Bundesamt
für Sicherheit in der
Informationstechnik

BSI – Technische Leitlinie

Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf

Teil 2: Sicherheitskonzepte

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 22899 9582-0
E-Mail: bsi@bsi.bund.de
Internet: https://www.bsi.bund.de

Gliederung

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung / Vorbemerkungen

Der vorliegende **Teil 2 der Technischen Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf** ordnet die in Teil 1 spezifizierten Gefährdungen und die Sicherheitsmaßnahmen für den erhöhten Schutzbedarf typischen Kommunikationsbeziehungen zu.

Ausgehend von herkömmlichen ISDN-basierten TK-Anlagen, VoIP- und Hybrid-Systemen als Basistechnologien werden außerdem spezielle Nutzungsformen dieser Basistechnologien betrachtet. Dabei werden insbesondere auf Unified Communication and Collaboration (UCC) basierende Systeme, spezielle TK-Systeme wie Videokonferenzsysteme, Kontaktcenter, Händlersysteme und Alarmierungssysteme sowie Provider-basierte TK-Dienste wie Soziale Netzwerke und Soziale Medien (engl. Social Networks and Social Media), Outsourcing und Cloud-Computing untersucht. Ergänzend zu den Basistechnologien und den hierauf basierenden speziellen Nutzungsformen wird die Integration von drahtlosen und mobilen Kommunikationssystemen in derartige Systeme zur Realisierung einer sicheren Gesamtlösung betrachtet (siehe Abbildung 1).

Um den Anwender dieser Technischen Leitlinie bei der Erstellung des Sicherheitskonzeptes zu unterstützen, werden in Kapitel 2 zunächst die grundlegende Vorgehensweise bei der Auswahl und Umsetzung der Sicherheitsmaßnahmen sowie die relevanten Kommunikationsschnittstellen einer Organisation spezifiziert.

In Kapitel 3 werden die in **Teil 1 der Technischen Leitlinie** erarbeiteten Sicherheitsmaßnahmen je Technologie diesen Kommunikationsschnittstellen zugeordnet. Diese Zuordnungen gelten grundsätzlich für alle Organisationsgrößen. Im Detail sind aber Sonderbetrachtungen für kleinere Standorte erforderlich.

Auf Basis der in Kapitel 2.4 skizzierten repräsentativen Einsatzszenarien für verschiedene Organisationsgrößen werden diese Szenarien in Kapitel 4 detailliert dargestellt und bezüglich ihrer Kommunikationsbeziehungen analysiert. Im Rahmen eines beispielhaften Sicherheitskonzepts werden für diese Szenarien die empfohlenen Maßnahmen für einen erhöhten Schutzbedarf dargestellt.

Aufbauend auf Teil 1 und Teil 2 enthält der **Teil 3 der Technische Leitlinie** abschließend einen Beschaffungsleitfaden, der zur Unterstützung bei der Beschaffung von TK-Lösungen Kriterien für die Auswahl von Komponenten einer TK-Lösung und Kriterien für die Prüfung von TK-Lösungen und deren Komponenten spezifiziert.

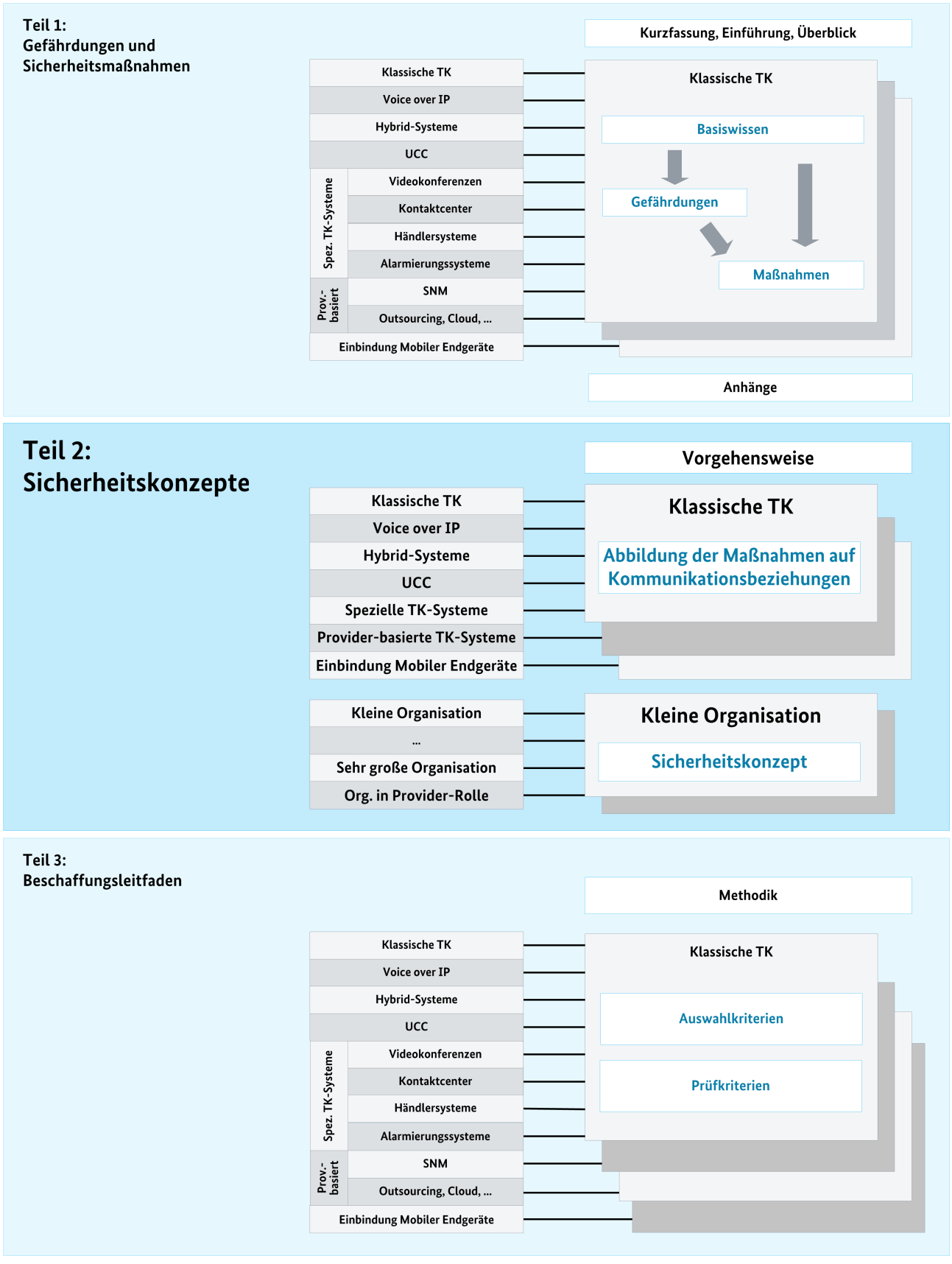

Abbildung 1: Struktur der Technischen Leitlinie

2 Vorgehensweise

2.1 Grundschutz als Ausgangsbasis

Unabhängig von der Größe eines Szenarios darf ein bestimmtes Sicherheitsniveau nicht unterschritten werden. Die Wahrung von vertraulichen Inhalten muss grundsätzlich gewährleistet werden.

Das normale Sicherheitsniveau hinsichtlich Verfügbarkeit bedeutet, dass Telekommunikation als zuverlässige Kommunikationsmöglichkeit genutzt werden kann. Jedoch sind hiermit noch nicht Anforderungen durch einen erhöhten Schutzbedarf abgedeckt. Ein erhöhter Schutzbedarf kann hinsichtlich Verfügbarkeit bestehen, z. B. dass auch durch gezielte Angriffe die Verfügbarkeit der Telekommunikation gegeben sein muss, sowie hinsichtlich Vertraulichkeit. Die Erreichung des normalen Sicherheitsniveaus ist vorrangig Gegenstand der vom Bundesamt für Sicherheit in der Informationstechnik veröffentlichten IT-Grundschutz-Kataloge (siehe [BSI GSK-2013]). Die konforme Umsetzung der darin für ein Szenario passenden Bausteine und Maßnahmen wird im Weiteren als Ausgangsbasis vorausgesetzt.

Schwerpunkt der nachfolgenden Ausführungen zur Erarbeitung von Sicherheitskonzepten für typische Beispielszenarien ist das Erreichen eines Sicherheitsniveaus, das erhöhtem Schutzbedarf gerecht wird. Die Ausführungen sollten daher insbesondere für ergänzende Sicherheitsanalysen herangezogen werden, falls bei erhöhtem Schutzbedarf gezielt bestimmte Gefährdungen mit Zusatzmaßnahmen mit einem überdurchschnittlichen Aufwand behandelt werden (siehe auch [BSI 100/3-2008]).

Im Sinne dieses Ansatzes verstehen sich die nachfolgenden Ausführungen als Hilfe, um für unterschiedliche Szenarien, bei denen im Rahmen eines strukturierten Risikomanagements ein erhöhter Schutzbedarf erkannt wird, gezielte Maßnahmen zu ergreifen.

2.2 Gestufte Umsetzung der Sicherheitsmaßnahmen

Aus den genannten Überlegungen und Ansätzen ergibt sich folgende Vorgehensweise, die auch für die nachträgliche Absicherung einer vorhandene Telekommunikationslösungen sinngemäß gilt.

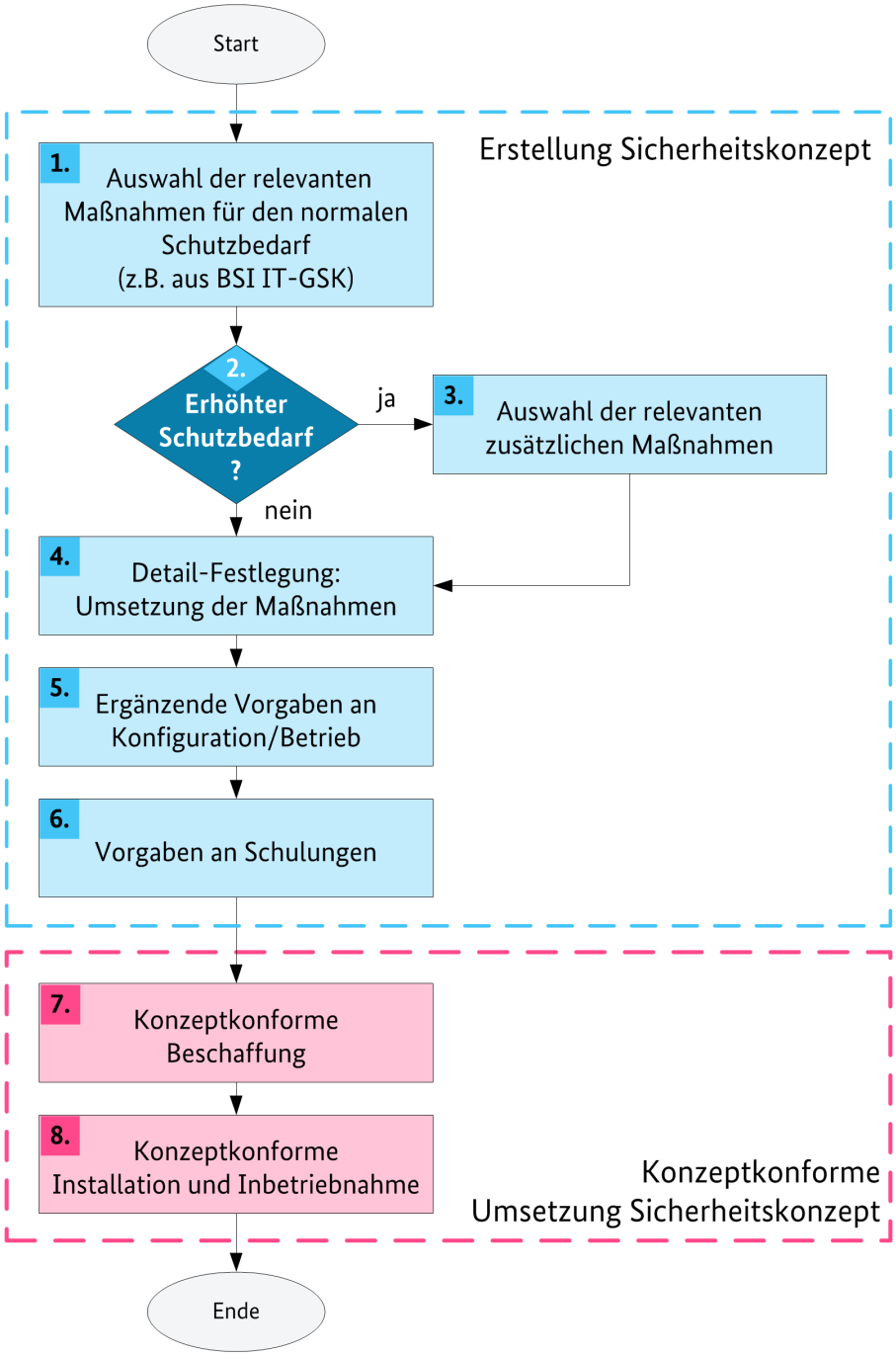

Abbildung 2: Gestufte Vorgehensweise

Für die einzelnen Stufen sind jeweils die folgenden Punkte zu beachten:

1. Auswahl der relevanten Maßnahmen für den normalen Schutzbedarf

   Unabhängig von einem ggf. erhöhten Schutzbedarf muss ein Sicherheitskonzept für eine TK-Lösung eine Absicherung gemäß normalem Schutzbedarf gewährleisten. Hierfür sind zunächst insbesondere die Maßnahmen der IT-Grundschutz-Kataloge auszuwählen, die für die eingesetzte Technik spezifiziert sind.

2. Feststellung des Schutzbedarfs

   Als grundlegendes Ergebnis der Analyse ist festzustellen, ob ein erhöhter Schutzbedarf besteht.

3. Auswahl der zusätzlich erforderlichen relevanten Maßnahmen

   Ergänzend zu den Maßnahmen für normalen Schutzbedarf sind für den erhöhten Schutzbedarf gemäß der Tabellen in Kapitel 3 die relevanten Maßnahmen entsprechend der eingesetzten Technik und Standortgröße auszuwählen.

4. Detail-Festlegungen zur Maßnahmen-Umsetzung

   Für die konkrete Festlegung, wie die entsprechenden Maßnahmen im Detail umzusetzen sind, ergeben sich wichtige Anforderungen, die bei der Beschaffung berücksichtigt werden müssen:

   - Insbesondere Maßnahmen für erhöhten Schutzbedarf können spezielle Funktionalitäten und Administrationsmöglichkeiten für die eingesetzten Endgeräte und zentralen Komponenten bedingen.
   - Zum Teil ist auch Zusatzequipment notwendig, für das der konkrete Einsatz und die Positionierung im Rahmen des Sicherheitskonzepts festgelegt werden muss.
   - Je nach Einsatz der Endgeräte werden spezielle Realisierungsformen erforderlich, z. B. Lösungen für mobilen Einsatz.

5. Vorgaben an Konfiguration und Betrieb

   Hiermit wird der Rahmen für den Betrieb der Lösung durch internes Personal wie auch durch externen Support geschaffen. Entsprechend dem festgestellten Schutzbedarf sind durch das Sicherheitskonzept insbesondere zu regeln:

   - Zulässige Formen der Administration innerhalb von Standorten, z. B. konfigurierende Zugriffe von Administrator-Arbeitsplätzen oder kontrollierende Zugriffe von Überwachungsplätzen aus. Diese sind entsprechend dem Schutzbedarf zu beschränken bzw. abzusichern.
   - Zulässige Formen der Remote-Administration von außerhalb der Standorte, z. B. Support-Zugriffe durch Externe sowie gegebenenfalls Zugriffe von Administrator-Heimarbeitsplätzen, etwa im Rahmen von Bereitschaftsregelungen.
   - Über die Absicherung des Remote-Zugriffs hinaus ist zu regeln, ob und inwiefern die Zugriffsmöglichkeiten Externer im Detail eingeschränkt werden. Bestimmte administrative Zugriffe können Externen grundsätzlich vorenthalten bzw. nur unter organisatorischen Zusatzauflagen wie z. B. Vier-Augen-Prinzip zugänglich gemacht werden.
   - Die dem Schutzbedarf angemessene Überwachungskonzeption legt fest, inwieweit typische Überwachungsmittel, z. B. Permanentüberwachung und Logging, sowie eventuell gezielte Zusatzhilfsmittel erforderlich sind. Hierbei sind Aspekte des Datenschutzes und der Mitbestimmungspflicht ebenso zu berücksichtigen wie gegebenenfalls einzuhaltende Aufbewahrungspflichten für Daten als Basis von Sicherheitsanalysen im Verdachts- oder Revisionsfall.

6. Gezielte Schulungskonzeption

   Eine umfassende Schulungskonzeption ist essentielle Voraussetzung, um das angestrebte Sicherheitsniveau zu erreichen. Gerade bei Telekommunikation kann die Technik nur die Voraussetzungen für das erreichbare Sicherheitsniveau schaffen, das tatsächlich erzielte Sicherheitsniveau ist stark vom Faktor Mensch abhängig.

   Mangelnde Bediensicherheit seitens der TK-Nutzer kann einerseits zu versehentlicher Gefährdung von Vertraulichkeit und Integrität führen sowie andererseits dazu führen, dass Nutzungsmöglichkeiten nicht verfügbar erscheinen, d. h. die Telekommunikationslösung erreicht nicht den vorgesehenen Nutzwert.

   Mangelnde Produkt- oder Konzeptkenntnis der Administratoren kann zur signifikanten Schwächung von ergriffenen Sicherheitsmaßnahmen führen.

   Hierzu sollte bereits im Rahmen des Sicherheitskonzepts festgelegt werden,

   - wann und in welcher Form welche Kenntnisse geschult werden sowie

- in welcher Form die sichere Anwendung der geschulten Inhalte gezielt unterstützt werden soll (Handzettel zur Telefonienutzung für Anwender, Arbeitsanweisungen, zugehörige Checklisten für Administratoren, ...).

7. Konzeptkonforme Beschaffung

   Die Umsetzung des ausgearbeiteten Sicherheitskonzepts beinhaltet einerseits die Beschaffung von TK-Komponenten durch

   - Austausch von Geräten,
   - Austausch von Software auf vorhandenen Geräten oder
   - Beschaffung zusätzlicher Ausstattung.

   Andererseits muss die Beschaffung von externen Dienstleistungen berücksichtigt werden:

   - Lieferanten müssen zur konzeptkonformen Detailkonzeption und Installation verpflichtet werden.
   - Supportleistungen müssen so angefragt und beauftragt werden, dass die Konzeptelemente zum sicheren Betrieb verbindlich geregelt sind und damit umgesetzt werden.

   Hilfestellung bei diesem wichtigen Schritt gibt der Beschaffungsleitfaden in Teil 3 dieser Technischen Leitlinie.

8. Konzeptkonforme Installation und Inbetriebnahme

   Eine gezielte Qualitätssicherung muss einer Freigabe zur produktiven Nutzung vorausgehen. Bei externen Installations- und Inbetriebnahmeleistungen ist eine formale Abnahme insbesondere der Vorgaben des Sicherheitskonzepts wichtig. Verstöße gegen das Sicherheitskonzept sollten zur Abnahmeverweigerung führen, dies ist für die Beschaffung zwingend zu vereinbaren.

   Bei Produktivsetzung sollte weiterhin geprüft werden:

   - Eindeutige, als Betriebsbasis brauchbare Dokumentation der Installationszustände
   - Einbindung der TK-Lösung in vorgesehene Überwachungs- und Logging-Lösungen

2.3 Kommunikationsbeziehungen einer Organisation

Die spezifischen Maßnahmen für die in Teil 1 der Technischen Leitlinie beschriebenen Technologien wurden nach Wirkbereichen (zentrales System, Endgeräte usw.) systematisiert dargelegt und soweit erläutert, dass ein grundsätzliches Verständnis der Maßnahmen gegeben ist.

Unterscheidungen wurden zunächst nur nach Technologien getroffen, d. h. es wird nach Maßnahmen unterschieden, die für klassische TK-Lösungen greifen, die für VoIP-Systeme greifen usw.

Hierauf aufbauend werden im Folgenden für eine Organisation die grundsätzliche Organisationsstruktur und mögliche Kommunikationsbeziehungen bzw. Kommunikationsendpunkte unterschieden und betrachtet, die sich aus der Praxiserfahrung ergeben.

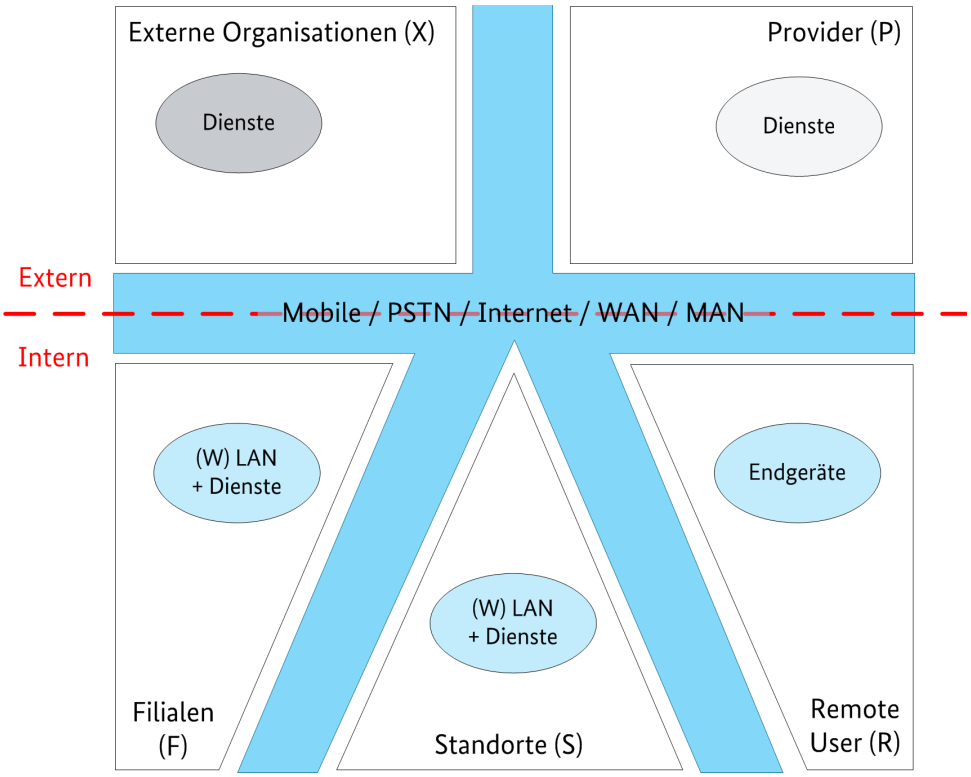

Abbildung 3: Typische Kommunikationsendpunkte einer Organisation

Es sind grundsätzlich fünf Kommunikationsendpunkte innerhalb einer Organisation zu betrachten (siehe Abbildung 3):

- Standorte

  Standorte unterhalten eigenständige TK-Installationen, z. B. mit eigener TK-Anlage. Jede Organisation umfasst mindestens einen Standort, abhängig von der Organisationsgröße jedoch auch mehrere Standorte, z. B. einen Hauptstandort und mehrere nachgelagerte Standorte unterschiedlicher Größe. Je nach Größe des Standortes und Betriebsstruktur der Organisation stellt ein Standort eigenes Know-how zum Betrieb der Anlage bereit und stellt ggf. für Außenstellen, d. h. nachgelagerte kleinere Standorte oder Filialen, zentrale Komponenten und Betrieb bzw. Support zur Verfügung.

- Filialen

  Filialen unterhalten keine eigenständige TK-Installation, sondern sind grundsätzlich an einen Standort angebunden, dessen zentrale Komponenten und Betriebsinfrastruktur mitgenutzt werden, z. B. TK-

Server mit umfassenden Funktionalitäten, Terminal-Server oder PSTN-Gateway. Abhängig von der Größe einer Organisation kann ein Standort mehrere Filialen anbinden.

Komponenten, die in Filialen trotzdem bereitgestellt werden können, sind:

- Komponenten für Notbetrieb, z. B. PSTN-Anschluss über ein Voice-Gateway zur Bereitstellung eines rudimentären TK-Servers oder über NTBA zur Bereitstellung eines Notfalltelefons
- Netz- und Sicherheitskomponenten zur sicheren Internet- bzw. WAN-Anbindung, z. B. Router mit integrierter Firewall und ggf. integriertem lokalem DNS- und DHCP-Server
- VPN-Gateway (dediziert oder integriert) zur gesicherten Internet-Anbindung an den übergeordneten Standort
- abgesetzte Komponenten einer Alarmierungslösung, z. B. Meldestation zur örtlichen Feuerwehr

Erfordern Außenstellen über die obigen Komponenten hinausgehende TK-Installationen, z. B. ein umfassendes lokales Notsystem oder ein Videokonferenzsystem mit Access-Server und MCU, werden derartige Außenstellen im Folgenden als kleine Standorte betrachtet.

- Remote User

  Remote User umfassen neben dem klassischen Heimarbeitsplatz auch alle mobilen Arbeitsplätze, z. B. Kommunikation von Nutzern auf Reisen. Remote User stellen keine eigene lokale TK- und Netzinfrastruktur, sondern nutzen den Arbeitsplatz und dessen Anbindung an Mobilfunk oder Internet zur Kommunikation.

Für die zuvor genannten internen Organisationseinheiten kann die IT-Sicherheit der Organisation verbindliche Sicherheitsvorgaben spezifizieren und durchsetzen.

- Provider

  Provider stellen eigene Dienste, z. B. für Social Media (siehe Kapitel „Soziale Netzwerke und Soziale Medien“ in Teil 1 der Technischen Leitlinie), zur Verfügung oder betreiben für eine Organisation ausgelagerte Dienste, z. B. Application Hosting oder UC as a Service (siehe Kapitel „Outsourcing, IP-Centrex, Cloud Computing und UC as a Service“ in Teil 1 der Technischen Leitlinie). Die Erfüllung von Vorgaben der IT-Sicherheit müssen hier über vertragliche Regelungen sichergestellt werden.

  In diesem Zusammenhang werden ausschließlich Provider betrachtet, die Dienste bereitstellen, sogenannte Service-Provider. Provider, die Netzverbindungen bereitstellen, sogenannte Netzwerk-Provider, werden im Rahmen dieser Leitlinie als Kommunikationsendpunkt nicht betrachtet.

- Externe Organisationen

  Externe Organisationen sind meist ebenfalls Standorte, die der eigenen Organisation Dienste bereitstellen, jedoch nicht den Weisungen der eigenen Organisation unterliegen, d. h. für die die IT-Sicherheit der eigenen Organisation keine verbindlichen Sicherheitsvorgaben durchsetzen kann. Andererseits fallen unter externe Organisationen auch solche, die eine Dienstleistung von der eigenen Organisation empfangen oder bzgl. der IT-Sicherheit (vertraglich) beeinflussbar sind, wie etwa Kunden oder Tochterunternehmen.

Diese Kommunikationsendpunkte kommunizieren sowohl innerhalb der Standorte bzw. Filialen über LAN bzw. WLAN als auch zu anderen Kommunikationsendpunkten via öffentlichem Netz, d. h. Mobilnetz, PSTN, Internet, WAN/MAN (siehe Abbildung 3). Insbesondere muss hier die interne Kommunikation einer Organisation zwischen Standorten, Filialen und Remote User von der externen Kommunikation zu Providern und externen Organisationen unterschieden und entsprechend abgesichert werden.

Zwischen den beschriebenen Kommunikationsendpunkten sind für ein Sicherheitskonzept die in Abbildung 4 dargestellten internen Kommunikationsbeziehungen im Detail zu berücksichtigen:

- Standort-interne Kommunikation, die ausschließlich das interne LAN bzw. WLAN als Kommunikationsbasis für den Zugriff auf die Dienste nutzt

- Kommunikation zwischen zwei Standorten, z. B. Zugriff auf einen Dienst eines übergeordneten Standortes; für die Kommunikation muss zwingend ein öffentliches Netz, d. h. Mobile Network, PSTN, Internet, WAN oder MAN, genutzt werden
- Kommunikation zwischen Standort und einer nachgelagerten Filiale über ein öffentliches Netz
- Filial-interne Kommunikation, die ausschließlich das interne LAN bzw. WLAN als Kommunikationsbasis für den Zugriff auf die Dienste nutzt
- Kommunikation zwischen zwei Filialen über ein öffentliches Netz
- Einbindung von Telearbeitsplätzen (Remote User) via öffentlichem Netz

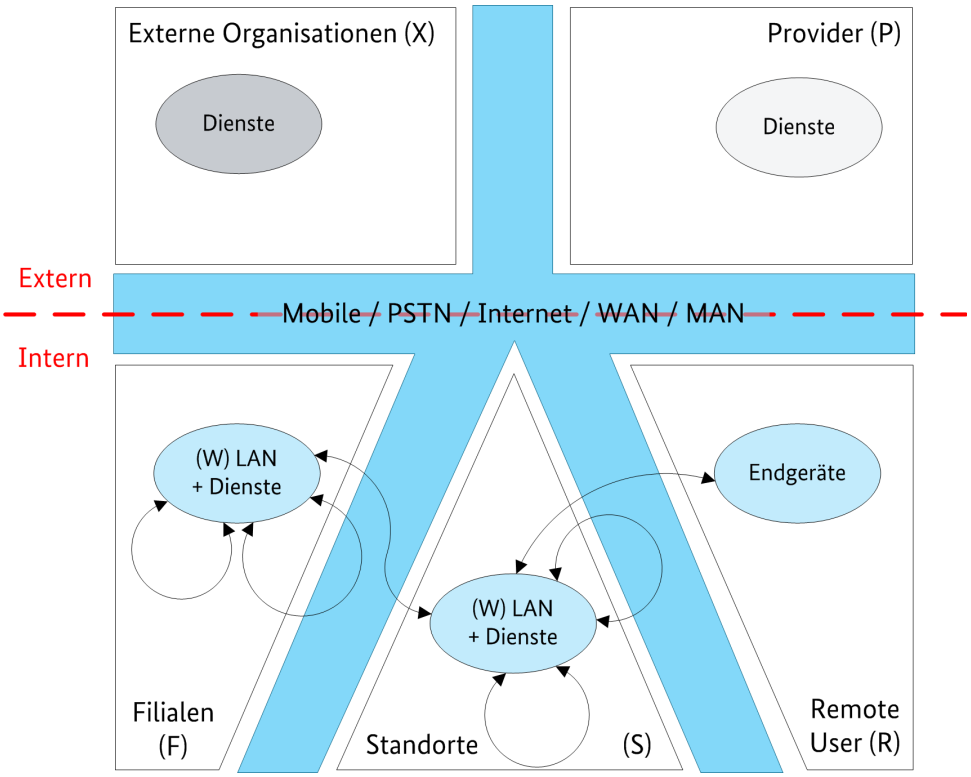

Abbildung 4: Interne Kommunikationsbeziehungen einer Organisation

Zwischen den beschriebenen Kommunikationsendpunkten sind darüber hinaus die in Abbildung 5 dargestellten externen Kommunikationsbeziehungen im Detail zu berücksichtigen:

- Kommunikation zwischen Standort und Provider-Diensten oder ausgelagerten eigenen Diensten via öffentlichem Netz
- Kommunikation zwischen einem Standort und einer externen Organisation über ein öffentliches Netz
- Kommunikation zwischen Filiale und Provider-Diensten via öffentlichem Netz
- Anbindung von Telearbeitsplätzen (Remote User) an Provider-Dienste über ein öffentliches Netz
- Anbindung von externen Organisationen an Provider-Dienste, z. B. zum Austausch von Informationen zwischen ausgelagerten Diensten der eigenen Organisation und externen Organisationen

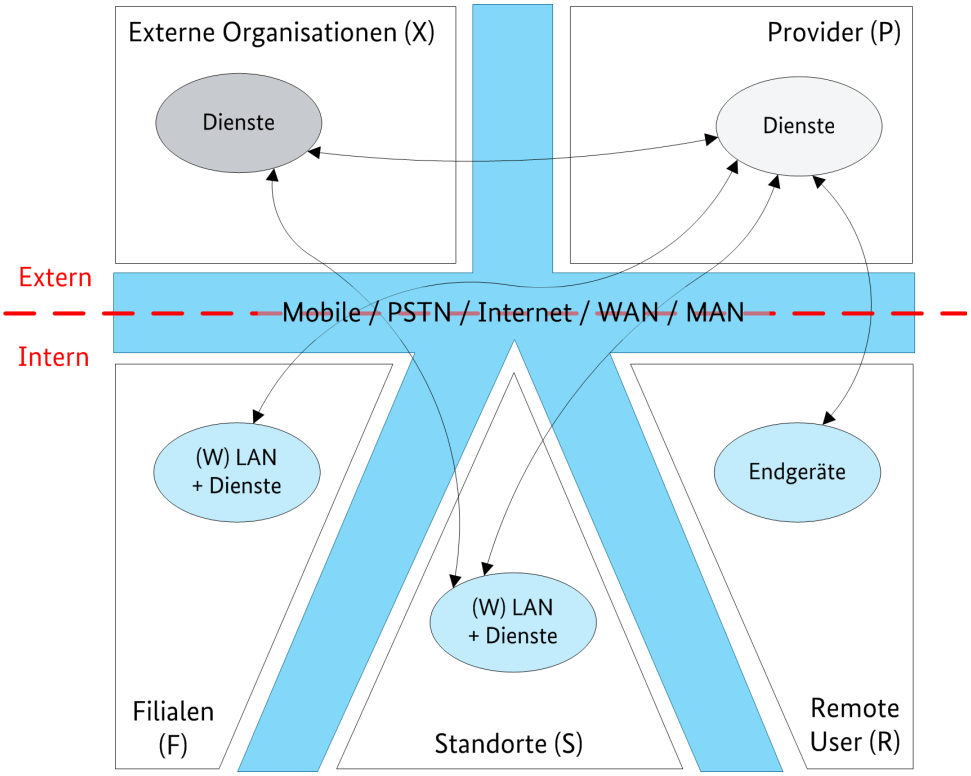

Abbildung 5: Externe Kommunikationsbeziehungen einer Organisation

Zusammenfassend listet Tabelle 1 die typischen Kommunikationsbeziehungen einer Organisation.

