP	Point to Point Tunneling Protocol
PSE	Personensucheinrichtung
PSK	Pre-Shared Key
PSTN	Public Switched Telephone Network

Q

QMS	Qualitäts-Management-System
QoS	Quality of Service
QSIG	Signalisierung am Q-Referenzpunkt

R

RADIUS	Remote Authentication Dial In User Service
RAM	Random Access Memory
RAN	Radio Access Network
RANAP	RAN Application Part
RAS	Registration, Admission and Status
RC4	Ron's Code 4
RCF	(H.323) Register Confirmation
rcp	remote copy
RDP	Remote Desktop Protocol
REST(-API)	Representational State Transfer (API)
rexec	remote execution
RFC	Request For Comment (IETF)
rlogin	remote login
RMS	Risiko-Management-System

RNC	Radio Network Controller
RNS	Radio Network Subsystem
RPC	Remote Procedure Call
RPID	Remote Party Identification
RR	Resource Record
RRJ	(H.323) Registration Reject
RRQ	(H.323) Register Request
RSA	Public-Key-Algorithmus nach R. Rivest, A. Shamir und L. Adleman
RSS	Really Simple Syndication
RTCP	RTP Control Protocol
RTP	Real-Time Transport Protocol
RZ	Rechenzentrum

S

S/MIME	Secure / Multipurpose Internet Mail Extensions
SA	(IPsec) Security Association
SaaS	Software as a Service
SAE	3GPP System Architecture Evolution
SBC	Session Border Controller
SBS	Social Business Software
SCP	Secure Copy Protocol
SDES	Security Descriptions for Media Streams
SDP	Session Description Protocol
SEGW	Security Gateway (Sicherheits-Gateway)
SFTP	SSH File Transfer Protocol
SGSN	(UMTS) Serving GPRS Support Node
SHA	Secure Hash Algorithm
SIG	Special Interest Group
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SIP/SIMPLE	Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions
SLA	Service Level Agreement
SMB	Server Message Block
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNM	Soziale Netzwerke und Medien
SNMP	Simple Network Management Protocol
SNP	Single Number Present
SNR	Single Number Reach
SNS	(BSI) “Sichere Netzübergreifende Sprachkommunikation”
SOA	Service-Oriented Architecture
SOHO	Small Office / Home Office
SP	(NIST) Special Publication
SPIM	Spam over Instant Messaging
SPIT	Spam over Internet Telephony
SQL	Structured Query Language
SRTCP	Secure RTP Control Protocol
SRTP	Secure Real-Time Transport Protocol

SS7	Signalling System No. 7
SSH	Secure Shell
SSID	Service Set IDentifier
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
STUN	Simple Traversal of UDP Through NATs

T

TA	Tunnelanfang
TAB	Technischen Anschlussbedingungen (Brandmeldeanlagen)
TAN	Transaktionsnummer
TAPI	Telephony Application Programming Interface
TC	Trust Center
TCP	Transmission Control Protocol
TDES	Triple DES (= 3DES)
TDM	Time Division Multiplex
TDoS	Telephony DoS
TE	Tunnelende
Telnet	Teletype Networking
TFTP	Trivial File Transfer Protocol
TIFF	Tagged Image File Format
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
TK	Telekommunikation
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TOS	Type of Service
TR	(BSI) Technische Richtlinie
TS	(ETSI) Technical Specification
TSAPI	Telephony Server API
TTLS	Tunneled TLS
TUM	True Unified Messaging
TURN	Traversal Using Relay NAT

U

UA	(SIP) User Agent
UAC	User Agent Client
UAS	User Agent Server
UC	Unified Communications
UCaaS	UC as a Service
UCC	Unified Communications & Collaboration
UDP	User Datagram Protocol
UE	User Equipment
UEA	UMTS Encryption Algorithm
UfAB V	Unterlage für die Ausschreibung und Bewertung von IT-Leistungen, Version 5
UM	Unified Messaging
UMTS	Universal Mobile Telecommunications System
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

