Bundesamt
für Sicherheit in der
Informationstechnik

BSI

Kompendium Videokonferenzsysteme

KoViKo - Version 1.0.1

Das Dokument reflektiert den Stand der Technik bis April 2020

An der Erstellung waren folgende Mitarbeiter des BSI (Bundesamt für Sicherheit in der Informationstechnik) beteiligt: Norbert Landeck, Christian Korbach und Markus Hermes

Weiterhin haben folgende Mitarbeiter der ComConsult Beratung und Planung GmbH maßgeblich mitgewirkt: Oliver Flüs, Daniela Gies, Leonie Herden, Dr. Simon Hoff, Dietlind Hübner, Benjamin Wagner und Nils Wantia

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

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Vorbemerkungen

Der Funktionsumfang und die Benutzerfreundlichkeit moderner Videokonferenzsysteme ist in den letzten Jahren so erstaunlich gewachsen, dass Videokonferenzsysteme nicht mehr aus dem Arbeitsalltag wegzudenken sind. Die klassische Telefonkonferenz und E-Mail-Kommunikation sind immer mehr den Hintergrund gerückt, da eine Web-Konferenz mit Sprache und Video in Verbindung mit Chat und dem Teilen von Desktops und Anwendungen bis hin zur gemeinsamen Bearbeitung von Dokumenten mit einer einzigen Plattform ausgesprochen leicht möglich ist.

Dabei verschwimmen die Grenzen zwischen Videokonferenzsystemen, sogenannten Meeting Solutions und Lösungen für Unified Communications & Collaboration (UCC) immer mehr. Bei modernen Videokonferenzsystemen kommen dabei praktisch alle Techniken zusammen, die hinsichtlich der Informationssicherheit interessante Herausforderungen darstellen:

- Web-Anwendungen und Web-Services sind die Basis für Apps, mit denen sich Nutzer via Standard-Clients z. B. mit Windows oder Mac OS an Konferenzen beteiligen.
- Videokonferenzlösungen werden immer häufiger mit Cloud-Komponenten oder sogar als rein Cloud-basierte Lösungen angeboten.
- Web-Server auf Endgeräten erleichtern die Administration und die Bedienung von spezifischen Videokonferenz-Terminals wie beispielsweise Raumsysteme.
- Speziell moderne Videokonferenz-Lösungen umfassen auch Raumsysteme, Kameras und Sprach-steuerungen als Endgeräte im Internet of Things (IoT) und es gibt sogar Schnittstellen zur Gebäudetechnik, z. B. zur automatischen Anpassung der Beleuchtung.
- Dienste der Künstlichen Intelligenz (KI) können eingesetzt werden, um einerseits über eine KI-basierte Sprachschnittstelle die Nutzung einer Videokonferenz zu vereinfachen, aber auch um Inhalte der Konferenz zu analysieren und Aktivitäten anzusteuern. Beispielsweise können die Namen von Teilnehmern automatisch dem jeweiligen Bild zugeordnet, automatisiert Dokumente bereitgestellt und sogar Protokolle von Konferenzen geführt werden.

Neben der Absicherung von Medienströme und Signalisierung und der sicheren Konfiguration und Administration eines Videokonferenzsystems sind daher eine Vielzahl von weiteren Sicherheitsmaßnahmen zu beachten.

Bereits 2014 hatte die Technische Leitlinie für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf BSI TL-02103 in der Version 2.0 (kurz: TLSTK-II, siehe [BSI TLSTK-2014]) Videokonferenzen, UCC und Cloud berücksichtigt. Jedoch haben insbesondere im Bereich der Videokonferenzlösungen die eben beschriebenen Entwicklungen eine Aktualisierung motiviert. Das vorliegende Kompendium beinhaltet diese Aktualisierung und ist so gestaltet, dass es weitgehend unabhängig von der TLSTK-II gelesen werden kann. Das Kompendium geht dabei bewusst über die TLSTK-II hinaus, indem es sich auch auf funktionale und operative Aspekte außerhalb der reinen Informationssicherheit konzentriert.

Der Inhalt dieses Kompendiums ist wie folgt strukturiert:

- Zunächst werden in Kapitel 2 der Funktionsumfang und in Kapitel 3 der technische Aufbau moderner Videokonferenzsysteme beschrieben. In Kapitel 4 werden dann die operativen Aspekte, d. h. Planung, Nutzung und Betrieb von Videokonferenzsystemen betrachtet.
- Auf dieser Basis wird dann in Kapitel 5 zunächst die Gefährdungslage analysiert, um dann entsprechend in Kapitel 6 Sicherheitsanforderungen abzuleiten und in Kapitel 7 Umsetzungsempfehlungen zu den

Anforderungen zu entwickeln. Vorgehensweise und Struktur orientieren sich dabei am BSI IT-Grundschutz-Kompendium (siehe [BSI GSK-2019]).

- Exemplarisch wird in Kapitel 8 dargestellt, wie die beschriebenen Sicherheitsanforderungen und -maßnahmen in Sicherheitskonzepten für unterschiedliche Nutzungsszenarien berücksichtigt werden können.
- Abschließend werden in Kapitel 9 Hilfsmittel zur Beschaffung einer Videokonferenzlösung bereitgestellt, die Auswahlkriterien und ein Beispiel für ein Leistungsverzeichnis liefern.

Als Anwender des Kompendiums Videokonferenzsysteme werden Entscheider, Planer, Beschaffer, Betreiber, Administratoren, Auditoren und auch Endnutzer adressiert, die über die Videokonferenzlösung Inhalte bzw. Informationen mit normalem und erhöhtem Schutzbedarf austauschen. Jedoch betrachtet das vorliegende Dokument nicht den Einsatz einer Videokonferenzlösung in Arbeitsbereichen mit Verschlusssachen (VS-Bereichen).

Durch die Bereitstellung der oben genannten Instrumente unterstützt das vorliegende Kompendium den jeweiligen Anwender bei der Absicherung aktueller Videokonferenzlösungen über den gesamten Lebenszyklus von der Planung bis zum Rückbau und berücksichtigt dabei insbesondere auch Bereiche mit erhöhtem Schutzbedarf.

2 Systembeschreibung

Schon in der Zeit des Integrated Services Digital Network (ISDN) im öffentlichen Festnetz hatte die audiovisuelle Kommunikation innerhalb und außerhalb von Institutionen deutlich an Bedeutung gewonnen. Jedoch hat erst die Übertragung von Videodatenströmen über IP-basierte Netze für einen signifikanten Qualitätssprung im Vergleich zu ISDN-basierter Technologie geführt. Heutige Videokonferenzsysteme ermöglichen die gleichzeitige Teilnahme vieler, gar hunderter Raumsysteme an Konferenzen mit hochauflösenden Videoformaten von HD (High Definition, 1280 x 720 Pixel), FullHD (1920 x 1080 Pixel) bis hin zu 4K bzw. UltraHD (3840 x 2160 Pixel). Die moderne Videokonferenz ist kein isolierter Dienst, sondern typischerweise in eine moderne Kommunikationslösung mit vielen Funktionen integriert. Daher erfolgt zunächst in Kapitel 2.1 eine Charakterisierung von Videosystemen und in Kapitel 2.4 abschließend eine Abgrenzung zu anderen Anwendungen und Systemen der Telekommunikation.

Unterhaltungen, die mit Kurznachrichten oder Gruppenunterhaltungen begonnen wurden, können bei Bedarf flexibel um Sprach- und Videokommunikation erweitert werden. Moderne Lösungen unterscheiden aus der Sicht des Anwenders nicht mehr zwischen Videokonferenzen mit zwei oder mehreren Teilnehmern. Neben Video- und Audiodaten können aktuelle Videokonferenzsysteme zusätzlich Anwendungsinhalte übertragen. Diese und weitere relevante Funktionen werden in Kapitel 2.2 detailliert betrachtet.

Klassische raumbasierte Videokonferenzsysteme haben einen hohen, aber bei weitem nicht flächendeckenden Verbreitungsgrad erreicht. Aufgrund der vergleichsweise hohen Investitionen war in der Vergangenheit der Nutzerkreis oft auf die Leitungsebene einer Institution begrenzt. Hieraus ergab sich ein erhöhter Schutzbedarf für die transportierten Inhalte und somit für das Videokonferenzsystem. Insbesondere durch die Integration von Arbeitsplatzrechnern und mobilen Endgeräten wie Smartphones und Tablets in Kommunikations- und Konferenzlösungen (Desktop-Video) durchdringen Videokonferenzen heute zunehmend breitere Anwenderschichten. Die Anwendungsfälle sind vielfältig und reichen von der Punkt-zu-Punkt-Kommunikation zwischen zwei Mitarbeitern einer Institution über Konferenzen mit mehreren Mitgliedern eines Teams, die an unterschiedlichen Orten teilnehmen, bis hin zur Unterstützung von Service-Technikern durch mobile Videokonferenzen. Kapitel 2.3 nennt typische Einsatzgebiete für Videokonferenzlösungen.

Vielfach steht nicht das Videobild der Teilnehmer im Vordergrund, sondern die gemeinsam bearbeiteten Inhalte. So gehören Funktionalitäten zum Teilen eines Bildschirms oder einer Anwendung ebenso wie die Darstellung von physischen und virtuellen Whiteboards zum typischen Leistungsumfang moderner Videokonferenzlösungen. Darüber hinaus sind die Teilnehmer nicht mehr an bestimmte Endgeräte oder dedizierte Raumsysteme gebunden. Moderne Lösungen ermöglichen Videokonferenzen zwischen einer hohen Vielfalt von Video-Endpunkten bzw. Video-Terminals, insbesondere Desktop-Arbeitsplätzen, Raumsystemen oder mobilen Endgeräten (siehe Abbildung 1).

Nicht zuletzt durch diese große Vielfalt erzeugen Videokonferenzsysteme vielfältige Gefährdungen für die Informationssicherheit. Teils ergeben sich diese aus den technischen Grundlagen der IP-basierten Kommunikation, teils aus dem Einsatzzweck und der Konfiguration von Videokonferenzsystemen. So stellen beispielsweise Sprachassistenzsysteme, deren Mikrofone ständig auf das Signalwort zur Aktivierung lauschen, eine grundsätzliche Gefährdung für alle im jeweiligen Konferenzraum besprochenen vertraulichen Inhalte dar. Es kann passieren, dass über das Mikrofon bzw. die zugehörige Sprachsteuerung unerwünschte Aktivitäten ausgelöst werden oder schlimmstenfalls vertrauliche Daten abfließen.

Durch die Verbreitung von Desktop-Video-Lösungen ergeben sich zudem vielfältige Herausforderungen in Hinblick auf den Datenschutz. So ist der Einsatz von Desktop-Video-Lösungen mit kaum zu kontrollierendem Kamerablickwinkel in Großraumbüros unter Datenschutzgesichtspunkten durchaus kritisch zu sehen.

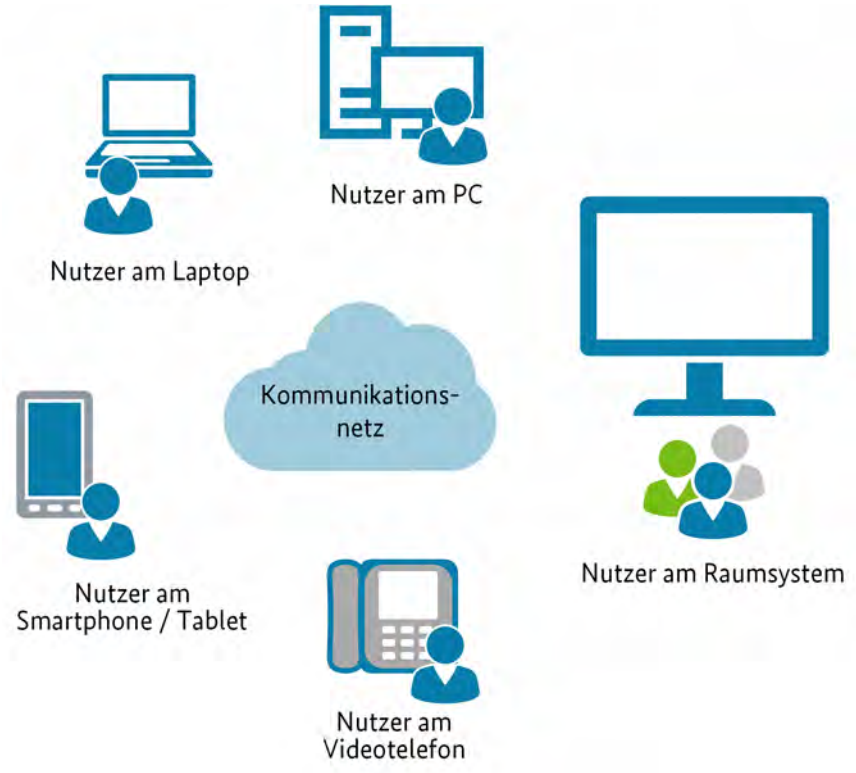

Abbildung 1: Teilnehmer einer Videokonferenz

2.1 Charakterisierung von Videokonferenzsystemen

Klassische Videokonferenzsysteme ermöglichen lediglich die Übertragung von Sprach- und Videodaten zwischen den Teilnehmern einer Videokonferenz. Sie sind typischerweise Hardware-basierte Systeme, die auf die Übertragung von Sprach- und Videodaten mittels IP-basierter Protokolle spezialisiert sind.

Jedoch ist die Übertragung von Videodaten längst nicht mehr nur diesen spezialisierten Systemen vorbehalten, sondern der Dienst Video wird auch in vielen modernen Lösungen zur Verfügung gestellt.

Grob lassen sich diese Anwendungen in die Kategorien Meeting Solutions, Unified Communications (UC) sowie Unified Communications and Collaboration (UCC) unterteilen (siehe Abbildung 2). Sofern hierfür Webtechniken genutzt werden, werden solche Dienste auch umgangssprachlich unter dem Begriff Webkonferenz zusammengefasst.

Der tatsächliche Funktionsumfang der am Markt erhältlichen Herstellerlösungen stimmt zwar selten exakt mit diesen Kategorien überein, jedoch lässt sich dadurch eine grundsätzliche Einordnung vornehmen. Die Einordnung spiegelt sowohl die Entwicklung der Lösungen am Markt als auch die Einsatzgebiete der Lösungen in der Praxis wider. Im Folgenden werden die Kategorien genauer erläutert.

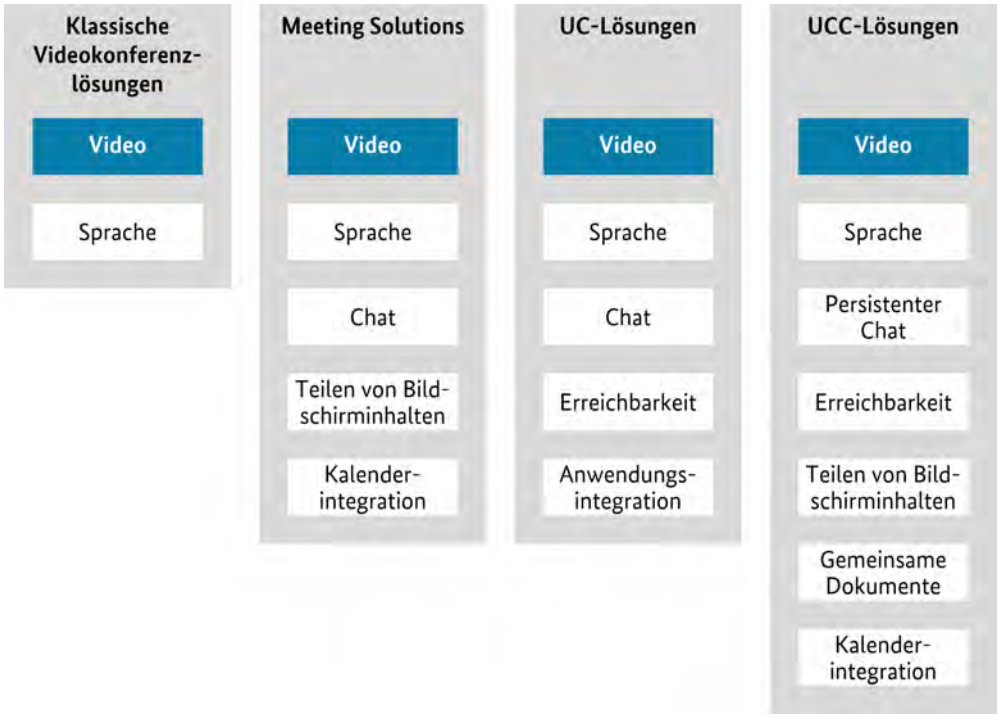

Abbildung 2: Moderne Videokonferenzlösungen

Meeting Solutions

Die Meeting Solutions sind eine Weiterentwicklung der klassischen Videokonferenzsysteme und der zugehörigen Infrastruktur. Hierbei ist die Funktionalität nicht auf die Übertragung der Sprach- und Videodaten beschränkt, sondern Meeting Solutions bieten zusätzlich die folgenden Möglichkeiten:

- Textnachrichten (auch Chat oder Instant Messaging genannt): Flüchtige Kurznachrichten zwischen zwei oder mehr Kommunikationspartnern
- Teilen von Bildschirminhalten: Präsentation und Freigabe des gesamten Bildschirms (Desktop Sharing) oder einzelner Anwendungen (Application Sharing). Dadurch ist das gemeinsame Arbeiten an Dokumenten möglich. Außerdem besteht die Möglichkeit zur temporären Übergabe der Anwendungskontrolle.
- Kalenderintegration: Möglichkeit der Planung von Konferenzen über eine Groupware- oder Kalenderanwendung

Die Komponenten einer Meeting Solution sind für die Videokommunikation optimiert und haben häufig den Charakter einer Vermittlungsplattform. Die Teilnehmer können mit unterschiedlichen Endpunkten, beispielsweise mittels dedizierter Konferenzsysteme oder über ihren Laptop, an einer Konferenz teilnehmen und so miteinander kommunizieren.