Abbildung 6 visualisiert diese Kommunikationsbeziehungen zwischen den Kommunikationsendpunkten von Organisationen.

Die Anwendbarkeit der in Teil 1 der Technischen Leitlinie spezifizierten Sicherheitsmaßnahmen wird in Kapitel 3 für die genannten Kommunikationsbeziehungen bewertet. Eventuell unterschiedliche Realisierungsoptionen, die sich aus ggf. unterschiedlichen Größenordnungen von Standorten bzw. Filialen ergeben, werden je Kommunikationsbeziehung erläutert.

Bez.	Beschreibung
Interne Kommunikation	
S-I	Standort-interne Kommunikation, die ausschließlich das interne LAN bzw. WLAN als Kommunikationsbasis für den Zugriff auf die Dienste nutzt
S-S	Kommunikation zwischen zwei Standorten, z. B. Zugriff auf einen Dienst eines übergeordneten Standortes; für die Kommunikation muss zwingend ein öffentliches Netz, d. h. Mobile Network, PSTN, Internet, WAN oder MAN, genutzt werden
S-F	Kommunikation zwischen Standort und einer nachgelagerten Filiale über ein öffentliches Netz
F-I	Filial-interne Kommunikation, die ausschließlich das interne LAN bzw. WLAN als Kommunikationsbasis für den Zugriff auf die Dienste nutzt
F-F	Kommunikation zwischen zwei Filialen über ein öffentliches Netz
R-S	Einbindung von Telearbeitsplätzen (Remote User) via öffentlichem Netz
Externe Kommunikation	
S-P	Kommunikation zwischen Standort und Provider-Diensten oder ausgelagerten eigenen Diensten via öffentlichem Netz
S-X	Kommunikation zwischen einem Standort und einer externen Organisation über ein öffentliches Netz
F-P	Kommunikation zwischen Filiale und Provider-Diensten via öffentlichem Netz
R-P	Anbindung von Telearbeitsplätzen (Remote User) an Provider-Dienste über ein öffentliches Netz
P-X	Anbindung von externen Organisationen an Provider-Dienste, z. B. zum Austausch von Informationen zwischen ausgelagerten Diensten der eigenen Organisation und externen Organisationen

Tabelle 1: Typische Kommunikationsbeziehungen einer Organisation

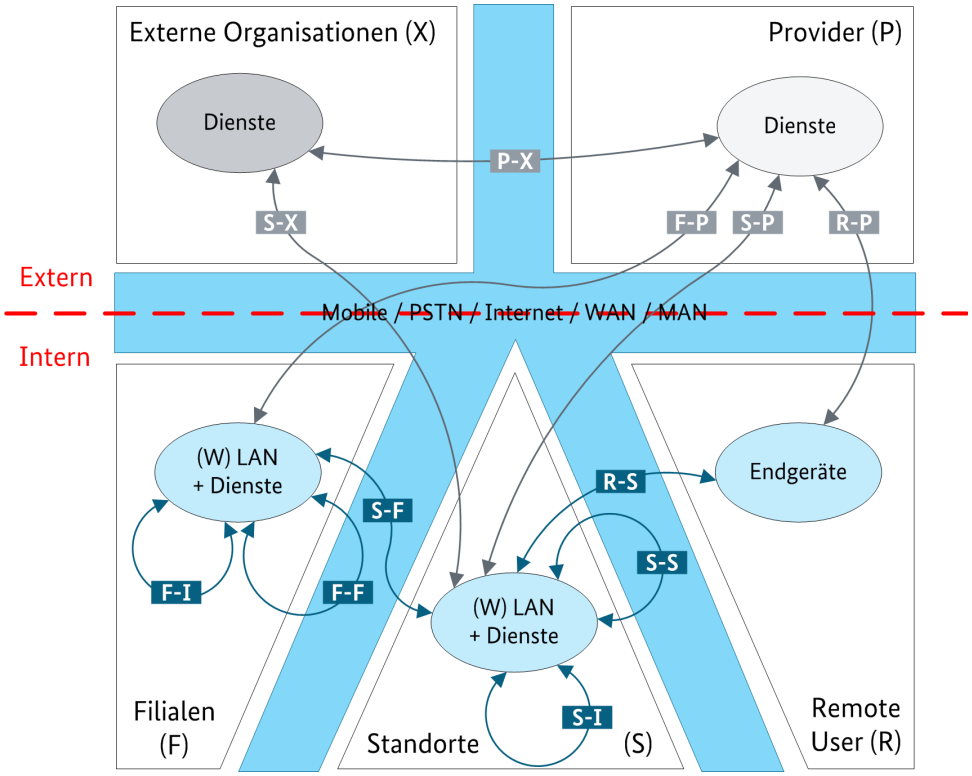

Abbildung 6: Typische Kommunikationsbeziehungen einer Organisation

2.4 Beschreibung der betrachteten Beispielszenarien

Zur Veranschaulichung der Nutzung der in Kapitel 3 vorgenommenen Zuordnung von Maßnahmen zu Kommunikationsschnittstellen werden im Folgenden sechs Beispielszenarien, die typische Organisationsgrößen beispielhaft darstellen, kurz beschrieben. In Kapitel 4 erfolgt dann eine detailliertere Beschreibung dieser Szenarien und eine mögliche Auswahl von Maßnahmen aus Teil 1 der Technischen Leitlinie.

2.4.1 Beispiel einer kleinen Organisation: Anwaltsbüro

Kleine Organisationen beschreiben die Fälle, bei denen IT-kompetentes Personal meist nicht vor Ort verfügbar ist. Im Sinne der Machbarkeit bestimmter Maßnahmen sind hier also klare Grenzen gesetzt. Typisch für eine kleine Organisation ist die Auslagerung von Diensten, hier zusammengefasst als UC as a Service, und Dienstleistungen, hier das Outsourcing von Betrieb und Wartung.

Die Größe der Organisation macht es zudem unwirtschaftlich, größere Ausbaustufen von zentralen Telefonie-Systemen einzusetzen. Es können daher im Detail technische Einschränkungen für bestimmte Sicherheitsmaßnahmen gegeben sein.

Als vereinfachtes Beispiel einer kleinen Organisation wird im Folgenden ein Anwaltsbüro mit ca. 10 Anwendern betrachtet, das einen zentralen Standort umfasst, Telearbeitsplätze (engl. Remote User) einbindet und die UCC-Dienste ausgelagert hat. Eine Anbindung an externe Organisationen ist nicht realisiert.

Abbildung 7 zeigt die in diesem Beispielszenario involvierten Organisationseinheiten, zwischen denen Kommunikationsbeziehungen auftreten.

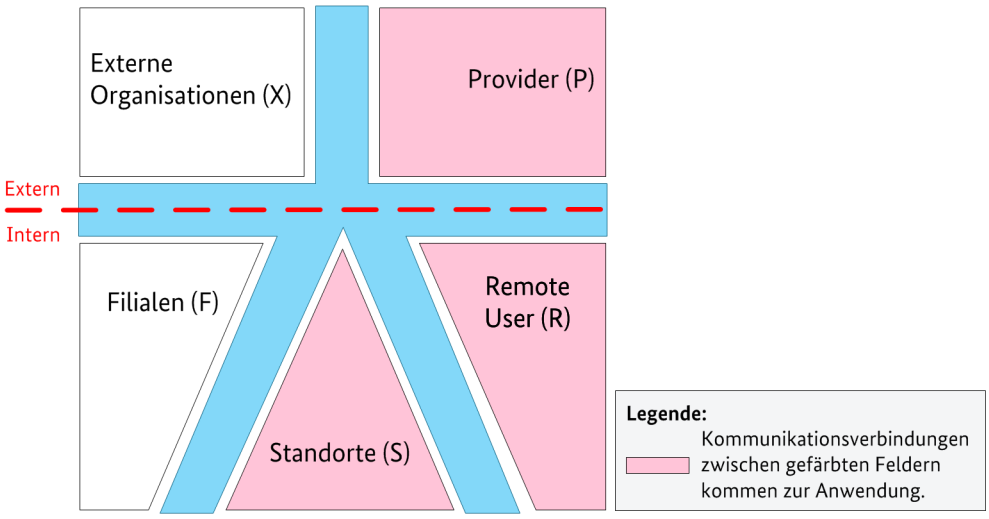

Abbildung 7: Beispielszenario einer kleinen Organisation – Anwaltsbüro

2.4.2 Beispiel einer mittleren Organisation: Großes Ingenieurbüro

Mittlere Organisationen erreichen an keinem Standort die Größenordnung einer großen Organisation. Jedoch erreicht die Anzahl der TK-Nutzer mindestens an einem Standort eine Anzahl, die den Aufbau eigener IT-Kompetenz, insbesondere eigener TK-Administratoren an diesem Standort sinnvoll macht. Auch kann die Anwenderzahl die Implementierung bzw. Beschaffung einer TK-Infrastruktur bedingen, mit der auch technisch anspruchsvolle Sicherheitsmaßnahmen umgesetzt werden können.

Diese günstigen Voraussetzungen bzgl. Machbarkeit und Wirtschaftlichkeit treffen jedoch nicht unbedingt an allen Standorten gleichermaßen zu. Häufig werden in Summe mehrere hundert TK-Nutzer erreicht, von denen sich jedoch der größere Teil an einem oder wenigen Standorten konzentriert, während an anderen Standorten lediglich die Größenordnung kleiner Organisationen gegeben ist.

Als vereinfachtes Beispiel einer mittleren Organisation wird im Folgenden ein großes Ingenieurbüro mit ca. 250 Anwendern betrachtet, das einen zentralen Standort und wenige Filialen umfasst, jedoch keine Anbindung weiterer kleinerer Standorte oder externer Organisationen erfordert. Sicherheitsfunktionen wie Malware-Schutz werden in den eigenen Räumlichkeiten des Ingenieurbüros bereitgestellt und von einem Provider betrieben, um für ein optimales Sicherheitsniveau die notwendige Kompetenz bereitstellen zu können.

Abbildung 8 zeigt die in diesem Beispielszenario involvierten Organisationseinheiten, zwischen denen Kommunikationsbeziehungen auftreten.

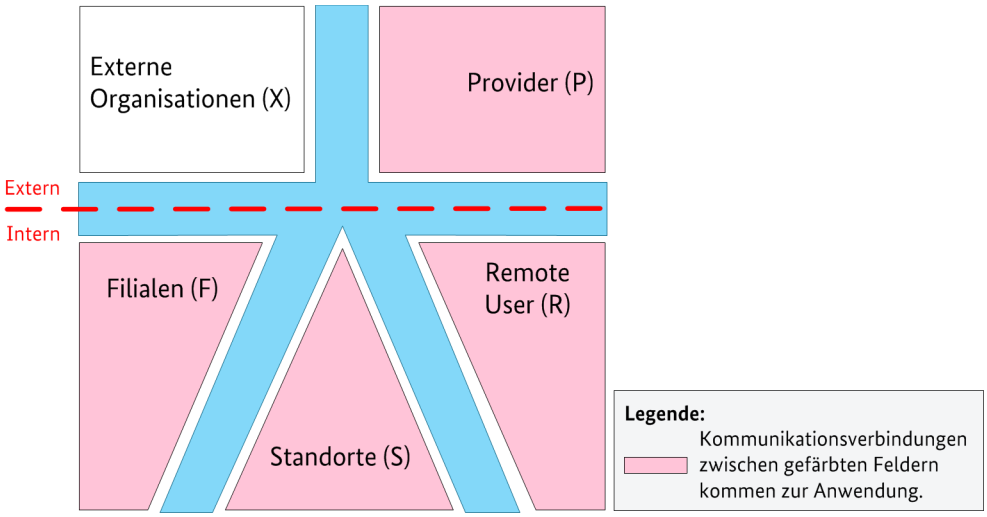

Abbildung 8: Beispielszenario einer mittleren Organisation – Ingenieurbüro

2.4.3 Beispiel 1 einer großen Organisation: Groß-Klinikum

Große Organisationen sind Szenarien, bei denen an einem einzigen zentralen Standort eine große Anzahl von TK-Anwendern, häufig mehr als 500, lokalisiert sind. Lokales Personal mit IT-Know-how kann hier typischerweise vorausgesetzt werden. Die Teilnehmerzahl bedingt für gewöhnlich zentrale Systeme, die keine funktionalen Einschränkungen bzgl. der Sicherheitsmaßnahmen aufweisen. Darüber hinaus binden große Organisationen meist etliche Außenstellen, Filialen sowie kleinere Standorte, ein.

Als erstes Beispiel einer großen Organisation wird im Folgenden ein Groß-Klinikum betrachtet, das einen sehr großen Standort und etliche Außenstellen umfasst. Eine Anbindung an Provider-Dienste ist in diesem Beispiel nicht erforderlich, jedoch müssen externe Organisationen (z. B. Arztpraxen) erreichbar sein.

Weiterhin sollen einige Außenstellen umfassend unabhängig arbeiten können, d. h. diese stellen kleine Standorte dar. Ein Großteil der Außenstellen stellt jedoch Filialen dar, die keinerlei eigene TK-Installation aufweisen. Darüber hinaus bedingt das Beispiel hohe Kommunikationsanforderungen und eine sichere Trennung kritischer Systeme, beispielsweise für Operations-Equipment.

Abbildung 9 zeigt die in diesem Beispielszenario involvierten Organisationseinheiten, zwischen denen Kommunikationsbeziehungen bestehen.

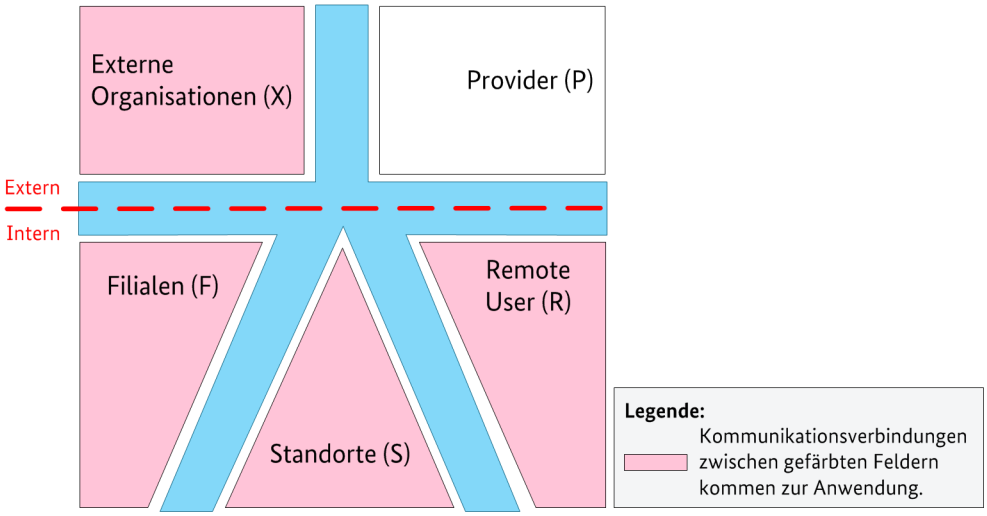

Abbildung 9: Beispielszenario einer großen Organisation – Groß-Klinikum

2.4.4 Beispiel 2 einer großen Organisation: Energieversorger

Als weiteres Beispiel für große Organisationen wird ein Energieversorger mit ca. 2000 Mitarbeitern beschrieben. Dieser hat einen zentralen Standort, an dem auch jegliche Verwaltung sowie das Händlersystem untergebracht ist, und bindet mehrere meist ausgelagerte Kontaktcenter an, die dann als externe Organisationen agieren und autark arbeitsfähig sein müssen. Die Steuerung der Anrufe erfolgt über einen VoIP-Provider. Weitere abgesetzte Standorte oder Filialen ohne eigene TK-Installation werden nicht eingebunden.

Abbildung 10 zeigt die in diesem Beispielszenario involvierten Organisationseinheiten, zwischen denen Kommunikationsbeziehungen auftreten.

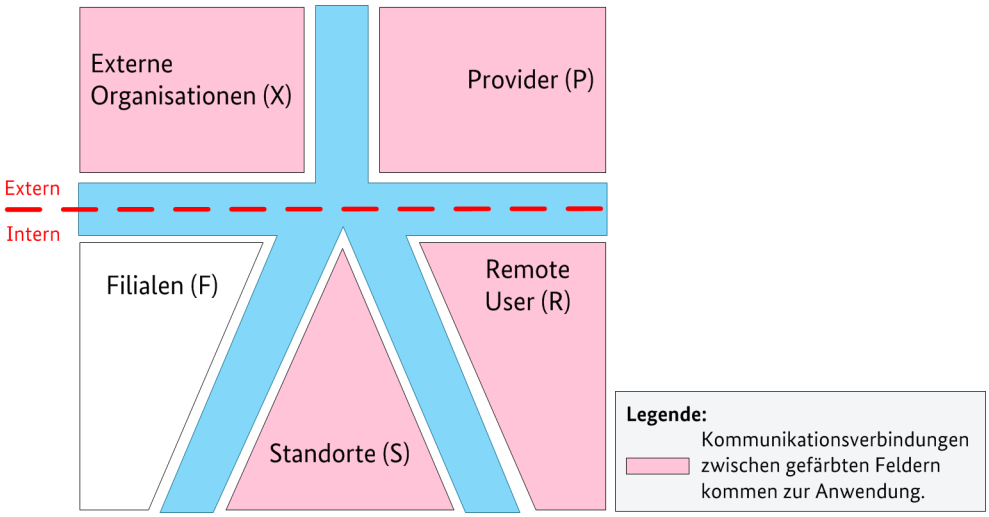

Abbildung 10: Beispielszenario einer große Organisation – Energieversorger

2.4.5 Beispiel einer sehr großen Organisation: Globaler Konzern

Sehr große Organisationen sind Szenarien, bei denen an einem oder mehreren zentralen Standort(en) eine große Anzahl von TK-Anwendern, in der Regel mehr als 5000, lokalisiert sind. Die Einrichtung von zentralen Systemen ohne grundlegende funktionale Einschränkungen und lokales Personal mit IT-Know-how können hier typischerweise vorausgesetzt werden.

Sehr große Organisationen umfassen meist alle in Kapitel 2.3 beschriebenen Organisationseinheiten, d. h.

- mehrere größere Standorte,
- ggf. viele Außenstellen (Filialen und kleinere Standorte),
- Remote User,
- Anbindung an Provider-Dienste und
- Kommunikation mit externen Organisationen.

Als vereinfachtes Beispiel einer sehr großen Organisation wird im Folgenden ein globaler Konzern mit mehreren großen Standorten mit jeweils mehreren tausend Anwendern und etlichen Außenstellen in Form kleinerer Standorte betrachtet. Für die Optimierung der Kommunikation mit externen Organisationen und Kunden wird eine Anbindung an Soziale Netzwerke und Medien (SNM) bereitgestellt.

Jedoch werden keine Filialen (siehe hierzu das Beispielszenario in Kapitel 2.4.2) eingebunden und eine Nutzung von Service-Provider-Diensten wie Outsourcing und Cloud Computing (siehe hierzu das Beispielszenario in Kapitel 2.4.1) ist nicht vorgesehen.

Abbildung 11 zeigt die in diesem Beispielszenario involvierten Organisationseinheiten, zwischen denen Kommunikationsbeziehungen bestehen.

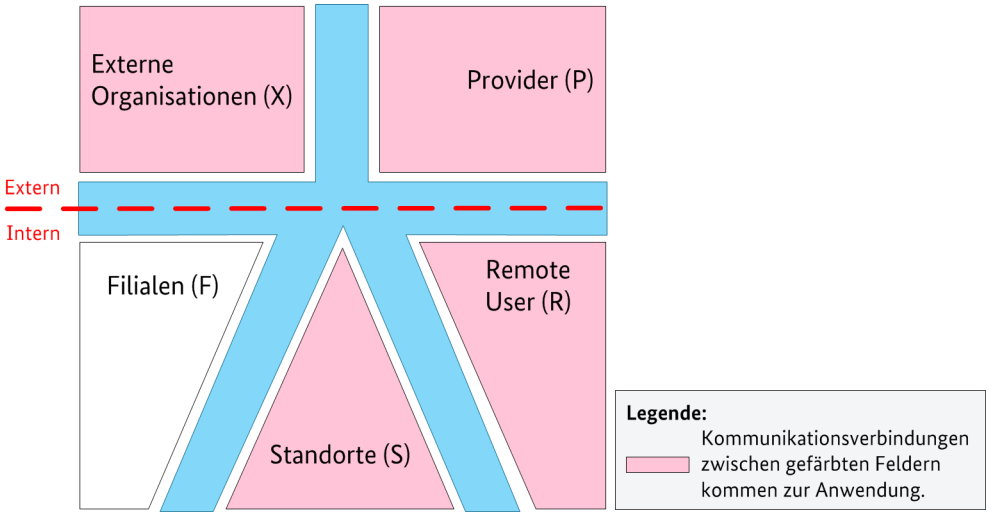

Abbildung 11: Beispielszenario einer sehr großen Organisation - Globaler Konzern

2.4.6 Beispiel einer Organisation in Provider-Rolle: IT-Dienstleister für Industriepark

Eine Organisation in Provider-Rolle muss verschiedenen (Kunden-)Organisationen verschiedener Größenordnung jeweils eine individuelle Lösung anbieten können. Dabei kann die Organisation die Ausprägung einer kleinen bis mittleren Organisation haben, die jedoch sehr flexibel agieren können muss. So ergeben sich Anforderungen, die einer großen Organisation entsprechen, sowie erhöhte Anforderungen bzgl. der Flexibilität.

Weiterhin müssen je nach Anspruch und Größe der (Kunden-)Organisationen diesen eigene Komponenten zugeordnet und eine sichere Trennung der Kommunikation gewährleistet werden. Aus wirtschaftlichen Gründen können verschiedene Dienste aber nur auf Basis einer einzigen, logisch separierten Infrastruktur erbracht werden. Hieraus resultiert die Forderung nach der Mandantenfähigkeit der Systeme.

Diese Diskrepanz zwischen Mandantenfähigkeit, Wirtschaftlichkeit und Sicherheitsanforderungen soll anhand eines IT-Dienstleisters für einen Industriepark dargestellt werden. Die Organisation hat keine Filialen und stellt seinen Kunden keine Dienste von externen Providern zur Verfügung. Allerdings soll den Kunden die Kommunikation zu anderen externen Organisationen ermöglicht werden.

Zu beachten ist die Bedeutung des Begriffs Provider: Eine Organisation in Provider-Rolle ist kein externer Dienstleister im Sinne von Abbildung 6 , sondern stellt eine Organisation dar, die weiteren Organisationen verschiedenster Ausprägung Infrastruktur und Dienste zur Verfügung stellt. Aus Sicht des IT-Dienstleisters sind diese Organisationen seine Kunden und damit nach Kapitel 2.3 externe Organisationen. Die Organisation in Provider-Rolle erbringt also Dienste und Dienstleistungen auf Basis der Infrastruktur an seinem Standort (S) für externe Organisationen am selben oder anderen Standorten (X).

Abbildung 12 zeigt die in diesem Beispielszenario involvierten Organisationseinheiten, zwischen denen Kommunikationsbeziehungen bestehen. Dabei werden - wie zuvor beschrieben - unter Externe Organisationen zusätzlich auch die Kunden des IT-Dienstleisters erfasst. Als Provider sind hier externe Dienstanbieter und nicht der IT-Dienstleister selbst zu verstehen. Standorte und Remote User sind eigene Organisationseinheiten des IT-Dienstleisters.

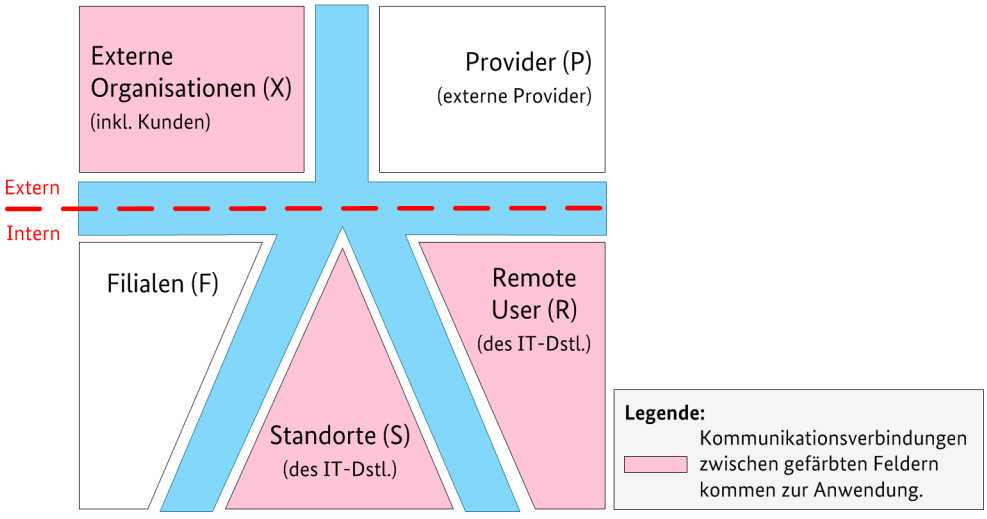

Abbildung 12: Beispielszenario Organisation in Provider-Rolle – IT-Dienstleister für einen Industriepark

3 Anwendbarkeit der Maßnahmen auf Kommunikationsbeziehungen

Die in Teil 1 der Technischen Leitlinie dargestellten Maßnahmen werden im Folgenden auf ihre Gültigkeit und ihre Anwendbarkeit für die in Kapitel 2.3 beschriebenen Kommunikationsbeziehungen bewertet.

Die Maßnahmen werden im entsprechenden Feld durch ein „+“ gekennzeichnet, wenn sie für die betrachteten Kommunikationsbeziehungen Gültigkeit besitzen. Sind Maßnahmen nicht eindeutig einer der aufgeführten Kommunikationsbeziehungen zuzuordnen, werden sie in den nachfolgenden Tabellen den in Kapitel 2.3 genannten Organisationseinheiten zugeordnet und markiert. Diese Zuordnung erfolgt auf Grundlage der relevanten Kommunikationsendpunkte bzw. des Aufstellungsortes der betroffenen TK-Komponenten, wobei gilt:

- Kommunikationsendpunkt Standort: Markierung unter Standort-intern für die TK-Komponenten eines Standortes und für Maßnahmen, die an einem Standort anzuwenden sind bzw. übergreifend für die gesamte Organisation zu ergreifen sind
- Kommunikationsendpunkt Filiale: Markierung unter Filial-intern für TK-Komponenten, die als Teil einer Gesamtlösung in der Filiale installiert sind, und für Maßnahmen, die in einzelnen Filialen zu berücksichtigen sind
- Kommunikationsendpunkt Remote User bzw. (Mobile) Endgeräte: Markierung unter Remote User-Standort für TK-Komponenten, die ggf. beim Remote User genutzt werden, und für Maßnahmen, die bei der Remote-User-Einbindung Gültigkeit haben
- Kommunikationsendpunkt Provider: Markierung unter Standort-Provider für „ausgelagerte“ TK-Komponenten und für Maßnahmen, die bei der Beauftragung und Nutzung jeder Art von Provider Anwendung finden
- Die Organisationseinheit „Externe Organisationen“ findet hier keine Anwendung, da dort in diesem Zusammenhang keine relevanten Endpunkte zu finden sind. Nur die Kommunikationsbeziehung selbst zu diesen wird berücksichtigt.
- Maßnahmen, die die Schnittstellen der TK-Komponenten adressieren, werden für die zutreffende Kommunikationsbeziehung bewertet.

Die folgenden Beispiele verdeutlichen diese Festlegungen:

Beispiel 1:

Maßnahmen-Nr.	**Titel**	**Kommunikationsbeziehung**										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	**S-I**	**S-S**	**S-F**	**F-I**	**F-F**	**R-S**	**S-P**	**S-X**	**F-P**	**R-P**	**P-X**
M-TK-1	Sperrung nicht benötigter oder sicherheitskritischer Leistungsmerkmale	+	-	-	-	-	-	+	-	-	-	-

Tabelle 2: Anwendbarkeit der Maßnahmen: Beispiel 1

Die Maßnahme M-TK 1 bezieht sich auf die Sperrung von Leistungsmerkmalen am zentralen Kommunikationssystem. Diese Maßnahme ist in ihrer Umsetzung auf das zentrale TK-System beschränkt und beinhaltet keine Kommunikationsbeziehungen. Bei Bereitstellung am zentralen Standort ist die Maßnahme somit am zentralen Standort der TK-Anlage sowie ggf. an nachgelagerten Standorten der Organisation zu ergreifen. Werden Dienste aus einer Provider-Infrastruktur heraus

genutzt (z. B. IP-Centrex), dann muss die Umsetzung der Maßnahme für die Kommunikationsbeziehungen Standort-Provider (S-P) vertraglich gefordert werden.

Beispiel 2:

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-19	Geschützte Übertragung von Sprachdaten	+	+	+	+	+	+	+	+	+	+	+

Tabelle 3: Anwendbarkeit der Maßnahmen: Beispiel 2

M-TK-19 bezieht sich auf die Übertragung von Sprachdaten, welche durch einen angemessenen Schutz abgesichert werden muss. Die Übertragung von Sprachdaten ist für jede der aufgeführten Kommunikationsbeziehungen umzusetzen.

Beispiel 3:

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-135	Schulung von Kontaktcenter-Administratoren und Schichtleitern/Supervisoren	+	-	-	-	-	-	-	-	-	-	-

Tabelle 4: Anwendbarkeit der Maßnahmen: Beispiel 3

M-TK-135 bezieht sich als übergreifende Maßnahmen auf die gesamte Organisation. Die Schulungen erfolgen üblicherweise zentral für alle Administratoren bzw. Supervisoren einer Organisation. Auch Supervisoren von in Filialen ausgelagerten Kontaktcentern werden in zentralen Standorten geschult.

Die Tabellen sollen den Zuständigen einer Organisation helfen, die für die Organisation bzw. Standorte relevanten Maßnahmen zu identifizieren. Hierfür sind im Einzelfall folgende Schritte auszuführen:

1. Identifizieren der organisationseigenen Kommunikationsverbindungen und -endpunkte
2. Identifizieren der in der Organisation vorkommenden Technologien und Schnittstellen und damit der relevanten Tabellen von Maßnahmen
3. Überprüfung der Maßnahmen in den entsprechenden Tabellen auf Markierung und damit Umsetzungsrelevanz.

In Kapitel 4 dieses Dokuments wird diese Vorgehensweise beispielhaft für repräsentative Beispielszenarien dargestellt.

Generell gelten die genannten Maßnahmen für alle Größen von Organisationen bzw. Standorten. Jedoch sind für kleinere Organisationen bzw. kleinere Standorte zum Teil Sonderbetrachtungen erforderlich.

Hierfür werden im Anschluss an jede Tabelle, sofern dies notwendig erscheint, Erläuterungen und Einschränkungen für kleinere Organisationen bzw. Standorte zu den zuvor gelisteten Maßnahmen gegeben. Hierbei werden kleinere Organisationen mit nur einem Standort, sofern nicht explizit anders angegeben, einem kleineren Standort gleichgesetzt.

Grundsätzlich gilt für kleinere Standorte, dass häufig das Betriebspersonal – sofern überhaupt vorhanden - nicht über das entsprechende Know-how für die Konfiguration und Administration einer TK-Lösung mit erhöhtem Schutzbedarf verfügt. Hier können Konfiguration, Administration und ggf. Planung und

Ersteinrichtung einem geeigneten Dienstleister übertragen werden. Zur Beauftragung der Fremdleistung sind die folgenden Punkte zu beachten:

- Zwingend ist auch für kleinere Standorte die Einarbeitung in die Sachverhalte des erhöhten Schutzbedarfs, um gezielt einen Dienstleister aussuchen zu können, der dann die nötige Sicherheit in der Administration der Lösung gewährleistet.
- Die geforderten Maßnahmen für die TK-Lösung sind in den vertraglichen Vereinbarungen angemessen zu berücksichtigen.
- Der Abschluss eines Support-Vertrags inklusive Beratungskompetenz für die Management-Maßnahmen der TK-Lösung ist für kleinere Standorte in der Regel als unverhältnismäßig teuer einzustufen. Stattdessen kann bei konkretem Bedarf eine fallweise Beauftragung erfolgen. Dies ist insbesondere für die sichere Administration von zentralen Komponenten, z. B. des SBC dringend zu empfehlen.
- Die mit externer Unterstützung meist verbundene längere Wartezeit im Störungsfall kann in kleineren Standorten häufig problemlos über die Ersatzlösung für Notrufe, z. B. über Mobilfunk überbrückt werden.
- Die Möglichkeit zum regelmäßigen Bezug von sicherheitsrelevanten Software-Updates muss in jedem Fall sichergestellt werden.

Für kleinere Standorte, die einen Verbund mit größeren Standorten bilden, wird empfohlen, die Konfiguration vom selben Personal (intern oder extern) durchführen zu lassen, das diese Arbeiten auch für den zentralen bzw. benachbarten größeren Standort vornimmt.

Die folgenden Tabellen betrachten ausschließlich Organisationseinheiten entsprechend obiger „reiner“ Definition (siehe Kapitel 2.3). Mischformen, z. B. Nutzung einer abgesetzten, dedizierten TK-Anlage im Verbund der Gesamtlösung, bedürfen einer Einzelfallbetrachtung.