US	United States (of America)
USA	United States of America
USB	Universal Serial Bus
USIM	UMTS Subscriber Identity Module
USM	User-based Security Model
USV	Unterbrechungsfreie Stromversorgung
UTRAN	UMTS Terrestrial Radio Access Network

V

VACM	View-based Access Control Model
VANC	VoLGA Access Network Controller
VBR	Variable Bit Rate
VBScript	Visual Basic Script
VDE	Verband der Elektrotechnik und Elektronik
VDI	Virtual Desktop Infrastructure
VID	VLAN-ID
VLAN	Virtual LAN
VLR	Visitor Location Register
VM	Virtual Machine
VoiceXML	Voice Extensible Markup Language
VoIP	Voice over IP
VoLGA	Voice over LTE via Generic Access Network
VoWLAN	Voice over WLAN
VPIM	Voice Profile for Internet Mail
VPLMN	Visited PLMN
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VTP	VLAN Trunk Protocol

W

W3C	World Wide Web Consortium
WAN	Wide Area Network
WebRTC	Web Real-Time Communication
WEP	Wired Equivalent Privacy
WINS	Windows Internet Naming Service
WLAN	Wireless Local Area Network
WMM	Wi-Fi Multimedia
WP2-PSK	WPA2-Personal
WPA	Wi-Fi Protected Access
WPA-PSK	WPA Pre-Shared Key
WRS	Wireless Relay Station
WSUS	(Microsoft) Windows Server Update Services
WWW	World Wide Web

X

XAUTH	Extended Authentication
XML	Extensible Markup Language
XMPP	eXtensible Messaging and Presence Protocol

Glossar

Begriff	Beschreibung
AAA	System aus einem oder mehreren Servern, das für die Zugangskontrolle zum Netzwerk die Funktionen Authentication, Authorization and Accounting (Authentisierung, Autorisierung und Abrechnung) realisiert. Die Kommunikation mit einem AAA-System geschieht typischerweise über das Protokoll RADIUS. Umgangssprachlich werden daher oft RADIUS-Server und AAA-Systeme gleich gesetzt.
ACL	Mittels Access Control Lists (ACLs) steuern Betriebssysteme und Anwendungsprogramme Zugriffe auf Daten und Funktionen. Insbesondere werden ACLs auf Netzwerk-Elementen (Router, Firewall) genutzt, um eine zulässige Kommunikation zu identifizieren.
Advanced Encryption Standard (AES)	Symmetrisches Verschlüsselungsverfahren mit einer variablen Schlüssellänge von 128, 192 oder 256 Bit. AES bietet ein sehr hohes Maß an Sicherheit. Das Verfahren wurde eingehenden kryptoanalytischen Prüfungen unterzogen.
Authentication-Server	Server, der die vom Benutzer übermittelten Authentifizierungsdaten verifiziert. Im Fall von RADIUS ist dies ein RADIUS-Server.