Unified Communications

Unified Communications beschreibt die Zusammenführung verschiedener Kommunikationsmedien auf eine IP-basierte Infrastruktur sowie auf eine einheitliche Nutzerschnittstelle. Hier hat sich die Videokommunikation als fester Bestandteil neben der Sprachkommunikation etabliert. Es werden unter anderem die folgenden UC-Dienste bereitgestellt:

- Chat
- Erreichbarkeit: Anzeige von Erreichbarkeits- und Ortsinformationen des Anwenders
- (Desktop-)Video: Videokommunikation über einen Arbeitsplatz-PC oder ein mobiles Endgerät mit zwei oder mehreren Teilnehmern

- Anwendungsintegration: Integration von Kommunikationsmöglichkeiten in die Arbeitsplatzanwendungen des Mitarbeiters sowie Erweiterung klassischer CTI-Funktionen um weitere Medien

Unified Communications and Collaboration

Der Begriff UCC beschrieb ursprünglich lediglich die Erweiterung von Unified Communications um Basisfunktionalitäten der Zusammenarbeit. Hierzu zählen beispielsweise Desktop Sharing und Application Sharing sowie Whiteboarding. Dabei können jeweils zu bearbeitende Inhalte über die Videokonferenz dargestellt und somit eine einfache Art der Zusammenarbeit an Inhalten realisiert werden.

Die Anwendungskategorie UCC hat sich in den letzten Jahren jedoch stark verändert. Moderne Lösungen dieser Kategorie greifen die Grundfunktionalitäten auf und erweitern diese um eine Vielzahl von Werkzeugen und Diensten zur Unterstützung der Zusammenarbeit.

Insbesondere legen diese Anwendungen einen sehr starken Fokus auf Team- bzw. Gruppenarbeit. Dementsprechend ist die Basis solcher Lösungen immer eine Gruppenunterhaltungsfunktion mit persistentem Chat zur Bearbeitung von Projekten im Team. Diese textbasierten Gruppenunterhaltungen werden im Gegensatz zu den flüchtigen Chats dauerhaft gespeichert und sind somit auch Nutzern, die erst später in ein Team eintreten, zugänglich. Bei Bedarf können sie zu Sprach- oder Videokonferenzen erweitert werden, um beispielsweise auf akuten Klärungsbedarf kurzfristig reagieren zu können.

Hinzu kommt eine Fülle von Zusatzfunktionen, die je nach Hersteller sehr unterschiedlich ausfallen können. Beispiele für typische Funktionalitäten sind:

- Gemeinsame Dokumente: Ein Team kann Dokumente gemeinsam, mitunter auch gleichzeitig bearbeiten.
- Bots: Assistenzprogramme, welche über Textnachrichten gesteuert werden können und vielfältige Zusatzfunktionen realisieren. Diese werden vielfach von Methoden der Künstlichen Intelligenz (KI) unterstützt.
- Schnittstellen: Weitere Anwendungen können über offene Schnittstellen integriert werden.

2.2 Funktionen und Leistungsmerkmale

Grundsätzlich können Videokonferenzen sowohl mit zwei als auch mit mehreren Teilnehmern durchgeführt werden. Auch in modernen Lösungen spiegelt sich diese Unterscheidung noch oft in den Anforderungen an die zugrundeliegende Technik wider und erfordert bei manchen Lösungen bis heute unterschiedliche Anwendungsprogramme.

An dieser Stelle wird lediglich ein Überblick über die möglichen Funktionen und Leistungsmerkmale von Videokonferenzlösungen und deren Komponenten gegeben. Der technische Aufbau und die zugrundeliegenden Architekturen werden in Kapitel 3 beschrieben.

Zu den klassischen Leistungsmerkmalen zählen neben der Echtzeit-Übertragung von Audio- und Videodaten der Teilnehmer auch die Darstellung des eigenen Video-Bildes sowie die Möglichkeit der reinen Audio-Teilnahme über eine klassische Telefonverbindung.

Im Zuge der noch immer nicht abgeschlossenen Umstellung zum IP-basierten Next Generation Network (NGN) als primäres Kommunikationsnetz der Netzbetreiber wäre grundsätzlich auch die Nutzung des NGN für Videokonferenzen analog zur Nutzung klassischer Telefoniedienste oder Videokonferenzen über ISDN möglich. Ein Vorteil läge in der Ende-zu-Ende-Dienstgüte auf den Übertragungsstrecken und der einheitlichen Nutzung des Session Initiation Protocol (SIP), welches bereits für die Telefonie genutzt wird. Dieses Modell hat sich jedoch nicht etabliert, sodass aktuell Videokonferenzen zumeist über eigene Netze der Institution auf Basis von Wide Area Networks (WAN), über die Infrastruktur von Cloud-Anbietern oder über das Internet aufgebaut werden.

Obwohl Videokonferenzsysteme in vielen Aspekten von der durch die Anwender genutzten Hardware abhängig sind, werden die zur Verfügung gestellten Funktionen und Leistungsmerkmale hauptsächlich durch die zentralen Software-Komponenten realisiert. So konnte das Leistungsspektrum von Videokonferenzsystemen in den letzten Jahren um eine Fülle von zusätzlichen Funktionen erweitert werden.

Im Folgenden werden die einzelnen Funktionen und Leistungsmerkmale, die durch moderne Videokonferenzsysteme bereitgestellt werden, betrachtet.

Verwaltung von Videokonferenzen

Der Leistungsumfang von Videokonferenzsystemen ist bei Weitem nicht auf die Konferenz an sich beschränkt. Vielmehr bieten moderne Systeme eine Vielzahl an Funktionen zur Verwaltung und zur Organisation von Videokonferenzen an. So stehen den Nutzern in Abhängigkeit von der eingesetzten Lösung mehrere Möglichkeiten zur Verfügung, um eine Videokonferenz zu planen. Zum einen bieten einige Systeme eine entsprechende Webschnittstelle zur Planung von Videokonferenzen an. Hierüber können Einladungen per E-Mail an die Teilnehmer der Konferenz gesendet werden. Zum anderen bieten viele Systeme eine Integration in Groupware-Systeme an. Hierbei können die Nutzer über ein Plug-in einem Kalender-Eintrag direkt eine Einladung zu einer Videokonferenz hinzufügen. Die Einwahl zu der Konferenz wird hierbei in der Regel über einen Link innerhalb der Einladung realisiert. Zusätzlich wird von vielen Systemen eine traditionelle Einwahlnummer für eine reine Audioverbindung über ein öffentliches oder privates Telekommunikationsnetz geboten.

Durch die Planung der Konferenzen werden meist automatisch auch die notwendigen Konferenzressourcen geprüft und reserviert. Hierdurch können etwaige Kapazitätsengpässe schon im Vorfeld einer Konferenz erkannt und vermieden werden.

Neben den geplanten, temporären Videokonferenzen können den Nutzern persönliche, virtuelle Konferenzräume dauerhaft zugewiesen werden. Diese Konferenzräume stehen dann den Nutzern jederzeit zur Verfügung, um mit weiteren Teilnehmern zu kommunizieren. Außerdem können Nutzer ad-hoc Konferenzen mit weiteren Teilnehmern innerhalb und außerhalb der Institution initiieren.

Bildverarbeitung

Während einer Videokonferenz werden verschiedene Mechanismen zur Bildverarbeitung und -optimierung zur Verfügung gestellt. Diese Mechanismen laufen in der Regel automatisiert, ohne dass die Nutzer hier eingreifen können oder müssen. Hierzu werden folgende Funktionen zur Optimierung des übertragenen Bildes genutzt:

- Wahl des Bildausschnittes (sogenanntes Cropping)

  Eine hochauflösende Kamera des Videokonferenzsystems ist in der Lage, große Teile des Raums in hoher Auflösung (beispielsweise 4K) abzudecken. Damit jedoch der oder die aktuellen Sprecher im Fokus sind, wird nur ein Teil des Bildes übertragen. Hierbei ist ein Videokonferenzsystem in der Lage, den oder die aktiven Sprecher zu erkennen und den übertragenen Bildausschnitt entsprechend anzupassen, sodass der oder die Sprecher vollständig zu sehen sind. Auf diese Weise sind die noch vielfach genutzten dreh- und schwenkbaren Kameras sowie die damit verbundene Mechanik entbehrlich.

- Unkenntlichmachung von Hintergründen

  Bei einer Videokonferenz wird typischerweise nicht nur der Nutzer, sondern auch der Hintergrund mit aufgezeichnet. Hierbei bieten einige Lösungen die Möglichkeit, diesen Hintergrund unkenntlich zu machen und somit nur den Sprecher zu übertragen. Auf diese Weise wird der Fokus auf den Sprecher und nicht auf die Umgebung gelegt, sodass sich die Teilnehmer keine Gedanken über den Hintergrund (beispielsweise das häusliche Arbeitszimmer) machen müssen. Die Unkenntlichmachung kann auch aus Gründen des Datenschutzes sinnvoll sein, wenn so nicht mehr ungewollt andere Personen oder Informationen preisgegeben werden.

- Belichtung und Kontrast

  Das von der Kamera aufgezeichnete Bild wird hinsichtlich einiger Bildparameter, z. B. Belichtung und Kontrast, so optimiert, dass ein qualitativ hochwertiges Videosignal an die Teilnehmer übertragen wird.

- Tagging von Teilnehmern

  Über eine Kopplung mit einem Verzeichnisdienst und einen Abgleich mit dort hinterlegten Bildern können die Teilnehmer identifiziert und deren Namen als Tags innerhalb der Videokonferenz dargestellt werden. Dies wird üblicherweise mit bildverarbeitenden Methoden aus dem Bereich der Künstlichen Intelligenz (KI) realisiert.

- Rednerfokus (Darstellung der verschiedenen Videosignale)

  Typischerweise werden den Teilnehmern mehrere Videosignale gleichzeitig angezeigt. Hierbei werden in Abhängigkeit von der Anzahl der Teilnehmer entweder alle anderen Teilnehmer oder nur eine Auswahl der Teilnehmer angezeigt. Dies ist insbesondere bei Konferenzen mit einer großen Teilnehmerzahl vorteilhaft. In solchen Fällen wird dann meist der Sprecher mit einem größeren Bild dargestellt, damit dieser noch gut zu erkennen ist.

Übertragenes Material

Wie bereits beschrieben, beschränken sich moderne Videokonferenzsysteme nicht mehr nur auf die Übertragung von Audio- und Videodaten, sondern bei der Nutzung von Laptops bzw. PCs oder Tablets können folgende Inhalte zusätzlich übertragen werden:

- Einzelne Anwendungsfenster
- Gesamter Desktop des Endgeräts
- Präsentationen
- Digitale Whiteboards zur gemeinsamen Bearbeitung

Darüber hinaus können auch Dateien zwischen den Teilnehmern ausgetauscht werden. Dies geschieht entweder über eine Direktübertragung zwischen den Teilnehmern oder über eine gemeinsame Dateiablage, auf die die Teilnehmer zugreifen können. Diese Dateiablage kann entweder integraler Bestandteil der Videokonferenzlösung sein oder außerhalb der Videokonferenzlösung realisiert werden.

Aufbereitung des Videomaterials

Während einer Videokonferenz kann durch das Videokonferenzsystem eine Transkodierung zwischen verschiedenen genutzten Video-Codecs durchgeführt werden. Hierdurch kann zum einen die genutzte Bandbreite optimiert werden. Zum anderen ist eine Transkodierung immer dann notwendig, wenn die Video-Endpunkte nicht den gleichen Codec unterstützen und somit die zentralen Systeme der Videokonferenzlösung (siehe hierzu Kapitel 3.2) als Vermittler agieren müssen. Eine Übersicht über die in Videokonferenzsystemen genutzten Codecs wird in Kapitel 3.4.2 gegeben.

Aufzeichnung und Nachbereitung

Videokonferenzen können aufgezeichnet werden, sodass die Audio- und Videosignale auch im Nachhinein, gegebenenfalls auch von weiteren Nutzern, betrachtet und sogar ausgewertet werden können. Eine solche Aufzeichnung kann über die Videokonferenzlösung ebenfalls verwaltet werden. Dies schließt die Speicherung der persistenten Daten sowie die spätere Bereitstellung des Materials für Nutzer mit ein.

Ein noch eher junges Leistungsmerkmal ist die automatische Transkription von Video-Aufzeichnungen, d. h. die Verschriftlichung der Sprachkommunikation. Dabei werden Methoden der automatischen Spracherkennung angewendet, welche gegebenenfalls sogar Wissen über fachspezifisches Vokabular hinzuziehen, um die Qualität der Transkription zu erhöhen. Im Ergebnis steht Teilnehmern oder weiteren Nutzern ein vollständiges Protokoll der Konferenz zur Verfügung, welches beispielsweise mit Schlagwörtern versehen werden kann.

Ein solches Protokoll kann ungleich schneller als das reine Videomaterial überflogen oder per Textsuche durchsucht werden. Dabei bleibt der Bezug zwischen Text und Videomaterial bestehen, sodass bei Bedarf an interessanten Stellen wiederum auf das Videomaterial zurückgegriffen werden kann.

Endpunkte der Videokonferenzsysteme

Um an einer Videokonferenz teilnehmen zu können, müssen den Nutzern entsprechende Endgeräte zur Verfügung stehen, die die Anfangs- und Endpunkte der Bild- und Tonübertragung darstellen. Die Spannweite der Video-Endpunkte, häufig auch Video-Terminals genannt, reicht hier von klassischen Raumsystemen, über Standard-IT-Ausstattung wie PC und Laptop und Videotelefone bis hin zu mobilen Endgeräten wie Smartphones oder Tablets (siehe Abbildung 1).

Die klassischen Raumsysteme unterscheiden Videokonferenzsysteme und Telepräsenzsysteme, die typischerweise mehrere große Monitore besitzen. Vor allem im Bereich der Raumsysteme gibt es derzeit viele Neuerungen. So sind beispielsweise Systeme am Markt verfügbar, die unter anderem eine vollständige Touch-Bedienung bieten.

Es besteht aber auch die Möglichkeit, Räume ohne dedizierte Videokonferenzausstattung entsprechend nachzurüsten. Hierbei können als Anzeige der Videokonferenz handelsübliche Projektoren oder große Monitore verwendet werden, an die Laptops oder PCs mit entsprechender Software angeschlossen werden. Zur Aufzeichnung des Videobildes und des Tons der Teilnehmer innerhalb des Raums können eine entsprechende Kamera sowie Mikrofone verwendet werden. Zusätzlich besteht die Möglichkeit, über einen HDMI-Dongle einen herkömmlichen TV-Monitor als Anzeigegerät einer Videokonferenz zu nutzen. Als kleinere Systeme stehen hier noch Tisch-Systeme oder Videotelefone mit integrierter Kamera und Mikrofon zur Wahl.

Für die Teilnahme an Videokonferenzen mit Hilfe von PCs oder Laptops stehen ebenfalls verschiedene Möglichkeiten zur Verfügung. Die Teilnehmer können entweder eine spezielle Software auf dem PC verwenden oder mit Hilfe eines Browsers an einer Videokonferenz teilnehmen. In der Regel wird bei Laptops die integrierte Kamera sowie das integrierte Mikrofon verwendet, es kann aber auch ein Headset zur Übertragung der Audio-Signale verwendet werden.