3.1 Klassische Telekommunikationstechnik

Die Anwendbarkeit der Maßnahmen für klassische Telekommunikationslösungen ist in die folgenden Blöcke aufgeteilt:

- Zentrale Anlage, siehe Tabelle 5
- Endgeräte, siehe Tabelle 6
- Netzwerk, siehe Tabelle 7
- Netz- und Systemmanagement, siehe Tabelle 8

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-1	Sperrung nicht benötigter oder sicherheitskritischer Leistungsmerkmale	+	-	-	-	-	-	+	-	-	-	-
M-TK-2	Schaffung eines zusätzlichen TK-Ersatzanschlusses für Notrufe	+	-	-	+	-	-	-	-	-	-	-
M-TK-3	Katastrophenschaltung	+	-	+	-	-	+	+	+	+	+	-
M-TK-4	Erhöhter Zutrittsschutz	+	-	-	-	-	-	+	-	-	-	-
M-TK-5	Geeignete Aufstellung der TK-Anlage	+	-	-	-	-	-	+	-	-	-	-
M-TK-6	Sichere Ablage von Kontaktinformationen	+	-	-	-	-	-	+	-	-	-	-
M-TK-7	Sicherer Umgang mit Daten zur Anlagennutzung	+	-	-	-	-	-	+	-	-	-	-
M-TK-8	Absicherung eines LAN-Anschlusses der ISDN-basierten TK-Anlage	+	-	-	-	-	-	+	-	-	-	-
M-TK-9	Absicherung der Kommunikation über ein IAD	+	-	-	-	-	-	+	-	-	-	-

Tabelle 5: Anwendbarkeit der Maßnahmen: Klassische TK – Zentrale Anlage

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-2 „Schaffung eines zusätzlichen TK-Ersatzanschlusses für Notrufe“

Für kleinere Standorte mit einem S_0-PSTN-Anschluss kann ein manuelles Umstecken als Lösung akzeptabel sein (Anlage abziehen, Notruftelefon direkt anstecken. Hierzu muss eine bebilderte Kurzanleitung vorhanden sein und die Ersatzausstattung bereitliegen, wobei die Bevorratung so ausgelegt sein muss, dass zusätzlich nur noch der funktionsfähige Zugang zum PSTN benötigt wird, insbesondere

- geeigneter Apparat (Endgerät),
- zusätzlicher, funktionierender NTBA sowie
- alle notwendigen Kabel für den Notanschluss.

zu M-TK-3 „Katastrophenschaltung“

Bei kleineren Standorten ist der Zweck dieser Maßnahme oft schon mit M-TK-2 und organisatorischer Festlegung zum Nutzungsrecht für den Ersatzanschluss erfüllt. Diese Maßnahme kann die Anlage sonst für kleinere Standorte unverhältnismäßig verteuern.

zu M-TK-4 „Erhöhter Zutrittsschutz“

Bei kleineren Standorten sind häufig die bezahlbaren (bau-)technischen Möglichkeiten beschränkt. In solchen Umgebungen ist so weit wie möglich eine konsequente organisatorische Umsetzung durchzuführen:

- Kein unbeaufsichtigter Zutritt von Fremden zu Räumen mit zentralen TK-Anlagen als Grundsatz und
- möglichst gezielte Aufstellung der Anlage in solchen Räumen, für die eine derartige Regelung auch aus anderen Gründen bereits umgesetzt wird.

Erscheint im konkreten Fall die Wirksamkeit bzw. die konsequente Umsetzbarkeit der organisatorischen Regelung fraglich, sollte in jedem Fall ein geschlossener, abschließbarer Schrank als minimaler technischer Schutz eingesetzt werden.

zu M-TK-5 „Geeignete Aufstellung der TK-Anlage“

Die Maßnahme umfasst bei kleineren Standorten im Wesentlichen den Zutrittsschutz, siehe Ausführungen zu M-TK-4. Die Installation einer USV u. ä. kann insbesondere für kleinere Standorte unverhältnismäßig sein, wenn diese nicht auch gleichzeitig für andere IT-Systeme genutzt wird. In solchen Standorten kann Maßnahme M-TK-2 zur Absicherung ausreichend sein.

zu M-TK-6 „Sichere Ablage von Kontaktinformationen“

Einem erhöhten Schutzbedarf für Vertraulichkeit kann bei kleineren Standorten im Zweifel durch den Verzicht der Speicherung in der zentralen Anlage (je nach Anzahl der häufigsten Gesprächspartner) entsprochen werden. Wird so verfahren, müssen hinsichtlich der TK-Anlage keine Schutzvorkehrungen zur sicheren Ablage getroffen werden.

Alternativ besteht in kleineren Standorten die Möglichkeit, derartige Kontaktinformationen über einen zentralen Standort verwalten zu lassen. Voraussetzung ist ein Zugriff auf eine solche zentrale Ablage über geeignet gesicherte Kommunikation.

zu M-TK-7 „Sicherer Umgang mit Daten zur Anlagennutzung“

Gerade bei kleinen Standorten ist auf eine gezielte Minimierung der erfassten Daten zu achten (Datenvermeidung statt Schutzmaßnahmen). Aufwendigere Maßnahmen zur Absicherung des Zugriffs zur Anlage sind in solchen Umgebungen oft nicht praktikabel (Alter der Anlage, Funktionalitäten einer für die Umgebungsgröße angemessenen Anlage, vorhandene Kenntnisse).

Bei in kleineren Standorten häufiger eingesetzten preisgünstigen Anlagen können solche Daten auf der Anlage selbst oft nur schwach geschützt werden. In einem solchen Fall bietet es sich an, ergänzend zur Datenvermeidung eine automatisierte Überführung solcher Daten von der Anlage auf eine separate, bereits gut geschützte Ablage einrichten zu lassen (z. B. vorhandene Fileserver). So wird eine möglichst kurze Verweildauer der Daten auf der Anlage erreicht.

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

Das Risiko für kleinere Standorte kann primär über den Zugangsschutz (M-TK-4) minimiert werden, sofern auch für Räume mit Anschlüssen zum Standort-LAN ein geeigneter Zugangsschutz realisiert werden kann.

In manchen kleinen Standorten kann keine der benannten technischen Vorkehrungen umgesetzt werden. Gründe hierfür sind fehlendes Know-how, fehlende Funktionalitäten oder eine für die Maßnahme ungeeignete Struktur der LAN-Technik. In solchen Fällen sollte auf die Nutzung des LAN-

Anschlusses der Anlage verzichtet werden, ggf. muss zusätzlich bei Lieferung und Erstkonfiguration der Anlage der Port deaktiviert werden, siehe M-TK-1.

zu M-TK-9 „Absicherung der Kommunikation über ein IAD“

Ist für kleinere Standorte eine Absicherung über eine Firewall unwirtschaftlich, so muss auf ein IAD verzichtet werden.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-10	Sperrung bestimmter Fax-Rufnummern	+	-	-	+	-	+	+	-	+	+	-
M-TK-11	Gesicherte Aufstellung der Faxlösung	+	-	-	+	-	+	-	-	-	-	-
M-TK-12	Verhinderung der Faxfunktionsnutzung bei ungeschützten Multifunktionsgeräten	+	-	-	+	-	+	-	-	-	-	-
M-TK-13	Sichere Nutzung von Faxgeräten und Multifunktionsgeräten mit Faxfunktion	+	-	-	+	-	+	-	-	-	-	-
M-TK-14	Sichere Aufbewahrung eingegangener Faxnachrichten	+	-	-	+	-	+	-	-	-	-	-
M-TK-15	Sicherung von Telefonie-Endgeräten in frei zugänglichen Räumen	+	-	-	+	-	+	-	-	-	-	-
M-TK-16	Einsatz sicherheitsintelligenter Endgeräte	+	-	-	+	-	+	-	-	-	-	-
M-TK-17	Aktivierung einer Warnung bei Nutzung unsicherer Merkmale	+	-	-	+	-	+	-	-	-	-	-
M-TK-18	Sicherer Umgang mit Schnittstellen am Telefonie-Endgerät	+	-	-	+	-	+	-	-	-	-	-
M-TK-19	Geschützte Übertragung von Sprachdaten	+	+	+	+	+	+	+	+	+	+	+
M-TK-20	Verzicht auf Einsatz von Wartungsapparaten	+	-	-	-	-	-	+	-	-	-	-
M-TK-21	Sperrung der Wartungsmöglichkeit per Wartungsapparat an der Anlage	+	-	-	-	-	-	+	-	-	-	-

Tabelle 6: Anwendbarkeit der Maßnahmen: Klassische TK - Endgeräte

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-14 „Sichere Aufbewahrung eingegangener Faxnachrichten“

Die Maßnahme kann bei kleineren Standorten im Wesentlichen organisatorisch umgesetzt werden, ohne hierfür spezielle Faxgeräte zu beschaffen.

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

Bei kleineren Standorten mit kurzen Wegen sollte in frei zugänglichen Räumen auf die Aufstellung von Telefonie-Endgeräten verzichtet werden, um die Beschaffung von Endgeräten mit eingeschränktem Funktionsumfang zu vermeiden.

zu M-TK-19 „Geschützte Übertragung von Sprachdaten“

Bei kleineren Standorten ist der Aspekt geschützter Kommunikation zwischen internen Telefonen am selben Standort nachrangig zu betrachten. Nur zum Schutz derartiger Telefonate ist die Beschaffung von Verschlüsselungsequipment in solchen Umgebungen typischerweise unverhältnismäßig: Telefonate vertraulichen Inhalts können hier leicht durch kurze Besprechungen (vier Augen-Gespräch) vermieden werden.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-22	Gesicherte Übertragung der Sprachdaten zwischen Partnerstandorten durch Leitungsverschlüsselung	-	+	-	-	-	-	+	+	-	-	+

Tabelle 7: Anwendbarkeit der Maßnahmen: Klassische TK – Netzwerk

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Bzgl. der Übertragung bestehen bei erhöhtem Schutzbedarf auch für kleinere Standorte keine Einschränkungen.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-23	Restriktive Einbindung externer Wartung	+	-	-	-	-	-	+	-	-	-	-
M-TK-24	Sichere Aufstellung von Administrationsendgeräten	+	-	-	+	-	+	+	-	-	-	-
M-TK-25	Sichere Konfiguration von Administrationsendgeräten	+	-	-	+	-	+	+	-	-	-	-
M-TK-26	Regelungen für sichere TK-Administration	+	-	-	+	-	+	+	-	-	-	-
M-TK-27	Sichere Konfiguration des Management-Zugangs zur TK-Anlage	+	-	-	-	-	-	+	-	-	-	-
M-TK-28	Protokollierung und regelmäßige Kontrolle von Fernwartungszugriffen	+	-	-	-	-	-	+	-	-	-	-
M-TK-29	Verfügbarkeitssicherung durch (automatisierte) Zustandsüberwachung	+	-	-	-	-	-	+	-	-	-	-
M-TK-30	Abschluss eines Support-Vertrags inklusive externer Beratungskompetenz	+	-	-	-	-	-	+	-	-	-	-

Tabelle 8: Anwendbarkeit der Maßnahmen: Klassische TK – Netz- und Systemmanagement

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-23 „Restriktive Einbindung externer Wartung“

Häufig kann im Fall von kleineren Standorten mangels Personalkapazitäten mit entsprechendem Know-how weder die geeignete Absicherung von externen Fernwartungszugriffen regelmäßig überprüft noch eine Kontrolle von Log-Informationen auf solche Zugriffsversuche realisiert werden. In diesem Fall sollte auf Fernwartungszugriffe durch Externe verzichtet werden. Der typische Bedarf an Konfigura-

tionsänderungen in einer solchen Umgebung rechtfertigt das Risiko eines schlecht gesicherten oder unbemerkt angegriffenen Fernwartungszugangs nicht. Störungsbehandlung und Änderungsdurchführung können meist sinnvoller vor Ort durchgeführt werden.

Alternativ kann ggf. die Wartungskonzeption für den Zentralstandort angewendet werden, wobei dann die vorgesehenen Zugriffskontrollen durch entsprechend kundiges Personal der Zentrale erfolgen sollten, falls in betroffenen Standorten kein solches ansässig ist.

zu M-TK-24, M-TK-25 und M-TK-26

Da in kleineren Standorten typischerweise kein eigenes Administrationspersonal vorhanden ist, sind die Maßnahmen hier nur sehr eingeschränkt anwendbar:

- Im Wesentlichen können sie sinngemäß auf mobile Administrationsgeräte angewendet werden, die von Externen fallweise zu Wartungs- und Support-Einsätzen mitgebracht werden (Techniker-Notebook o. Ä.). Die Aufstellung ist somit nur temporär, der Zugriff auf solche Geräte erfolgt ohnehin nur unter Aufsicht (da durch externes Personal).
- Denkbar ist auch die Aufstellung eines Konsol-Endgerätes direkt bei der TK-Anlage; für dieses greifen dann automatisch die Maßnahmen zur sicheren Aufstellung der TK-Anlage, sodass M-TK-24 entfällt.

zu M-TK-27, M-TK-28 und M-TK-29

Die hier beschriebenen Maßnahmeninhalte setzen das Vorhandensein einer zentralen Management-Lösung und/oder eines Log-Servers voraus sowie entsprechenden Personals, das die Protokollierungen kompetent prüfen kann. Die Voraussetzungen hierfür sind in kleineren Standorten häufig nicht gegeben. In diesen Fällen ist im Wesentlichen M-TK-27 zu beachten, in Form gezielter Abschaltung aller Management-Zugriffsmöglichkeiten. Statt einer Abschaltung der Management-Möglichkeiten per Konfiguration kann auch darauf verzichtet werden, die LAN-Schnittstelle der Anlage anzuschalten.

Alternativ kann bei kleineren Standorten, die mit größeren Standorten einen Verbund bilden, das Management-Konzept der Zentrale umgesetzt werden.

zu M-TK-30 „Abschluss eines Support-Vertrags inklusive externer Beratungskompetenz“

In kleineren Standorten ist der Abschluss eines umfassenden Support-Vertrags inklusive Beratungskompetenz i. d. R. als unverhältnismäßig teuer einzustufen. Stattdessen kann eine angepasste Anwendung der Maßnahme zum Einsatz kommen:

- Die Möglichkeit zum regelmäßigen Bezug von sicherheitsrelevanten Software-Updates ist essentiell und muss in jedem Fall sichergestellt werden.
- Bei konkretem Bedarf kann fallweise eine beratende Unterstützung beauftragt werden. Die hiermit meist verbundene längere Wartezeit im Störungsfall kann in kleinen Standorten häufig problemlos über die Ersatzlösung für Notrufe überbrückt werden.
- Ebenfalls kann der Abschluss eines Hardware-Wartungsvertrags für kleinere Standorte in Betracht gezogen werden.

3.2 Voice over IP

Die Anwendbarkeit der Maßnahmen für Telekommunikationslösungen basierend auf Voice over IP ist in die folgenden Blöcke aufgeteilt:

- Server und Anwendungen, siehe Tabelle 9
- Endgeräte, siehe Tabelle 10
- Netzwerk, siehe Tabelle 11
- Netz- und Systemmanagement, siehe Tabelle 12
- übergreifende Aspekte, siehe Tabelle 13

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-31	Durchgängige Verschlüsselung des Medienstroms	+	+	+	+	+	+	+	+	+	+	+
M-TK-32	Durchgängige Verschlüsselung der Signalisierung	+	+	+	+	+	+	+	+	+	+	+
M-TK-33	Absicherung von VoIP bei der Verwendung von Thin Clients	+	-	+	+	-	+	+	-	+	+	-
M-TK-34	Authentisierung zwischen Endgeräten und Servern des VoIP-Systems	+	-	+	+	-	+	+	-	+	+	-
M-TK-35	Authentisierung zwischen Servern	+	+	-	-	-	-	+	+	-	-	+
M-TK-36	Redundanz der Telefonie-Server	+	-	-	-	-	-	+	-	-	-	-
M-TK-37	Redundanz der Server und Gateways, von denen die Funktion des Telefonie-Servers und des Telefonie-Dienstes unmittelbar abhängt	+	-	-	-	-	-	+	-	-	-	-
M-TK-38	Schaffung eines zusätzlichen PSTN-Ersatzanschlusses für Notrufe	+	-	-	+	-	-	-	-	-	-	-
M-TK-39	Automatische PSTN-Umschaltung für kleinere Außenstellen	-	-	+	+	+	-	-	-	+	-	-
M-TK-40	Absicherung von Telefonie-Daten im Verzeichnisdienst	+	-	-	-	-	-	+	-	-	-	-
M-TK-41	Verfügbarkeit kritischer Telefonie-Daten	+	-	-	-	-	-	+	-	-	-	-
M-TK-42	Einschränkungen von DNS für VoIP	+	-	-	-	-	-	+	-	-	-	-
M-TK-43	Einschränkung von ENUM	+	-	-	-	-	-	+	-	-	-	-
M-TK-44	Redundante Internet-Anbindung für den IP-Anlagenanschluss	+	-	-	-	-	-	+	-	-	-	-

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-45	Zusätzlicher IP-Anlagenanschluss	+	-	-	-	-	-	+	-	-	-	-
M-TK-46	Zusätzlicher PSTN-Anschluss	+	-	-	-	-	-	+	-	-	-	-
M-TK-47	Verwendung eines Session Border Controller zur Absicherung eines IP-Anlagenanschlusses	+	-	-	-	-	-	+	-	-	-	-

Tabelle 9: Anwendbarkeit der Maßnahmen: Voice over IP – Server und Anwendungen

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-35 „Authentisierung zwischen Servern“

In kleineren Standorten ist in der Regel nicht davon auszugehen, dass verschiedene Sicherheitszonen im LAN implementiert werden. Daher ist für erhöhten Schutzbedarf hier die Authentisierung in jedem Fall zu empfehlen.

zu M-TK-36 und M-TK-37

Im Fall von kleineren Standorten ist im Regelfall der Einsatz redundanter Server unverhältnismäßig. Das damit zu entschärfende Verfügbarkeitsrisiko kann in solchen Szenarien zu einem großen Teil durch die Schaffung eines zusätzlichen TK-Ersatzanschlusses für Notrufe abgesichert werden.

Im Fall von mittleren Standorten, die im Verbund mit größeren Standorten sind, kann die Server-Redundanz über das Paar aus Server im eigenen Standort und dem Server in einem größeren verbundenen Standort realisiert werden, sodass im Standort keine zwingende Server-Dopplung anfällt. Entsprechend erhöht sich allerdings die Bedeutung der Server und damit der Schutzbedarf im verbundenen größeren Standort über dessen Standortgrenzen hinaus.

zu M-TK-38 „Schaffung eines zusätzlichen PSTN-Ersatzanschlusses für Notrufe“

In kleineren Standorten, die mit einem S_0-PSTN-Anschluss als Primäranschluss hinreichend ausgestattet sind, ist im Regelfall ein separater S_0-PSTN-Anschluss als unverhältnismäßig einzustufen. Als Minimalumfang einer Notrufmöglichkeit kann hier ein manuelles Umstecken als Lösung akzeptabel sein (Anlage abziehen, Notruftelefon direkt anstecken), wenn eine bebilderte Kurzanleitung vorhanden ist und die folgende empfohlene Ausstattung bereitliegt:

- geeigneter Apparat (Endgerät)
- zusätzlicher, funktionierender NTBA (Reserveteil)
- alle notwendigen Kabel für den Notanschluss

Die Bevorratung mit Ersatzausstattung muss so ausgelegt sein, dass zusätzlich nur noch der funktionsfähige Zugang zum PSTN benötigt wird, um die Notschaltung aufzubauen.

zu M-TK-39 „Automatische PSTN-Umschaltung für kleinere Außenstellen“

Kleinere Standorte binden in der Regel keine weiteren Außenstellen an, sodass die Maßnahme M-TK-38 „Schaffung eines zusätzlichen PSTN-Ersatzanschlusses“ diese Maßnahme bereits abdeckt.

zu M-TK-40 „Absicherung von Telefonie-Daten im Verzeichnisdienst“

Kleinere Standorte verwenden üblicherweise einen Verzeichnisdienst eines größeren Standorts bzw. eine kleinere Organisation setzt ggf. keinen Verzeichnisdienst ein. In diesem Fall ist diese Maßnahme entbehrlich bzw. wird im größeren Standort umgesetzt.

zu M-TK-41 „Verfügbarkeit kritischer Telefonie-Daten“

Die zur Verwaltung solcher Daten verwendeten Server sind in kleineren Standorten in ein angepasstes Redundanzkonzept (M-TK-36 und M-TK-37) und eine angemessene Datensicherung (M-TK-233) zu integrieren.

zu M-TK-42 und M-TK-43

In kleineren Standorten ist der Einsatz eines separaten, gemäß den Anforderungen dieser Maßnahme eingeschränkten DNS-Servers meist unverhältnismäßig. In solchen Fällen wird dringend empfohlen, auf DNS für VoIP zu verzichten.

In kleineren Standorten, die einen Verbund mit größeren Standorten bilden, kann alternativ die Anforderung durch Mitnutzung eines für VoIP abgesicherten dedizierten DNS-Servers realisiert werden.

zu M-TK-44 „Redundante Internetanbindung für den IP-Anlagenanschluss“

Für kleinere Standorte ist dies in den meisten Fällen nicht realisierbar. Hier muss auf einem anderen Weg sichergestellt werden, dass eine Anbindung an das PSTN möglich ist, auch wenn die Internet-Anbindung und damit der IP-Anlagenanschluss nicht verfügbar ist.

zu M-TK-45 „Zusätzlicher IP-Anlagenanschluss“

Der zweite IP-Anlagenanschluss macht meist nur Sinn, wenn eine redundante Internet-Anbindung vorhanden ist, da die Verfügbarkeit des ITSP als höher angesehen werden kann als die Verfügbarkeit der lokalen Internet-Anbindung (siehe M-TK-44). In kleineren Standorten ist diese Maßnahme in den meisten Fällen nicht realisierbar bzw. nicht wirtschaftlich.

zu M-TK-46 „Zusätzlicher PSTN-Anschluss“

Der zweite PSTN-Anschluss macht in der Regel nur Sinn, wenn eine Anlage mit automatischen Umschaltmöglichkeiten eingesetzt wird. Ist dies aus wirtschaftlichen Gründen in kleineren Standorten nicht der Fall, so ist über die „Schaffung eines zusätzlichen PSTN-Ersatzanschlusses für Notrufe“ (siehe M-TK-38) zumindest eine minimale Kommunikationsfähigkeit zu gewährleisten.

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

Insbesondere für kleinere Standorte können auch Kombigeräte eingesetzt werden, welche zugleich Firewall, SBC und Internet- bzw. WAN-Anbindung übernehmen können. Hierbei ist das Thema Verfügbarkeit angemessen zu berücksichtigen.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-48	Sicherung von IP-Telefonen in unübersichtlichen Umgebungen	+	-	-	+	-	+	-	-	-	-	-
M-TK-49	Warnung bei unsicheren Einstellungen	+	-	-	+	-	+	-	-	-	-	-
M-TK-50	Prozess zur Behandlung des Verlusts eines VoIP-Endgerätes	+	-	-	+	-	+	-	-	-	-	-
M-TK-51	Absicherung der Firmware	+	-	+	+	-	+	+	-	+	+	-
M-TK-52	Absicherung von Konfigurationsdateien	+	-	+	+	-	+	+	-	+	+	-
M-TK-53	Sicherheit von Softphones	+	-	-	+	-	+	-	-	-	-	-
M-TK-54	Sichere Konfiguration von Ethernet-Ports für den PC-Anschluss an IP-Telefonen	+	-	-	+	-	+	-	-	-	-	-
M-TK-55	Sichere Konfiguration von IP und von IP-basierten Diensten	+	-	-	+	-	+	-	-	-	-	-
M-TK-56	Einschränkung des lokalen Zugriffs auf die Konfiguration des IP-Telefons	+	-	-	+	-	+	-	-	-	-	-
M-TK-57	Benutzerabhängige Berechtigungen	+	-	-	+	-	+	-	-	-	-	-
M-TK-58	Schutz von teilnehmerspezifischen Daten auf einem IP-Telefon	+	-	-	+	-	+	-	-	-	-	-
M-TK-59	Einschränkung von Internet-Telefonie auf dedizierte, gehärtete Endgeräte	+	-	-	+	-	+	-	-	-	-	-

Tabelle 10: Anwendbarkeit der Maßnahmen: Voice over IP – Endgeräte

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-57 „Benutzerabhängige Berechtigungen“

In kleineren Standorten ist ein gestuftes Berechtigungskonzept typischerweise unverhältnismäßig. Die Unterscheidung zwischen Standard-Profil und einem Profil mit erweiterten Berechtigungen nach Authentisierung ist im Regelfall ausreichend.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-60	Sichere Konfiguration der Netzwerk-Komponenten	+	-	-	+	-	-	+	-	-	-	-
M-TK-61	Sicheres Routing	+	+	+	+	+	+	+	+	+	+	+
M-TK-62	Absicherung von Switch-Ports	+	-	-	+	-	-	+	-	-	-	-
M-TK-63	Quality of Service im Netzwerk	+	+	+	+	+	+	+	+	+	+	+
M-TK-64	Zugangskontrolle zum Netzwerk	+	-	-	+	-	-	+	-	-	-	-
M-TK-65	MAC Security im Anschlussbereich für Endgeräte	+	-	-	+	-	-	+	-	-	-	-
M-TK-66	VPN zur Kommunikation über eingeschränkt vertrauenswürdige Netze	-	+	+	-	+	+	+	+	+	+	+
M-TK-67	Netztrennung für VoIP	+	+	+	+	+	+	+	-	+	+	-
M-TK-68	Netztrennung zwischen IP-PBX und Session Border Controller	+	-	-	-	-	-	+	-	-	-	-
M-TK-69	Erkennung und Abwehr von DoS-Angriffen gegen VoIP und von SPIT durch IPS / IDS	+	-	-	+	-	-	+	+	-	-	-
M-TK-70	Angemessene Verfügbarkeit des LAN für die Verwendung von VoIP	+	-	-	+	-	-	+	-	-	-	-
M-TK-71	Angemessene Verfügbarkeit der vom VoIP-System genutzten Netzdienste	+	-	-	-	-	-	+	-	-	-	-
M-TK-72	Angemessene Verfügbarkeit der Stromversorgung für IP-Telefone	+	-	-	+	-	-	-	-	-	-	-

Tabelle 11: Anwendbarkeit der Maßnahmen: Voice over IP – Netzwerk

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-61 „Sicheres Routing“

Die Maßnahme ist nur insoweit relevant, wie im Netzwerk der Organisation mehr als eine Routing-Komponente eingesetzt wird. Daher kommt diese Maßnahme in kleineren Standorten häufig nicht in Betracht.

zu M-TK-63 „Quality of Service im Netzwerk“

Für kleinere Standorte ist die Maßnahme dann nicht relevant, wenn keine WAN-basierte Kommunikation zwischen Standorten genutzt wird und im lokalen Netz eine ausreichende Dimensionierung gewährleistet ist.

Für kleinere Standorte oder Filialen, die per WAN mit anderen Standorten verbunden sind, können abhängig von der Dimensionierung der WAN-Verbindung Anforderungen an die Quality of Service (QoS) relevant sein.

zu M-TK-64 und M-TK-65

In kleineren Standorten ist die Realisierung dieser Maßnahme häufig unverhältnismäßig. Das Risiko eines unbefugten Anschlusses von Endgeräten kann über einen physischen Zugangsschutz zu den Räumen oder ausschließlich über einen beaufsichtigten Zutritt zu Räumen mit LAN-Anschlüssen in der Regel ausreichend bewältigt werden.

zu M-TK-67 „Netztrennung für VoIP“

Mit Umsetzung der Verschlüsselungsansätze gemäß M-TK-31 und M-TK-32 ist ein Großteil der Risiken, gegen die sich diese Maßnahme wendet, bereits wirkungsvoll entschärft. Das Restrisiko konzentriert sich vor allem auf die Verfügbarkeit, insbesondere auf Denial-of-Service-Attacken. Hier muss in kleineren Standorten der Schutzbedarf bezüglich der Verfügbarkeit und der Aufwand für die Netztrennung abgewogen werden.

Wird Verschlüsselung nicht eingesetzt, ist die Umsetzung einer Netztrennung dagegen auch in kleineren Standorten als Muss anzusehen und mit weiteren Maßnahmen zu kombinieren.

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

In kleineren Standorten, die typisch Kombigeräte aus Firewall und SBC nutzen, kann eine Netztrennung mit dedizierter Firewall nicht umgesetzt werden.

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

In kleineren Standorten sind hier in die Firewall integrierte IPS/IDS-Lösungen zu bevorzugen.

zu M-TK-70 und M-TK-71

Für kleinere Standorte ist im Regelfall die hochredundante Auslegung von LAN und Server unverhältnismäßig. Eine grundlegende Verfügbarkeit kann hier durch Schaffung eines zusätzlichen TK-Ersatzanschlusses für Notrufe gewährleistet werden.

Falls kleinere Standorte einen Verbund mit größeren Standorten bilden, so kann die Server-Redundanz im Fehlerfall über die Mitnutzung eines Servers eines verbundenen größeren Standorts realisiert werden. Entsprechend erhöht sich allerdings die Bedeutung der Server im verbundenen Standort über dessen Standortgrenzen hinaus.

zu M-TK-72 „Angemessene Verfügbarkeit der Stromversorgung für IP-Telefone“

Eine redundante Stromversorgung der IP-Telefone über eine USV ist in kleineren Standorten unwirtschaftlich. Im Fall eines vollständige Stromausfalls ist eine grundlegende Erreichbarkeit über Mobiltelefone zu gewährleisten.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	**S-I**	**S-S**	**S-F**	**F-I**	**F-F**	**R-S**	**S-P**	**S-X**	**F-P**	**R-P**	**P-X**
M-TK-73	Sichere Administration des Telefonie-Servers	+	-	-	-	-	-	+	-	-	-	-
M-TK-74	Sichere Administration von PSTN-Gateways	+	-	-	-	-	-	+	-	-	-	-
M-TK-75	Sichere Administration von Anwendungs- und Management-Servern	+	-	-	-	-	-	+	-	-	-	-
M-TK-76	Sichere Administration von Abrechnungs- und Gebührenerfassungssystemen	+	-	-	-	-	-	+	-	-	-	-
M-TK-77	Sichere Verwaltung von Teilnehmerprofilen	+	-	-	-	-	-	+	-	-	-	-
M-TK-78	Sichere Administration von Endgeräten	+	-	+	+	-	+	+	-	-	-	-
M-TK-79	Sichere Administration von Netzkomponenten	+	-	+	+	-	+	+	-	+	-	-
M-TK-80	Überwachung der Komponenten des VoIP-Systems	+	-	-	-	-	-	+	-	-	-	-
M-TK-81	Datensicherung für die Elemente des VoIP-Systems	+	-	-	-	-	-	+	-	-	-	-
M-TK-82	VoIP-Tauglichkeit der IP-Infrastruktur für einen IP-Anlagenanschluss	+	-	-	-	-	-	+	-	-	-	-
M-TK-83	Überwachung der VoIP-Anbindung zum ITSP	+	-	-	-	-	-	+	-	-	-	-
M-TK-84	Sichere Administration des Session Border Controller	+	-	-	-	-	-	+	-	-	-	-

Tabelle 12: Anwendbarkeit der Maßnahmen: Voice over IP – Netz- und Systemmanagement

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Die hier beschriebenen Maßnahmeninhalte setzen das Vorhandensein einer zentralen Management-Lösung voraus sowie entsprechendes Personal, das u. a. die entsprechenden Protokollierungen kompetent prüfen kann. Diese Voraussetzungen sind in kleineren Standorten häufig nicht gegeben, sodass die Maßnahmen nur sehr eingeschränkt anwendbar sind.

Hier konzentriert sich die Umsetzung der genannten Maßnahmen daher auf das im Einzelfall sinnvoll Machbare, was aber grundsätzlich Härtungsmaßnahmen, wie die gezielte Deaktivierung aller nicht benötigten Dienste beinhalten sollte. Diese Maßnahmen sind bei der Erstkonfiguration zu ergreifen und können Bestandteil einer entsprechenden Dienstleistung sein.

zu M-TK-82 „VoIP-Tauglichkeit der IP-Infrastruktur für einen IP-Anlagenanschluss“

Diese Maßnahme ist auch für kleinere Standorte zwingend vor der Erstkonfiguration zu ergreifen und kann Bestandteil einer entsprechenden Dienstleistung sein.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-85	Notfallvorsorge für das VoIP-System	+	-	-	+	-	-	-	-	-	-	-
M-TK-86	Harmonisierung zwischen IT-Betrieb und VoIP-Anlagen-Betrieb	+	-	-	-	-	-	+	-	-	-	-

Tabelle 13: Anwendbarkeit der Maßnahmen: Voice over IP – Übergreifende Aspekte

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-85 „Notfallvorsorge für das VoIP-System“

Bei Installationen in kleineren Standorten ist der Zweck dieser Maßnahme oft schon durch die Schaffung eines zusätzlichen PSTN-Ersatzanschlusses für Notrufe und organisatorische Festlegung zum Nutzungsrecht für den PSTN-Ersatzanschluss erfüllt.

zu M-TK-86 „Harmonisierung zwischen IT-Betrieb und VoIP-Anlagen-Betrieb“

Kleinere Standorte sollten die Administration bzw. den Betrieb von allgemeiner IT und VoIP-Anlage an denselben Dienstleister vergeben.

3.3 Hybrid-Systeme

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 und Voice over IP zu berücksichtigen.

Für kleinere Standorte gelten für Hybrid-Systeme die für die Basistechnologien genannten Einschränkungen.