Brandmeldeanlage (BMA)	Eine Brandmeldeanlage (BMA) erfasst die Ereignisse von verschiedenen Brandmeldern (Sensoren) und wertet diese aus. Die Auswertung und ggf. erforderliche Reaktion werden im Rahmen eines vorbeugenden Brandschutzes an eine dedizierte Konsole oder an die zentrale TK-Lösung gemeldet.
Business Continuity Management (BCM)	BCM sichert in festgelegten Prozessen die Fortführung der Geschäftstätigkeit unter unvorhersehbaren erschwerten Bedingungen zu.
BYOD	Bring Your Own Device (BYOD) steht für die Möglichkeit private mobile Endgeräte, insbesondere Smartphones, in das Organisationsnetzwerk einzubinden. BYOD umfasst auch die entsprechenden Richtlinien einer Organisation, die Nutzungsart und -umfang der privaten Endgeräte regeln, insbesondere den Zugriff auf interne TK-Dienste und Soziale Netzwerke sowie das Verarbeiten und Speichern organisationsinterner Daten.
Codec	Codec ist eine Wortkreuzung aus den englischen Begriffen „coder“ und „decoder“. Ein Codec bezeichnet ein Verfahren, mit dem analoge Informationen in digitale Informationen umgewandelt werden. Bekannte Varianten sind Audio-Codec (Sprach-Codec) und Video-Codec, der Sprach bzw. Videoinformationen nach einem bestimmten Verfahren kodiert, dekodiert und ggf. komprimiert, wobei sowohl das sendende als auch das empfangende Gerät den gleichen Kodierungsstandard unterstützen müssen.
Computer Telephony Integration (CTI)	CTI bezeichnet die koordinierte Steuerung von Interaktionen über ein Telefon und einen PC, z. B. den automatischen Aufbau, Annahme und Beendigung von Telefongesprächen sowie Weitervermittlung von Gesprächen.
Conferencing	Durchführung von Besprechungen zwischen entfernten Teilnehmern über verschiedene Medien: Audio- oder Telefonkonferenz nutzt lediglich das Telefon-Medium Videokonferenz nutzt ergänzend zum Telefon auch Medien zur Übertragung der Bilder Web-Konferenz, auch Online Meeting genannt, nutzt zur Sprach- und Datenübertragung das Internet.
Demilitarisierte Zone (DMZ)	Eine demilitarisierte Zone bezeichnet eine Sicherheitszone, die typischerweise zwischen geschütztem (internen) Netz und externem Netz (z. B. Internet) eingerichtet wird. Für diese Sicherheitszone gilt meist, dass in einem festgelegten Rahmen (d. h. kontrolliert durch eine Firewall) ein Zugriff aus dem externen Netz gestattet wird (öffentlich erreichbarer Bereich der IT-Infrastruktur).