Darüber hinaus werden auch virtualisierte Clients für Videokonferenzen eingesetzt. Insbesondere bei Thin Clients ist hierfür oft eine entsprechende Zusatzausstattung für die Audio- und Videoaufnahme erforderlich.

Smartphones und Tablets haben sich mittlerweile als Selbstverständlichkeit in den Arbeitsalltag integriert. Daher ist es folgerichtig, dass auch diese Geräte als Endpunkte einer Videokonferenzlösung genutzt werden können. Hierbei kann analog zu PCs und Laptops entweder eine dedizierte Applikation des Herstellers des Videokonferenzsystems oder einfach ein Browser auf dem mobilen Endgerät genutzt werden.

Ebenfalls möglich ist eine reine Audio-Teilnahme an einer Videokonferenz beispielsweise via Telefon oder Telefonfunktion eines IP-Endgerätes, z. B. eines Smartphones. Diese Audio-Endpunkte werden im Folgenden mit den Video-Endpunkten zusammengefasst, lediglich bei spezifischen Unterschieden erfolgt eine gesonderte Betrachtung.

Leistungsmerkmale der Endgeräte

Die verschiedenen Endgeräte bieten eine Fülle an Funktionen und Integrationsmöglichkeiten mit weiteren Lösungen. So sind bei neueren Videokonferenzsystemen die Integration von Sprachsteuerung (siehe Kapitel 3) sowie eine Touch-Bedienung selbstverständlich geworden. Umgekehrt ist es aber auch möglich, mit Hilfe des Videokonferenzsystems Elemente einer intelligenten Raum- bzw. Gebäudeausrüstung zu steuern. Beispielsweise können Beleuchtung oder Verdunkelung von Fenstern reguliert werden.

Moderne Systeme verfügen darüber hinaus über eine erweiterte Diagnosefunktionalität, welche neben der Nutzung der Endpunkte und der Übertragungsqualität von Videokonferenzen auch die Auslastung der Räume erfassen kann, sofern diese Funktion aktiviert ist. Dies kann soweit gehen, dass ein Raumsystem die Anwesenheit von Personen in einem Raum beispielsweise über das Mikrofon erkennen kann. Eine solche

Funktion kann dann dazu genutzt werden, dass das Raumsystem von einem sehr energiesparenden Standby-Modus bereits erste Boot-Sequenzen durchläuft, sobald es die Anwesenheit von Personen bemerkt. Damit wird erreicht, dass die Anlage schneller für die eigentliche Videokonferenz betriebsbereit ist und lästige Wartezeiten vermieden werden.

Des Weiteren können nahezu beliebige Kombinationen aus Bildschirm, Kamera, Mikrofon und Lautsprecher genutzt werden, sofern diese entweder direkt an das Videokonferenzsystem oder mit Hilfe eines PCs oder Laptops angebunden werden können.

2.3 Einsatzgebiete

Durch den Einsatz von Videokonferenzlösungen werden virtuelle Konferenzräume geschaffen, in denen sowohl per Video- und Sprachübertragung kommuniziert als auch zu bearbeitende Inhalte übertragen werden können. Der wesentliche Mehrwert ist dabei immer die Überbrückung von geografischen Distanzen. Die Teilnehmer einer Videokonferenz können sich an unterschiedlichen Orten aufhalten und dennoch effizient miteinander kommunizieren und arbeiten.

Im Folgenden werden Einsatzgebiete aufgezeigt, welche die praktische Umsetzung dieses Ansatzes in Kombination mit dem aktuellen Marktangebot veranschaulichen und die Bandbreite der Nutzung von Videokonferenzsystemen illustrieren.

Reduktion von Reiseaufwänden und Reaktionszeiten

Über den Einsatz von Videokonferenzen kann der Reiseaufwand für Besprechungen deutlich reduziert werden. Gleichzeitig erhöht sich die Flexibilität für eine kurzfristige Reaktion auf einen akuten Besprechungsbedarf. Je mehr Funktionen die Videokonferenzlösung zur Verfügung stellt und je hochwertiger die Qualität der Umsetzung und Übertragung ist, desto besser kann die Lösung als Ersatz für Reisetätigkeiten genutzt werden.

So können inzwischen auch mobile Teilnehmer an Konferenzen gemeinsam mit aufwendigen Raumsystemen teilnehmen und dafür ihre mobilen Endgeräte nutzen, zum Beispiel Tablets oder Smartphones. Solche Teilnehmer müssen zwar gegenüber Nutzern von Video-Endpunkten mit zweckoptimierter Hardware Einbußen bei der Dialog-Qualität hinnehmen, jedoch werden diese Einbußen zugunsten der hohen Flexibilität vielfach hingenommen.

Typische Anwendungsfälle zur Reduktion von Reiseaufwänden und Reaktionszeiten sind Projekttreffen von verteilt arbeitenden Teams. Hierbei wird es den Mitgliedern des Teams ermöglicht, gemeinsame Besprechungen durchzuführen, ohne dass sich die Teilnehmer am gleichen Ort aufhalten müssen. Ein weiterer Anwendungsfall, der zunehmend an Bedeutung gewinnt, sind Bewerbungsgespräche, die nicht mehr zwingend als Vor-Ort-Gespräch stattfinden müssen, sondern mit Hilfe von Videokonferenzen flexibel durchgeführt werden können. Dadurch müssen die Bewerber keine aufwendigen Reisen durchführen.

Schaffung einer möglichst natürlichen Besprechungssituation

Der Einsatz von Videokonferenztechnik ermöglicht den Sichtkontakt zwischen Teilnehmern, ähnlich einem Gespräch von Angesicht zu Angesicht. Dies erlaubt insbesondere auch Interaktionen über Gestik und Mimik, welche bei einem Telefonat verloren gehen. Dadurch kann eine persönlichere Atmosphäre geschaffen werden, wodurch sich neben der Qualität auch die Art der Kommunikation verändert. Vielfach ist gerade dieser psychologische Effekt wichtig, um die Wahl zwischen persönlichem Treffen und Videokonferenz zugunsten der digitalen Option zu entscheiden.

Dieses Anwendungsgebiet wurde in der Vergangenheit vielfach über klassische Telepräsenzsysteme abgedeckt, welche insbesondere auf der Leitungsebene von Institutionen genutzt wurden. Inzwischen können jedoch auch vielfach moderne Standardsysteme genutzt werden und der potenzielle Nutzerkreis hat sich allein durch die Verfügbarkeit von leistungsfähiger Konferenztechnik erweitert.

Entscheidend ist in diesem Kontext jedoch die Qualität der Übertragung und der Konferenztechnik. Einfache Laptop-Kameras sind womöglich nicht ausreichend, um den Eindruck natürlicher Kommunikation und Interaktion zu erzeugen, da der Blick in eine Laptop-Kamera oft zu einer als unnatürlich empfundenen Perspektive des Teilnehmers führt. Je nach Einsatzzweck ist eine möglichst natürliche Gesprächssituation eine wesentliche Voraussetzung für eine geeignete Akzeptanz einer Konferenz zwischen Teilnehmern an verschiedenen Aufenthaltsorten.

Flexible Erweiterung von Besprechungen um entfernte Teilnehmer

Klassische Besprechungen können mit Hilfe von Videokonferenztechnik sowohl geplant als auch spontan um zusätzliche, auch entfernte Teilnehmer erweitert werden. Beispielsweise können Spezialisten zu einem Fachthema hinzugezogen werden.

Vielfach sind klassische Besprechungsräume mit technischen Hilfsmitteln zum Darstellen von Inhalten oder zur Nutzung von digitalen Whiteboards ausgestattet. Bei modernen Videokonferenzsystemen lässt sich die Nutzung dieser Hilfsmittel typischerweise auch auf virtuelle Besprechungen erweitern.

Erweiterung von Text- oder Sprachdialogen

Moderne Anwendungen aus dem Bereich UCC legen einen starken Fokus auf die Unterstützung der Zusammenarbeit von Teams. Dabei wird als Basisdienst ein persistenter (Gruppen-)Textchat zur Kommunikation genutzt. Allerdings besteht immer die Möglichkeit, aus dem Chat-Fenster heraus eine Konferenz zu starten, um Diskussionen zu beschleunigen oder Probleme kurzfristig zu lösen. Analog dazu können Telefonate oder Audiokonferenzen mit einem Mausklick zu Videokonferenzen erweitert werden, um das Konferenzerlebnis zu verbessern oder Inhalte zu präsentieren.

Die Ergebnisse der Konferenzen können im gemeinsamen Team-Bereich abgelegt werden, sodass sie für die Mitlieder des Teams zugänglich sind und im weiteren Projektverlauf genutzt werden können.

Dieser starke Fokus auf die Zusammenarbeit von flexiblen Teams spiegelt eine globale Entwicklung in der Arbeitswelt wider. Demnach orientieren sich immer mehr Institutionen weg von festen Fachbereichen und Zuständigkeiten hin zu flachen Hierarchien und dynamischen Arbeitsgruppen. Mit den klassischen Kommunikationswerkzeugen kann diese Entwicklung jedoch nicht vollzogen werden.

Erweiterung des Einsatzspektrums von Spezialisten

Die Verfügbarkeit von Spezialisten kann drastisch erhöht werden, wenn durch Videokonferenzsysteme die jeweilige Expertise über flexible Datenverbindungen anstelle von Außeneinsätzen genutzt werden kann.

Mit der richtigen Ausrüstung ist es zum Beispiel möglich, dass ein Techniker im Außeneinsatz bei einem schwierigen Problem kurzfristig einen Spezialisten hinzuzieht. Dieser beurteilt die Situation über das Videobild und kann mit entsprechenden Software-Werkzeugen sogar visuelle Hilfestellungen aus dem Bereich der Augmented Reality nutzen, um den Techniker bei der Lösung des Problems zu unterstützen. Dabei trägt der Techniker ein geeignetes Headset, welches sein Sichtfeld überträgt und es dem Spezialisten ermöglicht, Einblendungen für den Techniker darzustellen. So können beispielsweise Bauteile im Sichtfeld des Technikers visuell markiert werden.

Ein weiteres Beispiel ist der Bereich der Telemedizin. Ein Spezialist oder eine zusätzliche Anwendung aus dem Bereich der Medizintechnik können Patientendaten analysieren oder direkt mit Patienten oder Pflegekräften interagieren, ohne dafür vor Ort zu sein. Dadurch können Fachärzte effizient an mehreren Institutionen eingesetzt oder sogar physische Hausbesuche ersetzt werden.

2.4 Abgrenzung zu anderen Anwendungen und Systemen der TK

Im Zuge der Integration der verschiedenen Kommunikationsdienste für Text, Sprache und Video in übergreifende Anwendungen, kombiniert mit einer Vielzahl von Zusatzdiensten, ist die Videokonferenz nunmehr als ein Dienst unter vielen zu betrachten. Dies gilt beispielsweise für moderne UC-Lösungen, die neben Erreichbarkeitsdiensten auch Dienste zur Text-, Sprach- und Videokommunikation anbieten. Darüber hinaus etablieren sich UCC-Lösungen am Markt, die diese Dienste auf Mehrpunkt-Verbindungen ausweiten und sie um weitere Zusatzdienste zur Zusammenarbeit erweitern.

Im Fokus dieses Kompendiums stehen daher nicht nur die Plattformen mit Videokonferenzen (VK) als solche, sondern insbesondere die Integration von Videodiensten in diese Systeme und die dafür notwendigen Schnittstellen (siehe Abbildung 3). Mit Videokonferenzdiensten verwandte Dienste wie die Übertragung von Bildschirminhalten oder Whiteboard-Funktionen werden ebenfalls betrachtet.

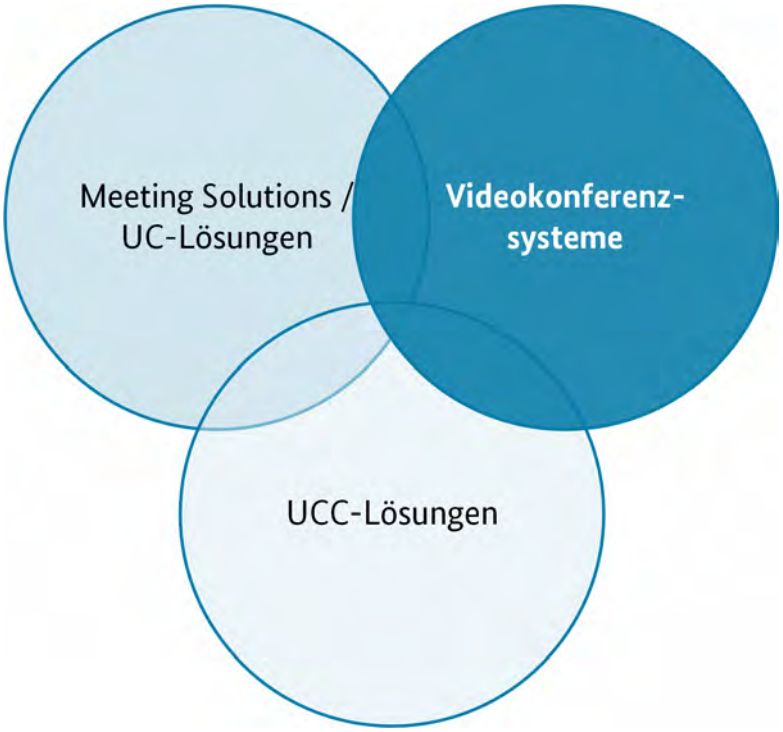

Abbildung 3: Betrachtete Technologien

Weitere Dienste im Umfeld dieser Anwendungen wie Textnachrichtendienste, Telefonie oder gemeinsame Bearbeitung von Dokumenten werden zwar im Rahmen der Integration in Videokonferenzen betrachtet, jedoch werden deren zugrundeliegenden Technologien nicht betrachtet. Gleiches gilt für Zusatzdienste, wie zum Beispiel Methoden der Künstlichen Intelligenz.

Nicht betrachtet werden weiterhin Konferenzlösungen, welche auf ISDN-Technik basieren. Zwar befinden sich solche Systeme weiterhin im Einsatz, allerdings hat es in diesem Umfeld in den letzten Jahren keine grundlegenden Änderungen gegeben. Daher gelten für diese Technik weiterhin die Ausführungen in der Technische Leitlinie Sichere TK-Anlagen des BSI (siehe [BSI TLSTK-2014]).

Ebenfalls nicht im Fokus dieses Kompendiums sind auf bestimmte Anwendungen spezialisierte Systeme zur Videoübertragung sowie Systeme für die bevorzugte Übertragung eines einzelnen Datenstroms zu vielen Endpunkten, wie sie beispielsweise für sogenannte Townhall Meetings genutzt werden.

3 Technischer Aufbau

Derzeit existiert eine Vielzahl unterschiedlicher Videokonferenzlösungen mit verschiedenen, teilweise hybriden Ansätzen. Diese Vielfalt ist primär bedingt durch die noch immer nicht abgeschlossene Ablösung von ISDN und die gleichzeitig fortschreitende Etablierung von Cloud-basierten Videokonferenzlösungen. In diesem Kapitel werden die verschiedenen Ausprägungen und die zugrundeliegenden Komponenten und Technologien betrachtet. Dabei spielt zunächst die Unterscheidung zwischen Systemen, die klassisch innerhalb einer Institution (On-Premises) aufgebaut werden, und Cloud-basierten Diensten eine entscheidende Rolle. Als zusätzliche Option werden hybride Systeme betrachtet.

Sowohl bei On-Premises-Installationen als auch bei Cloud-basierten Lösungen werden prinzipiell die gleichen Komponenten benötigt, um bestimmte Dienste zur Verfügung zu stellen. Deshalb werden zunächst die grundlegenden Komponenten einer Videokonferenzlösung dargestellt, unabhängig davon, ob diese Teil einer On-Premises-Installation oder einer Cloud-Lösung sind. Im Anschluss erfolgt eine detaillierte Erläuterung der Varianten On-Premises, Cloud und Hybrid. Schließlich wird die Integration weiterer Dienste und umgebender Systeme sowie die dafür notwendigen Protokolle und Schnittstellen dargestellt.

3.1 Grundlegende Funktionsweise

In den folgenden Abschnitten werden zunächst einige Grundlagen zur Übertragung von Videokonferenzen über IP-Netze dargestellt. Hierbei werden einerseits die Übertragung der Daten als auch die Speicherung von Daten betrachtet.