3.4 Unified Communications and Collaboration

Die Anwendbarkeit der Maßnahmen für UCC-Telekommunikationslösungen ist in die folgenden Blöcke aufgeteilt:

- Server und Anwendungen, siehe Tabelle 14
- Endgeräte, siehe Tabelle 15
- Netzwerk, siehe Tabelle 16
- Netz- und Systemmanagement, siehe Tabelle 17
- Übergreifende Aspekte, siehe Tabelle 18

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-87	Absicherung der E-Mail-Kommunikation eines UCC-Systems	+	+	+	-	-	+	+	-	+	+	-
M-TK-88	Absicherung des Sprachkanals zwischen TK-Anlage bzw. VoIP-Kommunikationssystem und UCC-Systemen	+	+	-	-	-	-	+	-	-	-	-
M-TK-89	Absicherung von CTI-Verbindungen und Schnittstellen zur Anwendungsintegration	+	+	+	-	-	+	+	-	+	+	-
M-TK-90	Absicherung der Kommunikation zwischen UCC-System und weiteren IT-Systemen	+	+	-	-	-	-	+	-	-	-	-
M-TK-91	Absicherung der Kommunikation zwischen UCC-System und Datenbank	+	-	-	-	-	-	+	-	-	-	-
M-TK-92	Schutz vor unberechtigtem Zugriff auf Datenbanksysteme	+	-	-	-	-	-	+	-	-	-	-
M-TK-93	Absicherung der Kommunikation eines Präsenzsystems	+	+	+	-	-	+	+	-	-	-	-
M-TK-94	Vermeidung der Speicherung von Präsenzinformationen	+	-	-	-	-	-	+	-	-	-	-
M-TK-95	Einschränkung der Sichtbarkeit von Präsenzinformationen	+	-	-	-	-	-	+	+	-	-	-
M-TK-96	Differenzierung der Sichtbarkeit von Präsenzinformationen	+	-	-	-	-	-	+	+	-	-	-
M-TK-97	Verhindern der Verbreitung von Malware und bösartigen Hyperlinks per Instant Messaging	+	-	-	+	-	+	+	-	-	-	-
M-TK-98	Vermeidung von Spam-over-Instant-Messaging	+	-	-	-	-	-	+	-	-	-	-
M-TK-99	Verhinderung des Datenabflusses durch Data Loss Prevention	+	-	-	+	-	+	+	-	-	-	-
M-TK-100	Sicherung von Konferenzräumen	+	-	-	-	-	-	+	-	-	-	-

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-101	Sicherer Umgang mit Gesprächs- und Konferenzaufzeichnungen	+	-	-	+	-	+	+	-	-	-	-
M-TK-102	Absicherung des telefonischen Zugriffs auf UCC-Anwendungen durch eine PIN	+	-	-	-	-	-	+	-	-	-	-
M-TK-103	Einschränkung der Zugriffsrechte	+	-	-	-	-	-	+	-	-	-	-
M-TK-104	Einschränkung von Weiterleitungszielen und gleichzeitiger Rufsingalisierung	+	-	-	-	-	-	+	-	-	-	-
M-TK-105	Deaktivierung der CTI-Funktion für Konferenztelefone	+	-	-	-	-	-	+	-	-	-	-

Tabelle 14: Anwendbarkeit der Maßnahmen: UCC – Server und Anwendungen

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-87 „Absicherung der E-Mail-Kommunikation eines UCC-Systems“

Geht die E-Mail-Kommunikation über einen Sicherheitsbereich hinaus, z. B. bei der Kopplung zweier Voicemail-Systeme über das WAN bzw. das Internet, so ist diese Maßnahme auch in kleineren Standorten umzusetzen.

zu M-TK-88 bis M-TK-91

Auch in kleineren Standorten sollte diesen Maßnahmen eine hohe Bedeutung zugemessen werden, jedoch ist damit zu rechnen, dass die Produkte für dieses Marktsegment keine entsprechende Verschlüsselung unterstützen.

zu M-TK-92 „Schutz vor unberechtigtem Zugriff auf Datenbanksysteme“

Auf kleinere Installationen ausgerichtete Produkte bieten häufig keine Möglichkeit zur Einrichtung umfassender Berechtigungskonzepte.

zu M-TK-93 „Absicherung der Kommunikation eines Präsenzsystems“

Diese Maßnahme ist in kleineren Standorten von geringer Relevanz, da hier der Präsenzstatus einen vergleichsweise geringen Informationsgehalt besitzt. Allerdings erhöht sich die Relevanz, falls das Präsenzsystem auch für Instant Messaging oder über Standort- oder Organisationsgrenzen hinweg eingesetzt wird.

zu M-TK-94 und M-TK-95

Diese Maßnahme ist auch für kleinere Standorte leicht umzusetzen, da praktisch alle Präsenzsysteme die Möglichkeit bieten, vor Aufnahme einer Person in die Kontaktliste die Bestätigung des Nutzers zu erfordern. Es ist jedoch darauf zu achten, dass die Nutzer eine einmal gegebene Freigabe wieder entziehen können, d. h. nicht erwünschte Personen sollen aus der Kontaktliste entfernt werden können, um die Sichtbarkeit der eigenen Präsenzinformation einzuschränken.

zu M-TK-96 „Differenzierung der Sichtbarkeit von Präsenzinformationen“

Nur wenige Produkte unterstützen derzeit eine differenzierte Behandlung der Zugriffsrechte auf die Präsenzinformationen eines Nutzers, insbesondere nicht für kleinere Installationen.

zu M-TK-97 „Verhindern der Verbreitung von Malware und bösartigen Hyperlinks per Instant Messaging“

Kann in kleineren Standorten aus Gründen der Produktverfügbarkeit eine Malware-Filterung weder am Client noch zentral durchgeführt werden, so sollte die Nutzung des Peer-to-Peer-Dateitransfers, die Übertragung von Hyperlinks und von Bilddateien organisatorisch verboten oder deaktiviert werden.

zu M-TK-98 „Vermeidung von Spam over Instant Messaging“

Wird in kleineren Standorten auf eine Verbindung zwischen organisationsinterner IM-Lösung und einem öffentlichen IM-Dienstleister verzichtet, so ist diese Maßnahme für kleinere Standorte von geringer Relevanz.

zu M-TK-99 „Verhinderung des Datenabflusses durch Data Loss Prevention“

DLP-Systeme sind in kleineren Standorten häufig nicht wirtschaftlich einzurichten und zu betreiben. Hier kommt der Sensibilisierung und Schulung der Anwender hinsichtlich Sicherheitsaspekten (siehe Maßnahmen M-TK-246 und M-TK-247) besondere Bedeutung zu.

zu M-TK-101 „Sicherer Umgang mit Gesprächs- und Konferenzaufzeichnungen“

Ist in kleineren Standorten eine Server-seitige oder Client-seitige Speicherung der Aufzeichnungen mit umfassender Einbindung in das Datensicherungskonzept und gesicherter Vernichtung von personenbezogenen Daten nicht möglich, so muss auf die Speicherung verzichtet werden. Ist die Speicherung unumgänglich, so muss mittels organisatorischer Regelungen der Umgang mit derartigen Daten festgelegt werden.

Maßnahmen-Nr.	**Titel**	**Kommunikationsbeziehung**										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	**S-I**	**S-S**	**S-F**	**F-I**	**F-F**	**R-S**	**S-P**	**S-X**	**F-P**	**R-P**	**P-X**
M-TK-106	Absicherung von UCC-Systemen auf Ebene der Endgeräte	+	-	-	+	-	+	-	-	-	-	-
M-TK-107	Möglichkeit zur individuellen Einstellung des Präsenzstatus	+	-	-	+	-	+	+	-	-	-	-
M-TK-108	Ständiges Einblenden der Teilnehmerliste	+	-	-	+	-	+	+	-	-	-	-
M-TK-109	Verwenden von Kameras mit geeigneter Brennweite	+	-	-	+	-	+	-	-	-	-	-
M-TK-110	Signalisierung der Kameraaktivität und Verwendung von Kameraabdeckungen	+	-	-	+	-	+	-	-	-	-	-
M-TK-111	Richtliniengesteuerte Aktivierung/Deaktivierung von Kamera und Mikrofon	+	-	-	+	-	+	-	-	-	-	-
M-TK-112	Geeignete Standortwahl und Umgebungsgestaltung bei Einsatz von Desktop-Video	+	-	-	+	-	+	-	-	-	-	-

Tabelle 15: Anwendbarkeit der Maßnahmen: UCC – Endgeräte und Clients

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-106 „Absicherung von UCC-Systemen auf Ebene der Endgeräte“

Für kleinere Standorte lässt sich eine Absicherung auch durch organisatorische Regelungen zur Zutrittskontrolle erreichen.

zu M-TK-107 und M-TK-108

Bei Bereitstellung des UCC-Dienstes durch einen Provider müssen diese Eigenschaften durch geeignete Produkt- und Anbieterauswahl sichergestellt werden.

zu M-TK-111 „Richtliniengesteuerte Aktivierung/Deaktivierung von Kamera und Mikrofon“

Für kleinere Standorte sollte die Maßnahme mittels organisatorischer Vorgaben umgesetzt werden.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-113	Netztrennung zwischen UCC-Systemen und weiteren IT-Systemen	+	-	-	-	-	-	+	-	-	-	-

Tabelle 16: Anwendbarkeit der Maßnahmen: UCC – Netzwerk

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-113 „Netztrennung zwischen UCC-Systemen und weiteren IT-Systemen“

Analog zu Maßnahme M-TK-67 „Netztrennung für VoIP“ ist mit der Umsetzung einer Verschlüsselung gemäß M-TK-31 und M-TK-32 ein Großteil der Risiken, gegen die sich diese Maßnahme wendet, bereits wirkungsvoll entschärft. Das Restrisiko konzentriert sich vor allem auf die Verfügbarkeit, insbesondere auf Denial-of-Service-Attacken.

Wird Verschlüsselung nicht eingesetzt, ist eine Umsetzung einer Netztrennung dagegen auch in kleineren Standorten als Muss anzusehen und mit weiteren Maßnahmen zu kombinieren.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-114	Sichere Administration der Server für UCC-Systeme	+	-	-	-	-	-	+	-	-	-	-
M-TK-115	Absicherung der Management-Schnittstellen eines UCC-Systems	+	-	-	-	-	-	+	-	-	-	-

Tabelle 17: Anwendbarkeit der Maßnahmen: UCC – Netz- und Systemmanagement

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Die hier beschriebenen Maßnahmeninhalte setzen auch für UCC das Vorhandensein einer zentralen Management-Lösung sowie entsprechenden Personals voraus. Diese Voraussetzungen sind in kleineren Standorten häufig nicht gegeben. Hier konzentriert sich die Umsetzung der genannten Maßnahmen auf das im Einzelfall sinnvoll Machbare, was aber grundsätzlich Härtungsmaßnahmen, wie die gezielte Deaktivierung aller nicht benötigten Dienste beinhalten sollte.

In kleineren Standorten, die zu einem Verbund mit einem zentralen Standort gehören, kann das Management-Konzept des zentralen Standortes umgesetzt werden bzw. ergänzend auf entsprechendes Personal des zentralen Standortes zurückgegriffen werden.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	**S-I**	**S-S**	**S-F**	**F-I**	**F-F**	**R-S**	**S-P**	**S-X**	**F-P**	**R-P**	**P-X**
M-TK-116	Koordination der Planung und Administration von UCC-Diensten	+	-	-	-	-	-	-	-	-	-	-

Tabelle 18: Anwendbarkeit der Maßnahmen: UCC – Übergreifende Aspekte

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Auch in kleineren Standorten sollte der Einsatz von UCC sorgfältig geplant werden. Insbesondere sollte der Betrieb aller UCC-Dienste von einem einheitlichen Betreiber, intern oder extern, geleistet werden.

3.5 Spezielle TK-Systeme

3.5.1 Videokonferenzen

Die Maßnahmen für Videokonferenzen umfassen lediglich die Blöcke:

- Zentrale Systeme, Server und Anwendungen, siehe Tabelle 19
- Video-Terminals, siehe Tabelle 20

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Auch in kleineren Standorten mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit und Integrität ist die Absicherung der Videokonferenzsysteme ein wesentlicher Bestandteil der Gesamtlösung. Daher sollten alle Maßnahmen auch für kleinere Standorte angemessen umgesetzt werden.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-117	Absicherung der zentralen Komponenten des Videokonferenzsystems	+	-	-	-	-	-	+	-	-	-	-
M-TK-118	Durchgängige Verschlüsselung eines mit IP übertragenen Video-Medienstroms	+	+	+	+	+	+	+	+	+	+	+
M-TK-119	Durchgängige Verschlüsselung einer IP-basierten Video-Signalisierung	+	+	+	+	+	+	+	+	+	+	+
M-TK-120	Authentisierung zwischen Video-Terminals und zentralen Video-Systemen	+	-	-	-	-	-	+	-	-	-	-
M-TK-121	Sichereres Ressourcen-Management für Videokonferenzen	+	-	-	-	-	-	-	-	-	-	-

Tabelle 19: Anwendbarkeit der Maßnahmen: Spezielle TK-Systeme – Videokonferenz – Zentrale Systeme, Server und Anwendungen

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-122	Einschränkung des lokalen Zugriffs auf die Konfiguration des Video-Terminals	+	-	-	+	-	+	-	-	-	-	-
M-TK-123	Automatische Annahme eines Video-Anrufs deaktivieren	+	-	-	+	-	+	-	-	-	-	-
M-TK-124	Deaktivierung / Ausschaltung des Video-Terminals	+	-	-	+	-	+	-	-	-	-	-
M-TK-125	Anzeige der aktuellen Teilnehmer und Benachrichtigung bei neu eintretenden Teilnehmern einer Videokonferenz	+	-	-	+	-	+	+	-	-	-	-

Tabelle 20: Anwendbarkeit der Maßnahmen: Spezielle TK-Systeme – Videokonferenz – Video-Terminals

3.5.2 Kontaktcenter

Die Anwendbarkeit der Maßnahmen für Kontaktcenter ist in die folgenden Blöcke aufgeteilt:

- Server und Anwendungen, siehe Tabelle 21
- Endgeräte und Clients, siehe Tabelle 22
- Netzwerk, siehe Tabelle 23
- Netz- und Systemmanagement, siehe Tabelle 24
- Übergreifende Aspekte, siehe Tabelle 25

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-126	Authentisierung am IVR-System	+	-	-	-	-	-	+	-	-	-	-
M-TK-127	Qualitätssicherung der Routing-Regeln	+	-	-	-	-	-	+	-	-	-	-

Tabelle 21: Anwendbarkeit der Maßnahmen: Spezielle TK-Systeme – Kontaktcenter – Server und Anwendungen

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-126 „Authentisierung am IVR-System“

In kleineren Standorten sollte mindestens eine Authentisierung mittels PIN zum Einsatz kommen. Eine sprachbasierte Anruferauthentisierung bzw. eine Zwei-Faktor-Authentisierung ist für kleinere Standorte in vielen Fällen zu aufwendig und kann aufgrund der räumlichen Gegebenheiten des Standortes organisatorisch umgesetzt werden.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-128	Data Loss Prevention am Agentenarbeitsplatz	+	-	-	+	-	+	-	-	-	-	-
M-TK-129	Authentisierung des Zugriffs auf Kontaktcenter-Anwendungen	+	+	+	+	+	+	+	-	+	+	-
M-TK-130	Verhinderung des automatisierten Zugriffs auf Internet-Kontaktformulare	+	+	+	+	+	+	+	-	+	+	-

Tabelle 22: Anwendbarkeit der Maßnahmen: Spezielle TK-Systeme – Kontaktcenter – Endgeräte und Clients

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Auch in kleineren Standorten mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit, insbesondere bei Verarbeitung von personenbezogenen Daten, ist die Absicherung der Kontaktcenter-Lösung ein Muss. Daher sollten alle Maßnahmen auch für kleinere Standorte angemessen umgesetzt werden.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-131	Beschränkung des Netzzugriffs auf dedizierte Räumlichkeiten im Kontaktcenter	+	-	-	-	-	-	+	-	-	-	-
M-TK-132	Hochverfügbare Auslegung der Netzkomponenten und Systeme im Kontaktcenter	+	+	-	-	-	-	+	-	-	-	-
M-TK-133	Absicherung der Übergänge in öffentliche Netze	+	-	-	-	-	-	+	-	-	-	-

Tabelle 23: Anwendbarkeit der Maßnahmen: Spezielle TK-Systeme – Kontaktcenter – Netzwerk

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-131 „Beschränkung des Netzzugriffs auf dedizierte Räumlichkeiten im Kontaktcenter“

In Kontaktcentern, die personenbezogene Daten verarbeiten, müssen auch für kleinere Standorte die Zugriffe auf die Anwendungen separiert werden.

zu M-TK-132 „Hochverfügbare Auslegung der Netzkomponenten und Systeme im Kontaktcenter“

Die Sicherung der Verfügbarkeit von Netzkomponenten und Systemen muss in kleineren Standorten abhängig von der Kritikalität der Anwendungen im Verbund der Organisation geplant werden.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-134	Absicherung der Management-Schnittstellen	+	-	-	-	-	-	+	-	-	-	-

Tabelle 24: Anwendbarkeit der Maßnahmen: Spezielle TK-Systeme – Kontaktcenter – Netz- und Systemmanagement

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Da auch in kleineren Standorten mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit ungesicherte Management-Schnittstellen eine Gefährdung darstellen, müssen diese für eine Kontaktcenter-Lösung auch in kleineren Standorten zwingend abgesichert werden. Welcher der genannten Aspekte für eine Absicherung umgesetzt wird, muss entsprechend der räumlichen Gegebenheiten der Kontaktcenter-Lösung im Einzelfall entschieden werden.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-135	Schulung von Kontaktcenter-Administratoren und Schichtleitern/Supervisoren	+	-	-	-	-	-	-	-	-	-	-
M-TK-136	Zutrittsbeschränkung für Kontaktcenter-Räumlichkeiten	+	-	-	-	-	-	-	-	-	-	-

Tabelle 25: Anwendbarkeit der Maßnahmen: Spezielle TK-Systeme – Kontaktcenter – Übergreifende Aspekte

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-136 „Zutrittsbeschränkung für Kontaktcenter-Räumlichkeiten“

In kleineren Standorten kann aufgrund der räumlichen Gegebenheiten eine Zutrittsbeschränkungen zu den Räumlichkeiten leichter als eine Absicherung der Arbeitsplätze umgesetzt werden.

3.5.3 Händlersysteme

Die Anwendbarkeit der Maßnahmen für Händlersysteme ist in die folgenden Blöcke aufgeteilt:

- Server und Anwendungen, siehe Tabelle 26
- Endgeräte und Clients, siehe Tabelle 27

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Auch in kleineren Standorten sollten die genannten Maßnahmen zur Absicherung von Händlersystemen vollständig umgesetzt werden.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-137	Verwendung dedizierter Händlersysteme	+	-	-	-	-	-	+	-	-	-	-
M-TK-138	Festlegung dedizierter Gesprächskreise	+	-	-	-	-	-	+	-	-	-	-

Tabelle 26: Anwendbarkeit der Maßnahmen: Spezielle TK-Systeme – Händlersysteme – Server und Anwendungen

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-139	Vermeidung von Fehlbedienung durch intuitive Bedienkonzepte	+	-	-	-	-	-	-	-	-	-	-

Tabelle 27: Anwendbarkeit der Maßnahmen: Spezielle TK-Systeme – Händlersysteme – Endgeräte und Clients

3.5.4 Alarmierungssysteme

Die Anwendbarkeit der Maßnahmen für Alarmierungssysteme ist in die folgenden Blöcke aufgeteilt:

- Zentrale Systeme, Server und Anwendung, siehe Tabelle 28
- Endpunkte von Alarmierungssystemlösungen, siehe Tabelle 29
- Netzwerk, siehe Tabelle 30
- Netz- und Systemmanagement, siehe Tabelle 31
- Übergreifende Aspekte, siehe Tabelle 32

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

In kleineren Standorten werden in der Regel einfache Alarmanlagen eingesetzt, die im Alarmfall die Polizei, einen Sicherheitsdienst oder eine Mobilfunknummer benachrichtigen. Diese einfachen Systeme binden typischerweise die TK-Lösung nicht umfassend an, sodass in diesen Fällen keine besonderen Maßnahmen zu ergreifen sind.

Wird allerdings in kleineren Standorten ein komplexes Alarmierungssystem mit vielfältigen Integrationspunkten in die TK-Lösung und das zentralen IT-Sytem realisiert, welches einen erhöhten Schutzbedarf hinsichtlich Verfügbarkeit und Integrität hat, so sind die spezifizierten Maßnahmen möglichst umfassend umzusetzen:

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	**S-I**	**S-S**	**S-F**	**F-I**	**F-F**	**R-S**	**S-P**	**S-X**	**F-P**	**R-P**	**P-X**
M-TK-140	Schaffung geeigneter Umgebungsbedingungen für zentrale Elemente eines Alarmierungssystems	+	-	-	+	-	-	+	-	-	-	-
M-TK-141	Sichere Konfiguration zentraler Elemente einer Alarmierungsgesamtlösung	+	-	-	+	-	-	+	-	-	-	-
M-TK-142	Absicherung der Anbindung von Alarmierungssystemen an TK-Infrastrukturen	+	+	-	+	-	-	+	-	+	-	-
M-TK-143	Verstärkte Absicherung der von Alarmsystemen mitgenutzten TK-Installationen	+	-	-	-	-	-	+	-	-	-	-

Tabelle 28: Anwendbarkeit der Maßnahmen: Spezielle TK-Systeme – Alarmierungssysteme – Zentrale Systeme, Server und Anwendungen

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

In kleineren Standorten ist eine Alarmierungslösung mit geringerem Umfang und Funktionalität zu erwarten. Hier sind die Maßnahmen angepasst umzusetzen, ohne den erhöhten Schutzbedarf des Standortes zu gefährden.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-144	Ausstattung und Anbringung der Endpunkte unter Berücksichtigung von Sicherheitsaspekten	+	-	-	+	-	+	-	-	-	-	-
M-TK-145	Verbindliche Regelungen für den Umgang mit Endpunkten zu Alarmierungssystemen	+	-	-	+	-	+	-	-	-	-	-

Tabelle 29: Anwendbarkeit der Maßnahmen: Spezielle TK-Systeme – Alarmierungssysteme – Endpunkte

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-144 „Ausstattung und Anbringung der Endpunkte unter Berücksichtigung von Sicherheitsaspekten“

Falls in kleineren Standorten aufgrund der räumlichen Gegebenheiten eine sichere Installation der Endpunkte nicht gewährleistet werden kann, ist in der Regel eine häufige Sichtprüfung (siehe M-TK-148) in den meist überschaubaren Räumlichkeiten ausreichend, um Manipulationen an den Endpunkten frühzeitig zu erkennen.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-146	Absicherung der Kommunikation zwischen Elementen eines Alarmierungssystems	+	+	+	-	-	-	+	-	+	-	-

Tabelle 30: Anwendbarkeit der Maßnahmen: Spezielle TK-Systeme – Alarmierungssysteme – Netzwerk

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Auch in kleineren Standorten ist die Absicherung der Kommunikation essentiell für einen erhöhten Schutzbedarf.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-147	Automatisierte Überwachung der Komponenten von Alarmierungssystemen	+	-	-	-	-	-	+	-	-	-	-
M-TK-148	Erhöhte Frequenz gezielter Sicht- und Zustandsprüfungen	+	-	-	+	-	+	-	-	-	-	-

Tabelle 31: Anwendbarkeit der Maßnahmen: Spezielle TK-Systeme – Alarmierungssysteme – Netz- und Systemmanagement

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-147 „Automatisierte Überwachung der Komponenten von Alarmierungssystemen“

Falls das in kleineren Standorten eingesetzte Alarmierungssystem keine automatisierte Überwachung zulässt, so erhöht dies die Relevanz der Maßnahmen M-TK-148 und M-TK-150.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-149	Schulung von Administratoren bzw. des Betriebspersonals von Alarmierungssystemen	+	-	-	-	-	-	-	-	-	-	-
M-TK-150	Bedarfsgerechte Notfallplanung und -vorsorge für Kopplung von Alarmsystemen und TK-Lösungen	+	-	-	-	-	-	-	-	-	-	-
M-TK-151	Erarbeitung sicherheitsrelevanter Regelungen für den Einsatz von Alarmierungssystemen	+	-	-	-	-	-	-	-	-	-	-
M-TK-152	Erstellung einer Konzeption zur integrierten Nutzung von Alarmsystem und TK-Lösungen	+	-	-	-	-	-	-	-	-	-	-
M-TK-153	Produktauswahl von Alarmierungssystemlösungen unter Sicherheitsgesichtspunkten	+	-	-	-	-	-	-	-	-	-	-
M-TK-154	Einweisung, Schulung und Sensibilisierung der Nutzer von Alarmsystemlösungen	+	-	-	+	-	+	-	-	-	-	-

Tabelle 32: Anwendbarkeit der Maßnahmen: Spezielle TK-Systeme – Alarmierungssysteme – Übergreifende Aspekte

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Auch in kleineren Standorten sind die genannten Maßnahmen essentiell für eine Alarmierungslösung mit erhöhtem Schutzbedarf hinsichtlich Verfügbarkeit und Integrität. Jedoch sollten die Regelungen, Konzeptionen und Schulungen ggf. der reduzierten Funktionalität der eingesetzten Lösung angepasst werden.

3.6 Provider-basierte TK-Dienste

3.6.1 Soziale Netzwerke und Soziale Medien

Die Anwendbarkeit der Maßnahmen für die Einbindung von Sozialen Netzwerken und Sozialen Medien ist in die folgenden Blöcke aufgeteilt:

- Server und Anwendungen, siehe Tabelle 33
- Endgeräte, siehe Tabelle 34
- Netzwerk, siehe Tabelle 35
- Netz- und Systemmanagement, siehe Tabelle 36
- Übergreifende Aspekte, siehe Tabelle 37

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	**S-I**	**S-S**	**S-F**	**F-I**	**F-F**	**R-S**	**S-P**	**S-X**	**F-P**	**R-P**	**P-X**
M-TK-155	Berechtigungskonzept zur Steuerung der Freigabe des Präsenzstatus	+	-	-	-	-	-	+	-	+	+	-
M-TK-156	Berechtigungskonzept und technische Umsetzung für externe Kommunikation mit Sozialen Netzwerken und Medien	+	-	-	-	-	-	+	-	+	+	-
M-TK-157	Kanalisierung des Zugriff auf dienstliche Accounts in Sozialen Netzwerken und Medien über Portallösung	+	-	-	-	-	-	+	-	+	+	-
M-TK-158	Dokumentation der Zugriffe und Aktivitäten bei Nutzung von Sozialen Netzwerken und Medien	-	-	-	-	-	-	+	-	+	+	-

Tabelle 33: Anwendbarkeit der Maßnahmen: Soziale Netzwerke und Soziale Medien – Server und Anwendungen

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-155 „Berechtigungskonzept zur Steuerung der Freigabe des Präsenzstatus“

In kleineren Standorten sollte diese Maßnahme durch Einstellungen auf der SNM-Plattform getroffen werden. Falls dies nicht möglich ist, sollte grundsätzlich auf die Anzeige des Präsenzstatus verzichtet werden.

zu M-TK-157 „Kanalisierung des Zugriff auf dienstliche Accounts in Sozialen Netzwerken und Medien über Portallösung“

In kleineren Standorten kann eine solche Portallösung ausgelagert realisiert sein.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-159	Vermeiden der bidirektionalen Kontaktsynchronisation mit Sozialen Netzwerken und Medien	-	-	-	-	-	-	+	-	+	+	-
M-TK-160	Host-basiertes Data Loss Prevention (DLP) bei Nutzung von Sozialen Netzwerken und Medien	-	-	-	-	-	-	+	-	+	+	-

Tabelle 34: Anwendbarkeit der Maßnahmen: Soziale Netzwerke und Soziale Medien – Endgeräte und Clients

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-159 „Vermeiden der bidirektionalen Kontaktsynchronisation mit Sozialen Netzwerken und Medien“

In kleineren Standorten sollte die korrekte Konfiguration durch externes Fachpersonal vorgenommen werden und es muss gewährleistet sein, dass diese nicht verändert wird. Die Vermeidung von nicht gewollten Konfigurationsänderungen kann beispielsweise durch die Einbettung von SNM in eine Portallösung (siehe M-TK-157) sichergestellt werden. In jedem Fall muss auch in kleineren Standorten bei Gebrauch von Plug-ins eine Sensibilisierung der Anwender erfolgen. Insbesondere bei der Nutzung von SNM-Anwendungen für mobile Endgeräte ist dies notwendig, da z. B. ohne Einsatz von MDM keine Kontrolle erfolgen kann, ob und wie SNM-Apps genutzt werden.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-161	Netzwerk-basiertes Data Loss Prevention (DLP) bei Nutzung Sozialer Netzwerke und Medien	+	-	-	-	-	-	-	-	-	-	-
M-TK-162	Verhinderung oder Einschränkung der Nutzung von Sozialen Netzwerken und Medien am Netzübergang	+	-	-	-	-	-	+	-	+	-	-
M-TK-163	Netztechnische Isolation von Clients und Infrastrukturteilen mit Zugriff auf Soziale Netzwerke und Medien	+	-	-	+	-	-	-	-	-	-	-

Tabelle 35: Anwendbarkeit der Maßnahmen: Soziale Netzwerke und Soziale Medien – Netzwerk

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-161 „Netzwerk-basiertes Data Loss Prevention (DLP) bei Nutzung Sozialer Netzwerke und Medien“

In kleineren Standorten sollte alternativ der Einsatz eines Host-basierten DLP erwogen werden.

zu M-TK-162 „Verhinderung oder Einschränkung der Nutzung von Sozialen Netzwerken und Medien am Netzübergang“

Für kleinere Standorte sollte alternativ die Nutzung von SNM auf die Nutzung von separaten Arbeitsplätzen eingeschränkt werden oder die Kanalisierung über eine Portallösung erwogen werden.

zu M-TK-163 „Netztechnische Isolation von Clients und Infrastrukturteilen mit Zugriff auf Soziale Netzwerke und Medien“

Wird in einem kleineren Standort die Einrichtung einer separaten Netzzone als nicht wirtschaftlich eingestuft, kann mit geringerem Aufwand die Nutzung von SNM ausschließlich auf dedizierte, nicht mit der Organisationsinfrastruktur verbundene Endgeräte beschränkt werden.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-164	Sichere Administration der Server-Systeme und Gateways zur Anbindung an Soziale Netzwerke und Medien	+	-	-	-	-	-	+	-	-	-	-
M-TK-165	Schulung der Administratoren für den Zugang zu Sozialen Netzwerken und Medien	+	-	-	-	-	-	-	-	-	-	-

Tabelle 36: Anwendbarkeit der Maßnahmen: Soziale Netzwerke und Soziale Medien – Netz- und Systemmanagement

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-165 „Schulung der Administratoren für den Zugang zu Sozialen Netzwerken und Medien“

In kleineren Organisationen wird die Administration häufig von externen Dienstleistern übernommen. Hier muss sichergestellt werden, dass für die Nutzung von SNM die korrekte und Sicherheit gewährleistende Konfiguration vorgenommen wird und dass die Administratoren des Providers stets auf einem aktuellen Kenntnisstand sind.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-166	Klärung und rechtsverbindliche Regelung juristischer Aspekte zur Nutzung Sozialer Netzwerke und Medien im dienstlichen Kontext	+	-	-	-	-	-	-	-	-	-	-
M-TK-167	Geeignete Einbindung der Nutzung von Sozialen Netzwerken und Medien in etablierte Prozesse	+	-	-	-	-	-	-	-	-	-	-
M-TK-168	Transparente und durchsetzbare Regelungen zur Nutzung Sozialer Netzwerke und Medien im dienstlichen Kontext	+	-	-	-	-	-	-	-	-	-	-
M-TK-169	Gezielte Trennung von dienstlichem und rein privatem Gebrauch von Sozialen Netzwerken und Medien	+	-	-	-	-	-	-	-	-	-	-
M-TK-170	Einschränkung oder Verbot der Privatnutzung von Sozialen Netzwerken und Medien am Arbeitsplatz	+	-	-	-	-	-	-	-	-	-	-
M-TK-171	Verbot der ungeschützten Übertragung vertraulicher Inhalte über Soziale Netzwerke und Medien	+	-	-	-	-	-	-	-	-	-	-
M-TK-172	Information und Schulung der Anwender bzgl. sicherer Nutzung von Sozialen Netzwerken und Medien	+	-	-	-	-	-	-	-	-	-	-
M-TK-173	Benennung von Ansprechpartnern	+	-	-	-	-	-	-	-	-	-	-

Tabelle 37: Anwendbarkeit der Maßnahmen: Soziale Netzwerke und Soziale Medien – Übergreifende Aspekte

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Kleinere Organisationen mit erhöhtem Schutzbedarf sollten alle Maßnahmen zu übergreifenden Aspekten ohne Einschränkung umsetzen.

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

Die Anwendbarkeit der Maßnahmen für die Nutzung von Outsourcing, IP-Centrex, Cloud Computing und UC as a Service (UCaaS) ist in die folgenden Blöcke aufgeteilt:

- Server und Anwendungen, siehe Tabelle 38
- Endgeräte, siehe Tabelle 39
- Netzwerk, siehe Tabelle 40
- Netz- und Systemmanagement, siehe Tabelle 41
- Übergreifende Aspekte, siehe Tabelle 42

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-174	Konsequente Verschlüsselung bei Transport, Speicherung und Verarbeitung von Daten	-	-	-	-	-	-	+	-	+	+	+
M-TK-175	Härtung der Virtualisierungsplattform	+	-	-	-	-	-	+	-	-	-	-
M-TK-176	Einsatz von UC-fähigem Virenschutz	+	-	-	+	-	+	+	-	-	-	-

Tabelle 38: Anwendbarkeit der Maßnahmen: Outsourcing, IP-Centrex, Cloud Computing und UC as a Service – Server und Anwendungen

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Für kleinere Standorte gibt es für die unter „Server und Anwendungen“ aufgeführten Maßnahmen keine Einschränkungen.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-177	Einsatz von Host-basierten DLP-Systemen bei Cloud-Nutzung	+	-	-	+	-	+	-	-	-	-	-

Tabelle 39: Anwendbarkeit der Maßnahmen: Outsourcing, IP-Centrex, Cloud Computing und UCaaS – Endgeräte und Clients

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Für kleinere Standorte gibt es für die unter „Endgeräte und Clients“ aufgeführte Maßnahme keine Einschränkungen.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-178	Einsatz von Netzwerk-basierten DLP-Systemen bei Cloud-Nutzung	+	-	-	+	-	-	+	-	-	-	-

Tabelle 40: Anwendbarkeit der Maßnahmen: Outsourcing, IP-Centrex, Cloud Computing und UCaaS – Netzwerk

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Für kleinere Standorte ist die unter „Netzwerk“ aufgeführte Maßnahme typischerweise nicht relevant, da sie aufgrund der Standortgröße meist nicht sinnvoll umsetzbar ist.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-179	Dem Schutzbedarf angepasste Überwachung der Dienste	-	-	-	-	-	-	+	-	-	-	-
M-TK-180	Regelmäßige Erstellung von Berichten und Informationspflicht bei Sicherheitsvorfällen	-	-	-	-	-	-	+	-	-	-	-

Tabelle 41: Anwendbarkeit der Maßnahmen: Outsourcing, IP-Centrex, Cloud Computing und UCaaS – Netz- und Systemmanagement

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Für kleinere Standorte gibt es für die unter „Netz- und Systemmanagement“ aufgeführten Maßnahmen keine Einschränkungen.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-181	Nachweis und Überprüfung der Vertrauenswürdigkeit des Dienstleisters	+	-	-	-	-	-	+	-	-	-	-
M-TK-182	Einsatz von sicherheitsüberprüftem Personal	+	-	-	-	-	-	+	-	-	-	-
M-TK-183	Regelmäßige Auditierung der Infrastruktur des Dienstleisters	+	-	-	-	-	-	+	-	-	-	-
M-TK-184	Festlegung des Speicherortes der Daten bei Outsourcing und Cloud-Nutzung	+	-	-	-	-	-	+	-	-	-	-
M-TK-185	Lesender Zugriff auf die vom Dienstleister bereitgestellten Komponenten	+	-	-	-	-	-	+	-	-	-	-

Tabelle 42: Anwendbarkeit der Maßnahmen: Outsourcing, IP-Centrex, Cloud Computing und UCaaS – Übergreifende Aspekte

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Für kleinere Standorte gibt es für die unter „Übergreifende Aspekte“ aufgeführten Maßnahmen keine Einschränkungen.