Begriff	Beschreibung
Denial of Service (DoS)	Ein Angriff vom Typ Denial of Service hat zum Ziel, die Arbeitsfähigkeit des angegriffenen Objekts möglichst stark zu reduzieren. Dies beinhaltet beispielsweise die systematische Überlastung einer Komponente durch unsinnigen Verkehr („Dummy Traffic“) oder die Herbeiführung eines Fehlerzustands durch das Einspielen fehlerhafter Nachrichten.
Diffie-Hellmann (DH)	Diffie-Hellman bezeichnet ein Schlüsselaustauschprotokoll, mit dem zwei Kommunikationspartner einen geheimen Schlüssel erzeugen, den nur diese beiden kennen. Beide senden über einen meist unsicheren Kanal jeweils eine Nachricht, aus denen dann der geheime Schlüssel erzeugt wird. Dieses mathematische Problem der Berechnung heißt Diffie-Hellman-Problem, das praktisch nicht lösbar ist. Somit kann ein Angreifer, der die Kommunikation abhört, i. A. nicht den Schlüssel reproduzieren. Um eine Kompromittierung des Verfahrens durch Modifikation der Nachrichten zu verhindern, wird das Protokoll durch digitale Signaturen ergänzt.
ETSI	Das European Telecommunications Standards Institute (ETSI) ist ein gemeinnütziges Institut, welches europaweite einheitliche Standards im Bereich der Telekommunikation spezifiziert.
GPRS	Der General Packet Radio Service, GPRS, ist ein paketorientierter Übertragungsdienst zur mobilen Datenkommunikation, mit dem Daten mit bis zu 115,2 kbit/s übertragen werden können.
GPS	Das Global Positioning System (GPS) ist ein weltweites Satellitensystem zur Ortung (Positionsbestimmung) und erreicht derzeit eine Genauigkeit von wenigen Metern. GPS ist das wichtigste Ortungsverfahren und wird in vielen Navigationssystemen genutzt.
IEEE	Das Institute of Electrical and Electronics Engineers (IEEE) ist eine Organisation von Personen aus Elektrotechnik und Ingenieurwesen und ist die weltweit führende Organisation für die Standardisierung im Bereich der Elektronik und der Informationstechnik. Bekannteste Standards sind die Standards IEEE 802.3 (Ethernet), IEEE 802.11 (WLAN) und IEEE 802.1X (Port-basierte Netzwerkzugangskontrolle) für LANs.
IETF	Die Internet Engineering Task Force (IETF) ist ein internationales Gremium aus Fachleuten der Informationstechnik, welches die Internet-Spezifikationen erarbeitet. Die relevanten Dokumente heißen RFC (Request for Comments) und sind durchnummeriert. Jeder RFC erhält eine Kategorisierung: Historic, Experimental, Informational oder Standards Track von Proposed Standard über Draft Standard bis Standard. RFCs haben aus historischen Gründen zwar Empfehlungscharakter, faktisch jedoch haben RFCs mit der Kategorisierung „Standards Track“ normativen Charakter.
IM / Chat / Gruppen-Chat	Instant Messaging (IM) bezeichnet den spontanen Versand von Kurznachrichten in Quais-Echtzeit zwischen zwei (Chat) oder mehreren Kommunikationspartnern (Gruppen-Chat).
IPS / IDS	Ein Intrusion Prevention System (IPS) bietet die Möglichkeit unerwünschte Zugriffe, Inhalte und Angriffe zu erkennen und zu unterbinden. Sobald das IPS einen Verstoß gegen die vereinbarten Regeln erkennt, erfolgen eine Protokollierung, eine Meldung an den Administrator und eine Unterbrechung der als Angriff erkannten Kommunikation. Im Gegensatz hierzu unterstützt ein Intrusion Detection System (IDS) lediglich Angriffserkennung, Protokollierung und Meldung.
ISM-Frequenzband	Lizenzfrei nutzbare Frequenzbänder, die für industrielle, wissenschaftliche und medizinische Zwecke verwendet werden können (ISM = Industrial-Scientific-Medical)
ITU	Die International Telecommunication Union (ITU), d. h. die Internationale Fernmeldeunion, mit Sitz in Genf ist eine Unterorganisation der Vereinten Nationen und erstellt Richtlinien für die technischen Aspekte der Telekommunikation.
Kontaktcenter-Agenten und -Supervisoren	Als Kontaktcenter, früher auch Callcenter oder Telefon-Beratungszentrum genannt, übernimmt für eine Organisation die Kunden- bzw. Marktkontakte. Die Mitarbeiter des Kontaktcenter, die die Anrufe tätigen (outbound) oder annehmen (inbound), werden Agenten genannt, die Schichtleiter werden häufig als Supervisoren bezeichnet.