3.1.1 Übertragung von Daten

Die Übertragung mittels IP-basierter Protokolle bei Videokonferenzen unterscheidet sich wesentlich von der ISDN-Technologie, welche verbindungsorientiert und leitungsvermittelnd arbeitet. Bei der Übertragung mittels IP-basierter Protokolle werden die Signalisierungs- und Nutzdaten zwischen den zentralen Systemen der Videokonferenzlösung und den Video-Endpunkten, d. h. den Nutzerschnittstellen, grundsätzlich paketvermittelt übertragen. Die Nutzdaten enthalten die Audio- und Videodaten, gemeinsam auch als Mediendaten bezeichnet, und werden in zwei Medienströmen übertragen, einen Medienstrom für die Audiodaten und einen Medienstrom für die Videodaten. Dabei werden Signalisierungs- und Mediendaten als Datenpakete über ein gemeinsames IP-Netz übertragen. Die Pakete werden also nicht mehr über dedizierte Signalisierungs- und Nutzkanäle übertragen, sondern werden individuell anhand der im Paket spezifizierten Informationen vermittelt. Bei der Übertragung wird in der Regel kein Unterschied zwischen Signalisierungsdaten, Datenpaketen für Sprache bzw. Video und Datenpaketen für andere Anwendungen gemacht, sofern dies in den Netzkomponenten nicht explizit konfiguriert wird.

In IP-basierten Netzen bestehen technologiebedingt Bandbreitenschwankungen für die einzelnen Kommunikationsbeziehungen. Außerdem können einzelne IP-Pakete aufgrund der Routing-Entscheidungen verschiedene Wege durch das Netz nehmen und dadurch sogar in unterschiedlicher Reihenfolge beim Empfänger eintreffen. Dadurch drohen Qualitätsverluste bei der Übertragung der Mediendaten durch Paketverluste, Verzögerungen (Delay) und durch Jitter, d. h. der Schwankung des Delay. Allgemein gilt: Je höher Delay oder Jitter sind, desto schlechter ist die realisierbare Sprach- und Bildqualität.

Für die Signalisierung wird das Session Initiation Protocol (SIP) oder H.323 verwendet. Bei Browser-basierten Konferenzen über WebRTC-Verbindungen kann die Signalisierung über verschiedenste

Protokolle wie WebSocket oder XMLhttpRequest (XHR) erfolgen. Für der Übertragung der Mediendaten wird analog zu VoIP-Systemen meist das Real-Time Transport Protocol (RTP) eingesetzt, das auf dem User Datagram Protocol (UDP) basiert. Eine Übersicht über die verwendeten Protokolle und deren Funktion wird in Kapitel 3.4.2 gegeben.

3.1.2 Speicherung von Daten

Im Rahmen der Realisierung der verschiedenen Funktionen werden sowohl durch die Komponenten der Videokonferenzlösung als auch durch externe Dienste vielfältige Daten gespeichert. Dazu zählen insbesondere die folgenden Daten:

- Konfigurationsdaten der Komponenten
- Benutzerdaten
- Protokolldaten zu durchgeführten Videokonferenzen (typische Metadaten)
- (persistente) Chat-Nachrichten
- Dateien, die von den Nutzern in einer Datei-Ablage gespeichert werden
- Aufzeichnungen von Videokonferenzen

Vielfach werden dabei personenbezogene Daten gespeichert. Dies trifft insbesondere auf Verbindungsinformationen sowie sämtliche nutzerbezogenen Daten zu.

Die Speicherung der Daten kann in Abhängigkeit der Architektur und der jeweiligen Komponente, die die Daten speichert, innerhalb der Videokonferenzlösung oder mittels externer Dienste und Speicherorte geschehen. Dabei kann es sich bei den Datensätzen sowohl um flüchtige Daten, die nur während einer Konferenz gespeichert werden, als auch um persistente, d. h. dauerhaft gespeicherte Daten handeln.

3.1.3 Verschlüsselung von Daten

Die Verschlüsselung der Daten findet bei Videokonferenzlösungen auf verschiedenen Ebenen je nach Art der Daten statt. Grundsätzlich kann zwischen drei Arten von Verschlüsselung der Daten unterschieden werden:

- Verschlüsselung der Daten bei der Signalisierung
- Verschlüsselung bei der Übertragung der einzelnen Medienströme
- Verschlüsselung bei der Speicherung von Daten

Eine Ende-zu-Ende-Verschlüsselung ist bei der Signalisierung und beim Transport der Mediendaten zwar grundsätzlich wünschenswert, in der Praxis lässt sich diese jedoch nur unter bestimmten Voraussetzungen realisieren. Bei der Beschreibung der Komponenten in Kapitel 3.2.1 wird genauer auf diese Problematik eingegangen.

3.1.4 Integration von Mehrwertdiensten

Videokonferenzen konnten bereits vor der Umstellung der Übertragungstechnik auf IP-basierte Protokolle neben der Übertragung von Audio- und Videodaten zusätzliche Dienste einbinden. So können den Teilnehmern beispielsweise eine Präsentations- oder Chat-Funktion zur Verfügung gestellt werden. Solche zusätzlichen Funktionen sind entweder Bestandteil der Videokonferenzlösung oder werden von ergänzenden Mehrwertdiensten zur Verfügung gestellt. Diese können über diverse Schnittstellen und Protokolle in der Videokonferenzlösung genutzt werden. Kapitel 3.4 gibt eine Übersicht zu den vielfältigen Schnittstellen und Protokollen, die dazu eingesetzt werden.

3.2 Komponenten einer Videokonferenzlösung

Wie bereits in Kapitel 2.2 dargestellt, bieten moderne Videokonferenzlösungen eine Vielzahl an Funktionen. Um diese Funktionen bereitstellen zu können, sind verschiedene Komponenten notwendig. Hierzu zählen insbesondere die zentralen Dienste einer Videokonferenzlösung sowie die Video-Endpunkte (siehe Abbildung 4).

Die Komponenten stehen nicht immer als eigenständige Einheiten in einer Videokonferenzlösung zur Verfügung. In der Regel werden mehrere Komponenten in einer Einheit zusammengefasst. Die Aufgabe der Komponenten innerhalb der Videokonferenzlösung bleibt damit jedoch unverändert.

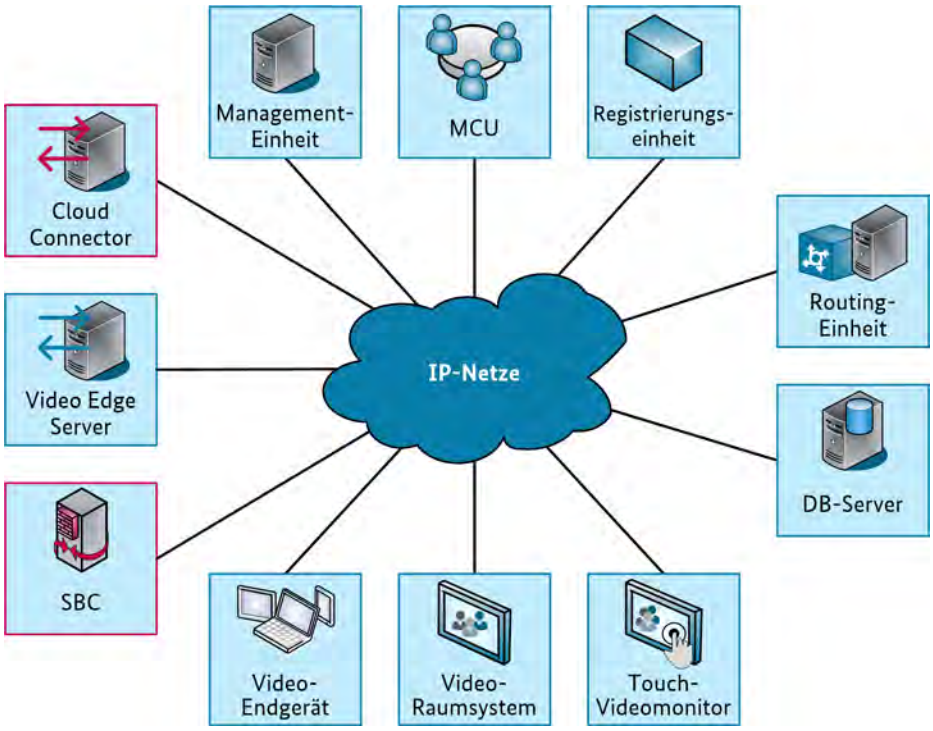

Abbildung 4: Komponenten von Videokonferenzsystemen

In diesem Kapitel werden die folgenden Komponenten genauer betrachtet:

- Multipoint Control Unit (MCU)
- Registrierungseinheit
- Routing-Einheit
- Management-Einheit
- Session Border Controller (SBC)
- Cloud Connector
- Video Edge Server
- Optionale Komponenten eines Videokonferenzsystems
- Video-Endpunkte

Der direkte Kontakt der Teilnehmer erfolgt über die Video-Endpunkte, die die Anfangs- und Endpunkte der Bild- und Tonübertragung darstellen. Video-Endpunkte umfassen dedizierte Endpunkte wie Raumsysteme und Video-Telefone sowie multifunktionale Video-Endgeräte. Video-Endgeräte können

wiederum Desktop-Systeme wie Standard-PC-Systeme, aber auch mobile Endgeräte wie Laptops, Tablets, Smartphones und gegebenenfalls sogar Geräte des Internet of Things (IoT) sein.

Darüber hinaus können auch reine Audio-Endgeräte, z. B. Telefone oder Telefonfunktion von Endgeräten, in eine Videokonferenz eingebunden werden.

3.2.1 Multipoint Control Unit

Multipoint Control Units (MCUs) sind Komponenten, welche als Verteiler zwischen Endpunkten betrieben werden. Sie dienen dem Management von Konferenzschaltungen und steuern den Austausch von Mediendaten zwischen Konferenzteilnehmern. MCUs sind auch unter dem Begriff Mehrpunkt-Videokonferenzbrücken bekannt.

Eine MCU kann auf unterschiedliche Arten realisiert werden. Es existieren sowohl Hardware- als auch Software-Lösungen, die als eigenständige Lösung verfügbar sind oder in andere Komponenten integriert werden. Der Positionierung kann On-Premises oder in der Cloud erfolgen.

MCUs kommen häufig bei Gruppenkonferenzen mit mehr als zwei Teilnehmern zum Einsatz, sind jedoch nicht zwingend notwendig (siehe Abbildung 5). Vor allem bei größeren Teilnehmerzahlen sind sie jedoch ein Mittel, um die Anzahl der nötigen Verbindungen zu reduzieren. Eine MCU empfängt die Mediendaten jedes Konferenzteilnehmers und verteilt sie auf alle anderen Teilnehmer. Die empfangenen Medienströme werden dabei dekodiert, verarbeitet und erneut kodiert, bevor sie wieder versendet werden. Bei der Verarbeitung kann z. B. ein Videosignal herunter skaliert werden, um die benötigte Bandbreite an die Kapazität des Empfängers anzupassen. Zu den weiteren Funktionen von MCUs gehören unter anderem die Weiterleitung der Signalisierung, das Aufzeichnen von Mediendaten und die Transkodierung zwischen verschiedenen Formaten (siehe Kapitel 3.4.2).

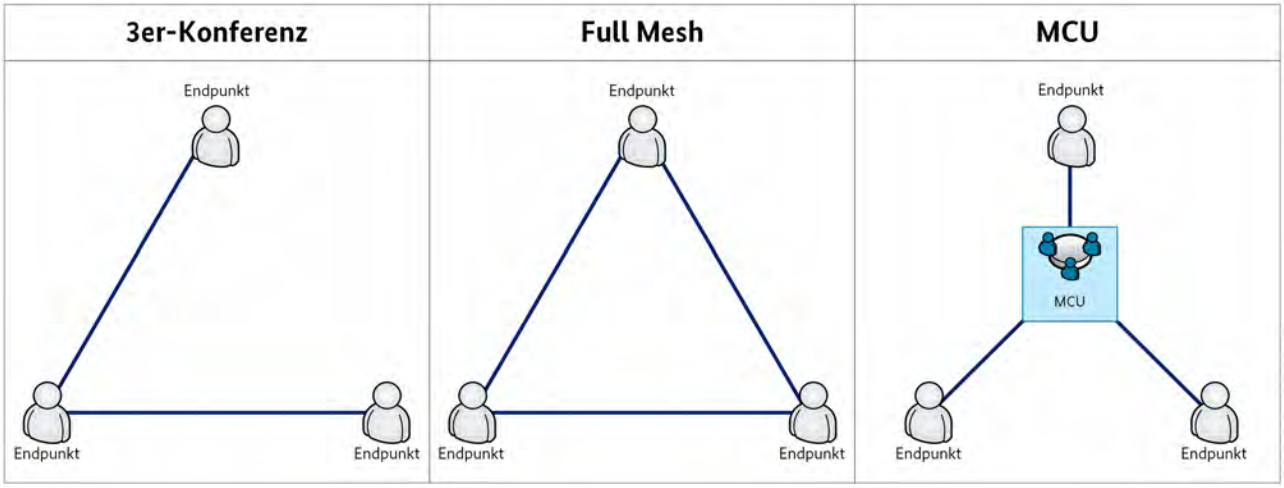

Abbildung 5: Topologievarianten für 3er-Konferenz mit und ohne MCU-Einsatz

Durch MCUs kann die Netzlast, die durch Videokonferenzen entsteht, verringert werden. Einerseits wird die Anzahl der Medienströme reduziert, da jeder Konferenzteilnehmer nur eine Verbindung zur MCU unterhält. Andererseits werden überflüssige Nutzdaten vermieden, da Videosignale herunter skaliert werden, wenn sie nicht in voller Qualität verarbeitet werden müssen, da sie am Endpunkt nur als ein Teilbild dargestellt werden.

Innerhalb einer Videokonferenzlösung können auch mehrere MCUs eingesetzt werden. Diese dienen dann in abgesetzten Standorten einer Institution als Konzentrator, da zwischen den MCUs die Mediendaten nur einmal übertragen werden müssen.

Werden die Mediendaten einer Videokonferenz verschlüsselt, bildet eine MCU üblicherweise einen Verschlüsselungsendpunkt, da sie in der Regel auf die Inhalte der Medienströme zugreift. Dieser Umstand

erfordert, dass die MCU durch geeignete Schutzmaßnahmen abgesichert wird. Die Sicherheitsparameter werden zwischen MCU und jedem Konferenzteilnehmer separat ausgehandelt. MCUs können bezüglich der Verschlüsselung konfiguriert werden, sodass z. B. nur verschlüsselte Mediendaten akzeptiert werden. Bei Einsatz einer MCU kann jedoch keine echte Ende-zu-Ende-Verschlüsselung der Medienströme erreicht werden. Eine Ende-zu-Ende-Verschlüsselung kann nur in dem Sinne erreicht werden, dass die Medienströme zwischen Teilnehmer und MCU verschlüsselt werden.

Technisch ist es zwar möglich, dass eine MCU lediglich als Verteilungspunkt agiert, die Medienströme also ohne Verarbeitung an die Konferenzteilnehmer verteilt. In dem Fall kann eine Ende-zu-Ende-Verschlüsselung der Medienströme zwischen den Teilnehmern erreicht werden. Dann geht jedoch jegliches Optimierungspotenzial sowie mögliche Zusatzdienste der MCU verloren. Zudem müssen die an der Videokonferenz beteiligten Endpunkte jeweils die Medienströme aller anderen Teilnehmer entschlüsseln und die Mediendaten verarbeiten. Dies kann in Abhängigkeit von der Teilnehmeranzahl der Videokonferenz eine nicht unerhebliche Belastung für die Hardware der jeweiligen Endpunkte bedeuten. Außerdem wird eine MCU, die nur als Sternpunkt fungiert und die Medienströme nicht aktiv verarbeitet, von den Herstellern der Videokonferenzsysteme nicht empfohlen und somit nur eingeschränkt unterstützt.

Eine weitere Besonderheit bei der Realisierung einer Ende-zu-Ende-Verschlüsselung der Medienströme stellen Teilnehmer dar, die sich nur per Audio über öffentliche Telekommunikationsnetze einwählen. Da diese Netze in Verantwortung der jeweiligen Provider (PSTN/NGN sowie Mobilfunknetz) liegen, kann auf die Übertragung der Audiodaten kein Einfluss genommen werden. Daher muss damit gerechnet werden, dass Audiodaten, sofern sie über öffentliche Telekommunikationsnetze übertragen werden, nicht im Sinne einer Ende-zu-Ende-Verschlüsselung abgesichert werden.

Somit ist eine Ende-zu-Ende-Verschlüsselung der Medienströme zwischen den Endpunkten der Videokonferenz zwar technisch möglich, jedoch nur mit einigen Einschränkungen realisierbar.