3.7 Einbindung Mobiler Endgeräte

Die Anwendbarkeit der Maßnahmen zur Einbindung mobiler Endgeräte ist in die folgenden Blöcke aufgeteilt:

- Server und Anwendungen, siehe Tabelle 43
- Endgeräte, siehe Tabelle 44
- Netzwerk, siehe Tabelle 45
- Netz- und Systemmanagement, siehe Tabelle 46

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-186	Gegenseitige Authentisierung von mobilen Endgeräten und einer zentralen Komponente der FMC- oder UCC-Lösung	+	-	-	+	-	+	+	-	-	+	-
M-TK-187	Schutz von Servern für mobile Endgeräte	+	-	-	-	-	-	+	-	-	-	-
M-TK-188	Verwendung einer Ende-zu-Ende-Verschlüsselung für die Telekommunikation	+	-	-	+	-	+	+	-	-	+	-
M-TK-189	Verschlüsselung von Nachrichten	-	-	-	+	-	+	-	-	-	-	-
M-TK-190	Einsatz von Server-based Computing	+	-	-	-	-	-	+	-	-	-	-
M-TK-191	Verschlüsselung, Integritätsschutz und Authentisierung auf der Luftschnittstelle	+	-	-	+	-	+	-	-	-	-	-
M-TK-192	Ende-zu-Ende-Verschlüsselung für Medienströme	+	+	+	+	+	+	+	+	+	+	-
M-TK-193	Absicherung Authentication-Server	+	-	-	-	-	-	+	-	-	-	-

Tabelle 43: Anwendbarkeit der Maßnahmen: Einbindung Mobiler Endgeräte – Server und Anwendungen

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Auch in kleineren Standorten mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit und Integrität ist insbesondere die Absicherung der mobilen Endgeräte ein wesentlicher Bestandteil der Gesamtlösung. Daher sollten alle Maßnahmen auch für kleinere Standorte angemessen umgesetzt werden.

zu M-TK-190 „Einsatz von Server-based Computing“

Eine lokale Installation von Terminalservern oder vergleichbaren Lösungen ist in kleineren Standorten unüblich. Eher werden, falls verfügbar, Terminalserver von einem größeren Standort der Organisation mitgenutzt.

zu M-TK-193 „Absicherung Authentication-Server“

Für eine kleine Institution ist meist von der Verwendung von PSKs auszugehen und es wird kein RADIUS-Server genutzt oder es wird ein RADIUS-Server von einem größeren Standort der Organisation mitgenutzt.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-194	Einsatz von abhörsicheren Mobiltelefonen	-	-	-	-	-	+	-	-	-	-	-
M-TK-195	Absicherung aller Kommunikationsschnittstellen des Endgerätes	-	-	-	-	-	+	-	-	-	-	-
M-TK-196	Schutz der organisationsinternen Daten auf einem mobilen Endgerät	-	-	-	-	-	+	-	-	-	-	-
M-TK-197	Erweiterung von Data Loss Prevention auf mobile Endgeräte	-	-	-	-	-	+	-	-	-	-	-
M-TK-198	Sperrung des mobilen Endgerätes für Nutzereingaben	-	-	-	-	-	+	-	-	-	-	-
M-TK-199	Benutzerauthentisierung am mobilen Endgerät	-	-	-	-	-	+	-	-	-	-	-
M-TK-200	Automatische Handlungen bei Verletzung von Sicherheitsrichtlinien auf mobilen Endgeräten	+	-	-	-	-	+	-	-	-	-	-
M-TK-201	Rollenbasierte Zugriffsberechtigungen auf Objekte des mobilen Endgerätes	+	-	-	-	-	+	-	-	-	-	-
M-TK-202	Schutz des mobilen Endgerätes vor schadenstiftender Software	+	-	-	-	-	+	-	-	-	-	-
M-TK-203	Deaktivierung der automatischen Rufannahme	-	-	-	-	-	+	-	-	-	-	-
M-TK-204	Schutz vor unerwünschter Konfigurationsänderung über die GSM/UMTS-Funkschnittstelle	-	-	-	-	-	+	-	-	-	-	-
M-TK-205	Schutzmaßnahmen für das Herunterladen von Inhalten	-	-	-	-	-	+	-	-	-	-	-
M-TK-206	Prozess zur Behandlung des Verlusts eines mobilen Endgerätes	+	-	-	-	-	+	-	-	-	-	-
M-TK-207	Einsatz von DECT-Endgeräten mit verbesserter DECT-konformer Verschlüsselung	-	-	-	+	-	+	-	-	-	-	-
M-TK-208	Einsatz von DECT-Endgeräten mit zusätzlicher Verschlüsselung	-	-	-	+	-	+	-	-	-	-	-
M-TK-209	Sichere Konfiguration und Verwendung des Bluetooth-Adapters	+	-	-	+	-	+	-	-	-	-	-
M-TK-210	Einsatz von Bluetooth-Endgeräten mit zusätzlicher Verschlüsselung	-	-	-	+	-	+	-	-	-	-	-

Tabelle 44: Anwendbarkeit der Maßnahmen: Einbindung Mobiler Endgeräte – Endgeräte

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Auch in kleineren Standorten mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit und Integrität ist insbesondere die Absicherung der mobilen Endgeräte ein wesentlicher Bestandteil der Gesamtlösung. Daher sollten die meisten der genannten Maßnahmen auch für kleinere Standorte umgesetzt werden. Ausnahmen sind:

zu M-TK-197 Erweiterung von Data Loss Prevention auf mobile Endgeräte

Für einen kleinen Standort muss der Aufwand für die Einrichtung von Data Loss Prevention beachtet werden. Eine organisatorische Maßnahme, verbunden mit der Vermeidung der Speicherung kritischer Daten, ist ggf. für einen kleineren Standort die zu bevorzugende Lösung.

zu M-TK-200 bis M-TK-202

Die Umsetzung dieser Maßnahmen setzt in der Regel eine zentrale Systemverwaltung (z. B. MDM) voraus bzw. das System ist für den Einsatz in größeren Organisationen konzipiert. Für eine kleinere Organisation kann sich ein solches System als überdimensioniert erweisen.

Die strikte Umsetzung der Maßnahmen M-TK-195 und M-TK-196 trägt stark zur Reduktion des Restrisikos bei und ist ggf. für kleinere Organisationen ausreichend.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	**S-I**	**S-S**	**S-F**	**F-I**	**F-F**	**R-S**	**S-P**	**S-X**	**F-P**	**R-P**	**P-X**
M-TK-211	Berücksichtigung der Sicherheit bei der Vertragsgestaltung mit einem Dienstanbieter	+	-	-	-	-	-	-	-	-	-	-
M-TK-212	Trennung von LAN- und WLAN-Verkehr im kabelbasierten Netz	+	-	-	+	-	-	-	-	-	-	-
M-TK-213	Absicherung des LAN-Zugangs für Access Points	+	-	-	+	-	-	-	-	-	-	-
M-TK-214	Berücksichtigung der Anforderungen einer Sprachübertragung bei der Planung der Funkzellen	+	-	-	+	-	-	-	-	-	-	-
M-TK-215	Absicherung bei Anschluss von Radio Fixed Parts an ein LAN	+	-	-	+	-	-	-	-	-	-	-
M-TK-216	Absicherung von Bluetooth Access Points bei Anschluss an ein LAN	+	-	-	+	-	-	-	-	-	-	-

Tabelle 45: Anwendbarkeit der Maßnahmen: Einbindung Mobiler Endgeräte – Netzwerk

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-211 „Berücksichtigung der Sicherheit bei der Vertragsgestaltung mit einem Dienstanbieter“

Die Gestaltungsmöglichkeiten sind üblicherweise abhängig vom Umfang der eingekauften Leistung stark eingeschränkt.

zu M-TK-212 „Trennung von LAN- und WLAN-Verkehr im kabelbasierten Netz“

Die Umsetzung der Verschlüsselungsansätze gemäß M-TK-191 und M-TK-192 entschärft einen Großteil der mit einem drahtlosen Netzzugang verbundenen Risiken. Das Restrisiko, das eine Trennung von LAN und WLAN erforderlich macht, ergibt sich primär aus heterogenen Nutzergruppen und Endgerätetypen mit eingeschränkten Sicherheitsfunktionen, für die der Zugang zu LAN-Ressourcen streng reglementiert werden muss. Eine solche Situation ist für kleinere Organisationen eher die Ausnahme.

zu M-TK-213, M-TK-215 und M-TK-216

Die Absicherung des LAN-Zugangs für WLAN Access Points, DECT Radio Fixed Parts oder Bluetooth Access Points ist für flächendeckende größere Installationen von besonderer Wichtigkeit, da die Gefährdungslage proportional zur Anzahl der Access Points bzw. Fixed Parts wächst. Für kleinere Standorte sind die Maßnahmen daher von geringerer Relevanz, sofern im Rahmen der Übersichtlichkeit

ein unbeaufsichtigter physischer Zugriff auf Access Points bzw. Fixed Parts und zugehörige Netzanschlüsse verhindert werden kann.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-217	Fernadministration der mobilen Endgeräte durch ein Mobile Device Management	+	-	-	-	-	+	-	-	-	-	-
M-TK-218	Regelmäßige, möglichst automatische Sicherung von Daten und Konfiguration mobiler Endgeräte	+	-	-	-	-	+	-	-	-	-	-
M-TK-219	Einschränkung der Apps	+	-	-	-	-	+	-	-	-	-	-
M-TK-220	Überwachung der Endgeräte hinsichtlich Anomalien	+	-	-	-	-	+	-	-	-	-	-
M-TK-221	Kontinuierliche Überwachung der Luftschnittstelle	+	-	-	+	-	-	-	-	-	-	-
M-TK-222	Kontinuierliche Überwachung der WLAN-Infrastruktur	+	-	-	+	-	-	-	-	-	-	-
M-TK-223	Fernadministration der WLAN-Endgeräte	+	-	-	+	-	-	-	-	-	-	-
M-TK-224	Protokollierung des Einsatzes zusätzlicher Verschlüsselung	+	-	-	+	-	+	-	-	-	-	-
M-TK-225	Verzicht auf den Einsatz von DECT bei erhöhtem Schutzbedarf	+	-	-	+	-	+	-	-	-	-	-
M-TK-226	Verzicht auf den Einsatz von Bluetooth bei erhöhtem Schutzbedarf	+	-	-	+	-	+	-	-	-	-	-

Tabelle 46: Anwendbarkeit der Maßnahmen: Einbindung Mobiler Endgeräte – Netz- und Systemmanagement

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Auch in kleineren Standorten mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit und Integrität ist insbesondere die Absicherung der mobilen Endgeräte ein wesentlicher Bestandteil der Gesamtlösung. Daher sollten die genannten Maßnahmen auch für kleinere Standorte weitestgehend umgesetzt werden. Ausnahmen sind:

zu M-TK-217 bis M-TK-220

Die Umsetzung der Maßnahmen mittels MDM erleichtert bei einer größeren Anzahl von Endgeräten erheblich den Betrieb und mindert das Risiko von Fehlkonfiguration und der damit verbundenen Gefährdungen für die IT-Sicherheit. Eine solche Management-Lösung ist auch für kleinere Standorte/Organisationen sehr zu empfehlen und könnte für kleinere Standorte durch einen Dienstanbieter oder durch einen größeren Standort der Organisation realisiert werden.

Die Einrichtung eines MDM ist für kleinere Standorte nur dann entbehrlich, wenn eine den Vorgaben entsprechende sichere Endgeräte-Konfiguration mit anderen Mitteln sichergestellt werden kann.

zu M-TK-221 und M-TK-222

Für kleinere Standorte ist die Verfügbarkeitsüberwachung der Luftschnittstelle und insbesondere der Access Points von geringerer Relevanz, sofern das mit WLAN versorgte Gebiet überschaubar und die Anzahl der Access Points gering ist.

Soll die Überwachung der Luftschnittstelle und der Access Points von einem größeren Standort aus erfolgen, ist bei der Festlegung der Polling-Intervalle und der zu überwachenden Parameter die in kleineren Standorten/Filialen geringere verfügbare Kapazität der WAN-Verbindung zu den Filialen zu berücksichtigen.

zu M-TK-223 „Fernadministration der WLAN-Endgeräte“

Ist die Einrichtung einer Fernadministration für kleinere Standorte mit einer geringen Anzahl von Endgeräten nicht geeignet umsetzbar, so muss eine den Vorgaben entsprechende Konfiguration der Endgeräte mit anderen Mitteln für den Schutzbedarf angemessen sichergestellt werden.

3.8 Generell zu ergreifende Sicherheitsmaßnahmen

Die Anwendbarkeit der generell zu ergreifenden Sicherheitsmaßnahmen ist in die folgenden Blöcke aufgeteilt:

- Auslegung der passiven Netzinfrastruktur bei erhöhtem Schutzbedarf, siehe Tabelle 47
- Absicherung von Servern des Telekommunikationssystems, siehe Tabelle 48
- Sicheres Netz- und Systemmanagement, siehe Tabelle 49
- Datenschutz, siehe Tabelle 50
- Auswahl von Dienstanbietern, siehe Tabelle 51
- Notfallvorsorge, siehe Tabelle 52
- Organisatorische Maßnahmen, siehe Tabelle 53

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	**S-I**	**S-S**	**S-F**	**F-I**	**F-F**	**R-S**	**S-P**	**S-X**	**F-P**	**R-P**	**P-X**
M-TK-227	Sichere Kabelführung	+	-	-	+	-	-	+	-	-	-	-

Tabelle 47: Anwendbarkeit der Maßnahmen: Generell zu ergreifende Sicherheitsmaßnahmen – Passive Netzinfrastruktur

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Im Fall eines erhöhten Schutzbedarfs sollte die Maßnahme auch von kleineren Standorten angemessen umgesetzt werden.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-228	Produktauswahl von TK-Lösungen unter Berücksichtigung von Sicherheitsaspekten	+	-	-	-	-	-	+	-	-	-	-
M-TK-229	Härtung von Servern des Telekommunikationssystems	+	-	-	-	-	-	+	-	-	-	-
M-TK-230	Spezielle Absicherung von virtualisierten TK-Servern	+	-	-	-	-	-	+	-	-	-	-
M-TK-231	Einschränkung und Kontrolle von Berechtigungen für die Administration eines Servers des Telekommunikationssystems	+	-	-	-	-	-	+	-	-	-	-
M-TK-232	Einschränkung und Kontrolle des Zugangs zu einem Server des Telekommunikationssystems	+	-	-	-	-	-	+	-	-	-	-
M-TK-233	Physische Sicherheit der Server der Telekommunikationslösung	+	-	-	-	-	-	+	-	-	-	-
M-TK-234	Berücksichtigung der Server der TK-Lösung im Datensicherungskonzept der Organisation	+	-	-	-	-	-	+	-	-	-	-
M-TK-235	Schutz vor schadenstiftender Software für die Server der TK-Lösung	+	-	-	-	-	-	+	-	-	-	-
M-TK-236	Einbindung der Server der TK-Lösung in das Patch-Management der Organisation	+	-	-	-	-	-	+	-	-	-	-

Tabelle 48: Anwendbarkeit der Maßnahmen: Generell zu ergreifende Sicherheitsmaßnahmen – Server der Telekommunikationssystems

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-228, M-TK-229, M-TK-230 und M-TK-236

Der mit der Umsetzung dieser Maßnahmen verbundene Aufwand kann für einen kleineren Standort hinsichtlich der Personalkapazität und der notwendigen Kompetenz erheblich sein. Trotzdem ist auch für kleinere Standorte die grundlegende Umsetzung bei der Produktauswahl, der Härtung und dem Patch-Management dringend zu empfehlen.

Bei der Bereitstellung von TK-Lösungen durch Provider sollte die Produktauswahl implizit durch geeignete Auswahl des Providers berücksichtigt werden.

zu M-TK-231 „Einschränkung und Kontrolle von Berechtigungen für die Administration eines Servers des Telekommunikationssystems“

Das hier einzurichtende Berechtigungskonzept richtet sich nach der Größe und Organisationsstruktur der Organisation. Für einen kleineren Standort, insbesondere falls kein zentraler Standort vorhanden ist, genügt oft ein entsprechend einfaches Konzept.

zu M-TK-232 „Einschränkung und Kontrolle des Zugangs zu einem Server des Telekommunikationssystems“

Für einen kleineren Standort kann bereits durch Umsetzung der Maßnahme M-TK-231 die zwingende Notwendigkeit einer Kontrolle für den lokalen Zugang nicht mehr gegeben sein. Für Fernwartungszugänge kann mangels Personalkapazitäten mit entsprechendem Know-how oft weder die geeignete Absicherung von externen Fernwartungszugriffen regelmäßig überprüft noch eine Kontrolle von Log-Informationen auf solche Zugriffsversuche realisiert werden. In diesem Fall sollte auf Fernwartungszugriffe durch Externe verzichtet werden.

zu M-TK-233 „Physische Sicherheit der Server der Telekommunikationslösung“

Diese Maßnahme ist eine wesentliche Grundlage für die Wahrung der Verhältnismäßigkeit bei der Umsetzung anderer Maßnahmen und sollte auch in kleineren Standorten angemessen realisiert werden.

Insbesondere in kleineren Standorten sind häufig die (bau-)technischen Möglichkeiten eingeschränkt. In solchen Umgebungen ist so weit wie möglich die Übersichtlichkeit der Umgebungsgröße gezielt für konsequente organisatorische Umsetzung auszunutzen, z. B.:

- Unterbringung der Server in abschließbaren Schränken
- kein unbeaufsichtigter Zutritt Fremder zu Räumen, in denen Server untergebracht sind

zu M-TK-234 „Berücksichtigung der Server der TK-Lösung im Datensicherungskonzept der Organisation“

Auch in kleineren Standorten ist schnelle Wiederherstellung der vollen Funktionsfähigkeit der TK-Lösung von entscheidender Bedeutung. Hier ist insbesondere im Fall einer Auslagerung des TK-Anlagenbetriebs vertraglich die Umsetzung der Maßnahme sicherzustellen.

zu M-TK-235 „Schutz vor schadenstiftender Software für die Server der TK-Lösung“

Für einen kleineren Standort kann zur Umsetzung dieser Maßnahme die Gewährleistung einer angemessenen Perimetersicherheit und des Schutzes der genutzten Endgeräte vor schadenstiftender Software ausreichend sein.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	**S-I**	**S-S**	**S-F**	**F-I**	**F-F**	**R-S**	**S-P**	**S-X**	**F-P**	**R-P**	**P-X**
M-TK-237	Sichere Konfiguration des Netzwerkmanagement-Protokolls	+	-	-	-	-	-	+	-	-	-	-
M-TK-238	Überwachung der Komponenten des Telekommunikationssystems	+	-	-	-	-	-	+	-	-	-	-
M-TK-239	Erweiterung von Penetrationstests auf die verwendeten TK-Technologien	+	-	-	-	-	-	+	-	-	-	-
M-TK-240	Ergänzung der Überwachung um Honeypots für die verwendeten TK-Technologien	+	-	-	-	-	-	+	-	-	-	-
M-TK-241	Erweiterung des Verwundbarkeits-Managements für die verwendeten TK-Technologien	+	+	+	+	+	+	+	+	+	+	-

Tabelle 49: Anwendbarkeit der Maßnahmen: Generell zu ergreifende Sicherheitsmaßnahmen – Sicheres Netz- und Systemmanagement

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Die Voraussetzungen für das Vorhandensein einer zentralen Management-Lösung und/oder eines Log-Servers sind in kleineren Standorten häufig nicht gegeben, da eine solche Lösung unverhältnismäßig bzw. mangels entsprechend kompetenten Personals sinnlos ist. In dieser Situation sollte ein kleinerer Standort im Wesentlichen alle Management-Zugriffsmöglichkeiten gezielt abschalten.

In kleineren Standorten, die zu einem Verbund mit einem zentralen Standort gehören, kann das Management-Konzept des zentralen Standorts umgesetzt werden bzw. ergänzend auf entsprechendes Personal des zentralen Standorts zurückgegriffen werden.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-242	Schutz von Verbindungsdaten	+	+	+	+	-	-	+	-	+	-	-
M-TK-243	Nutzung von speziell abgesicherten Räumlichkeiten	+	-	-	+	-	+	-	-	-	-	-
M-TK-244	Sichere Außerbetriebnahme von Komponenten des Telekommunikationssystems	+	-	-	+	-	+	+	-	-	-	-

Tabelle 50: Anwendbarkeit der Maßnahmen: Generell zu ergreifende Sicherheitsmaßnahmen – Datenschutz

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Besteht für einen kleineren Standort ein erhöhter Schutzbedarf hinsichtlich Vertraulichkeit, so sollten die genannten Maßnahmen auch für kleinere Standorte vollständig umgesetzt werden.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-245	Nachweis der Vertrauenswürdigkeit des Dienstanbieters	+	-	-	-	-	-	-	-	-	-	-

Tabelle 51: Anwendbarkeit der Maßnahmen: Generell zu ergreifende Sicherheitsmaßnahmen – Auswahl von Dienstanbietern

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Besteht für einen kleineren Standort ein erhöhter Schutzbedarf hinsichtlich Vertraulichkeit und Integrität, so kommt dem Nachweis der Vertrauenswürdigkeit auch für kleinere Standorte eine essentielle Bedeutung zu.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	S-I	S-S	S-F	F-I	F-F	R-S	S-P	S-X	F-P	R-P	P-X
M-TK-246	Notfallvorsorge für alle Teilsysteme der TK-Lösung	+	-	-	-	-	-	-	-	-	-	-

Tabelle 52: Anwendbarkeit der Maßnahmen: Generell zu ergreifende Sicherheitsmaßnahmen – Notfallvorsorge

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

Besteht für einen kleineren Standort ein erhöhter Schutzbedarf, so kommt der Notfallvorsorge auch für kleinere Standorte eine essentielle Bedeutung zu.

Maßnahmen-Nr.	Titel	Kommunikationsbeziehung										
	Legende: S – Standort, I – Intern, F – Filiale, R – Remote User, P – Provider, X – Externe Organisation	**S-I**	**S-S**	**S-F**	**F-I**	**F-F**	**R-S**	**S-P**	**S-X**	**F-P**	**R-P**	**P-X**
M-TK-247	Sensibilisierung der Anwender von TK-Diensten hinsichtlich Sicherheitsaspekten	+	-	-	-	-	-	-	-	-	-	-
M-TK-248	Schulung der Anwender von TK-Diensten zu Sicherheits- und Datenschutzaspekten	+	-	-	-	-	-	-	-	-	-	-
M-TK-249	Schulung der Administratoren von TK-Lösungen	+	-	-	-	-	-	+	-	-	-	-

Tabelle 53: Anwendbarkeit der Maßnahmen: Generell zu ergreifende Sicherheitsmaßnahmen – Organisatorische Maßnahmen

Erläuterungen bzw. Einschränkungen für kleinere Organisationen und kleinere Standorte:

zu M-TK-249 „Schulung der Administratoren von TK-Lösungen“

In kleineren Standorten kann diese Maßnahme im Wesentlichen durch das Studium der entsprechenden Dokumentation und Handbücher umgesetzt werden. Da in kleineren Standorten die TK-Administration häufig ausgelagert wird, ist hier das primäre Ziel den zuständigen Anwender in die Lage zu versetzen, Administrationsleistungen gezielt einkaufen und bewerten zu können.

Alternativ kann in kleineren Standorten, die einen Verbund mit größeren Standorten bilden, auf die Administratoren eines zentralen Standortes zugegriffen werden.

4 Sicherheitskonzepte für Beispielszenarien

4.1 Beispiel einer kleinen Organisation: Anwaltsbüro

Anhand eines kleinen Anwaltsbüros mit ca. 10 Mitarbeitern soll im Folgenden ein mögliches Szenario für die Kommunikationslösung einer kleinen Organisation dargestellt werden. Zunächst werden die Ausgestaltung dieses einzelnen zentralen Standorts und die auftretenden Anforderungen kurz beschrieben. Darauf wird eine mögliche Lösung präsentiert und anhand der vorigen Kapitel eine Priorisierung von Maßnahmen getroffen.

4.1.1 Rahmenbedingungen

In diesem Szenario soll vorrangig die Einbindung von verschiedenen Endgeräte-Typen und deren flexibler Einsatz, z. B. zur Anbindung von Telearbeitsplätzen, dargestellt werden. Aus wirtschaftlichen Gründen ist kein eigenes IT-kompetentes Personal vorhanden. Also werden Dienste und Dienstleistungen ausgelagert und u. a. Betrieb und Wartung von externen Unternehmen geleistet. Insbesondere werden TK-Applikationen und TK-Dienste, die hier unter dem Begriff Unified Communications and Collaboration (UCC) zusammengefasst sind, nicht zentral bereitgestellt, sondern extern erbracht (eng. hosting). UCC-Dienste werden also von einem oder mehreren Providern „as a Service“ (UCaaS) erbracht.

An die Internetverbindung bestehen trotz der Auslagerung der Applikationen und Dienste keine gesonderten Leistungsanforderungen, lediglich eine Ausweichverbindung via UMTS-/LTE-Backup soll gewährleistet werden. Außerdem wird Wert darauf gelegt, dass im Fall eines Ausfalls der Internetverbindung für wichtige Faxe und Telefonate eine Notfallverbindung über das öffentliche Telefonnetz zur Verfügung steht.

Des Weiteren sollen Mitarbeiter des Büros auch von Telearbeitsplätzen aus Zugang zum LAN haben und auf gemeinsame Dienste zugreifen können, auch wenn diese als externe Lösung realisiert sind.

4.1.2 Umsetzungsbeispiel

Abbildung 13 stellt ein mögliches Szenario eines Anwaltsbüros mit genannten Anforderungen und dessen Kommunikationsverbindungen schematisch dar. Im folgenden Text wird dieses Szenario näher beschrieben.

Hinweis: Zur besseren Übersicht wurde in Abbildung 13 auf die grafische Darstellung aller Verbindungen verzichtet und nur die für das Szenario essentiellen Verbindungen dargestellt, z. B. VPN und UCaaS-Transport.

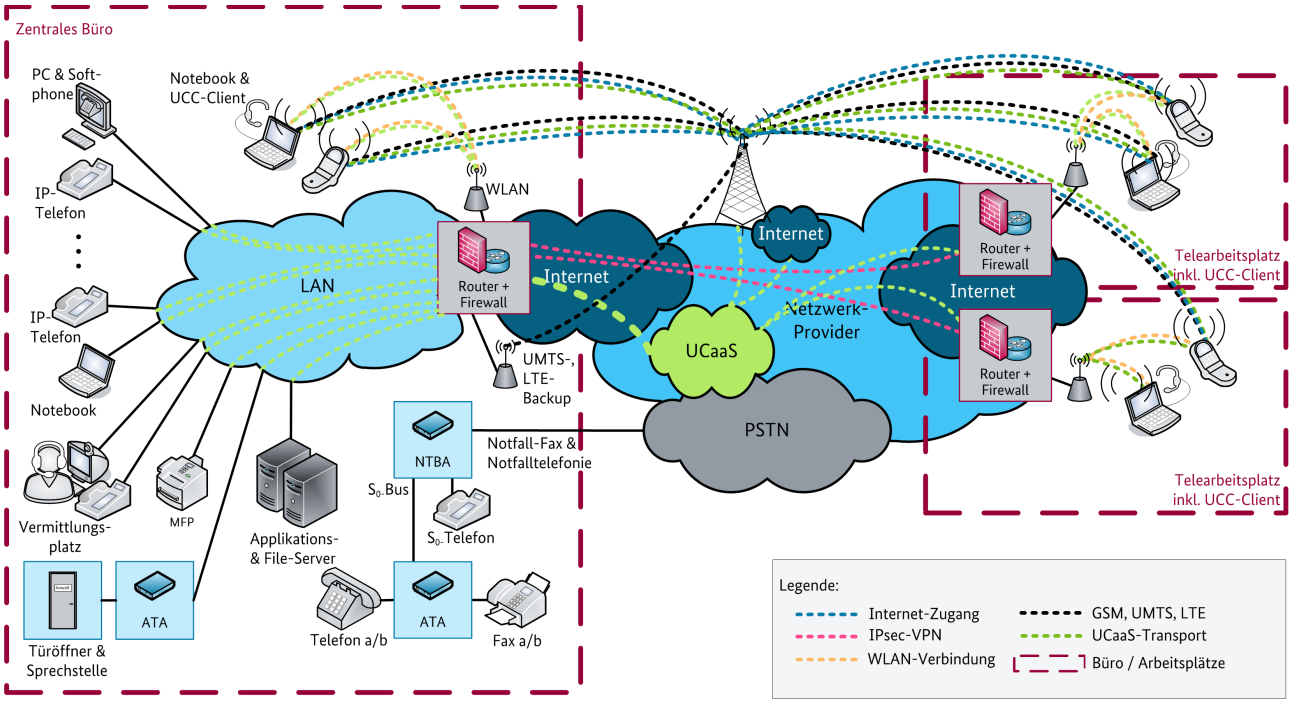

Abbildung 13: Darstellung Beispielszenario Anwaltsbüro

Dienste

Sämtliche TK-Dienste werden von einem Provider über UCaaS in einer Public Cloud bezogen. Die Kommunikation zum UCaaS-Provider erfolgt grundsätzlich über eine Ende-zu-Ende-Verschlüsselung mit Zertifikats-basierter Authentisierung. Der UCaaS-Provider muss die Sonderanforderungen eines Anwaltsbüros erfüllen: E-Mail-Verschlüsselung, gesetzeskonforme Archivierung, Backup-/Rückspiegelung auf lokale Server im zentralen Büro, Computer Telephony Integration (CTI) für gängige Anwaltskanzleiprogramme wie z. B. DATEV. Die zentrale UCaaS-Lösung stellt Telefonie, E-Mail-Kommunikation und Unified Messaging, sowie weitere UCC-Dienste (z. B. Desktop-Video und Webkonferenz) zur Verfügung.

Endgeräte und Arbeitsplatzausstattungen

Ein stationärer Arbeitsplatz, bestehend aus einem PC mit Softphone/UCC-Client mit Headset oder zusätzlichem IP-Telefon, wird direkt über das LAN des Standortes angebunden. Als spezielle Ausprägung eines PC-Arbeitsplatzes wird im Sekretariat des Hauptstandortes eine Vermittlungsplatz-Anwendung betrieben.

Fax- und Multifunktionsgeräte am Hauptstandort oder am Telearbeitsplatz können entweder direkt IP-basiert oder mittels Analogue Telephony Adapter (ATA) an die UCaaS-Lösung angebunden werden. Diese ermöglichen eine IP-basierte Anbindung analoger Nebenstellen. Eine Einbindung weiterer analoger Nebenstellen, z. B. der Türsprechanlage, erfolgt ebenfalls via ATA.

Ein mobiler Arbeitsplatz, bestehend aus Notebook mit UCC-Client und Smartphone, soll sowohl über das WLAN im zentralen Büro als auch am Telearbeitsplatz einen Netzwerkzugang erhalten. Zusätzlich soll der Zugang aber auch über GSM/UMTS/LTE und öffentliche Hotspots gewährleistet sein. Der UCaaS-Provider soll hierbei jeweils direkt und nicht über die zentrale Anbindung erreicht werden können. Dies hat geringere Latenzen und Schaffung von Redundanz zur Folge. Die Anbindung an das Netz im Hauptbüro kann über einen VPN-Client erfolgen, der einen IPsec-Tunnel zum Router aufbaut. Da ein Split Tunneling aus Sicherheitsgründen unbedingt zu vermeiden ist, kann vom Notebook aus in diesem Fall nur mit Umweg über die Zentrale auf den UCaaS-Dienst zugegriffen werden. Bei der gleichzeitigen Arbeit mit internen

Anwendungen und Video- oder Webkonferenzen sind somit Qualitätsprobleme zu erwarten. Es kann in diesem Fall auf andere UCC-Clients ausgewichen oder auf den gleichzeitigen Gebrauch von internen Anwendungen verzichtet werden. Der direkte Zugriff auf den UCaaS-Dienst steht als Redundanzoption zur Verfügung.

Infrastruktur Zentralstandort

Die Anbindung des zentralen Büros erfolgt über eine kostengünstige SDSL- und oder ADSL-Leitung. Wenn erhöhte Kapazitätsanforderungen bestehen, können hier gegebenenfalls mehrere Leitungen gebündelt werden. Auf eine automatische, umfassende Redundanz der zentralen Internet-Anbindung wird aus Gründen von Kosten und Handhabbarkeit verzichtet. Zum Einsatz kommt ein Multifunktions-Router, der sowohl die erforderlichen Firewall-Funktionalitäten zur Internetabschottung als auch ein UMTS-/LTE-Backup realisiert.

Der LAN-Aufbau im zentralen Büro ist einfach: Durch Nutzung von zwei Switches mit Unterstützung von Power over Ethernet (PoE) wird eine grundlegende Ausfallsicherheit geschaffen. Bei Ausfall eines Switches kann durch einfaches Umstecken der Komponenten auf den anderen Switch eine schnelle Wiederherstellung der Betriebsbereitschaft erzielt werden. Sofern die Verkabelungssituation und die Port-Anzahl eines Switches dies zulassen, werden Telefone und PCs jeweils direkt am Switch angeschlossen und nicht in Reihe geschaltet. So sind während einer Wartung des Telefons nicht beide Systeme außer Betrieb. Werden darüber hinaus statt 24-Port-Switches jeweils zwei 12-Port-Switches eingesetzt, kann eine Trennung der Switches für Voice-over-IP-Endgeräte (VoIP-Switch) und Daten-Endgeräte bzw. Server (Data-Switch) erfolgen. Ein massiver Datenverkehr zwischen zwei PCs oder zwischen einem PC und einem Server würde dann lediglich den VoIP-Verkehr von auf den PCs installierten Softphones beeinträchtigen.Das LAN ist zugunsten eines einfachen Betriebs nicht in weitere VLANs separiert.