Begriff	Beschreibung
LTE	Long Term Evolution (LTE) bezeichnet den Mobilfunkstandard der vierten Generation (3,9G), der auf UMTS basiert und sehr schnelle Datenübertragungen bis zu 300 Mbit/s ermöglicht. Erst mit LTE-Advanced ist die 4G-Definitionen der ITU-T vollständig erfüllt.
Man-in-the-Middle-Attacke	Der Angreifer positioniert sich zwischen zwei Kommunikationspartner und täuscht beiden Parteien vor, der jeweils erwartete eigentliche Partner zu sein. Dabei kann der Man in the Middle den Dialog zwischen den beiden Parteien belauschen oder auch verfälschen. Ziel ist oft die Ermittlung von Passwörtern.
Mobile Device Management (MDM)	System zur zentralisierten Verwaltung von mobilen Endgeräten einer Organisation inkl. Inventarisierung, Rollout und Fernkonfiguration, Systemmanagement und Endgeräteüberwachung sowie Fernwartung und Support
Multipoint Control Unit (MCU)	Mehrpunkt-Videokonferenzbrücke, die als Sternverteiler das Management und die Verwaltung von Konferenzschaltungen zwischen drei oder mehr Teilnehmern einer Videokonferenz durchführen.
Personal Identification Number (PIN)	Konfigurierbare, auf beiden Geräten gleiche Identifikation zur Erzeugung eines Initialisierungsschlüssels
Personensucheinrichtung (PSE)	Personensucheinrichtungen bzw. -anlagen dienen der Ortung, d. h. dem Auffinden insbesondere von Personen in Echtzeit. PSE sind immer Teil einer TK-Lösung.
Präsenzdienste	Präsenzdienste verarbeiten Informationen zur Gesprächsbereitschaft und zu den verfügbaren Kommunikationskanälen sowie zu deren grafischer Darstellung.
Pre-Shared Key (PSK)	Ein PSK ist ein vorab vereinbarter bzw. verteilter Schlüssel, der bis zur Verteilung eines neuen PSK für jede Verbindung verwendet wird
Provider	Dienstanbieter mit verschiedenen Schwerpunkten, z. B. Netzwerk-Provider, der als Mobilfunkprovider, Internet-Service-Provider oder Carrier die Infrastruktur für den Daten- und Sprachtransport bereitstellt, oder Service Provider, der über die Netzwerk-Bereitstellung hinausgehende Dienstleistungen erbringt, beispielsweise den Netzbetrieb einer Organisation oder die Bereitstellung von Sozialen Medien
Public Key Infrastructure (PKI)	System zum Erstellen, Verteilen und Prüfen von digitalen Zertifikaten
Quality of Service (QoS)	Quality of Service definiert die Dienstgüte z. B. von Daten- und Sprachübertragungen. Insbesondere In Weitverkehrsnetzen sind häufig spezielle Mechanismen zur Zusicherung von QoS. Wichtige Basis für QoS-Mechanismen sind IEEE 802.1Q für kabelgebundene Netze und IEEE 802.11e für WLAN.
RSA	RSA ist ein populärer Public-Key-Algorithmus, der nach seinen Erfindern R. Rivest, A. Shamir und L. Adleman benannt ist. RSA, ein asymmetrisches kryptografisches Verfahren zur Verschlüsselung und zur digitalen Signatur, verwendet ein Schlüsselpaar, bestehend aus einem privaten Schlüssel, der zum Entschlüsseln oder Signieren von Daten verwendet wird, und einem öffentlichen Schlüssel, mit dem man verschlüsselt oder Signaturen prüft.
Shared Secret	In der Praxis stellen Shared Secrets (gemeinsames Geheimnis) oftmals die einfachste Form dar, eine gesicherte Kommunikationsbeziehung zu etablieren, indem das gemeinsame Geheimnis für kryptografische Operationen auf beiden Seiten benutzt wird, z. B. als symmetrischer Schlüssel zur Verschlüsselung der zu übertragenden Daten
Smartphone	Smartphones sind eine Weiterentwicklung bzw. Kombination von Mobiltelefonen und PDAs und bezeichnen intelligente mobile Endgeräte, die eine Vielzahl von Applikationen (Apps) bereitstellen. Wichtige Funktionalitäten eines Smartphones sind u. a. mobiles Telefonieren, Internet-Anbindung via WLAN oder Mobilfunk, Medienabspielgerät, Digital- und Videokamera sowie ein GPS-Navigations- bzw. Ortungsgerät. Bekannteste Smartphone-Plattformen sind Android und Apple iOS.