3.2.2 Registrierungseinheit

Die Registrierungseinheit übernimmt primär die Funktionen der Zugangskontrolle der Video-Endpunkte. Das bedeutet, dass sich die Video-Endpunkte an der Registrierungseinheit anmelden und so Zugang zu den zentralen Diensten erhalten. Dadurch können in der Registrierungseinheit die registrierten Endpunkte eingesehen werden. Insbesondere bei älteren Videokonferenz-Raumsystemen erfolgt eine Registrierung in der Regel manuell bei der Installation und Inbetriebnahme. Bei neueren Video-Endpunkten kann bei der Inbetriebnahme der Endpunkte eine automatische Registrierung sowie Authentisierung zum Beispiel mittels Zertifikaten erfolgen.

Die Registrierungseinheit ist bei SIP und H.323 unterschiedlich aufgebaut. Bei SIP wird die Rolle durch den SIP-Registrar, bei H.323 durch den Gatekeeper umgesetzt. WebRTC-basierte Lösungen nutzen zur Registrierung Webtechniken (siehe Kapitel 3.4).

3.2.3 Routing-Einheit

Die Routing-Einheit übernimmt die Auflösung der Adressen und das Routing der Signalisierung. Somit erfolgt der Verbindungsaufbau über die Routing-Einheit, während der Austausch der Mediendaten typischerweise über MCUs oder direkt zwischen den Endpunkten erfolgt.

Bei SIP werden die Rollen durch Proxy-Server und Redirect-Server umgesetzt. Bei H.323 erfolgt dies durch den Gatekeeper.

3.2.4 Management-Einheit

Die Management-Einheit beinhaltet die Verwaltung von Konferenzräumen und anderen Ressourcen, inklusive der Reservierung von Nutzer-Zuordnungen. Dies beinhaltet auch die Verwaltung von PINs oder Passwörtern für den Zugang zu einer Videokonferenz.

Häufig werden Schnittstellen zu einer Groupware-Anwendung erforderlich, z. B. für die Einladungen zu einer Videokonferenz in Verbindung mit der Buchung der zugehörigen Ressourcen. Dabei werden Verweise in der Form eins Uniform Resource Locators (URL) erstellt, welche auf die entsprechende Videokonferenz verweisen. Diese Verweise können im Anschluss zum Beispiel über einen Instant-Messaging-Dienst oder per E-Mail versendet werden.

Sehr verbreitet sind Plug-ins für Groupware-Anwendungen, welche bei der Erstellung einer Termineinladung die Kopplung zur Management-Einheit verwalten und den Verweis auf die notwendigen Ressourcen in den Termineintrag integrieren.

Die Management-Einheit beinhaltet auch eine Benutzerverwaltung. Diese ermöglicht dem Administrator, den Nutzern der Videokonferenzlösung Rechte zuzuweisen. Dazu gehören beispielsweise Berechtigungen zur Erstellung von geplanten Videokonferenzen oder die Zuteilung eines persönlichen virtuellen Konferenzraums. Um die beschriebenen Funktionalitäten zu gewährleisten, müssen Daten über Nutzer und Geräte gespeichert werden. Dabei ist es im Einzelfall interessant, wo die Daten abgelegt werden (siehe Kapitel 3.1.2).

Darüber hinaus muss die Videokonferenzlösung selbst konfiguriert werden können. Dazu gehören Einstellungen der vernetzten Systemkomponenten sowie der Video-Endpunkte.

3.2.5 Session Border Controller

Session Border Controller (SBC) sind Sicherheitselemente, die am Netzrand eingesetzt werden. Sie dienen der Zugangskontrolle und regeln Verbindungen über Netzgrenzen hinweg durch die Freigabe von Ports. Eingehende Signalisierungen sowie Medienströme werden dazu anhand bestimmter Merkmale unterschieden, etwa durch Absender und Empfänger. SBCs können so konfiguriert werden, dass sie nur bestimmte Verbindungen zulassen, während andere blockiert werden.

Grundsätzlich realisiert der SBC eine Protokollvalidierung für alle übertragenen Daten (Signalisierungs- und Mediendaten), wobei die Kommunikation auch über Network Address Translation (NAT) erfolgen kann. Werden verschiedene Protokolle im VoIP-Netz genutzt, erfolgt die Umsetzung dieser Protokolle im SBC. Solche Grundfunktionalitäten werden ergänzt um eine Firewall-Funktion für die VoIP-Protokolle, die gegebenenfalls durch einen Signalisierungs- und RTP-Proxy ergänzt wird und Schutz vor Attacken wie z. B. vom Typ Denial of Service (DoS) bietet.

Ein SBC agiert somit als Application Layer Gateway, das audio- und videospezifische Sicherheitsfunktionen bietet. Zu beachten ist hierbei jedoch, dass SBCs auf die Behandlung von Audio- und Videodaten spezialisiert sind und somit keinen Ersatz für eine traditionelle Firewall bieten. SBCs werden oft in Kombination mit SIP-Trunks eingesetzt. Ein SIP-Trunk bezeichnet dabei die Verbindung zwischen verschiedenen IP-basierten Systemen. Dies kann bei einem Übergang zu einem Provider, bei der Verbindung mit Videokonferenzsystemen einer anderen Institution sowie bei der Verbindung mit weiteren Telekommunikationssystemen wie UC- oder UCC-Systemen der Fall sein.

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

- Limitierung der Bandbreite

  Dies kann für alle Gespräche insgesamt oder je Gespräch erfolgen und wird dann gegebenenfalls von Call Admission Control (CAC) genutzt.

- Call Admission Control

  Mittels CAC können Verbindungsanforderungen nach festgelegten Regeln, z. B. Verfügbarkeit der erforderlichen Bandbreite, akzeptiert oder abgelehnt werden, um eine geforderte Dienstgüte für die Sprachübertragung gewährleisten zu können.

- Traffic Shaping

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

Bei der Übertragung der Mediendaten, d. h. der Medienströme, übernimmt der SBC die folgenden Funktionen, die sich zum Teil mit denen einer MCU überschneiden:

- Umwandlung von Codecs (Transkodierung)

  Die nutzbaren Sprach- und Video-Codecs können eingeschränkt werden, sodass z. B. für die Audiodaten nur G.711 A-law und G.729 verwendet werden dürfen.

- Entfernung bzw. Modifikation VoIP-spezifischer Header
- Priorisierung von markierten IP-Paketen entsprechend den Festlegungen während der Signalisierung

Da der SBC sowohl Signalisierung als auch die Medienströme terminiert, muss der SBC bei verschlüsselten Medienströmen zwingend als Verschlüsselungsendpunkt dienen können. Daher ist der SBC eine entscheidende Sicherheitskomponente, die eine entsprechende Vertrauenswürdigkeit haben muss.

Hersteller von Videokonferenzlösungen bieten zum Teil proprietäre Videokonferenz-Gateways an. Diese realisieren ähnlich wie ein SBC Übergänge in andere Netze. Diese Übergänge können jedoch grundsätzlich auch durch einen herstellerunabhängigen SBC realisiert werden, da dieser weitgehend ähnliche Funktionen bietet.

3.2.6 Cloud Connector

Ein Cloud Connector stellt eine Komponente dar, die die Kommunikationsverbindung zwischen einer Cloud-basierten Videokonferenzlösung und dem Netz der Institution aufbaut und absichert. Typischerweise authentisiert und verschlüsselt der Cloud Connector die gesamte Kommunikation zwischen der Cloud-Lösung und den jeweiligen Standorten der Institution (siehe Abbildung 6). Insbesondere werden keine eingehenden Verbindungen angenommen, die nicht von einem entsprechenden Cloud Connector des Cloud-Dienstes initiiert wurden.

Als Sicherheitskomponente muss ein Cloud Connector in einer DMZ positioniert werden. Abhängig vom Cloud-Dienst wird eine Cloud Connector unterschiedlich realisiert, beispielsweise:

- Wird ein Cloud-Dienst als Infrastructure-as-a-Service (IaaS) realisiert, kann ein Cloud Connector durch ein VPN-Gateway realisiert werden.
- Wird ein Cloud-Dienst als Software-as-a-Service (SaaS) realisiert, kann ein Cloud Connector durch ein eventuell bereits bestehendes Secure Web Gateway realisiert werden.

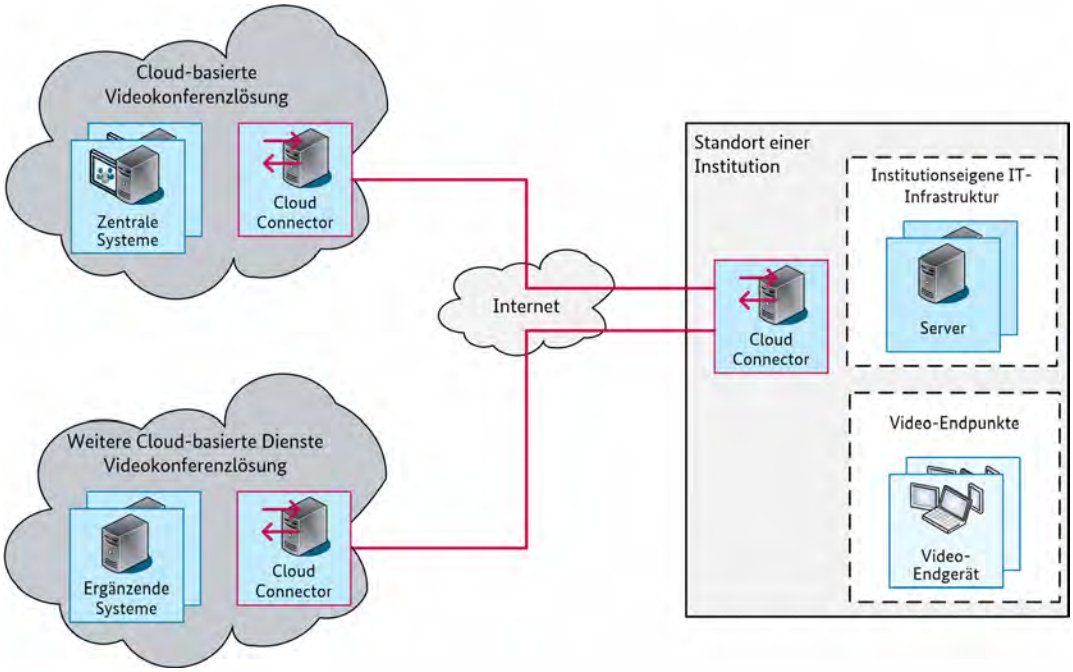

Abbildung 6: Cloud-Connector-Nutzung bei Cloud-basierter Videokonferenzlösung

3.2.7 Video Edge Server

Edge-Komponenten führen üblicherweise eine Datenverarbeitung am Rand (englisch Edge) des Netzes durch, d. h. am Übergang zwischen einem Provider oder einer Cloud und dem institutionseigenen Netz. Je nach Ausprägung kann eine solche Komponente eine Cloud-Komponente darstellen, die on-premises positioniert ist, aber vom Cloud-Provider betrieben wird (siehe [NIST SP-2018]). In Videokonferenzlösungen soll damit bei einer Cloud-basierten Realisierung eine Optimierung des Datenstroms bzw. die Einsparung von Bandbreiten erreicht werden.

Realisiert wird dieser Ansatz über sogenannte spezielle Server, im Folgenden Video Edge Server genannt. Im Falle von Videokonferenzlösungen aus der Cloud bündeln diese unterschiedliche Datenströme, ähnlich der Funktionsweise einer MCU. Dadurch wird ein zusätzlicher Sternpunkt gebildet.

Ein Video Edge Server kann zum Beispiel dann sinnvoll eingesetzt werden, wenn bei einer Cloud-basierten Videokonferenz mit vielen Teilnehmern mehrere Teilnehmer an einem Standort, zum Beispiel dem Hauptsitz einer Institution, teilnehmen. Da sich alle Teilnehmer mit einer MCU in der Cloud verbinden müssen, werden ohne Video Edge Server mehrere parallele Datenströme zur MCU aufgebaut. Diese erzeugen eine unnötig hohe Belastung des Netzes oder des Internetzugangs. In diesem Fall kann ein Video Edge Server die ausgehenden Verbindungen der Teilnehmer des Standorts in einen einzelnen Datenstrom bündeln und an die MCU weiterleiten (siehe Abbildung 7). Gleiches gilt für die Verbindung in Gegenrichtung. Die Datenströme aller übrigen Teilnehmer außerhalb des Standorts können an der MCU gebündelt und von dort aus zum Video Edge Server gesendet werden. Der Video Edge Server teilt diesen Datenstrom wiederum individuell auf die lokalen Teilnehmer des Standorts auf.

Um diese Funktionen ausführen zu können, muss der Video Edge Server die Datenströme entschlüsseln und anschließend wieder verschlüsseln. Es handelt sich demnach um einen weiteren Verschlüsselungsendpunkt in der Verbindungskette.

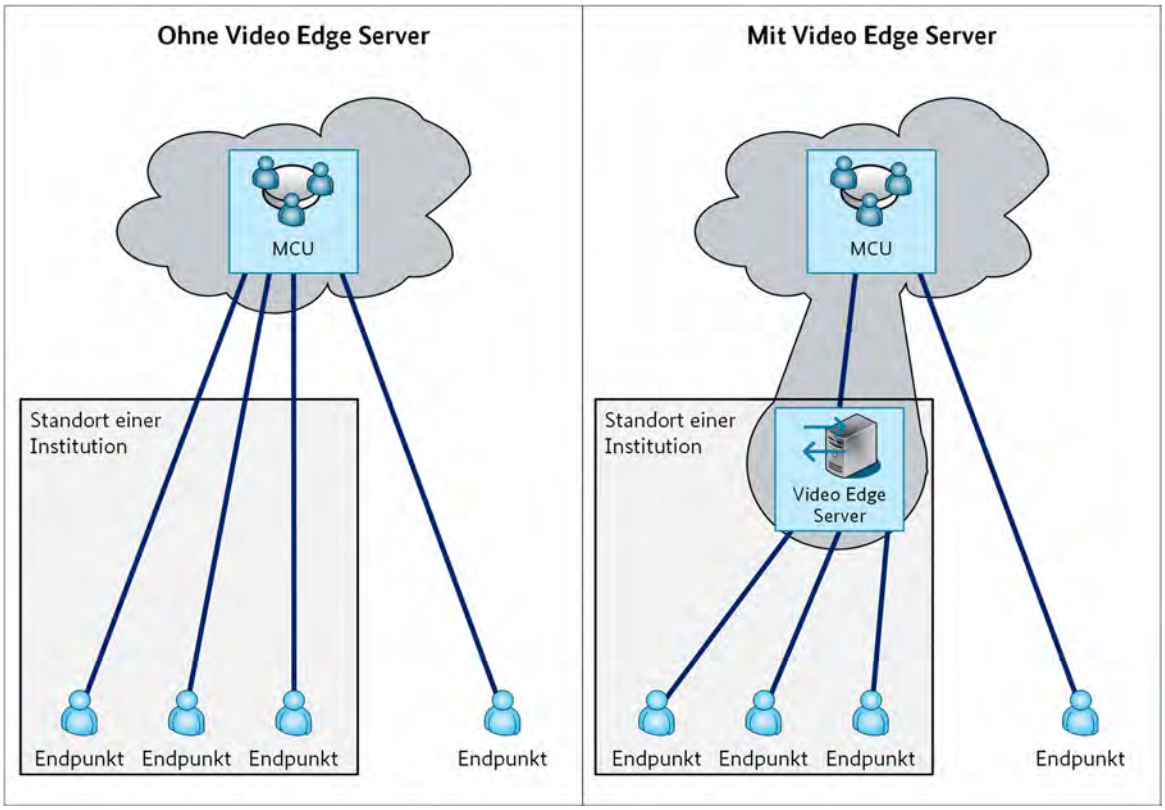

Abbildung 7: Topologie mit und ohne Video Edge Server bei Nutzung einer Cloud-basierten MCU

3.2.8 Weitere Komponenten

In diesem Abschnitt werden Komponenten für Dienste beschrieben, die zwar für die Bereitstellung der Funktionalität für Videokonferenzen prinzipiell nicht notwendig sind, aber in modernen Videokonferenzlösungen häufig bereitgestellt werden.