Ebenfalls realisiert dieser Router für das Hauptbüro die WLAN-Versorgung, ggf. über eine Zusatzantenne oder einen separaten Access Point. Über unterschiedliche WLAN-SSIDs wird ein Gast-WLAN, z. B. für Kunden, zur Verfügung gestellt.

Das Hauptbüro selbst verfügt über keine zentralen Systeme der TK-Infrastruktur. Bei Ausfall der Internetleitung besteht jedoch eine Notfallanbindung für Fax und Telefonie. Diese besteht aus einer Anbindung direkt an das öffentliche Telefonnetz (PSTN). Im Büro findet sich hierzu ein NTBA, an den direkt ein S_0-Telefon sowie über den S_0-Bus ein ATA angeschlossen werden können. Der ATA ermöglicht die Anbindung herkömmlicher Telefone und Faxgeräte. Ebenfalls Teil der Telefonie-Redundanz ist die Anbindung an den UCaaS-Provider über direkt eingebundene Smartphones. Entsprechende Änderungen des Routings und der Weiterleitungen sind mit dem UCaaS-Provider zu vereinbaren.

Infrastruktur Telearbeitsplätze

Die Telearbeitsplätze sind ebenfalls mit einem Multifunktions-Router mit gleicher Funktionalität wie im zentralen Büro, jedoch ggf. mit kleinerer Bauart ausgestattet. Dieser kann sich mit dem zentralen Router optional über einen IPsec-Tunnel verbinden. Ein solches Site-to-Site-VPN tunnelt dann sämtliche Kommunikation zur Zentrale und koppelt diesen in das interne Netz oder über den zentralen Internet-Breakout aus. Ein solches Konstrukt ist insofern nachteilig, da es zu Qualitäts- und Bandbreitenproblemen bei der Nutzung von UCC führen kann. Dies gilt insbesondere bei der Nutzung von Video- und Webkonferenzen.

Alternativ kann, wie oben beschrieben, ein IPsec-Tunnel mittels VPN-Client vom Notebook aus aufgebaut werden. Somit kann bei Qualitätsproblemen situationsabhängig das VPN getrennt werden und ein direkter Zugriff auf den UCaaS-Dienst erfolgen. Ein Zugriff auf den UCaaS-Dienst kann durch andere Endgeräte (IP-Telefon, Smartphone, Videoterminal etc.) weiterhin direkt erfolgen. Dies setzt zwingend eine Absicherung der Verbindungen zwischen Endgerät und UCaaS-Dienst voraus. Dadurch, dass der UCaaS-Provider bei Ausfall der Anbindung an den Zentralstandort direkt erreicht werden kann, besteht eine zusätzliche Redundanz bzgl. des zentralen Internet-Breakouts und des zentralen VPN-Routers. Außerdem kann mit jedem mobilen Arbeitsplatz autark von der UCC- bzw. Kommunikationsanbindung gearbeitet werden.

4.1.3 Maßnahmenauswahl

In diesem Szenario finden sich aus Abbildung 6 die folgenden Kommunikationsbeziehungen und -endpunkte wieder:

- interne Kommunikation: S-I, R-S
- externe Kommunikation: S-P, R-P

Neben der Umsetzung der Maßnahmen, die die IT-Grundschutz-Kataloge empfehlen, ergeben sich gemäß Kapitel 3 weitere Maßnahmen aus Teil 1 der Technischen Leitlinie, die dieses exemplarische Anwaltsbüro für einen umfassenden Schutz umsetzen sollte.

In diesem Szenario werden durch die Organisation keine Maßnahmen umgesetzt, welche sich auf die zentralen Systeme sowie die Lösungsarchitektur beziehen, da deren Umsetzung in der Verantwortung des externen UCaaS-Providers liegen. Die geeignete Umsetzung und Protokollierung ist gemäß der Maßnahmen bzgl. Outsourcing und UCaaS vom Provider einzufordern.

Die Umsetzung von Maßnahmen bzgl. klassischer Telefonie beschränken sich auf die Schaffung eines Ersatzanschlusses auf ISDN-Basis.

Auf den Einsatz spezieller TK-Systeme, wie z. B. Kontaktcenter oder Alarmierungssysteme, wird in diesem Szenario verzichtet. Somit entfallen diesbezügliche Maßnahmen.

Auf einige Maßnahmen, wie z. B. das Vorhalten speziell gesicherter Räume oder den Aufbau von speziell geschultem IT-Personal, muss aus Wirtschaftlichkeitsgründen verzichtet werden.

Eine Tabelle, die den einzelnen Beispielszenarien die Maßnahmen zuordnet, die darin zu berücksichtigen sind, findet sich in Kapitel 4.7.

4.2 Beispiel einer mittleren Organisation: Ingenieurbüro

Als Beispiel einer mittleren Organisation wird im Folgenden ein Ingenieurbüro betrachtet, das einen zentralen Standort und wenige Außenstellen in Form von Filialen umfasst, jedoch keine Anbindung an externe Organisationen erfordert. Provider-Dienste werden hingegen für den Betrieb der Know-how-intensiven Sicherheitsfunktionalitäten in Anspruch genommen. Eine Remote-User-Einbindung ist ebenfalls vorgesehen und erfolgt wie im Szenario für kleine Organisationen beschrieben.

4.2.1 Rahmenbedingungen

Die Anzahl der Anwender des zentralen Standorts des Ingenieurbüros rechtfertigt den Aufbau eigener IT-Kompetenz, insbesondere eigener TK-Administratoren an diesem Standort. Zudem bedingt die Anwenderanzahl die Beschaffung und Implementierung einer TK-Infrastruktur, die eine gute Ausgangssituation auch für technisch anspruchsvolle Sicherheitsmaßnahmen bietet. Am Hauptstandort werden die UCC-Dienste auch für die Filialen bereitgestellt und ein Übergang der TK-Lösung zum öffentlichen Telefonnetz realisiert.

Die Voraussetzungen bzgl. Machbarkeit und Wirtschaftlichkeit treffen nicht für die Filialen zu. In Summe werden zwar etwa 250 TK-Nutzer erreicht, von denen sich aber der größere Teil am zentralen Standort konzentriert. Die TK-Nutzer in den Filialen sollen ausschließlich auf Dienste und Anwendungen sowie auf die Betriebsunterstützung zurückgreifen können, die im Hauptstandort zur Verfügung gestellt werden.

4.2.2 Umsetzungsbeispiel

Abbildung 14 stellt ein mögliches Szenario eines Ingenieurbüros mit den genannten Anforderungen dar. Im folgenden Text wird dieses Szenario näher beschrieben.

Hinweis: Zur besseren Übersicht wurde in Abbildung 14 auf die grafische Darstellung aller Verbindungen verzichtet und nur die für das Szenario essentiellen Verbindungen dargestellt, z. B. VPN und Backup.

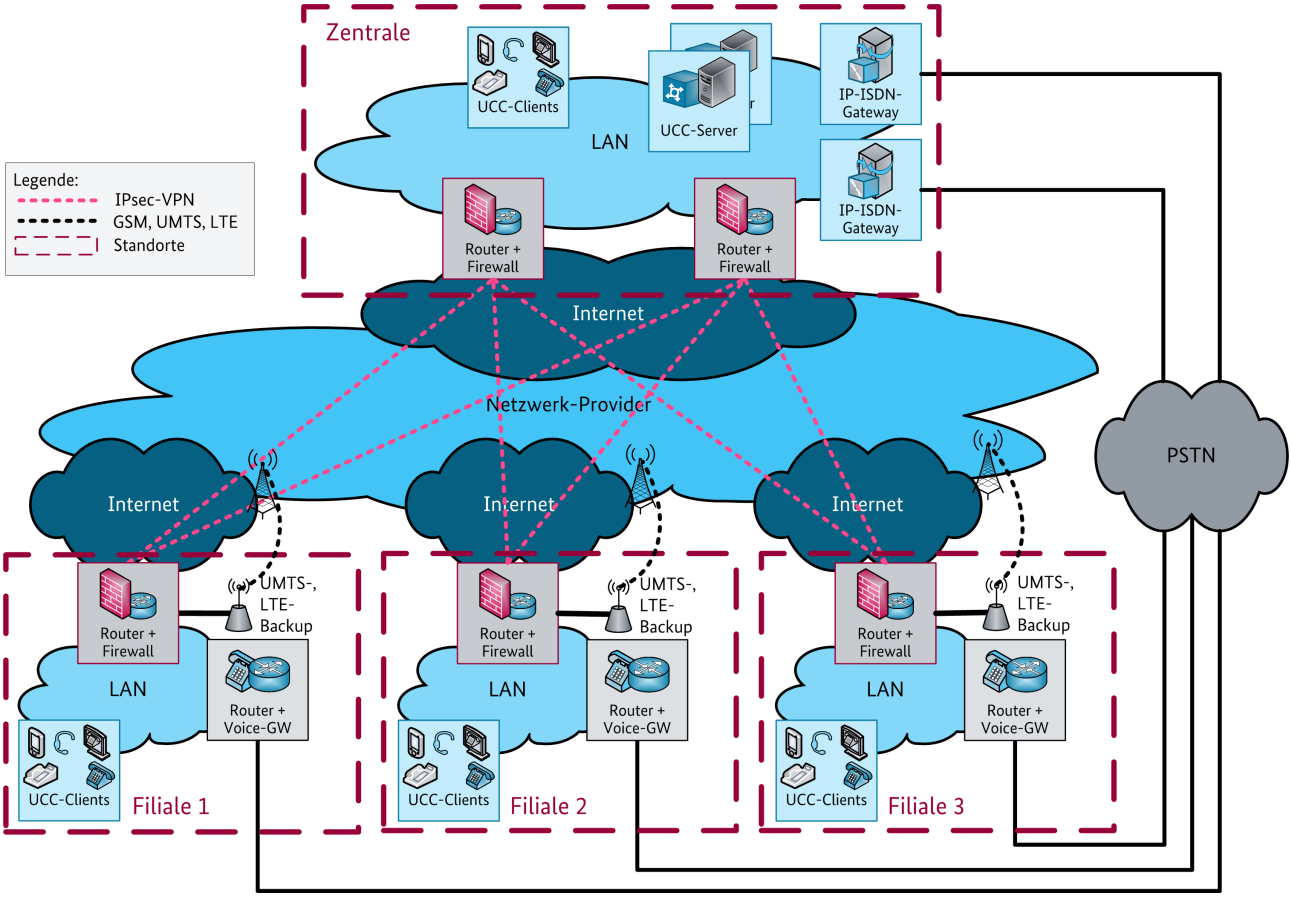

Abbildung 14: Darstellung Beispielszenario Ingenieurbüro

Dienste

Sämtliche UCC-Dienste werden im Zentralstandort unternehmensweit bereitgestellt. Es wird im Schwerpunkt IP-basierte Telekommunikation eingesetzt. Hierzu zählen die Dienste Telefonie, UCC und SNM. Zudem werden mobile Endgeräte und Remote User in die Lösung eingebunden. Außer Videokonferenz werden keine weiteren speziellen TK-Anwendungen eingesetzt.

Endgeräte und Arbeitsplatzausstattungen

Die Einbindung der unterschiedlichen UCC-Clients/-Endgeräte wird sowohl in der Zentrale als auch in den Filialen analog zu dem Beispiel-Szenario für kleine Organisationen realisiert.

Infrastruktur Zentralstandort

Der Zentralstandort verfügt über einen redundanten Internetzugang, der über VPN-Router mit integrierter Firewall zum Standort-LAN hin abgesichert ist.

Das LAN wird als mehrstufiges Netzwerk ausgelegt, das gemäß der Anforderungen des Ingenieurbüros keine zusätzlichen Maßnahmen für eine Hochverfügbarkeit erfüllt. Auf eine logische Netztrennung wird aus Komplexitätsgründen verzichtet. Ebenso wird auf Quality-of-Service verzichtet, da dies im vorliegenden LAN nicht erforderlich und im Internet-basierten Weitverkehrsnetz keinen Effekt zeigen würde. Es wird eine Netzzugangskontrolle mit Zertifikats-basierter Authentisierung nach 802.1X mit EAP-TLS umgesetzt.

Sämtliche weiteren Sicherheitsfunktionen zur externen Kommunikation wie Web-Proxy, Malware Detection bzw. Spyware Detection, Data Loss Prevention (DLP), SPAM- und URL-Filter werden in den eigenen Räumlichkeiten realisiert. Die notwendige Kompetenz für eine optimales Sicherheitsniveaus wird durch einen Provider bereitgestellt. Hierzu müssen die Browser und/oder die Personal Firewalls (mobiler

Endgeräte) entsprechend für ausschließliche Proxy-Nutzung bzw. für HTTP-Redirection konfiguriert sein. Damit ist dann kein direkter Zugang mehr ins Internet möglich, sondern nur noch über die Proxy-Server/Gateways.

Da keine SIP-Trunks genutzt werden und aufgrund des einfachen Netzaufbaus mit einstufigen Firewalls in Verbindung mit IPsec-Tunneln kein Firewall-/NAT-Traversal für VoIP erforderlich ist, kann auf den (teuren) Einsatz von Session Border Controller (SBC) komplett verzichtet werden.

Alle UCC-Server sind redundant ausgelegt und in der Zentrale lokalisiert. Alle Clients aus allen Standorten (Zentrale und Filialen) melden sich dort an. Den Zugang zum öffentlichen Telefonnetz (PSTN) ermöglichen in der Zentrale zwei redundante IP-ISDN-Gateways.

Infrastruktur Filialen

Das hier dargestellte Ingenieurbüro hat seine Filialen über Internet-VPN (IPsec-Tunnel) an die Zentrale angebunden. Diese Anbindung wird durch Multinfunktionsrouter mit integrierter IPsec-Funktionalität realisiert (Site-to-Site-VPN).

In den Filialen wird ein einfaches LAN gemäß der Beschreibung des Szenarios für kleine Organisationen umgesetzt. Da die Filialen jedoch per Site-to-Site-VPN mit dem Zentralstandort gekoppelt sind, muss auch hier eine Netzzugangskontrolle auf Basis von 802.1X realisiert werden. Das Management der Switches und der 802.1X-Konfiguration erfolgt aus dem Zentralstandort heraus durch eigenes IT-Personal.

Da alle UCC-Dienste aus der Zentrale bezogen werden, besteht keine direkte Konnektivität unter den Filialen, sondern nur über die Zentrale. Diese einfache WAN-Struktur birgt den Nachteil, dass die Medienströme von Sprachverbindungen zwischen zwei Filialen grundsätzlich über die Zentrale geführt werden, woraus u. a. höhere Latenzen resultierten. In dem hier aufgeführten Beispiel erfolgt daher nur die Signalisierung der Sprachverbindungen über das WAN, die Medienströme werden über das öffentliche Netz (PSTN) geführt. Damit entfallen mögliche Einschränkungen für die Sprachqualität aufgrund der nicht durchgängigen Realisierbarkeit von Quality of Service (QoS) in einem Internet-VPN. Ein Nachteil bei dieser Lösung ist, dass interne Gespräche (Medienströme) zwischen zwei Organisationsfilialen über das PSTN nicht mit vertretbarem Aufwand verschlüsselt übertragen werden können.

In den Filialen ist der Zugang jeweils durch ein Notbetriebs-Gateway realisiert, bestehend aus einer Call-Control-Einheit und einem Voice Gateway, die hier in einem multifunktionalen Router integriert sind. Das Notbetriebs-Gateway ermöglicht den Filialen bei Ausfall des WANs, der Leitungsanbindung oder der zentralen UCC-Server eine eingeschränkte interne Telefoniefunktion sowie ein- und ausgehende Telefonate zu externen Teilnehmern.

Infrastruktur Telearbeitsplätze

Die Einbindung von Telearbeitsplätzen wird analog zu dem Beispiel-Szenario für eine kleine Organisationen realisiert.

4.2.3 Maßnahmenauswahl

In diesem Szenario finden sich aus Abbildung 6 die folgenden Kommunikationsbeziehungen wieder:

- interne Kommunikation: S-I, S-F, F-I, F-F, R-S
- externe Kommunikation: S-P, F-P, R-P

Neben der Umsetzung der Maßnahmen, die die IT-Grundschutz-Kataloge empfehlen, ergeben sich aus Kapitel 3 weitere Maßnahmen aus Teil 1 der Technischen Leitlinie, die dieses exemplarische Ingenieursbüro für einen umfassenden Schutz umsetzen sollte.

Es werden im wesentlichen alle Maßnahmen bzgl. der eingesetzten TK-Dienste umgesetzt. Die Umsetzung von Maßnahmen bzgl. DLP und Malware liegt in der Verantwortung eines externen Dienstleisters. Ein Outsourcing von TK-Diensten findet aber nicht statt. Auf einige kosten- und personalintensive Maßnahmen, wie z.B. den Aufbau eigener Honeypots, wird verzichtet.

Eine Tabelle, die den einzelnen Beispielszenarien die Maßnahmen zuordnet, die darin zu berücksichtigen sind, findet sich in Kapitel 4.7.

4.3 Beispiel 1 einer großen Organisation: Groß-Klinikum

Große Organisationen sind Szenarien, bei denen an einem einzigen zentralen Standort eine große Anzahl von TK-Anwendern, in der Regel mehr als 500, lokalisiert sind. Als Beispiel hierfür wird im Folgenden ein Groß-Klinikum herangezogen. An einen zentralen Standort werden diverse Außenstellen, Filialen und kleinere Standorte, angebunden. Dies können beispielsweise weitere Kliniken oder Forschungseinrichtungen sein.

4.3.1 Rahmenbedingungen

Im beschriebenen Groß-Klinikum kann Personal mit IT-Know-how vorausgesetzt werden. Die Anwenderzahl bedingt die Einrichtung von zentralen Systemen, die grundlegende funktionale Einschränkungen unwahrscheinlich machen. Auch eine Kommunikation zu externen Organisationen wie Arztpraxen o. ä. soll gewährleistet sein. Eine Anbindung von weiteren Provider-Diensten ist nicht vorgesehen. Des Weiteren müssen Systeme wie Pieper, Notfall-, Alarmierungs-, Ortungs- und Abrechnungssysteme sowie Systeme für Operations-Equipment und Ähnliches sicher getrennt integriert sein.

Die Anbindung der Außenstellen bedingt gewisse Leistungsanforderungen, z. B. für Videokonferenzsysteme (VCS) und das Verschicken von Röntgenbildern. Die kleineren Standorte des Klinikums müssen unabhängig arbeiten können, während die Einbindung von Filialen analog zum Beispiel einer mittleren Organisation realisiert werden kann. Ebenso ist die Anbindung der Remote User analog zum Szenario einer kleinen Organisation durchzuführen.

4.3.2 Umsetzungsbeispiel

Abbildung 15 stellt ein mögliches Szenario eines Groß-Klinikums mit genannten Anforderungen dar. Im folgenden Text wird dieses Szenario näher beschrieben.

Hinweis: Zur besseren Übersicht wurde in Abbildung 15 auf die grafische Darstellung aller Verbindungen verzichtet und nur die für das Szenario essentiellen Verbindungen dargestellt, z. B. Firewall-Anbindungen der Sicherheitszonen.

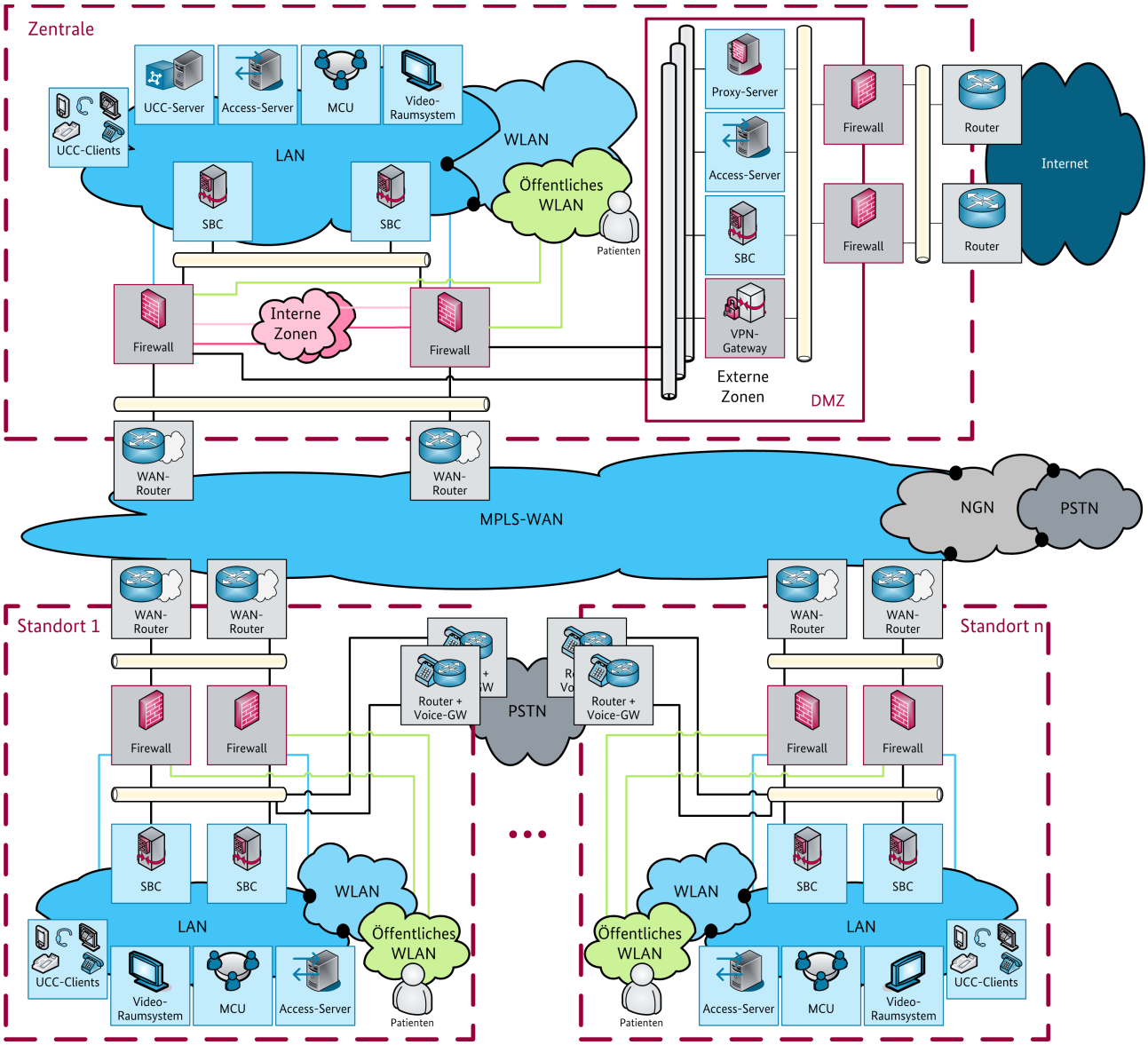

Abbildung 15: Darstellung Beispielszenario Groß-Klinikum

Dienste

Sämtliche UCC-Dienste werden im Zentralstandort bereitgestellt. Im modernen Krankenhausbetrieb kommen, außer den Anwendungen Kontaktcenter und Händlersysteme, nahezu alle TK-Anwendungen zum Einsatz. Insbesondere die Einbindung verschiedenster Alarmierungssysteme ist hervorzuheben. Zudem werden Videokonferenzsysteme und die zugehörigen MCU intern bereitgestellt, um Videokonferenzen z. B. zwischen Operateuren und Fachärzten an anderen Standorten zu ermöglichen. Es ist kein Outsourcing von Diensten vorgesehen.

Endgeräte und Arbeitsplatzausstattungen

Die Einbindung der unterschiedlichen UCC-Clients/-Endgeräte wird sowohl in der Zentrale als auch in den abgesetzten Standorten analog zu dem Beispiel-Szenario für eine kleine Organisationen realisiert.

Neben herkömmlichen UCC-Clients und IP-Telefonen werden Pager, DECT-Endgeräte, Mobiltelefone, Patiententerminals, OP-Kameras sowie Videokonferenz-Raumsysteme eingesetzt.

In die UCC-Lösung integriert sind insbesondere:

- eine CTI-Kopplung mit dem Krankenhausinformationssystem,
- Alarm- und Notrufsysteme,
- Schwesternrufanlage / Lichtrufanlage,
- Personensuchanlage / Suchruf-Funktion (Pager-Service) mit Ortungsinformationen aus dem Netzwerk-Management-System (angemeldeter persönlicher Apparat/UCC-Client, WLAN-Position eines persönlichen Endgerätes).

Infrastruktur Zentralstandort

Ein Groß-Klinikum benötigt einen öffentlichen Internetzugang für alle Medien, um sich mit anderen Kliniken, Forschungseinrichtungen etc. austauschen zu können. Daher ist in der Zentrale ein ausgeprägter redundanter Internetzugang, eine DMZ mit unterschiedlichen Diensten und ein Extranet-Bereich für weitere Services, die von öffentlichen Netzwerken aus erreicht werden sollen, vorhanden. Dienste in der DMZ können sein:

- Session Border Controller (SBC)

  Dieser kann zur Terminierung von SIP-Trunks über das Internet dienen, beispielsweise von verschiedenen VoIP-Providern wie z. B. sipgate und Skype.

- Access-Server

  Dies könnte beispielsweise ein Microsoft Lync 2013 Edge Server sein oder für Video ein Cisco VCS/Expressway Gateway. Letzteres arbeitet jeweils mit den anderen Video-Servern im LAN als Peer-to-Peer-Anbindung über die Firewalls zusammen. Sofern die SBCs nicht nur VoIP, sondern auch Video terminieren können, können die SBCs die Aufgaben der Access-Server (insbesondere Video-Firewall und NAT Traversal) übernehmen.

- Proxy-Server / Reverse-Proxy-Server für Webzugang
- VPN-Gateway für RAS-Einwahl und/oder Einbindung von externen Organisationen über IPsec-Tunnel (natürlich in jeweils getrennten VLANs bzw. Subnetzen).

Die Kopplung der Zentrale mit den Standorten erfolgt über ein MPLS-Weitverkehrsnetz, da für die Sprach- und Videodatenübertragung zwischen den Standorten QoS/CoS benötigt wird.

Das LAN der Zentrale ist über die zentralen Firewalls gegen das MPLS-Netz abgesichert. Diese beiden Firewalls bilden so eine zentrale Kommunikationsverteilungszone für die in Kliniken übliche Trennung in Sicherheitszonen. Dies ist sinnvoll, da kritische Daten (Röntgenbilder, medizinische Befunde etc.) über das Netz übertragen werden.

Insbesondere werden alle erforderlichen Sicherheitsfunktionalitäten für die externe Kommunikation, z. B. Proxy-Server, durch die Zentrale bereitgestellt. Über die Firewalls wird ein möglicher Provider-Zugriff auf das LAN abgesichert und es besteht die Möglichkeit der selektiven Verschlüsselung von Datenströmen (wichtig wegen Zuordnung von CoS zur Anwendung von QoS) durch die Firewall. Um eine Doppelverschlüsselung zu vermeiden, kann VoIP hiervon beispielsweise ausgenommen werden, da bereits eine Ende-zu-Ende-Verschlüsselung bzw. eine Verschlüsselung zwischen den SBCs für Signalisierung und Datenstrom möglich ist. Weiterhin werden über die Kommunikationsverteilungszone interne Sicherheitszonen separiert (z. B. Laborsysteme, medizinische Geräte oder Bilddatenspeicher), auf die grundsätzlich nur ein exklusiver Zugriff für bestimmte LAN-Clients und/oder eine eingeschränkte Kommunikation zu bzw. von anderen Zonen gewährt werden soll.

Für die Patienten wird ein Internetzugang über WLAN zur Verfügung gestellt. Ebenso können spezielle Services genutzt werden, die in den externen Sicherheitszonen positioniert sind, z. B. ein Patienteninformationssystem oder ein Buchungssystem für Zusatzleistungen.

Am zentralen Standort werden alle UCC-basierten Dienste, d. h. Audio-, Video-, Webkonferenzen sowie Instant Messaging, bereitgestellt. Insbesondere sind hier die zentralen Management-Instanzen lokalisiert. Auf eine Separierung oder Zonierung von zentralen UCC-Komponenten wie z. B. Trennung von UCC-Servern und UCC-Clients wurde hier bewusst zur Vermeidung einer zu hohen Komplexität verzichtet.

Über das WAN wird mittels eines Next Generation Network (NGN) ein redundanter Zugang zum PSTN bereitgestellt. Dies erfolgt für die Zentrale durch Auskopplung eines SIP-Trunk-VLAN, das auf den SBCs in der Zentrale terminiert wird. Die Absicherung der Standort-Telefonie erfolgt über einen direkten PSTN-Anschluss via integriertem Voice Gateway.

Infrastruktur abgesetzte Standorte

An den abgesetzten Standorten werden die UCC-basierten Dienste, d. h. Audio-, Video-, Webkonferenzen sowie Instant Messaging, via WAN-Verbindung aus der Zentrale genutzt. Es werden die in der Zentrale bereitgestellten gemeinsamen Sicherheitsfunktionalitäten genutzt. In den abgesetzten Standorten werden zusätzlich umfassende Videokonferenzsysteme mit SBC, Access-Server und MCU eingerichtet, die auch ohne die Anbindung an die Zentrale autark verfügbar sein müssen. Die Realisierung der beschriebenen UCC-Dienste kann wie im Beispiel einer mittleren Organisation umgesetzt werden.

Es wird ein hierarchisches SBC-Konzept realisiert: Alle peripheren SBCs in den abgesetzten Standorten und in der DMZ der Zentrale terminieren auf den zentralen SBCs im LAN der Zentrale, sodass Firewall-Regeln jeweils nur für diese zentralen SBCs erstellt werden müssen.

Infrastruktur Filialen, Telearbeitsplätze und Remote User

Die Einbindung von Filialen, Telearbeitsplätzen und Remote User wird analog zu den Beispiel-Szenarien für kleine und mittlere Organisationen realisiert.

4.3.3 Maßnahmenauswahl

In diesem Szenario finden sich aus Abbildung 6 die folgenden Kommunikationsbeziehungen wieder:

- interne Kommunikation: S-I, S-S, S-F, F-I, F-F, R-S
- externe Kommunikation: S-X

Neben der Umsetzung der Maßnahmen, die die IT-Grundschutz-Kataloge empfehlen, ergeben sich aus Kapitel 3 weitere Maßnahmen aus Teil 1 der Technischen Leitlinie, die dieses exemplarische Groß-Klinikum für einen umfassenden Schutz umsetzen sollte.

In diesem Szenario wird eine hohe Anzahl der beschriebenen Maßnahmen umgesetzt. Einzige Ausnahmen sind Maßnahmen bzgl. des Einsatzes von klassischer oder hybrider TK-Anlagen, Thin Clients sowie Outsourcing von Diensten. Es entfallen zudem die Maßnahmen bzgl. Kontaktcenter und Händlerarbeitsplätze.

Eine Tabelle, die den einzelnen Beispielszenarien die Maßnahmen zuordnet, die darin zu berücksichtigen sind, findet sich in Kapitel 4.7.

4.4 Beispiel 2 einer großen Organisation: Energieversorger

Als weiteres Beispiel einer großen Organisation wird im Folgenden ein Energieversorger mit ca. 2000 Mitarbeitern beschrieben. Dieser hat nur einen großen Standort und besitzt keine weiteren Außenstellen.

4.4.1 Rahmenbedingungen

Dieser exemplarische Energieversorger handelt selbst mit Strom und Gas, also ist die Einbindung von Händlersystemen zwingende Voraussetzung. Dieses gesamte Kommunikationssystem muss hochverfügbar sein, denn beispielsweise findet ein 24-Stunden-Handel mit Strom statt. Die größtenteils in eine externe Organisation ausgelagerte Kontaktcenter-Lösung muss ebenfalls hochverfügbar sein.

Darüber hinaus bedingt das Beispielszenario eines Energieversorgers ähnliche Anforderungen wie das Beispielszenario des Groß-Klinikums.

4.4.2 Umsetzungsbeispiel

Abbildung 16 stellt ein mögliches Szenario eines Energieversorgers mit den genannten Anforderungen schematisch dar. Im folgenden Text wird dieses Szenario näher beschrieben.

Hinweis: Zur besseren Übersicht wurde in Abbildung 16 auf die grafische Darstellung aller Verbindungen verzichtet und nur die für das Szenario essentiellen Verbindungen dargestellt, z. B. Firewall-Anbindungen der Sicherheitszonen.