Begriff	Beschreibung
SOAP	SOAP ist ein Protokoll zum Austausch XML-basierter Nachrichten über das insbesondere auch die Funktion eines Remote Procedure Call (RPC) realisiert werden kann.
Softphone	Softphones bieten die Möglichkeit über einen Computer Telefonie-Dienste zu nutzen und sind als Software-Komponente auf einem Endgerät, z. B. Notebook, Smartphone oder Tablet, realisiert. Ein Softphone kann auch dediziert ohne UCC-Funktionalität auftreten, jedoch beinhaltet ein UCC-Client i.d.R. ein Softphone.
Syslog	Syslog dient der Übermittlung von Log-Nachrichten in einem IP-basierten Netz. Diese Nachrichten können sowohl lokal auf dem System verarbeitet werden als auch an entfernte Syslog-Server übermittelt werden.
Tablet	Tablets sind tragbare, flache Computer, die i.d.R. mit Touchscreen, aber ohne Tastatur ausgestattet sind. Sie sind bzgl. Funktionalität und Bedienung vergleichbar zu modernen Smartphones, bieten jedoch z. T. keine Mobilfunk-Schnittstelle. Üblicherweise basieren Tablets ebenfalls auf den Betriebssysteme wie Android oder Apple iOS.
Telearbeitsplatz / Remote User	Ein Telearbeitsplatz, auch Remote User genannt, ermöglicht einem Mitarbeiter einer Organisation den Zugriff auf die Organisationsinfrastruktur von außerhalb der Organisation, z. B. vom Heimarbeitsplatz, aus einem Hotel oder von unterwegs.
Totmannschaltung	Eine Totmannschaltung überprüft als Teil einer TK-Lösung, ob eine Person handlungsfähig ist, und löst andernfalls einen vordefinierten Alarm aus.
Tracking	Tracking, auch Spurbildung genannt, ermöglicht die Nachverfolgung von (bewegten) Personen oder Objekten. Dies beinhaltet nicht nur den Aufenthaltsort (insbesondere als GPS-Tracking für PSE genutzt) sondern auch Gewohnheiten und Abwesenheiten.
UCC-Client	Dedizierte Software-Komponente auf einem Endgerät, z. B. Notebook, Smartphone oder Tablet, mit der UCC-Dienste, z. B. Präsenzdienste, genutzt werden können.
UCC-Endgerät	Hardware-Komponente, auf der ein UCC-Client verfügbar ist.
UM	Unified Messaging (UM) integriert verschiedene Nachrichtenformate, z. B. E-Mail, Fax, SMS und Sprachnachrichten, in einem einheitlichen System bzw. können über eine einzige Nutzerschnittstelle Nachrichten unterschiedlichen Formats versenden.
UMTS	Das Universal Mobile Telecommunications System (UMTS) bezeichnet den Mobilfunkstandard der dritten Generation (3G). Mit UMTS sind schnelle Datenübertragungen, bis zu 2 Mbit/s und erstmals komplexe Multimedia-Anwendungen möglich.
Virtualisierung	Erzeugung von nicht physischen, jedoch separierten Netzwerk-, Server- oder Software-Elementen und Zusammenfassung auf einer physischen Komponente, z. B. Unabhängige, virtuelle Routing-Instanzen auf einer Netzwerk-Komponente.
Wi-Fi	Wi-Fi stellt ein Gütesiegel der Wi-Fi Alliance dar, welches bestätigt, dass ein Gerät gewisse Interoperabilitäts- und Konformitätstests bestanden hat (z. B. WPA2). Die Wi-Fi Alliance, ein Herstellerkonsortium, hat basierend auf IEEE 802.11 mit Wi-Fi einen Industriestandard geschaffen. Bekannte Standards sind Wi-Fi Protected Access (WPA bzw. WPA2), der auf IEEE 802.11i basiert (WPA) und mit WPA2 alle zwingenden Anforderungen von IEEE 802.11i abdeckt, und Wi-Fi Multimedia (WMM) zur Nutzung von Unterhaltungselektronik und Multimedia über WLAN, basierend auf dem IEEE 802.11e-Standard.
Zertifikat	Von einer Certificate Authority (CA, Zertifizierungsstelle) beglaubigter öffentlicher Schlüssel, der einer Person oder einem Objekt zugeordnet ist. Von einer Certificate Authority wird auch die Certificate Revocation List (CVA) generiert, eine Zertifikatssperrliste, in der alle Zertifikate aufgeführt werden, die innerhalb ihres Gültigkeitszeitraums manuell für ungültig erklärt wurden.

Stichwortverzeichnis / Index