Erreichbarkeitsanzeige

In vielen Kommunikationslösungen mit Funktionalitäten für Videokonferenzen werden Dienste eingesetzt, welche die Erreichbarkeit bzw. Präsenz eines Nutzers anderen Nutzern signalisieren. Die Erreichbarkeitsanzeige der Nutzer wird typischerweise durch einen separaten Dienst zur Verfügung gestellt, der mit der Videokonferenzlösung interagiert. Der Erreichbarkeitsdienst, häufig auch als Präsenzdienst bezeichnet, bezieht Erreichbarkeitsinformationen einzelner Anwender wahlweise vom Groupware-Client oder vom Groupware-Server. Zusätzlich werden weitere Informationen aus dem zentralen Videokonferenz-Routing, z. B. Belegt-Status, bezogen. Weitere Informationen zu Erreichbarkeitsdiensten können dem BSI-Dokument [BSI TLSTK-2014] entnommen werden.

Chat

Chat, auch als Instant Messaging bezeichnet, ist ein Zusatzdienst, der von modernen Videokonferenzlösungen in der Regel zur Verfügung gestellt wird und bei verschiedenen Lösungen sehr unterschiedlich ausgeprägt sein kann. Ein wichtiges Merkmal ist die Persistenz von Chats. Persistente Chats können dauerhaft von den Nutzern eingesehen und genutzt werden.

Die Aufzeichnung und Archivierung von Chat-Inhalten kann somit ein wichtiger Bestandteil eines Chat-Dienstes sein und findet sich aus diesem Grund in zahlreichen Produkten wieder. Der Chat-Dienst kann entweder direkt als Bestandteil der Videokonferenzlösung oder als separates System mit Schnittstellen zur Videokonferenzlösung realisiert sein.

Weitere Informationen zum Chat-Dienst können dem BSI-Dokument [BSI TLSTK-2014] entnommen werden.

TLS Inspection

Eine verschlüsselte Kommunikation zwischen Konferenzteilnehmern kann an bestimmten Punkten, meist Firewall oder Load Balancer, terminiert werden, um eine TLS (vormals SSL) bzw. HTTPS Inspection vorzunehmen. Dies ermöglicht, die Paketdaten auf schadhafte Inhalte zu untersuchen. Durch die Entschlüsselung der Pakete können nicht nur die Verbindungsinformationen, sondern auch die Nutzdaten auf Anwendungsebene analysiert werden. TLS Inspection bietet im Rahmen von Videokonferenzen jedoch bezogen auf die übertragenen Videodaten nur begrenzten Nutzen, da diese üblicherweise nicht durchsucht werden. Die Analyse beschränkt sich auf Nutzdaten wie Signalisierung und API-Aufrufe sowie auf Zusatzdienste wie beispielsweise Chat oder eine Statusnachricht der Erreichbarkeitsanzeige.

3.2.9 Video-Endpunkte

Es existiert eine Vielzahl unterschiedlicher Video-Endpunkte, über die Nutzer an Videokonferenzen teilnehmen können. Verfügbar sind einerseits Hardware-Lösungen in Form von Komplettsystemen, z. B. Raumsystemen, und in Form von einzelnen Teilkomponenten, wie Monitor und separate Kamera. Andererseits existieren auch reine Software-Lösungen, die auf PCs mit Standard-Betriebssystemen und entsprechender Standard-Peripherie betrieben werden können. Ebenso gibt es Apps, mit denen Smartphones und Tablets als mobile Endgeräte für Videokonferenzen genutzt werden können.

Darüber hinaus sind auch reine Audio-Teilnehmer in eine Videokonferenz integrierbar. Hierzu gehören Hardware-Lösungen wie Telefone, aber auch Software-Lösungen wie die Telefonfunktion eines Smartphones.

Hardware-Lösungen

Hardware-Lösungen können darauf ausgelegt sein, die vollständige Ausstattung eines Konferenzraums bereitzustellen. Hierzu gibt es Raumsysteme, die alle erforderlichen Komponenten wie Bildschirme, Kameras und Mikrofone als dedizierte Komponenten zur Verfügung stellen oder sie in einem einzigen Gerät integrieren. Letztere sind in unterschiedlichen Größen verfügbar, typischerweise im Bereich von 20 bis 90 Zoll mit einer Auflösung zwischen 1080p und 2160p. Kameras sind häufig schwenkbar und bieten eine Zoom-Funktion. Neuere Raumsysteme beinhalten keine schwenkbaren Kameras mehr, sondern beinhalten Kameras mit sehr hohen Blickwinkeln und Auflösungen. Ihre Auflösung ist in der Regel größer als die der angeschlossenen Bildschirme, sodass nur ein Ausschnitt des kompletten Bildes übertragen wird. Die Netzanbindung erfolgt kabelgebunden oder drahtlos. Raumsysteme sind meist als kompakte Geräte verfügbar, die an einer Wand befestigt oder mit einem Bodenstativ aufgestellt werden können.

In diesem Kontext sind auch Telepräsenz-Lösungen zu nennen, die als erweitere Raumsysteme konzipiert sind und die Immersion während Videokonferenzen möglichst weit verstärken sollen. Telepräsenz-Lösungen bestehen meist aus mehreren hochauflösenden Monitoren, Kameras und Mikrofonen und sind oft mit passenden Tischen und Sitzen fest im Konferenzraum verbaut. In der Vergangenheit kam häufig spezielle technische Ausstattung wie etwa in Hardware realisierten Codec-Einheiten zum Einsatz. Mittlerweile existieren jedoch auch Raumsysteme, die sich in Bild- und Tonqualität und durch die Nutzung mehrerer Bildschirme Telepräsenz-Systemen annähern, sodass die Unterschiede zwischen Telepräsenz- und Videokonferenz-Lösungen abnehmen. Nichtsdestotrotz erfüllen diese Systeme einen speziellen Bedarf und werden weiterhin produziert und genutzt.

Videotelefone stellen eine kompakte Form von Endpunkten dar. Sie ähneln üblichen (VoIP-)Telefonen und bestehen aus einer Basisstation und einem Hörer. In der Basisstation sind jedoch zusätzlich ein Bildschirm zur Video-Übertragung und eine Kamera integriert. Aufgrund der kompakten Bauart und Größe eignen sich Videotelefone für den Betrieb an Schreibtisch-Arbeitsplätzen. Videotelefone können außerdem unabhängig von der PC- und Arbeitsplatzausstattung eingesetzt werden.

Mit Hardware-Teilkomponenten kann auch eine bereits vorhandene Standard-Ausstattung zu einem vollwertigen Endpunkt für ein Videokonferenzsystem ausgebaut werden. Einige Hersteller liefern z. B. Produkte, die bereits eine Kamera, ein Mikrofon und eine Netzanbindung beinhalten und die an einen beliebigen Monitor angeschlossen werden können. Auch einzelne Kameras, Headsets und Freisprecheinrichtungen, auch Konferenz-Spinnen genannt, werden im Zusammenhang mit Videokonferenzlösungen angeboten. Weiterhin existieren Geräte, die lediglich die Netzanbindung realisieren und die mit beliebiger Peripherie kombiniert werden können.

Software-Lösungen

Um an Videokonferenzen teilzunehmen, können ebenso reine Software-Clients genutzt werden. Diese werden entweder auf einem PC installiert oder in Form einer Browser-Anwendung verwendet. Dazu muss der PC sowohl mit einer Kamera als auch mit einem Headset ausgerüstet sein. Im Falle eines Laptops können diese Lösungen auch mobil genutzt werden. Darüber hinaus existieren Software-Clients ebenfalls in Form von Apps, die auf Smartphones oder Tablets installiert werden können.

Eine Besonderheit stellen hier noch Umgebungen mit virtualisierten Desktops dar. Hierbei rangieren die Lösungen von einer reinen Applikationsvirtualisierung über Terminal Server bis hin zur einer vollständigen Desktop-Virtualisierung über eine Virtual Desktop Infrastructure (VDI). Die in dem BSI-Dokument [BSI TLSTK-2014] beschriebenen Probleme bezüglich Sprachübertragung bei virtualisierten Clients haben bei Videokonferenzlösungen ein besonderes Gewicht, da die übertragene Datenmenge und die Echtzeit-Anforderungen deutlich höher sind.

Außerdem ist zwischen dem Einsatz von physischen Thin Clients und typischen Fat Clients mit Browser oder Soft Thin Client zu unterscheiden. Im Gegensatz zu Thin Clients sind Fat Clients vollwertige Desktop-Computer, die ausreichend Prozessorkapazität und Ressourcen wie Speicher, Laufwerke, Grafikkarten etc. beinhalten. Bei Thin Clients besteht die Herausforderung in der Verarbeitung der Medienströme. Diese müssen bei Thin Clients im Normalfall zentral auf dem Terminal Server oder dem virtualisierten Client auf einer VDI-Lösung terminiert und verarbeitet werden, denn zwischen Thin Client und zentraler Komponente werden nur Bildschirmänderungen, Tastatur und Maus-Bewegungen per Terminal-Server-Protokoll übertragen, z. B. via Remote Desktop Protocol (RDP) oder Independent Computing Architecture (ICA). Diese Protokolle haben jedoch oft Schwierigkeiten mit dem Echtzeitcharakter von Sprach- und Videoübertragungen. Daher gibt es Ansätze, Sprache und Video doch auf dem Thin Client (z. B. per Application Streaming) zu terminieren, der dann an dieser Stelle wieder als Fat Client zu betrachten ist.

Zusätzliche Peripherie

Weitere, zum Teil optionale Peripheriegeräte erweitern den Funktionsumfang einer Videokonferenzlösung oder tragen zum Bedienkomfort bei. Weit verbreitet sind Fernbedienungen, mit denen Endgeräte via Infrarot oder Bluetooth vom Sitzplatz aus gesteuert werden können. Zu diesem Zweck existieren auch spezielle Tablets, die sowohl als flexible Eingabegeräte als auch als zusätzliche Bildschirme genutzt werden können. Für Konferenzräume gibt es zudem digitale Whiteboards. Darauf geschriebene oder gezeichnete Inhalte können während einer Konferenz direkt an andere Teilnehmer übertragen werden.

Zur drahtlosen Verbindung mit mobilen Endgeräten wie Laptops, Tablets und Smartphones mit Konferenzlösungen sind dedizierte Kopplungsgeräte verfügbar. Zwischen mobilem Gerät und Kopplungsgerät wird eine Funkverbindung hergestellt, während das Kopplungsgerät via WLAN, Ethernet oder HDMI mit der Videokonferenzlösung verbunden wird. Vom Mobilgerät können dann, z. B. über eine Browser-Anwendung, Bildschirminhalte oder Dateien geteilt werden.

Zur Steuerung von Videokonferenz-Lösungen können auch Sprachassistenten eingesetzt werden. Funktionen wie das Erstellen von Konferenzen, die Einladung von Teilnehmern und die Annahme von Anrufen kann so via Sprachsteuerung erfolgen.

3.3 Architekturen

Bei modernen Videokonferenzlösungen haben sich seit der Verbreitung von Diensten aus der Cloud sehr unterschiedliche Architekturen etabliert. Dabei werden zwar grundsätzlich die oben genannten Komponenten eingesetzt, jedoch befinden sich diese an grundlegend unterschiedlichen Standorten.

Der Austausch der Video- und Audiodaten zwischen den Komponenten nutzt die zwei Ebenen Signalisierung und Übertragung der Mediendaten (siehe Kapitel 3.4.2). Bei allen Standards, insbesondere ISDN, H.323 und SIP, wird zuerst auf der Signalisierungsebene die Verbindung ausgehandelt und aufgebaut. Erst danach erfolgt die Übertragung der Mediendaten. Die genannten Standards unterscheiden sich im Detail bei der Signalisierung und der Medienübertragung in den genutzten Protokollen und Codecs.

Die einzelnen Dienste einer Videokonferenzlösung werden häufig in einzelnen Komponenten zusammengefasst. Bei den Lösungen in der Cloud ist die Aufteilung der Dienste auf die zur Realisierung eingesetzten Komponente für den Cloud-Kunden im Regelfall sogar intransparent, da dieser lediglich einen Dienst bestellt und die technische Lösung dahinter vollständig in den Verantwortungsbereich des Anbieters fällt.

Grundsätzlich kann demnach zwischen Videokonferenzlösungen, die On-Premises installiert werden, und Lösungen aus der Cloud unterschieden werden. Hinzu kommt ein großes Spektrum von Hybridlösungen, die sowohl On-Premises-Dienste als auch Dienste aus der Cloud einsetzen.

3.3.1 On-Premises

Bei den traditionellen On-Premises-Architekturen werden sämtliche zentrale Komponenten, die zur Nutzung der Videokonferenzlösung benötigt werden, typischerweise im Rechenzentrum der Institution implementiert. Dies schließt insbesondere auch Gateways zur Anbindung an das öffentliche Telekommunikationsnetz sowie das Internet ein. Auch die Endgeräte, die von den Nutzern der Institutionen zur Teilnahme an Videokonferenzen verwendet werden, sind typischerweise im Netz der jeweiligen Institution eingebunden. Dies schließt die Anbindung abgesetzter Außenstellen via WAN oder Site-to-Side VPN sowie die Integration externer Teilnehmer über VPN-Verbindungen ein.

Im Mittelpunkt der Videokonferenzlösung (siehe Abbildung 8) steht die Systemlandschaft mit den zentralen Komponenten. Diese realisieren die Registrierung der Endpunkte und das Routing der Signalisierung mittels SIP oder H.323. Ein weiteres Kernstück einer Videokonferenzlösung ist die MCU, die die verschiedenen Videoströme verarbeitet und Ressourcen für Videokonferenzen vorhält. Außerdem werden Gateways für die Durchführung von Videokonferenzen mit internen und externen Videokonferenzsystemen eingesetzt. Um diese zentralen Systeme gruppieren sich gegebenenfalls weitere Dienste und Komponenten (siehe Kapitel 3.2.8).

Für die zentrale Systemlandschaft muss der Aspekt der Verfügbarkeit von Diensten und Daten entsprechend umgesetzt werden. Fallen zentrale Infrastrukturen aus, so kann der entsprechende Dienst nicht genutzt werden. Im Fall von kritischen Komponenten käme dies dem Ausfall der gesamten Konferenzfunktion gleich. Gleiches gilt für die Netzinfrastruktur zwischen den zentralen Komponenten und Endpunkten.

Grundsätzlich können die zentralen Komponenten eines Videokonferenzsystems auch als Virtuelle Maschinen (VM) auf einem Virtualisierungs-Host betrieben werden, sofern der Hersteller diese Betriebsform unterstützt. Dies gilt sogar für MCUs. Dabei sind jedoch die folgende Aspekte zu berücksichtigen, die im BSI-Dokument [BSI TLSTK-2014] ausführlich für VoIP beschrieben sind:

- Die VMs konkurrieren bei einer Überbuchung des Virtualisierungshosts um Ressourcen, was sich negativ auf die Leistung des Videokonferenzsystems auswirken und im schlimmsten Fall für den Nutzer deutlich spürbar sein kann.

- Die Anforderungen bezüglich Bandbreite und Echtzeit-Übertragung sind bei Videokonferenzen erheblich höher als bei einer reinen Sprachübertragung, sodass sich Probleme weitaus intensiver auswirken.
- Die zentralen Komponenten eines Videokonferenzsystems verarbeiten schützenswerte Daten, die häufig mit einem erhöhten Schutzbedarf hinsichtlich Vertraulichkeit und Integrität verbunden sind. Hier ist insbesondere die Frage zu klären, ob die Schutzmaßnahmen der Virtualisierungslösung ausreichen, um solche VMs mit anderen gegebenenfalls unsicheren VMs zusammen auf einem Virtualisierungs-Host betreiben zu dürfen, oder ob hier eine physische Trennung notwendig ist.

An eine Videokonferenzlösung sind oft eine Vielzahl weiterer Server und Dienste angebunden, im Folgenden Umsysteme genannt. Hier sind insbesondere die folgenden Dienste und Server relevant:

- Datenbanken
- Verzeichnisdienst
- Identitätsmanagement, in Form eines Identity and Access Management (IAM)
- Groupware-Server

Zur Anbindung externer und mobiler Teilnehmer sowie zur Bereitstellung eines Gateways für Web Real-Time Communication (WebRTC) zur Einbindung in Webangebote wird typischerweise ein Access Server in der Demilitarisierten Zone (DMZ) betrieben, der an das Videokonferenzsystem gekoppelt ist. In der DMZ wird zudem ein Web-Server zur Bereitstellung von WebRTC-Angeboten bereitgestellt. Aus Komplexitätsgründen wurde in der grafischen Darstellung nur eine einheitlichen DMZ dargestellt, eine eventuelle Unterteilung in weiteren Netzzonen bzw. Sicherheitszonen wird nicht betrachtet. Für die Einbindung von Außenstellen und zur Anbindung an das öffentliche Telekommunikationsnetz werden entsprechende Gateways und Access Server bereitgestellt. An großen Außenstellen kann zudem eine weitere MCU bereitgestellt werden. Zur Zonierung zwischen Außenstellen und zentralem Standort bzw. den Übergängen in das öffentliche Netz können Security Appliances, z. B. Firewalls, Intrusion Prevention Systems, Intrusion Detection Systems oder SBC, zum Einsatz kommen. Je nach Sicherheitsanforderungen kann auch in den Außenstellen eine Absicherung über Sicherheitskomponenten wie Firewall und SBC realisiert werden.