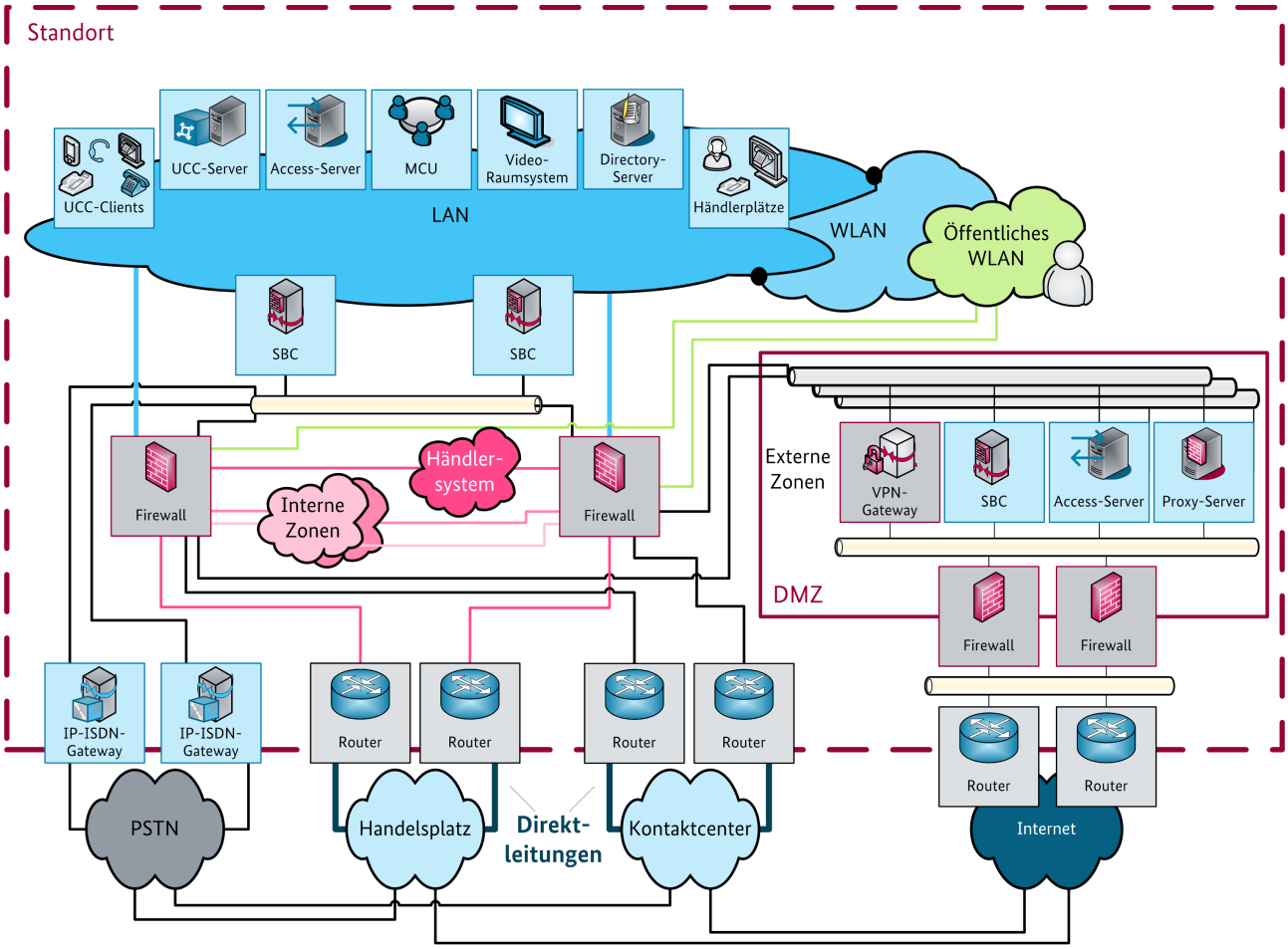

Abbildung 16: Darstellung Beispielszenario Energieversorger

Dienste

Sämtliche UCC-Dienste werden analog zum Beispiel des Großklinikums bereitgestellt. Zusätzlich werden interne und externe Kontaktcenter angebunden, die die externe Kundenkommunikation bedienen. Eine zentral bereitgestellte Händlerlösung wird mit den Systemen eines externen Handelsplatzes (z. B. Energiebörse) gekoppelt.

Endgeräte und Arbeitsplatzausstattungen

Die Einbindung der unterschiedlichen UCC-Clients/-Endgeräte wird analog zu dem Beispiel-Szenarien für kleine und mittlere Organisationen realisiert.

Neben herkömmlichen UCC-Clients und IP-Telefonen werden Spezialendgeräte bzw. -Softclients an den Händlerarbeitsplätzen eingesetzt.

Infrastruktur Zentralstandort

Das Szenario des Energieversorgers weist für den zentralen Standort grundsätzlich die gleiche interne Netzstruktur auf wie das Szenario des Groß-Klinikums in Kapitel 4.3. Aus Sicherheitsgründen, insbesondere um Gefährdungen, die aus zusätzlichen Netzübergängen wie z. B. einen NGN-PSTN-Übergang zu vermeiden, wird hier über IP-ISDN-Gateways eine direkte Anbindung der UCC-Dienste an das PSTN realisiert.

Als Besonderheit verfügt der Energieversorger über eine Direktanbindung an das Handelssystem der Energiebörse. Die entsprechende Applikation wird dabei aus einer gesonderten Zone „Händlersystem“ per

VDI den jeweiligen Händlern zur Verfügung gestellt. Eine Kommunikation zum Handelsplatz ist nur diesen Servern über die zentralen Firewalls erlaubt. Die Anbindung zum Handelsplatz ist via dedizierten Datendirektleitungen vollredundant ausgelegt. Zusätzlich könnte dieser aber auch in Notfällen bei zuvor vorgenommenen Sicherheitsmaßnahmen, wie Ende-zu-Ende-Verschlüsselung, über das PSTN bzw. über das Internet erreicht werden.

Die telefonische Kundenkommunikation erfolgt über mehrere meist ausgelagerte Kontaktcenter. Auch diese sind über Datendirektleitungen redundant an den Energieversorger angebunden. Die Steuerung der Kundenanrufe erfolgt als Dienstleistung von einen VoIP-Provider, der eine prozentuale Lastverteilung der Kundenanrufe auf die externen Kontaktcenter durchführt und dies auch entsprechend im Notfallkonzept berücksichtigt. Die Agenten des Kontaktcenters können über VDI auf das CRM-System des Energieversorgers zugreifen. Die Server hierfür stehen in einer gesonderten Zone. Über diese wird auch die CTI-Kopplung der TK-Anlage des jeweiligen Kontaktcenters an das CRM-System des Energieversorgers realisiert.

Infrastruktur weitere Standorte, Filialen, Telearbeitsplätze und Remote User

Die Einbindung von weiteren Standorten, Filialen, Telearbeitsplätzen und Remote User wird analog zu den Beispiel-Szenarien für kleine und mittlere Organisationen realisiert.

4.4.3 Maßnahmenauswahl

In diesem Szenario finden sich aus Abbildung 6 die folgenden Kommunikationsbeziehungen wieder:

- interne Kommunikation: S-I, R-S
- externe Kommunikation: S-P, S-X, P-X

Neben der Umsetzung der Maßnahmen, die die IT-Grundschutz-Kataloge empfehlen, ergeben sich aus Kapitel 3 weitere Maßnahmen aus Teil 1 der Technischen Leitlinie, die dieser exemplarische Energieversorger für einen umfassenden Schutz umsetzen sollte.

In diesem Szenario werden im wesentlichen Maßnahmen analog zum Szenario Groß-Klinikum umgesetzt. Zusätzlich werden Maßnahmen bzgl. der Händlersysteme und des Einsatzes von Thin Clients umgesetzt. Die externen Kontaktcenter werden analog zu Outsourcing von TK-Diensten behandelt.

Eine Tabelle, die den einzelnen Beispielszenarien die Maßnahmen zuordnet, die darin zu berücksichtigen sind, findet sich in Kapitel 4.7.

4.5 Beispiel einer sehr großen Organisation: Globaler Konzern

Sehr große Organisationen sind Szenarien, bei denen an einem oder mehreren zentralen Standort(en) eine große Anzahl von TK-Anwendern, in der Regel mehr als 5000, lokalisiert sind. Hier soll als vereinfachtes Beispiel ein globaler Konzern mit mehreren großen Standorten in verschiedenen Ländern mit jeweils mehreren tausend Anwendern und etlichen kleineren Standorten mit unterschiedlicher Anwenderzahl betrachtet werden. Dieses Unternehmen betreibt jedoch keine Filialen und erfordert externe Kommunikationsverbindungen nur zu externen Organisationen, z. B. zu Partnerfirmen, d. h. eine Anbindung an Provider-Dienste ist nicht vorgesehen.

Die kleineren Standorte des Konzerns können analog zum Beispiel einer großen Organisation, dem Groß-Klinikum realisiert werden. Ebenso ist die Anbindung der Remote User analog zum Szenario einer kleinen Organisation durchzuführen.

4.5.1 Rahmenbedingungen

Der hier dargestellte globale Konzern weist eine hierarchische Struktur autarker Standorte auf. In den Produktionsländern gibt es jeweils einen zentralen Standort des Konzerns (Landeszentrale). Jeder Landeszentrale sind weitere nationale Standorte (Regionalzentren) zugeordnet. Personal mit IT-Know-how und die Einrichtung von zentralen Systemen ohne grundlegende funktionale Einschränkungen werden hier an jedem Standort vorausgesetzt, um die Unabhängigkeit jedes Standortes zu gewährleisten. Eine leistungsfähige und sichere Verbindung zwischen den Standorten muss gewährleistet sein.

Zur Optimierung der Kommunikation mit Kunden stellt der Globale Konzern ein Extranet auf Basis von Sozialen Netzwerken und Medien (SNM) zur Verfügung.

Die weiteren Anforderungen an die einzelnen Standort sind dieselben, die im Beispielszenario Groß-Klinikum an den zentralen Standort gestellt werden.

4.5.2 Umsetzungsbeispiel

Abbildung 17 stellt ein mögliches Szenario eines globalen Konzerns mit den genannten Anforderungen dar. Abbildung 18 bietet eine Detaildarstellung der zuvor abgebildeten Standorte. Im folgenden Text wird dieses Szenario näher beschrieben.

Hinweis: Zur besseren Übersicht wurde in den folgenden Abbildungen auf die grafische Darstellung aller Verbindungen verzichtet und nur die für das Szenario essentiellen Verbindungen dargestellt, z. B. WAN-Anbindungen oder Firewall-Anbindungen der Sicherheitszonen.

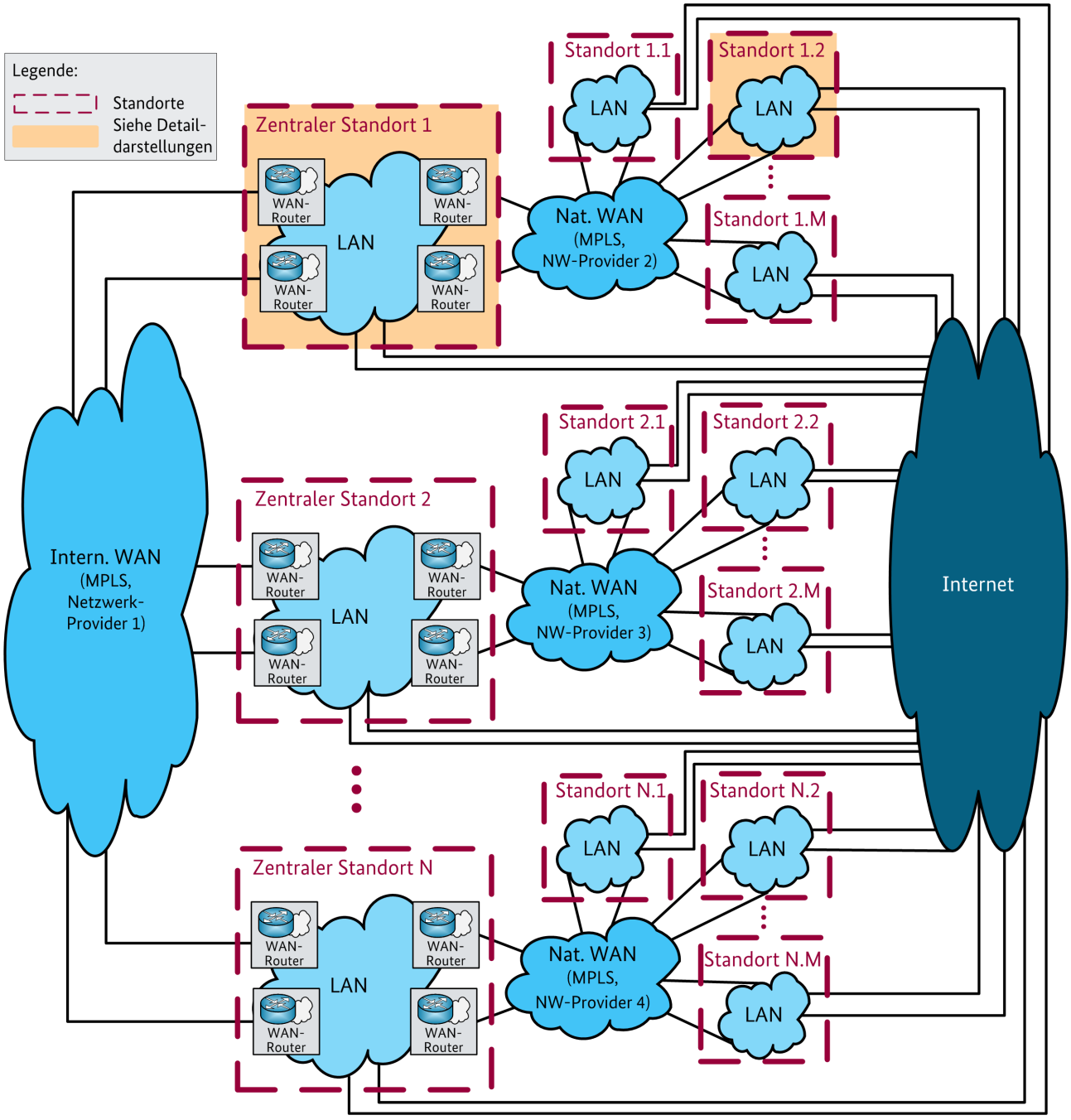

Abbildung 17: Darstellung Beispielszenario globales Unternehmen

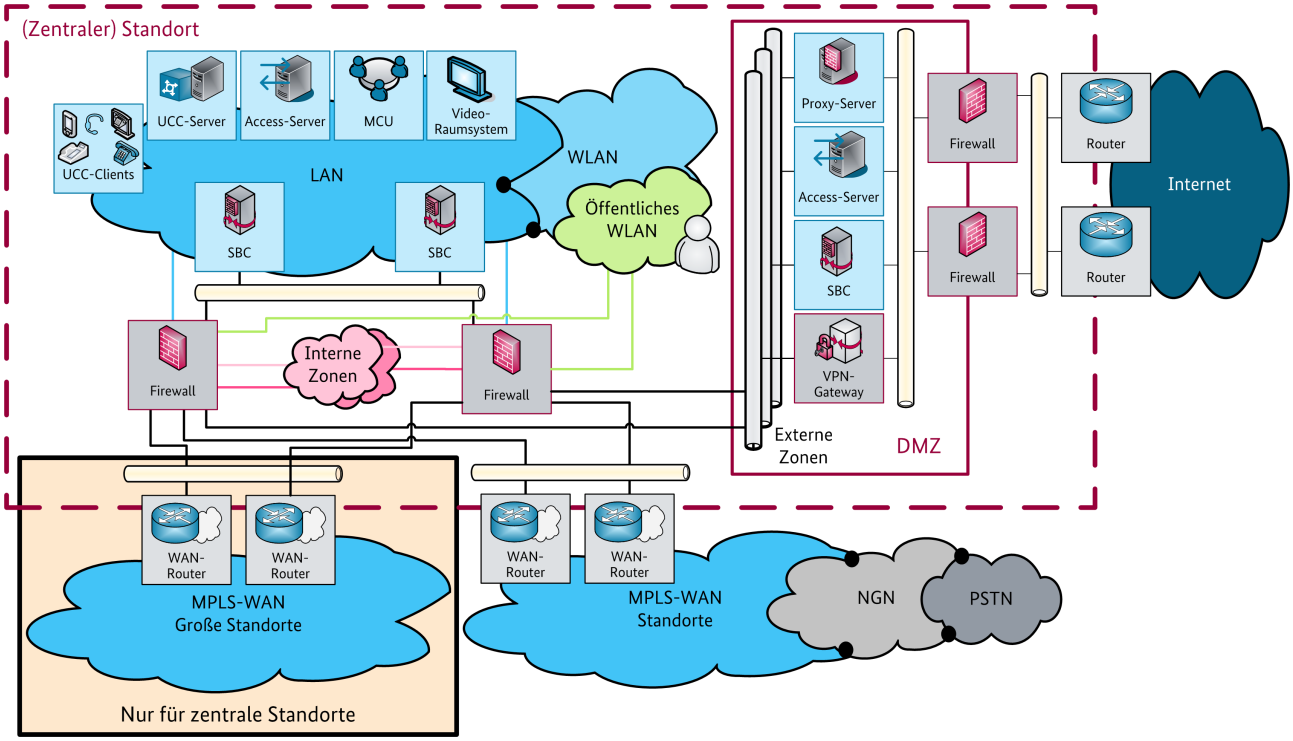

Abbildung 18: Detaildarstellung für die einzelnen Standorte eines globalen Unternehmens

Dienste

Sämtliche UCC-Dienste werden analog zum Beispiel des Großklinikums bereitgestellt. Zusätzlich werden eigene Kontaktcenter sowie spezielle Alarmierungslösungen im Produktions- und Logistikumfeld betrieben.

Endgeräte und Arbeitsplatzausstattungen

Die Einbindung der unterschiedlichen UCC-Clients/-Endgeräte wird analog zu dem Beispiel-Szenarien für kleine und mittlere Organisationen realisiert.

Neben herkömmlichen UCC-Clients und IP-Telefonen werden insbesondere Videoterminals und Videokonferenz-Raumsysteme eingesetzt.

Infrastruktur Zentralstandort

Alle Landeszentralen des globalen Konzerns sind über redundante Anbindungen an ein MPLS-WAN (Internationales WAN) eines internationalen Netzwerk-Providers miteinander vernetzt. Die Landeszentralen verfügen darüber hinaus noch über eine zweite Weitverkehrsnetzanbindung an ein MPLS-WAN eines nationalen Netzwerk-Providers (Nationales WAN) . Die Regionalzentren sind ebenfalls redundant über das Nationale WAN an die jeweiligen Landeszentralen angebunden.

Für die Datenkommunikation zwischen den Standorten erfolgt eine Verschlüsselung generell durch die entsprechenden MPLS-Provider. Die Sprachkommunikation wird sowohl für die Signalisierung als auch für den Medienstrom Ende-zu-Ende, d. h. SBC-zu-SBC verschlüsselt.

Die Datenkommunikation mit externen Organisationen geschieht primär über Internet-VPN per IPsec-Tunnel. Sofern erforderlich (z. B. QoS), kann auch eine Anbindung über ein MPLS-WAN erfolgen.

Sämtliche interne Sprachkommunikation wird über die MPLS-WAN-Infrastruktur abgewickelt. Für internationale Telefonate zu externen Teilnehmern nutzen die jeweiligen zentralen Standorte

(Landeszentralen) und deren zugeordnete Standorte (Regionalzentren) möglichst die nationalen MPLS-Provider-Zugänge der entsprechenden Landeszentralen als Breakout im Sinne eines Least Cost Routing.

Der Aufbau der internen Netzinfrastrukturen sowohl der Landeszentralen als auch der Regionalzentren entspricht dem des zentralen Standortes aus dem Beispielszenario 1 für große Organisationen, dem Groß-Klinikum. Jeder zentrale Standort ist mit eigener redundanter UCC-Infrastruktur ausgestattet und kann mit externen Organisationen Kommunikationsbeziehungen aus dem gesamten UCC-Spektrum etablieren.

Für interne Zugriffe auf SNM wird eine Authentisierung und eine nutzerbezogene Berechtigung entweder an einem Secure Web-Gateway oder einer vergleichbaren Komponente in einer DMZ oder an einer Firewall-Stufe durchgeführt. Die Berechtigungen sind feingranular in dem Sinne, dass einem internen Nutzer, dass einem internen Nutzer nicht der vollständige Funktionsumfang des SNM zur Verfügung steht.

Infrastruktur Filialen, Telearbeitsplätze und Remote User

Die Einbindung von Filialen, Telearbeitsplätzen und Remote User wird analog zu den Beispiel-Szenarien für kleine und mittlere Organisationen realisiert.

4.5.3 Maßnahmenauswahl

In diesem Szenario finden sich aus Abbildung 6 die folgenden Kommunikationsbeziehungen wieder:

- interne Kommunikation: S-I, S-S, R-S
- externe Kommunikation: S-X

Neben der Umsetzung der Maßnahmen, die die IT-Grundschutz-Kataloge empfehlen, ergeben sich aus Kapitel 3 weitere Maßnahmen aus Teil 1 der Technischen Leitlinie, die dieser exemplarische globale Konzern für einen umfassenden Schutz umsetzen sollte.

In diesem Szenario im wesentlichen Maßnahmen analog zum Szenario Groß-Klinikum umgesetzt. Zusätzlich werden Maßnahmen für die eigenen Kontaktcenter und die Alarmierungssysteme umgesetzt. Es werden zudem Maßnahmen für die Nutzung von externen SNM-Plattformen umgesetzt. Der Betreiber der SNM-basierten Extranet-Plattform wird im Sinne eines Cloud Service Provider behandelt.

Eine Tabelle, die den einzelnen Beispielszenarien die Maßnahmen zuordnet, die darin zu berücksichtigen sind, findet sich in Kapitel 4.7.

4.6 Beispiel einer Organisation in Provider-Rolle: IT-Dienstleister eines Industrieparks

Als Beispiel für eine Organisation in Provider-Rolle wird im Folgenden ein IT-Dienstleistungsunternehmen für einen Industriepark herangezogen.

4.6.1 Rahmenbedingungen

Dieser exemplarische IT-Dienstleister hat einen Standort mittlerer Größenordnung und hat keine Außenstellen. Er stellt seinen Kunden TK-bezogene Dienstleistungen zur Verfügung, nutzt jedoch selber keine Dienste von externen Providern. Die Kunden selbst stellen sich aus der Sicht des exemplarischen IT-Dienstleisters als externe Organisationen dar. Zusätzlich soll diesen aber die Kommunikation zu anderen externen Organisationen ermöglicht werden.

Den Kunden des IT-Dienstleisters müssen individuelle Lösungen angeboten werden. Dabei kann eine Kunden-Organisation die Ausprägung einer kleinen bis hin zu einer mittleren Organisation haben. So ergeben sich aus den Einzel-Anforderungen der Kunden-Organisationen die Anforderungen einer großen Organisation, die allerdings sehr flexibel agieren können muss.

Des Weiteren müssen je nach Anspruch und Größe der Kunden-Organisationen für diese eigene Komponenten bereitgestellt werden; hierfür ist eine sichere Trennung der Kommunikation unabdingbar. Aus wirtschaftlicher Gründen werden jedoch verschiedene Dienste gemeinsam für mehrere bzw. alle Kunden-Organisationen bereitgestellt.

4.6.2 Umsetzungsbeispiel

Abbildung 19 stellt ein mögliches Szenario eines IT-Dienstleisters mit genannten Anforderungen dar. Im folgenden Text wird dieses Szenario näher beschrieben.

Hinweis: Zur besseren Übersicht wurde in Abbildung 19 auf die grafische Darstellung aller Verbindungen verzichtet und nur die für das Szenario essentiellen Verbindungen dargestellt, z. B. VLAN-Anbindungen der Mandanten und internen Sicherheitszonen.

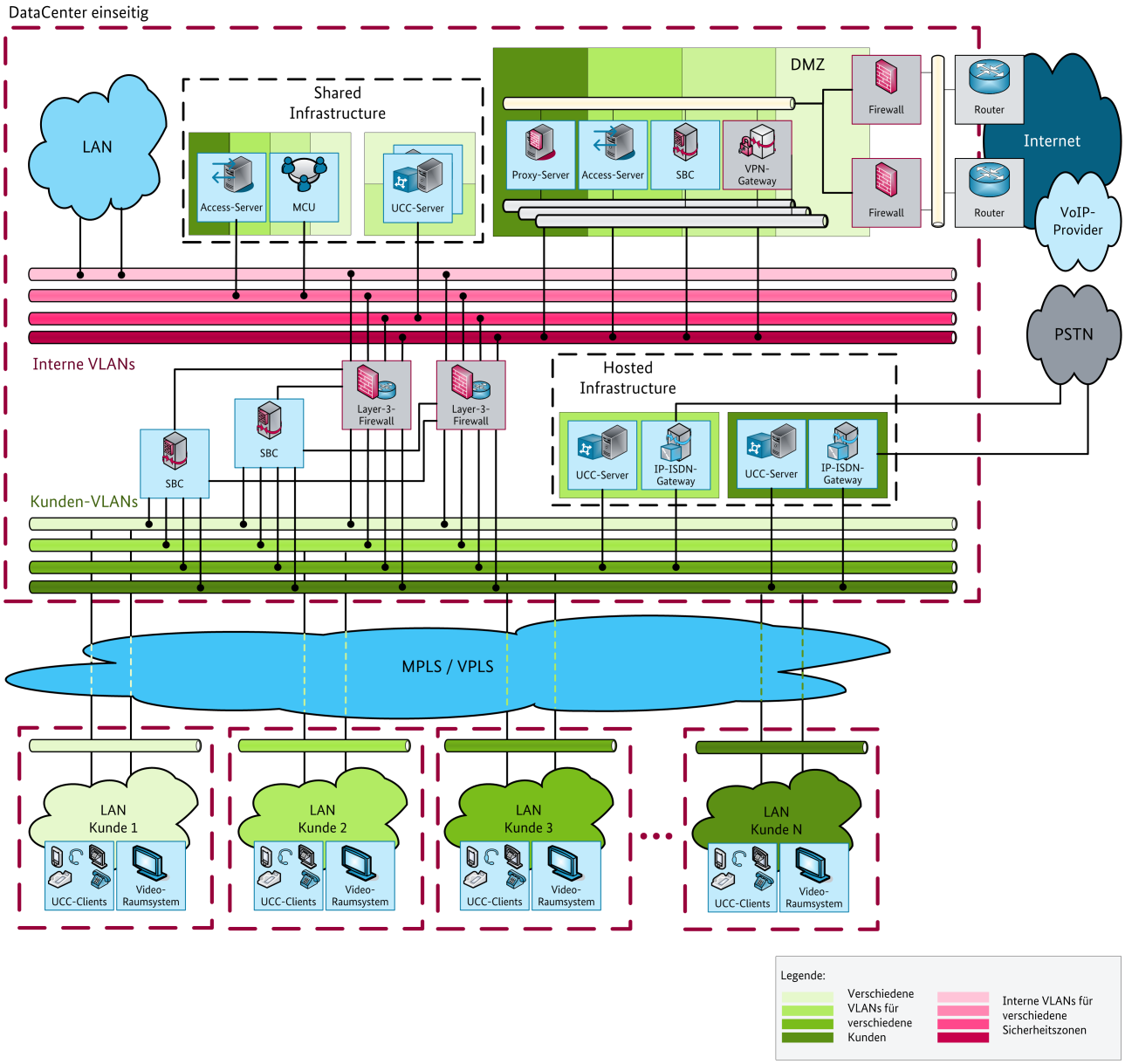

Abbildung 19: Darstellung Beispielszenario IT-Dienstleister für einen Industriepark

Dienste

Als Full-Service-Provider stellt der IT-Dienstleister seinen im Industriepark ansässigen Kunden umfassende Leistungen für die Netzwerk-Infrastruktur zur Verfügung, insbesondere LAN, Intra- und Inter-Standort-Konnektivität, WAN und Internet-VPN auf Basis von IPsec. Darüber hinaus werden sämtliche UCC-Dienste für die Kunden zentral im Rechenzentrum des Dienstleisters bereitgestellt. Die UCC-Dienste werden in Form von Managed Services sowohl für einige Kunden auf einer gemeinsamen Plattform (Shared Infrastructure) als auch in Form eines dedizierten Hosting für Einzelkunden (Hosted Infrastructure) bereitgestellt. Dabei wird die Hosted Infrastructure abhängig von den Sicherheitsanforderungen des Kunden ggf. als Private Cloud realisiert.

Endgeräte und Arbeitsplatzausstattungen

Der IT-Dienstleister bindet gemäß der Anforderungen seiner Kunden viele Varianten von Endgeräten und UCC-Clients an die Infrastruktur an.

Die Endgeräte von Kunden mit dediziert gehosteten UCC-Diensten können direkt über die private Netzinfrastruktur auf die UCC-Server zugreifen. Der Zugriff auf die Shared Infrastructure erfolgt stets entkoppelt über Sicherheits-Gateways.

Infrastruktur Zentralstandort

Die netzwerktechnische Anbindung der Kunden erfolgt über ein mandantenfähiges Campus-Netzwerk auf MPLS-Basis. Hierüber können für die Kunden sowohl Layer-3- als auch Layer-2-Verbindungen über Virtual Private LAN Service (VPLS) realisiert werden. Ggf. notwendige Routing-Komponenten sind aus Gründen der besseren Übersicht nicht eingezeichnet.

Eine Verschlüsselung im Campus-Netzwerk durch den Provider ist auf Wunsch des Kunden möglich. Unabhängig davon werden für VoIP und hierauf aufsetzende Video- und UCC-Dienste stets die Signalisierungs- und Media-Datenströme verschlüsselt. Telefonate ins öffentliche Netz werden über IP-ISDN-Gateways geführt, die für die Kunden dediziert bereitgestellt werden.

Kommunikationsziele innerhalb des Industrieparks werden entweder über das interne Firewall-System und ggf. über die Shared Infrastructure oder direkt über die Hosted Infrastructure erreicht. Der Internetzugang erfolgt über die zentralen DMZ-Dienste.

Für die Nutzung der UCC-Dienste im Bereich Shared Infrastructure terminieren die zentralen Session Border Controller die Kommunikation der Endgeräte. Die interne Kommunikation zu den UCC-Services in der Shared-Infrastructure-Zone ist nur zwischen den dortigen Servern und den zentralen SBCs über die zentralen Firewalls erlaubt. Der Zugang zum öffentlichen Netz für die gemeinsam bereitgestellten UCC-Dienste erfolgt über SIP-Trunks eines VoIP-Providers (Anbindung über Internet), die auf dem SBC in der DMZ terminiert sind.

4.6.3 Maßnahmenauswahl

In diesem Szenario finden sich aus Abbildung 6 die folgenden Kommunikationsbeziehungen wieder:

- interne Kommunikation: S-I, R-S
- externe Kommunikation: S-X

Neben der Umsetzung der Maßnahmen, die die IT-Grundschutz-Kataloge empfehlen, ergeben sich aus Kapitel 3 weitere Maßnahmen aus Teil 1 der Technischen Leitlinie, die dieser exemplarische IT-Dienstleister für einen umfassenden Schutz umsetzen sollte.

Der IT-Dienstleister setzt ein umfassendes Bündel von, teilweise kundenspezifisch ausgeprägten, Maßnahmen um. Insbesondere realisiert er eine logische Netztrennung verschiedener Mandanten und die Bereitstellung dedizierter TK-Infrastruktur auf Kundenanforderung. Als Organisation in Providerrolle werden zudem Maßnahmen zur Absicherung der Speicherung und Übertragung von Daten sowie zum Schutz vor Malware ergriffen, die in Multimandantenumgebungen notwendig sind. Dies entspricht den Maßnahmen im Falle eines Outsourcing von TK-Diensten.

Eine Tabelle, die den einzelnen Beispielszenarien die Maßnahmen zuordnet, die darin zu berücksichtigen sind, findet sich in Kapitel 4.7.

4.7 Maßnahmenzuordnung für die Beispielszenarien

Die folgende Tabelle ordnet den zuvor dargestellten Beispielszenarien Maßnahmen zu, die in Teil 1 der Technischen Leitlinie spezifiziert und für das jeweilige Szenario als relevant erkannt wurden.

In der Tabelle sind lediglich die explizit für diese Technologie spezifizierten Maßnahmen gelistet. Maßnahmen einer anderen Technologie, z. B. VoIP-Maßnahmen, auf die in der betrachteten Technologie verwiesen wird, sind hier nicht nochmals gelistet, sind jedoch ebenfalls angemessen umzusetzen.

Die Maßnahmen werden den Beispielszenarien mit einer lediglich zweistufige Priorisierung – relevant und nicht relevant – zugeordnet. Eine weitergehende Priorisierung der Maßnahmen kann nicht pauschalisiert erfolgen, sondern muss für die jeweiligen Einsatzszenarien im Einzelfall erfolgen.

	Legende: - = nicht relevant für dieses Szenario + = relevant für umfassenden Schutz	**Anwaltsbüro**	**Ingenieur-Büro**	**Groß-Klinikum**	**Energieversorger**	**Globaler Konzern**	**IT-Dienstleister für Industriepark**
Klassische Telekommunikationstechnik							
M-TK-1	Sperrung nicht benötigter oder sicherheitskritischer Leistungsmerkmale	-	+	+	+	+	+
M-TK-2	Schaffung eines zusätzlichen TK-Ersatzanschlusses für Notrufe	+	+	+	+	+	+
M-TK-3	Katastrophenschaltung	-	-	+	-	-	-
M-TK-4	Erhöhter Zutrittsschutz	-	+	+	+	+	+
M-TK-5	Geeignete Aufstellung der TK-Anlage	-	+	+	+	+	+
M-TK-6	Sichere Ablage von Kontaktinformationen	+	+	+	+	+	+
M-TK-7	Sicherer Umgang mit Daten zur Anlagennutzung	-	+	+	+	+	+
M-TK-8	Absicherung eines LAN-Anschlusses der ISDN-basierten TK-Anlage	-	-	-	-	-	-
M-TK-9	Absicherung der Kommunikation über ein IAD	+	+	+	+	+	+
M-TK-10	Sperrung bestimmter Fax-Rufnummern	-	-	+	+	+	+
M-TK-11	Gesicherte Aufstellung der Faxlösung	-	-	+	+	+	+
M-TK-12	Verhinderung der Faxfunktionsnutzung bei ungeschützten Multifunktionsgeräten	-	-	+	+	+	+
M-TK-13	Sichere Nutzung von Faxgeräten und Multifunktionsgeräten mit Faxfunktion	+	+	+	+	+	+

	Legende: - = nicht relevant für dieses Szenario + = relevant für umfassenden Schutz	**Anwaltsbüro**	**Ingenieur-Büro**	**Groß-Klinikum**	**Energieversorger**	**Globaler Konzern**	**IT-Dienstleister für Industriepark**
M-TK-14	Sichere Aufbewahrung eingegangener Faxnachrichten	+	+	+	+	+	+
M-TK-15	Sicherung von Telefonie-Endgeräten in frei zugänglichen Räumen	+	+	+	+	+	+
M-TK-16	Einsatz sicherheitsintelligenter Endgeräte	-	+	+	+	+	+
M-TK-17	Aktivierung einer Warnung bei Nutzung unsicherer Merkmale	-	-	+	+	+	+
M-TK-18	Sicherer Umgang mit Schnittstellen am Telefonie-Endgerät	+	+	+	+	+	+
M-TK-19	Geschützte Übertragung von Sprachdaten	+	+	+	+	+	+
M-TK-20	Verzicht auf Einsatz von Wartungsapparaten	-	-	-	-	-	-
M-TK-21	Sperrung der Wartungsmöglichkeit per Wartungsapparat an der Anlage	-	-	-	-	-	-
M-TK-22	Gesicherte Übertragung der Sprachdaten zwischen Partnerstandorten durch Leitungsverschlüsselung	-	+	+	+	+	+
M-TK-23	Restriktive Einbindung externer Wartung	-	+	+	+	+	+
M-TK-24	Sichere Aufstellung von Administrationsendgeräten	-	+	+	+	+	+
M-TK-25	Sichere Konfiguration von Administrationsendgeräten	-	+	+	+	+	+
M-TK-26	Regelungen für sichere TK-Administration	+	+	+	+	+	+
M-TK-27	Sichere Konfiguration des Management-Zugangs zur TK-Anlage	-	+	+	+	+	+
M-TK-28	Protokollierung und regelmäßige Kontrolle von Fernwartungszugriffen	-	+	+	+	+	+
M-TK-29	Verfügbarkeitssicherung durch (automatisierte) Zustandsüberwachung	+	+	+	+	+	+
M-TK-30	Abschluss eines Support-Vertrags inklusive externer Beratungskompetenz	-	+	+	+	+	+
Voice over IP							
M-TK-31	Durchgängige Verschlüsselung des Medienstroms	+	+	+	+	+	+
M-TK-32	Durchgängige Verschlüsselung der Signalisierung	+	+	+	+	+	+

	Legende: - = nicht relevant für dieses Szenario + = relevant für umfassenden Schutz	**Anwaltsbüro**	**Ingenieur-Büro**	**Groß-Klinikum**	**Energieversorger**	**Globaler Konzern**	**IT-Dienstleister für Industriepark**
M-TK-33	Absicherung von VoIP bei der Verwendung von Thin Clients	-	-	-	+	-	-
M-TK-34	Authentisierung zwischen Endgeräten und Servern des VoIP-Systems	+	+	+	+	+	+
M-TK-35	Authentisierung zwischen Servern	-	+	+	+	+	+
M-TK-36	Redundanz der Telefonie-Server	-	+	+	+	+	+
M-TK-37	Redundanz der Server und Gateways, von denen die Funktion des Telefonie-Servers und des Telefonie-Diensts unmittelbar abhängt	-	+	+	+	+	+
M-TK-38	Schaffung eines zusätzlichen PSTN-Ersatzanschlusses für Notrufe	+	+	+	+	+	+
M-TK-39	Automatische PSTN-Umschaltung für kleinere Außenstellen	-	+	+	+	+	+
M-TK-40	Absicherung von Telefonie-Daten im Verzeichnisdienst	-	+	+	+	+	+
M-TK-41	Verfügbarkeit kritischer Telefonie-Daten	-	+	+	+	+	+
M-TK-42	Einschränkungen von DNS für VoIP	-	+	+	+	+	+
M-TK-43	Einschränkung von ENUM	-	+	+	+	+	+
M-TK-44	Redundante Internetanbindung für den IP-Anlagenanschluss	-	-	+	+	+	+
M-TK-45	Zusätzlicher IP-Anlagenanschluss	-	-	+	+	+	+
M-TK-46	Zusätzlicher PSTN-Anschluss	+	+	-	-	-	-
M-TK-47	Verwendung eines Session Border Controller zur Absicherung eines IP-Anlagenanschlusses	-	-	+	+	+	+
M-TK-48	Sicherung von IP-Telefonen in unübersichtlichen Umgebungen	-	+	+	+	+	+
M-TK-49	Warnung bei unsicheren Einstellungen	-	+	+	+	+	+
M-TK-50	Prozess zur Behandlung des Verlusts eines VoIP-Endgerätes	+	+	+	+	+	+
M-TK-51	Absicherung der Firmware	-	+	+	+	+	+
M-TK-52	Absicherung von Konfigurationsdateien	-	+	+	+	+	+

	Legende: - = nicht relevant für dieses Szenario + = relevant für umfassenden Schutz	**Anwaltsbüro**	**Ingenieur-Büro**	**Groß-Klinikum**	**Energieversorger**	**Globaler Konzern**	**IT-Dienstleister für Industriepark**
M-TK-53	Sicherheit von Softphones	+	+	+	+	+	+
M-TK-54	Sichere Konfiguration von Ethernet-Ports für den PC-Anschluss an IP-Telefonen	+	+	+	+	+	+
M-TK-55	Sichere Konfiguration von IP und von IP-basierten Diensten	+	+	+	+	+	+
M-TK-56	Einschränkung des lokalen Zugriffs auf die Konfiguration des IP-Telefons	-	+	+	+	+	+
M-TK-57	Benutzerabhängige Berechtigungen	+	+	+	+	+	+
M-TK-58	Schutz von teilnehmerspezifischen Daten auf einem IP-Telefon	-	+	+	+	+	+
M-TK-59	Einschränkung von Internettelefonie auf dedizierte, gehärtete Endgeräte	-	-	+	+	+	+
M-TK-60	Sichere Konfiguration der Netzwerk-Komponenten	+	+	+	+	+	+
M-TK-61	Sicheres Routing	-	+	+	+	+	+
M-TK-62	Absicherung von Switch-Ports	+	+	+	+	+	+
M-TK-63	Quality of Service im Netzwerk	-	-	+	+	+	+
M-TK-64	Zugangskontrolle zum Netzwerk	-	+	+	+	+	+
M-TK-65	MAC Security im Anschlussbereich für Endgeräte	-	-	+	+	+	+
M-TK-66	VPN zur Kommunikation über eingeschränkt vertrauenswürdige Netze	+	+	+	+	+	+
M-TK-67	Netztrennung für VoIP	-	-	+	+	+	+
M-TK-68	Netztrennung zwischen IP-PBX und Session Border Controller	-	-	+	+	+	+
M-TK-69	Erkennung und Abwehr von DoS-Angriffen gegen VoIP und von SPIT durch IPS / IDS	-	-	+	+	+	+
M-TK-70	Angemessene Verfügbarkeit des LAN für die Verwendung von VoIP	-	-	+	+	+	+
M-TK-71	Angemessene Verfügbarkeit der vom VoIP-System genutzten Netzdienste	-	-	+	+	+	+
M-TK-72	Angemessene Verfügbarkeit der Stromversorgung für IP-Telefone	-	-	+	+	+	+

	Legende: - = nicht relevant für dieses Szenario + = relevant für umfassenden Schutz	Anwaltsbüro	Ingenieur-Büro	Groß-Klinikum	Energieversorger	Globaler Konzern	IT-Dienstleister für Industriepark
M-TK-73	Sichere Administration des Telefonie-Servers	-	+	+	+	+	+
M-TK-74	Sichere Administration von PSTN-Gateways	-	+	+	+	+	+
M-TK-75	Sichere Administration von Anwendungs- und Management-Servern	-	+	+	+	+	+
M-TK-76	Sichere Administration von Abrechnungs- und Gebührenerfassungssystemen	-	-	+	+	+	+
M-TK-77	Sichere Verwaltung von Teilnehmerprofilen	-	+	+	+	+	+
M-TK-78	Sichere Administration von Endgeräten	+	+	+	+	+	+
M-TK-79	Sichere Administration von Netzkomponenten	+	+	+	+	+	+
M-TK-80	Überwachung der Komponenten des VoIP-Systems	-	+	+	+	+	+
M-TK-81	Datensicherung für die Elemente des VoIP-Systems	-	+	+	+	+	+
M-TK-82	VoIP-Tauglichkeit der IP-Infrastruktur für einen IP-Anlagenanschluss	-	-	+	+	+	+
M-TK-83	Überwachung der VoIP-Anbindung zum ITSP	-	-	+	+	+	+
M-TK-84	Sichere Administration des Session Border Controller	-	-	+	+	+	+
M-TK-85	Notfallvorsorge für das VoIP-System	+	+	+	+	+	+
M-TK-86	Harmonisierung zwischen IT-Betrieb und VoIP-Anlagen-Betrieb	-	+	+	+	+	+
Hybrid-Anlagen							
-	leer						
Unified Communications and Collaboration							
M-TK-87	Absicherung der E-Mail-Kommunikation eines UCC-Systems	-	+	+	+	+	+
M-TK-88	Absicherung des Sprachkanals zwischen TK-Anlage bzw. VoIP-Kommunikationssystem und UCC-Systemen	-	+	+	+	+	+
M-TK-89	Absicherung von CTI-Verbindungen und Schnittstellen zur Anwendungsintegration	-	+	+	+	+	+

	Legende: - = nicht relevant für dieses Szenario + = relevant für umfassenden Schutz	**Anwaltsbüro**	**Ingenieur-Büro**	**Groß-Klinikum**	**Energieversorger**	**Globaler Konzern**	**IT-Dienstleister für Industriepark**
M-TK-90	Absicherung der Kommunikation zwischen UCC-System und weiteren IT-Systemen	-	+	+	+	+	+
M-TK-91	Absicherung der Kommunikation zwischen UCC-System und Datenbank	+	+	+	+	+	+
M-TK-92	Schutz vor unberechtigtem Zugriff auf Datenbanksysteme	+	+	+	+	+	+
M-TK-93	Absicherung der Kommunikation eines Präsenzsystems	-	+	+	+	+	+
M-TK-94	Vermeidung der Speicherung von Präsenzinformationen	-	+	+	+	+	+
M-TK-95	Einschränkung der Sichtbarkeit von Präsenzinformationen	+	+	+	+	+	+
M-TK-96	Differenzierung der Sichtbarkeit von Präsenzinformationen	+	+	+	+	+	+
M-TK-97	Verhindern der Verbreitung von Malware und bösartigen Hyperlinks per Instant Messaging	-	+	+	+	+	+
M-TK-98	Vermeidung von Spam over Instant Messaging	-	+	+	+	+	+
M-TK-99	Verhinderung des Datenabflusses durch Data Loss Prevention	+	+	+	+	+	+
M-TK-100	Sicherung von Konferenzräumen	-	+	+	+	+	+
M-TK-101	Sicherer Umgang mit Gesprächs- und Konferenzaufzeichnungen	+	+	+	+	+	+
M-TK-102	Absicherung des telefonischen Zugriffs auf UCC-Anwendungen durch eine PIN	+	+	+	+	+	+
M-TK-103	Einschränkung der Zugriffsrechte	+	+	+	+	+	+
M-TK-104	Einschränkung von Weiterleitungszielen und gleichzeitiger Rufsignalisierung	-	+	+	+	+	+
M-TK-105	Deaktivierung der CTI-Funktion für Konferenztelefone	-	+	+	+	+	+
M-TK-106	Absicherung von UCC-Systemen auf Ebene der Endgeräte	+	+	+	+	+	+
M-TK-107	Möglichkeit zur individuellen Einstellung des Präsenzstatus	+	+	+	+	+	+
M-TK-108	Ständiges Einblenden der Teilnehmerliste	+	+	+	+	+	+
M-TK-109	Verwenden von Kameras mit geeigneter Brennweite	+	+	+	+	+	+

	Legende: - = nicht relevant für dieses Szenario + = relevant für umfassenden Schutz	Anwaltsbüro	Ingenieur-Büro	Groß-Klinikum	Energieversorger	Globaler Konzern	IT-Dienstleister für Industriepark
M-TK-110	Signalisierung der Kameraaktivität und Verwendung von Kameraabdeckungen	+	+	+	+	+	+
M-TK-111	Richtliniengesteuerte Aktivierung/Deaktivierung von Kamera und Mikrofon	-	-	+	+	+	+
M-TK-112	Geeignete Standortwahl und Umgebungsgestaltung bei Einsatz von Desktop-Video	+	+	+	+	+	+
M-TK-113	Netztrennung zwischen UCC-Systemen und weiteren IT-Systemen	-	+	+	+	+	+
M-TK-114	Sichere Administration der Server für UCC-Systeme	-	+	+	+	+	+
M-TK-115	Absicherung der Management-Schnittstellen eines UCC-Systems	-	+	+	+	+	+
M-TK-116	Koordination der Planung und Administration von UCC-Diensten	-	+	+	+	+	+
Spezielle TK-Systeme							
Videokonferenz							
M-TK-117	Absicherung der zentralen Komponenten des Videokonferenzsystems	-	+	+	+	+	+
M-TK-118	Durchgängige Verschlüsselung eines mit IP übertragenen Video-Medienstroms	+	+	+	+	+	+
M-TK-119	Durchgängige Verschlüsselung einer IP-basierten Video-Signalisierung	+	+	+	+	+	+
M-TK-120	Authentisierung zwischen Video-Terminals und zentralen Video-Systemen	-	+	+	+	+	+
M-TK-121	Sicheres Ressourcenmanagement für Videokonferenzen	+	+	+	+	+	+
M-TK-122	Einschränkung des lokalen Zugriffs auf die Konfiguration des Video-Terminals	-	+	+	+	+	+
M-TK-123	Automatische Annahme eines Video-Anrufs deaktivieren	-	+	+	+	+	+
M-TK-124	Deaktivierung / Ausschaltung des Video-Terminals	-	+	+	+	+	+
M-TK-125	Anzeige der aktuellen Teilnehmer und Benachrichtigung bei neu eintretenden Teilnehmern bei einer Videokonferenz	-	+	+	+	+	+
Kontaktcenter							
M-TK-126	Authentisierung am IVR-System	-	-	-	+	+	+

	Legende: - = nicht relevant für dieses Szenario + = relevant für umfassenden Schutz	Anwaltsbüro	Ingenieur-Büro	Groß-Klinikum	Energieversorger	Globaler Konzern	IT-Dienstleister für Industriepark
M-TK-127	Qualitätssicherung der Routing-Regeln	-	-	-	+	+	+
M-TK-128	Data Loss Prevention am Agentenarbeitsplatz	-	-	-	+	+	+
M-TK-129	Authentisierung des Zugriffs auf Kontaktcenter-Anwendungen	-	-	-	+	+	+
M-TK-130	Verhinderung des automatisierten Zugriffs auf Internet-Kontaktformulare	-	-	-	+	+	+
M-TK-131	Beschränkung des Netzzugriffs auf dedizierte Räumlichkeiten im Kontaktcenter	-	-	-	+	+	+
M-TK-132	Hochverfügbare Auslegung der Netzkomponenten und Systeme im Kontaktcenter	-	-	-	+	+	+
M-TK-133	Absicherung der Übergänge in öffentliche Netze	-	-	-	+	+	+
M-TK-134	Absicherung der Management-Schnittstellen	-	-	-	+	+	+
M-TK-135	Schulung von Kontaktcenter-Administratoren und Schichtleitern/Supervisoren	-	-	-	+	+	+
M-TK-136	Zutrittsbeschränkung für Kontaktcenter-Räumlichkeiten	-	-	-	+	+	+
Händlersysteme							
M-TK-137	Verwendung dedizierter Händlersysteme	-	-	-	+	-	-
M-TK-138	Festlegung dedizierter Gesprächskreise	-	-	-	+	-	-
M-TK-139	Vermeidung von Fehlbedienung durch intuitive Bedienkonzepte	-	-	-	+	-	-
Alarmierungssysteme							
M-TK-140	Schaffung geeigneter Umgebungsbedingungen für zentrale Elemente eines Alarmierungssystems	-	-	+	+	+	+
M-TK-141	Sichere Konfiguration zentraler Elemente einer Alarmierungsgesamtlösung	-	-	+	+	+	+
M-TK-142	Absicherung der Anbindung von Alarmierungssystemen an TK-Infrastrukturen	-	-	+	+	+	+
M-TK-143	Verstärkte Absicherung der von Alarmierungssystemen mitgenutzten TK-Installationen	-	-	+	+	+	+
M-TK-144	Ausstattung und Anbringung der Endpunkte unter Berücksichtigung von Sicherheitsaspekten	-	-	+	+	+	+
M-TK-145	Verbindliche Regelungen für den Umgang mit Endpunkten zu Alarmierungssystemen	-	-	+	+	+	+

	Legende: - = nicht relevant für dieses Szenario + = relevant für umfassenden Schutz	Anwaltsbüro	Ingenieur-Büro	Groß-Klinikum	Energieversorger	Globaler Konzern	IT-Dienstleister für Industriepark
M-TK-146	Absicherung der Kommunikation zwischen Elementen eines Alarmierungssystems	-	-	+	+	+	+
M-TK-147	Automatisierte Überwachung der Komponenten von Alarmierungssystemen	-	-	+	+	+	+
M-TK-148	Erhöhte Frequenz gezielter Sicht- und Zustandsprüfungen	-	-	+	+	+	+
M-TK-149	Schulung der Administratoren bzw. des Betriebspersonals von Alarmierungssystemen	-	-	+	+	+	+
M-TK-150	Bedarfsgerechte Notfallplanung und -vorsorge für Kopplung von Alarmierungssystemen	-	-	+	+	+	+
M-TK-151	Erarbeitung sicherheitsrelevanter Regelungen für den Einsatz von Alarmierungssystemen	-	-	+	+	+	+
M-TK-152	Erstellung einer Konzeption zur integrierten Nutzung von Alarmierungssystem und TK-Lösungen	-	-	+	+	+	+
M-TK-153	Produktauswahl von Alarmierungssystemlösungen unter Sicherheitsgesichtspunkten	-	-	+	+	+	+
M-TK-154	Einweisung, Schulung und Sensibilisierung der Nutzer von Alarmierungssystemen	-	-	+	+	+	+
Provider-basierte TK-Dienste							
Soziale Netzwerke und Soziale Medien							
M-TK-155	Berechtigungskonzept zur Steuerung der Freigabe des Präsenzstatus	-	+	+	+	+	+
M-TK-156	Berechtigungskonzept und technische Umsetzung für externe Kommunikation mit Sozialen Netzwerken und Medien	-	+	+	+	+	+
M-TK-157	Kanalisierung des Zugriff auf dienstliche Accounts in Sozialen Netzwerken und Medien über Portallösung	-	+	+	+	+	+
M-TK-158	Dokumentation der Zugriffe und Aktivitäten bei Nutzung von Sozialen Netzwerken und Medien	+	+	+	+	+	+
M-TK-159	Vermeiden der bidirektionalen Kontaktsynchronisation mit Sozialen Netzwerken und Medien	+	+	+	+	+	+
M-TK-160	Host-basiertes Data Loss Prevention (DLP) bei Nutzung von Sozialen Netzwerken und Medien	-	-	+	+	+	+
M-TK-161	Netzwerk-basiertes Data Loss Prevention (DLP) bei Nutzung Sozialer Netzwerke und Medien	-	-	+	+	+	+
M-TK-162	Verhinderung oder Einschränkung der Nutzung von Sozialen Netzwerken und Medien am Netzübergang	-	-	+	+	+	+
M-TK-163	Netztechnische Isolation von Clients und Infrastrukturteilen mit Zugriff auf Soziale Netzwerke und Medien	-	-	+	+	+	+

	Legende: - = nicht relevant für dieses Szenario + = relevant für umfassenden Schutz	Anwaltsbüro	Ingenieur-Büro	Groß-Klinikum	Energieversorger	Globaler Konzern	IT-Dienstleister für Industriepark
M-TK-164	Sichere Administration der Server-Systeme und Gateways zur Anbindung an Soziale Netzwerke und Medien	-	-	+	+	+	+
M-TK-165	Schulung der Administratoren für den Zugang zu Sozialen Netzwerken und Medien	-	+	+	+	+	+
M-TK-166	Klärung und rechtsverbindliche Regelung juristischer Aspekte zur Nutzung Sozialer Netzwerke und Medien im dienstlichen Kontext	+	+	+	+	+	+
M-TK-167	Geeignete Einbindung der Nutzung von Sozialen Netzwerken und Medien in etablierte Prozesse	+	+	+	+	+	+
M-TK-168	Transparente und durchsetzbare Regelungen zur Nutzung Sozialer Netzwerke und Medien im dienstlichen Kontext	+	+	+	+	+	+
M-TK-169	Gezielte Trennung von dienstlichem und privatem Gebrauch von Sozialen Netzwerken und Medien	+	+	+	+	+	+
M-TK-170	Einschränkung oder Verbot der Privatnutzung von Sozialen Netzwerken und Medien am Arbeitsplatz	+	+	+	+	+	+
M-TK-171	Verbot der ungeschützten Übertragung vertraulicher Inhalte über Soziale Netzwerke und Medien	+	+	+	+	+	+
M-TK-172	Information und Schulung der Anwender bzgl. sicherer Nutzung von Sozialen Netzwerken und Medien	+	+	+	+	+	+
M-TK-173	Benennung von Ansprechpartnern	+	+	+	+	+	+
Outsourcing, IP-Centrex, Cloud Computing und UC as a Service							
M-TK-174	Konsequente Verschlüsselung bei Transport, Speicherung und Verarbeitung von Daten	+	-	-	+	-	+
M-TK-175	Härtung der Virtualisierungsplattform	-	-	-	+	-	+
M-TK-176	Einsatz von UC-fähigem Virenschutz	+	-	-	+	-	+
M-TK-177	Einsatz von Host-basierten DLP-Systemen bei Cloud-Nutzung	+	-	-	-	-	-
M-TK-178	Einsatz von Netzwerk-basierten DLP-Systemen bei Cloud-Nutzung	-	-	-	-	-	-
M-TK-179	Dem Schutzbedarf angepasste Überwachung der Dienste	+	-	-	+	-	-
M-TK-180	Regelmäßige Erstellung von Berichten und Informationspflicht bei Sicherheitsvorfällen	+	-	-	+	-	-
M-TK-181	Nachweis und Überprüfung der Vertrauenswürdigkeit des Dienstleisters	+	-	-	+	-	-
M-TK-182	Einsatz von sicherheitsüberprüftem Personal	+	-	-	+	-	-

	Legende: - = nicht relevant für dieses Szenario + = relevant für umfassenden Schutz	Anwaltsbüro	Ingenieur-Büro	Groß-Klinikum	Energieversorger	Globaler Konzern	IT-Dienstleister für Industriepark
M-TK-183	Regelmäßige Auditierung der Infrastruktur des Dienstleisters	+	-	-	+	-	-
M-TK-184	Festlegung des Speicherortes der Daten bei Outsourcing und Cloud-Nutzung	+	-	-	-	-	-
M-TK-185	Lesender Zugriff auf die vom Dienstleister bereitgestellten Komponenten	-	-	-	-	-	-
Einbindung Mobiler Endgeräte							
Mobilfunk und Fixed Mobile Convergence							
M-TK-186	Gegenseitige Authentisierung von mobilen Endgeräten und einer zentralen Komponente der FMC- bzw. UCC-Lösung	+	+	+	+	+	+
M-TK-187	Schutz von Servern für mobile Endgeräte	-	+	+	+	+	+
M-TK-188	Verwendung einer Ende-zu-Ende-Verschlüsselung für die Telekommunikation	+	+	+	+	+	+
M-TK-189	Verschlüsselung von Nachrichten	-	+	+	+	+	+
M-TK-190	Einsatz von Server-based Computing	+	-	-	+	-	-
M-TK-191	Verschlüsselung, Integritätsschutz und Authentisierung auf der Luftschnittstelle	+	+	+	+	+	+
M-TK-192	Ende-zu-Ende-Verschlüsselung für Medienströme	+	+	+	+	+	+
M-TK-193	Absicherung Authentication-Server	+	+	+	+	+	+
M-TK-194	Einsatz von abhörsicheren Mobiltelefonen	-	-	-	-	-	-
M-TK-195	Absicherung aller Kommunikationsschnittstellen des Endgerätes	-	+	+	+	+	+
M-TK-196	Schutz der organisationsinternen Daten auf einem mobilen Endgerät	+	+	+	+	+	+
M-TK-197	Erweiterung von Data Loss Prevention auf mobile Endgeräte	+	+	+	+	+	+
M-TK-198	Sperrung des mobilen Endgerätes für Nutzereingaben	-	+	+	+	+	+
M-TK-199	Benutzerauthentisierung am mobilen Endgerät	+	+	+	+	+	+
M-TK-200	Automatische Handlungen bei Verletzung von Sicherheitsrichtlinien auf mobilen Endgeräten	-	-	+	+	+	+

	Legende: - = nicht relevant für dieses Szenario + = relevant für umfassenden Schutz	Anwaltsbüro	Ingenieur-Büro	Groß-Klinikum	Energieversorger	Globaler Konzern	IT-Dienstleister für Industriepark
M-TK-201	Rollenbasierte Zugriffsberechtigungen auf Objekte des mobilen Endgerätes	-	+	+	+	+	+
M-TK-202	Schutz des mobilen Endgerätes vor schadenstiftender Software	+	+	+	+	+	+
M-TK-203	Deaktivierung der automatischen Rufannahme	+	+	+	+	+	+
M-TK-204	Schutz vor unerwünschter Konfigurationsänderung über die GSM/UMTS-Funkschnittstelle	+	+	+	+	+	+
M-TK-205	Schutzmaßnahmen für das Herunterladen von Inhalten	+	+	+	+	+	+
M-TK-206	Prozess zur Behandlung des Verlusts eines mobilen Endgerätes	+	+	+	+	+	+
M-TK-211	Berücksichtigung der Sicherheit bei der Vertragsgestaltung mit einem Dienstanbieter	+	+	+	+	+	+
M-TK-217	Fernadministration der mobilen Endgeräte durch ein Mobile Device Management	-	-	+	+	+	+
M-TK-218	Regelmäßige, möglichst automatische Sicherung von Daten und Konfiguration mobiler Endgeräte	-	-	+	+	+	+
M-TK-219	Einschränkung von Apps	+	+	+	+	+	+
M-TK-220	Überwachung der Endgeräte hinsichtlich Anomalien	-	-	+	+	+	+
Wireless LAN							
M-TK-191	Verschlüsselung, Integritätsschutz und Authentisierung auf der Luftschnittstelle	+	+	+	+	+	+
M-TK-192	Ende-zu-Ende-Verschlüsselung für Medienströme	+	+	+	+	+	+
M-TK-193	Absicherung Authentication Server	+	+	+	+	+	+
M-TK-212	Trennung von LAN und WLAN-Verkehr im kabelbasierten Netz	-	-	+	+	+	+
M-TK-213	Absicherung des LAN-Zugangs für Access Points	-	-	+	+	+	+
M-TK-214	Berücksichtigung der Anforderungen einer Sprachübertragung bei der Planung der Funkzellen	-	-	+	+	+	+
M-TK-221	Kontinuierliche Überwachung der Luftschnittstelle	-	-	+	+	+	+
M-TK-222	Kontinuierliche Überwachung der WLAN-Infrastruktur	-	-	+	+	+	+

	Legende: - = nicht relevant für dieses Szenario + = relevant für umfassenden Schutz	Anwaltsbüro	Ingenieur-Büro	Groß-Klinikum	Energieversorger	Globaler Konzern	IT-Dienstleister für Industriepark
M-TK-223	Fernadministration der WLAN-Endgeräte	-	-	+	+	+	+
DECT							
M-TK-207	Einsatz von DECT-Endgeräten mit verbesserter DECT-konformer Verschlüsselung	-	-	+	+	+	+
M-TK-208	Einsatz von DECT-Endgeräten mit zusätzlicher Verschlüsselung	-	-	+	+	+	+
M-TK-215	Absicherung bei Anschluss von Radio Fixed Parts an ein LAN	-	-	+	+	+	+
M-TK-224	Protokollierung des Einsatzes zusätzlicher Verschlüsselung	-	-	+	+	+	+
M-TK-225	Verzicht auf den Einsatz von DECT bei erhöhtem Schutzbedarf	-	-	+	+	+	+
Bluetooth							
M-TK-209	Sichere Konfiguration und Verwendung des Bluetooth-Adapters	+	+	+	+	+	+
M-TK-210	Einsatz von Bluetooth-Endgeräten mit zusätzlicher Verschlüsselung	+	+	+	+	+	+
M-TK-216	Absicherung von Bluetooth Access Points bei Anschluss an ein LAN	-	-	+	+	+	+
M-TK-226	Verzicht auf den Einsatz von Bluetooth bei erhöhtem Schutzbedarf	-	-	+	+	+	+
Generell zu ergreifende Sicherheitsmaßnahmen							
M-TK-228	Sichere Kabelführung	-	-	+	+	+	+
M-TK-228	Produktauswahl von TK-Lösungen unter Berücksichtigung von Sicherheitsaspekten	+	+	+	+	+	+
M-TK-229	Härtung von Servern des Telekommunikationssystems	+		+	+	+	+
M-TK-230	Spezielle Absicherung von virtualisierten TK-Servern	-	-	+	+	+	+
M-TK-231	Einschränkung und Kontrolle von Berechtigungen für die Administration eines Servers des Telekommunikationssystems	-	+	+	+	+	+
M-TK-232	Einschränkung und Kontrolle des Zugangs zu einem Server des Telekommunikationssystems	-	+	+	+	+	+
M-TK-233	Physische Sicherheit der Telekommunikationslösung	-	+	+	+	+	+
M-TK-234	Berücksichtigung der Server der TK-Lösung im Datensicherungskonzept der Organisation	-	-	+	+	+	+

	Legende: - = nicht relevant für dieses Szenario + = relevant für umfassenden Schutz	**Anwaltsbüro**	**Ingenieur-Büro**	**Groß-Klinikum**	**Energieversorger**	**Globaler Konzern**	**IT-Dienstleister für Industriepark**
M-TK-235	Schutz vor schadenstiftender Software für die Server der TK-Lösung	-	+	+	+	+	+
M-TK-236	Einbindung der Server der TK-Lösung in das Patch-Management der Organisation	-	+	+	+	+	+
M-TK-237	Sichere Konfiguration des Netzwerk-Management-Protokolls	-	+	+	+	+	+
M-TK-238	Überwachung der Komponenten des Telekommunikationssystems	-	+	+	+	+	+
M-TK-239	Erweiterung von Penetrationstests auf die verwendeten TK-Technologien	-	+	+	+	+	+
M-TK-240	Ergänzung der Überwachung um Honeypots für die verwendeten TK-Technologien	-	-	+	+	+	+
M-TK-241	Erweiterung des Verwundbarkeits-Managements für die verwendeten TK-Technologien	-	+	+	+	+	+
M-TK-242	Schutz von Verbindungsdaten	+	+	+	+	+	+
M-TK-243	Nutzung von speziell abgesicherten Räumlichkeiten	-	+	+	+	+	+
M-TK-244	Sichere Außerbetriebnahme von Komponenten des Telekommunikationssystems	-	+	+	+	+	+
M-TK-245	Nachweis der Vertrauenswürdigkeit des Dienstanbieters	+	+	+	+	+	+
M-TK-246	Notfallvorsorge für alle Teilsysteme der TK-Lösung	+	+	+	+	+	+
M-TK-247	Sensibilisierung der Anwender von TK-Diensten hinsichtlich Sicherheitsaspekten	+	+	+	+	+	+
M-TK-248	Schulung der Anwender von TK-Diensten zu Sicherheits- und Datenschutzaspekten	+	+	+	+	+	+
M-TK-249	Schulung der Administratoren von TK-Lösungen	-	+	+	+	+	+

Tabelle 54: Auswahl von Maßnahmen für Beispielszenarien

Literaturverzeichnis

[BSI 100/3-2008] BSI, „BSI-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz, Version 2.5“, Mai 2008, verfügbar unter https://www.bsi.bund.de/DE/Publikationen/BSI_Standard/it_grundschutzstandards.html

[BSI GSK-2013] BSI, „IT-Grundschutz-Kataloge“, September 2013, verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/itgrundschutz_node.html

Abkürzungsverzeichnis

A

ADSL	Asymmetric Digital Subscriber Line
ATA	(ISDN) Analogue Telephony Adapter

B

BSI	Bundesamt für Sicherheit in der Informationstechnik

C

CoS	Class of Service
CRM	Customer Relationship Management
CTI	Computer Telephony Integration

D

DECT	Digital Enhanced Cordless Telecommunications
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name Service
DoS	Denial of Service

E

ENUM	E.164 Telephon NUmber Mapping

F

F	Filiale
FMC	Fixed Mobile Convergence

G

GAU	Größter Anzunehmender Unfall
GSK	(BSI IT-) Grundschutz-Kataloge
GSM	Global System for Mobile Communications
GW	Gateway

H

HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over TLS / HTTP Secure

I

I	intern
IAD	Integrated Access Device
IDS	Intrusion Detection System
IM	Instant Messaging
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	IP Security

ISDN	Integrated Services Digital Network
IT	Information Technology
ITSP	IP Telephony Service Provider
IVR	Interactive Voice Response

L

LAN	Local Area Network
LTE	Long Term Evolution

M

MAC	Media Access Control
MAN	Metropolitan Area Network
MCU	Multipoint Control Unit
MFP	Multifunctional Printer
MDM	Mobile Device Management
MPLS	Multiprotocol Label Switching

N

NAT	Network Address Translation
NGN	Next Generation Network(s)
NTBA	Network Termination for ISDN Basic Rate Access
NW	Netzwerk

P

P	(Service) Provider
PBX	Private Branch eXchange
PC	Personal Computer
PIN	Personal Identification Number
PoE	Power over Ethernet
PSK	Pre-Shared Key
PSTN	Public Switched Telephone Network

Q

QoS	Quality of Service

R

R	Remote User
RADIUS	Remote Authentication Dial In User Service
RAS	Registration, Admission and Status

S

S	Standort
SBC	Session Border Controller
SDSL	Symmetric Digital Subscriber Line
SIP	Session Initiation Protocol
SNM	Soziale Netzwerke und Medien

SPIM	Spam over Instant Messaging
SPIT	Spam over Internet Telephony
SSID	Service Set Identifier

T

TK	Telekommunikation

U

UC	Unified Communications
UCaaS	UC(C) as a Service
UCC	Unified Communications & Collaboration
UMTS	Universal Mobile Telecommunications System
URL	Uniform Resource Locator
USV	Unterbrechungsfreie Stromversorgung

V

VCS	Video Conference System
VDI	Virtual Desktop Infrastructure
VLAN	Virtual LAN
VoIP	Voice over IP
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network

W

WAN	Wide Area Network
WLAN	Wireless Local Area Network

X

X	Externe Organisation

Stichwortverzeichnis / Index