In Abbildung 8 sind als exemplarische Teilnehmer am Zentralstandort und in den Außenstellen jeweils ein Videokonferenz-Client auf einem PC, Tablet oder Smartphone sowie ein herkömmliches Videoraumsystem und ein Touch-Videomonitor abgebildet. Die Teilnehmer der Außenstellen sind per WAN mit der zentralen Videokonferenzlösung verbunden. Zudem sind externe Teilnehmer dargestellt, die sich via Internet bzw. über das öffentliche Telekommunikationsnetz mit den zentralen Systemen verbinden.

Die in diesem Kapitel beschriebenen Nutzungsaspekte von Videokonferenzen machen deutlich, dass bei einer modernen On-Premises-Lösung erhöhte technische Herausforderungen bestehen. Dies gilt insbesondere für Videokonferenzen über Vertrauensgrenzen hinweg, internationale Videokonferenzen und die Einbindung von weltweit verteilten mobilen Video-Teilnehmern.

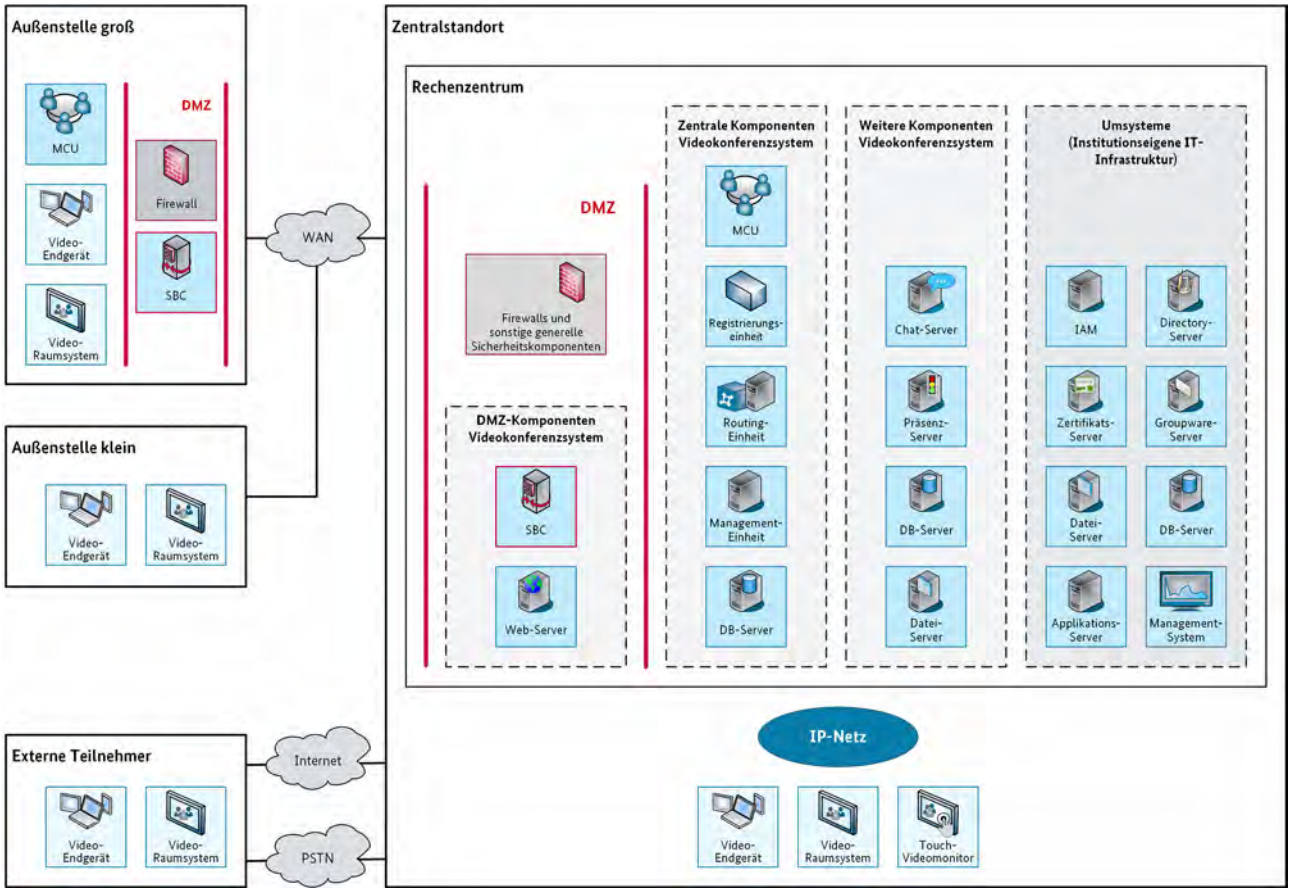

Abbildung 8: On-Premises-Architektur für Videokonferenzsysteme

3.3.2 Cloud

Der globale Trend zu IT-Diensten aus der Cloud kann insbesondere auch bei Videokonferenzlösungen beobachtet werden. Fast jeder Anbieter von Videokonferenzlösungen hat inzwischen Dienste aus der Cloud im Angebot und vielfach werden ausschließlich Lösungen aus der Cloud angeboten.

Für diesen Trend gibt es viele Gründe: Nicht zuletzt sind Videokonferenzlösungen verbindende Systeme, die auf möglichst gut vernetzten Infrastrukturen mit zentralen und verteilten Komponenten aufbauen. Strukturen in der Cloud bieten dafür gute Voraussetzungen.

Eine Multipoint Control Unit (MCU) als zentrale Komponente einer Videokonferenzlösung in der Cloud bietet viele Möglichkeiten, die eine On-Premises-Variante nicht leisten kann. Ein wichtiger Punkt ist hier die Skalierbarkeit. Eine Cloud-basierte MCU kann durch die automatische Allokation zusätzlicher Ressourcen aus der Sicht des Kunden flexibel skaliert werden, sodass keine Festlegung auf eine bestimmte Anzahl unterstützter Verbindungen notwendig ist. So können zeitweise auch hohe Bedarfe an gleichzeitigen Verbindungen gedeckt werden, ohne dass dafür jederzeit die maximalen Ressourcen vorgehalten und somit auch finanziert werden müssen.

Durch die Installation in der Cloud sind solche MCUs sehr gut vernetzt und können von vielen verschiedenen Orten aus performant erreicht werden. Große Distanzen können bei stark vernetzten Anbietern über das Backbone-Netz des Anbieters überbrückt werden und unterliegen dadurch nicht der prinzipiellen Unsicherheit einer Ende-zu-Ende-Verbindung über das Internet.

Abbildung 9 gibt einen Überblick über die Architektur von Videokonferenzsystemen aus der Cloud. Die zentralen Komponenten befinden sich demnach außerhalb der institutionseigenen Infrastruktur in den

Rechenzentren des Cloud-Anbieters. Innerhalb der Institution verbleiben lediglich die Endpunkte sowie die spezifischen Komponenten zur Anbindung der Cloud, z. B. Cloud Connector. Abhängig von der eingesetzten Lösung sollte in den Standorten auch ein SBC zur Terminierung der Medienströme positioniert werden.

Darüber hinaus gibt es typischerweise ergänzende Strukturen außerhalb des Videokonferenzsystems, wobei diese vielfach ebenfalls in eine Cloud ausgelagert werden können. Dementsprechend muss auch die Integration weiterer Cloud-Dienste betrachtet werden. Dies können beispielsweise Dienste aus den Bereichen IoT oder Künstliche Intelligenz sowie Speicherdienste sein, deren Funktionen mit denen des Videokonferenzsystems verknüpft werden sollen. Darüber hinaus können dazu aber auch z. B. Groupware-, Datenbank- oder Directory-Server zählen.

Schließlich bedeutet der Einsatz einer Cloud-basierten Lösung für die jeweiligen Institutionen einen typischerweise geringeren, beziehungsweise veränderten Administrationsaufwand. Es sind weniger Konfigurationsarbeiten und dazu benötigtes Wissen erforderlich, jedoch mehr Arbeiten und Wissen für die Integration mit anderen Diensten sowie die Integration in das eigene Netz.

So lassen sich auch Verknüpfungen mit anderen Diensten aus der Cloud, wie beispielsweise mit Datenspeichern oder Verzeichnis- und damit verbundenen Single-Sign-On-Diensten, realisieren.

In Abbildung 9 sind als exemplarische Teilnehmer am Zentralstandort und in einer Außenstelle jeweils ein Videokonferenz-Client auf einem PC, Tablet oder Smartphone sowie ein herkömmliches Videokonferenzraumsystem und ein Touch-Videomonitor abgebildet. Die Teilnehmer der Außenstelle sind per WAN und Site-to-Side-VPN mit der zentralen Videokonferenzlösung verbunden, sodass in der Außenstelle auf einen SBC verzichtet werden kann. Zudem sind vereinfachend externe Teilnehmer dargestellt, die sich nur via Internet mit den zentralen Systemen verbinden. Ebenso wird zur Vereinfachung eine angemessene Absicherung der Cloud-Dienste, z. B. über Firewalls, vorausgesetzt und nicht explizit dargestellt.

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

Mittlerweile haben sich verschiedene Anbieter von Cloud-basierten Diensten im Bereich der Meeting Solutions etabliert. Diese Dienste versprechen verschiedene Charakteristika, die insbesondere für Videokonferenzlösungen vorteilhaft sind:

- Weitreichende Flexibilität in Bezug auf die räumliche Verteilung der Anwender: Selbst mobile Clients können über ihren Internetzugang meist problemlos integriert werden.
- Einheitliche Plattform für die Kommunikation über Vertrauensgrenzen hinweg
- Hohe Skalierbarkeit: Die erforderlichen Kapazitäten, z. B. bezüglich der Anzahl potenzieller Teilnehmer, müssen nicht bereits bei der Einführung der Lösung kalkuliert werden. Zusätzliche Kapazitäten, aber auch nicht mehr benötigte Kapazitäten können kurzfristig allokiert bzw. deallokiert werden. Die Leistungen werden typischerweise nutzungsbasiert abgerechnet.
- Einheitliche Nutzer- und Bedienoberflächen für heterogene und verteilte Institutionen
- Einrichtung und Bedienung durch webbasierte Administrationsoberflächen

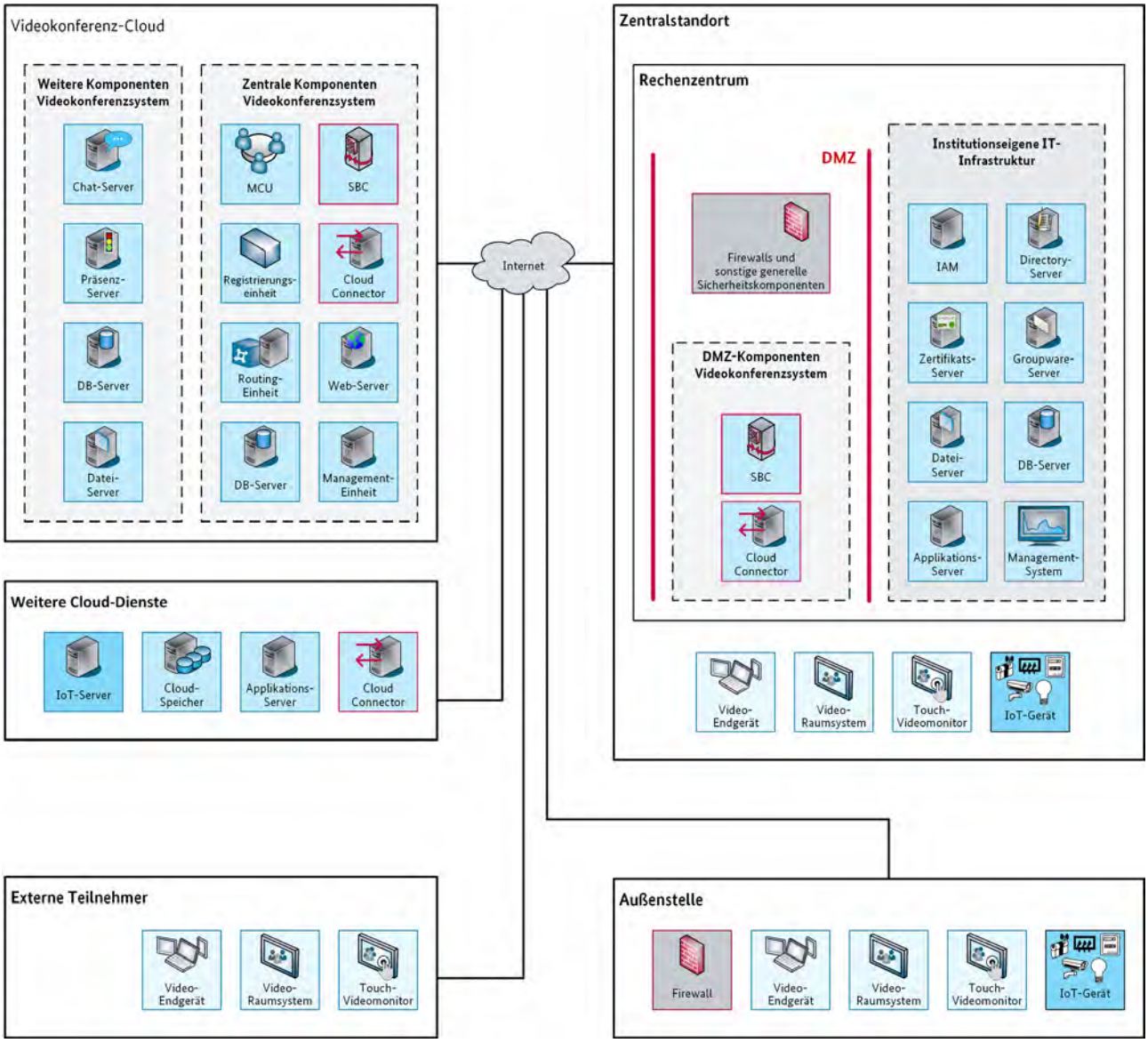

Abbildung 9: Cloud-basierte Architektur von Videokonferenzsystemen

Jedoch gibt es hinsichtlich der Datensicherheit und Verfügbarkeit einige Aspekte, die zu beachten sind.

Das Thema Datensicherheit ist besonders relevant, wenn schützenswerte Daten nicht mehr im eigenen Rechenzentrum, sondern beim jeweiligen Anbieter gespeichert sind. Der genaue Speicherort der Daten unterliegt dabei der Verantwortung des Anbieters und entzieht sich meist vollständig der Kontrolle des Kunden. Dies hat zur Folge, dass sensible Daten außerhalb der Europäischen Union gespeichert werden könnten und somit die in der EU gültige Rechtslage eingeschränkt ist. Es gelten vorrangig nationale Gesetzgebungen zur Herausgabe von Anwenderdaten desjenigen Landes, in dem die Daten gespeichert sind. So unterliegen beispielsweise Daten in US-amerikanischen Rechenzentren und gegebenenfalls sogar generell Daten bei Diensten US-amerikanischer Unternehmen dem USA Freedom Act bzw. dem CLOUD Act (Clarifying Lawful Overseas Use of Data Act).

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

Des Weiteren muss die Frage der Verfügbarkeit von Diensten und Daten auch für Cloud-Lösungen gestellt werden. Fallen beim Anbieter zentrale Infrastrukturen aus, so kann eventuell die gesamte Videokonferenzlösung nicht genutzt werden. Gleiches gilt für die Netzinfrastruktur zwischen den zentralen Komponenten in der Cloud und den Endpunkten. In der lokalen Infrastruktur behält der Cloud-Kunde weiterhin die Kontrolle, doch während Konfigurationen zur Qualitätssicherung im Wide Area Network (WAN) zumeist in Abstimmung mit dem WAN-Provider realisierbar sind, entzieht sich das Internet dem Einfluss sowohl von Kunden als auch von Providern.

Umgehen lässt sich diese Problematik durch den Einsatz von redundanten Internet-Anbindungen oder Direktverbindungen. Eine Direktverbindung ist eine bei vielen Cloud-Anbietern kostenpflichtig buchbare Verbindung mit definierten Leistungsmerkmalen zwischen den Netzen des Cloud-Anbieters und einem Übergabepunkt unter der Kontrolle des Cloud-Kunden. Dies kann je nach Anbieter ein spezielles Netz, eine Punkt-zu-Punkt Verbindung oder eine Anbindung über einen WAN-Provider sein. Mit der Hilfe von Direktverbindungen kann bei der Nutzung von Cloud-Angeboten der Weg über das Internet vermieden werden. Somit lassen sich vollständig kontrollierbare Strecken schaffen, die sowohl die Definition von Servicevereinbarungen mit verbindlichen Verfügbarkeitswerten als auch die Implementierung von qualitätssichernden Maßnahmen auf der gesamten Übertragungsstrecke erlauben.

3.3.3 Hybrid

Hybridlösungen beinhalten sowohl Komponenten einer Videokonferenzlösung aus der Cloud als auch Komponenten, die On-Premises positioniert sind. Daraus ergibt sich eine Vielzahl von möglichen Kombinationen, welche unter diese Kategorie fallen.

Hybridlösungen werden aus unterschiedlichen Gründen eingesetzt. In der Vergangenheit wurden klassische Videokonferenzsysteme häufig für institutionsinterne Videokonferenzen eingesetzt und durch sogenannte Web-Konferenzlösungen für Videokonferenzen über Vertrauensgrenzen hinweg ergänzt. Darüber hinaus gibt es diverse Dienste aus der Cloud, welche die Interoperabilität zwischen verschiedenen Videokonferenzlösungen, sowohl aus der Cloud als auch On-Premises, ermöglichen.

Seitens der Anbieter werden Hybridlösungen häufig als Übergangslösung für eine schrittweise Migration einer On-Premises-Installation hin zu einer Videokonferenzlösung aus der Cloud angeboten. Dabei werden die bestehenden Komponenten zunächst um wenige Dienste ergänzt. Im weiteren Verlauf werden dann einzelne On-Premises-Komponenten ersetzt, bis eine vollständige Lösung aus der Cloud erreicht ist, bei der die verbliebene Videokonferenz-Hardware des Cloud-Kunden lediglich aus Endpunkten besteht.

Ein relativ neuer Trend sind Video Edge Server zur Ergänzung von reinen Cloud-Lösungen (siehe Kapitel 3.2.7). Diese bündeln die erforderlichen parallelen Verbindungen zur Cloud und realisieren so ebenfalls eine Hybridlösung.

Abbildung 10 zeigt eine generische Architektur für einen Hybrid-Ansatz mit einem Video Edge Server. In der Praxis gibt es hier eine Vielzahl von Gestaltungsmöglichkeiten für Hybridlösungen, da prinzipiell die Möglichkeiten einer On-Premises- mit denen einer Cloud-Lösung beliebig kombiniert werden können.

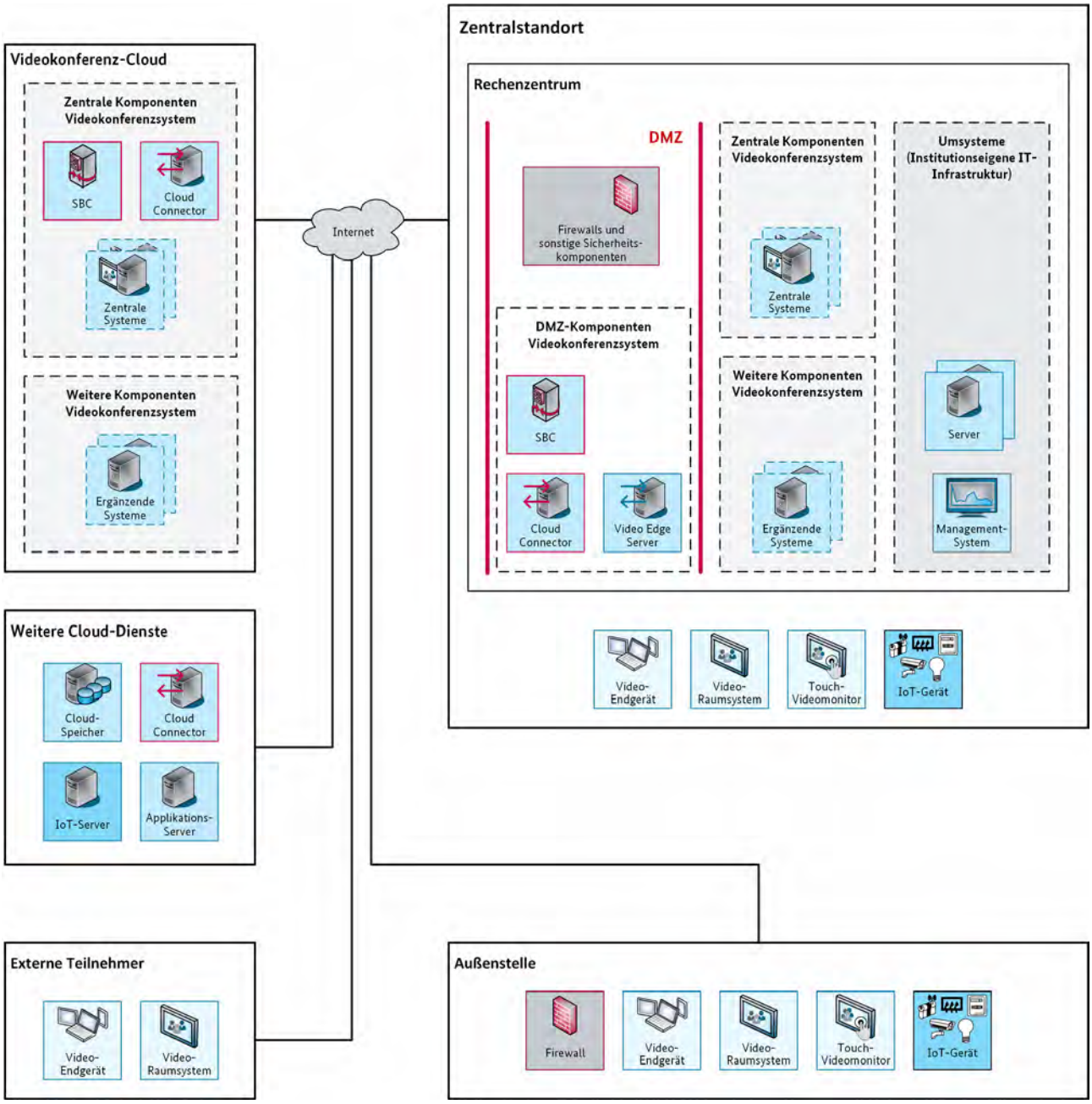

Abbildung 10: Generische Hybrid-Architektur mit Video Edge Server

3.4 Schnittstellen und Protokolle

Moderne Videokonferenzlösungen zeichnen sich durch die Kombination einer Vielfalt von Diensten zur Kommunikation und Zusammenarbeit aus. Dementsprechend muss eine Vielzahl von Schnittstellen und Protokollen unterstützt werden.

3.4.1 Integration externer Dienste

Über die eigentliche Kernfunktionalität hinaus integrieren Videokonferenzlösungen häufig zusätzliche externe Dienste. Besonders Meeting Solutions bieten zahlreiche Schnittstellen, die das Anwendungsgebiet der Videokonferenzlösung erweitern sollen. Ziel ist es dabei oft, mit dem Funktionsspektrum die technische Ausstattung eines Konferenzraums möglichst vollständig abzubilden. Zu den wichtigsten externen Diensten gehören:

Speicherdienste

Eine Verknüpfung zu Speicherdiensten und dazugehörigen Datei-Servern erlaubt es, von Endpunkten der Videokonferenzlösung auf dort gespeicherte Dateien zuzugreifen. So können während einer laufenden Konferenz z. B. relevante Dokumente geöffnet und auf dem Bildschirm geteilt werden. Ein angeschlossener Datei-Server kann auch genutzt werden, um aufgenommene Videokonferenzen zu speichern. Manche Videokonferenzlösungen besitzen bereits einen internen Speicherdienst. Dieser kann jedoch mit externen Geräten erweitert werden.

Einige Hersteller liefern dedizierte Speicherlösungen in Form von proprietären Lösungen. Es können jedoch üblicherweise auch andere Geräte, z. B. in Form eines gewöhnlichen SAN (Storage-Area-Network) oder NAS (Network-Attached Storage), verwendet werden. Die Anbindung kann über Ethernet, Fibre Channel oder Fibre Channel over Ethernet erfolgen. Speicherlösungen können üblicherweise auch in Form von Cloud-Diensten genutzt werden.

Verzeichnisdienste

Die Integration von Verzeichnisdiensten findet in den meisten Fällen über das weitgehend standardisierte Protokoll Lightweight Directory Access Protocol (LDAP, siehe [IETF RFC4511-2006]) statt. Auch ein Zugriff über proprietäre Mechanismen, z. B. Microsoft Active Directory, ist üblich. Während Verzeichnisdienste vorrangig für die Pflege interner Kontakte eingesetzt werden, werden externe Kontakte oft in separaten Datenbanken, z. B. einem Customer Relationship Management System (CRM-System), gepflegt. Diese Systeme können entweder ebenfalls über eine LDAP-Schnittstelle oder alternativ über eine Datenbankschnittstelle wie Open DataBase Connectivity (ODBC) bzw. Structured Query Language (SQL) integriert werden.

Verzeichnisdienste werden zudem häufig für die Pflege und den automatisierten Import von Benutzer-konten sowie die automatisierte Provisionierung neu angelegter Nebenstellen genutzt. In diesem Fall wird meist eine Nutzerauthentisierung im Zusammenspiel mit dem Institutionsverzeichnis per Single Sign-On implementiert, um Mehrfachauthentisierungen des Anwenders zu vermeiden.

Die Realisierung von Single Sign-On wird dabei je nach Videokonferenzlösung unterschiedlich gelöst. Bei einem vollständigen Single Sign-On werden von einem Nutzer an einem Windows-Client lediglich bei der Anmeldung an der Domäne seine Log-In-Daten abgefragt. Eine zusätzliche Authentisierung am Videokonferenz-Client auf dem PC ist somit nicht mehr notwendig. Dies wird jedoch nicht von allen Herstellern so umgesetzt. Vielfach sind zwar die Anmeldedaten der Domäne automatisch auch die Anmeldedaten des Videokonferenzsystems, jedoch muss der Nutzer diese Daten zusätzlich bei der Anmeldung am Videokonferenz-Client erneut eingeben.

Als Alternative zur Integration von Verzeichnisdiensten zur Authentisierung der Nutzer kann ein übergeordnetes IAM genutzt werden. Hierbei werden zunächst die Daten aus gegebenenfalls mehreren Verzeichnisdiensten konsolidiert, sodass Informationen zur Authentisierung der Nutzer aus einer gemeinsamen Quelle kommen.

Sofern Verzeichnisdienste oder ein IAM in die Videokonferenzlösung eingebunden werden, spielt der Zugriff auf diese im Sicherheitskonzept einer Videokonferenzlösung eine zentrale Rolle. Durch die Integration von Verzeichnis und Datenbank kann zudem ein unautorisierter Zugriff oder eine Kompromittierung von schützenswerten Daten erfolgen. Die Integration von Verzeichnisdiensten und Datenbanken muss daher sorgfältig abgesichert werden.

E-Mail-Server

Videokonferenzlösungen können mit E-Mail-Servern verbunden werden. E-Mails werden über die standardmäßig genutzten Protokolle Simple Mail Transfer Protocol (SMTP) oder Simple Mail Transfer Protocol Secure (SMTPS) verschickt und über POP3 oder IMAP abgerufen. Die Anbindung kann ebenfalls genutzt werden, um Kommunikationspartner via E-Mail zu einer Konferenz einzuladen. Dabei werden Links, mit denen Teilnehmer sich in eine Konferenz einwählen können, via E-Mail verschickt.

Anwendungsintegration

Verschiedene Arten von Anwendungen können in Videokonferenzlösungen integriert werden. In vielen Fällen liefern Hersteller Plug-ins, mit denen die Videokonferenzlösung entsprechend erweitert werden kann. Ein häufiger Anwendungsfall ist dabei die Integration von Office-Anwendungen. Dadurch können Kontaktkarten von Mitarbeitern mitsamt Verbindungsmöglichkeiten dargestellt werden. Weiterhin werden häufig Plug-ins für Groupware-Clients eingesetzt, welche die Erstellung von Videokonferenzen im bekannten Kalenderkontext ermöglichen.

UCC-Infrastruktur

Videokonferenzlösungen können in UCC-Infrastrukturen eingebunden werden. Hierdurch kann die Lösung mit zahlreichen anderen Kommunikationslösungen und -netzen verbunden werden. Dazu gehören vor allem Festnetz-, Mobilfunk-, VoIP- und Chat-Komponenten von UCC-Lösungen, die in Videokonferenzlösungen integriert werden.

Streaming-Plattformen

Laufende oder aufgezeichnete Videokonferenzen können als Live Stream auf Streaming-Plattformen wiedergegeben werden. Nutzer von Social Media und Lernplattformen können eine Konferenz über den Browser als Zuschauer mitverfolgen.

Cloud-Dienste

Viele der bereits beschriebenen Anwendungsfälle, wie etwa die Nutzung externer Speicher- und Verzeichnisdienste, können auch durch die Vernetzung mit entsprechenden Cloud-Diensten umgesetzt werden (siehe [BSI Cloud]). Dazu zählt die Integration von Office-Anwendungen, sodass z. B. Konferenzteilnehmer gemeinsam an Dokumenten arbeiten können. Weiterhin werden viele Funktionen aus dem Bereich der Künstlichen Intelligenz oder dem Internet of Things (IoT) typischerweise als Cloud-Dienste eingebunden.

Raumsteuerung

Besitzt der Konferenzraum eine technische Gebäudeausrüstung, können diese mit Videokonferenz-lösungen verbunden werden. Diese kann dann die Raumsteuerung nutzen, um z. B. bei Beginn einer Konferenz die Fenster zu verdunkeln.

Sprachassistenten und Chat Bots

Durch die Integration von Sprachassistenten und spezifischen Chat Bots kann der Bedienkomfort einer Videokonferenzlösung erhöht werden. Befehle können so via Sprachsteuerung gegeben oder in den Chat einer Konferenz eingegeben werden, um Funktionen der Videokonferenzlösung oder anderer externer Dienste zu nutzen. Sprachassistenten und Chat Bots können zumeist als Plug-ins installiert werden.

3.4.2 Protokolle

Die Übertragung von Daten über ISDN tritt angesichts der Verbreitung IP-basierter Anschlüsse an öffentliche Netze zunehmend in den Hintergrund. Details hierzu können dem BSI-Dokument [BSI TLSTK-2014] entnommen werden.

Im Folgenden wird daher ausschließlich auf die relevanten Protokolle und Codecs für die Übertragung mittels IP-basierter Netze eingegangen.

Signalisierung

Bei der Übertragung der Daten zur Signalisierung werden unterschiedliche Protokolle eingesetzt. Zu nennen sind hier insbesondere SIP und H.323.

SIP wird verwendet, um die erforderlichen Informationen für den Aufbau und die Steuerung einer Sitzung auszutauschen (siehe [IETF RFC3261-2002]). Die für eine Videoübertragung nötigen Details wie unterstützte Sprach- und Video-Codecs werden mittels des Session Description Protocol (SDP) innerhalb der SIP-Protokolldateneinheit ausgehandelt. Außerdem werden Informationen zu weiteren übertragenen Medien ausgehandelt.

Weitere Details zu SIP können dem BSI-Dokument [BSI TLSTK-2014] entnommen werden. In den letzten Jahren sind jedoch mehrere Schwachstellen bei der Implementierung von SIP bekannt geworden. Durch Manipulation der Signalisierung kann ein Video-Endpunkte zu unerwünschtem Verhalten gezwungen oder vollständig zum Absturz gebracht werden. Gründe für diese Schwachstellen liegen hauptsächlich in der unzureichenden Kontrolle von Menge und Inhalt eingehender Pakete.

Der von der International Telecommunication Union (ITU) definierte Standard H.323 ist Teil einer Reihe von Standards für die Videokommunikation mittels ISDN (siehe [ITU H323-2009]). Diese referenziert diverse Unterprotokolle, z. B. für die Rufsignalisierung (siehe [ITU H225-2009]), für die Sicherheit (siehe [ITU H235-2005]) sowie für das Öffnen und Schließen von Kanälen zur Medienübertragung (siehe [ITU H245-2011]). Der ebenfalls enthaltene Standard H.320 gibt die Rahmenspezifikation für schmalbandige Videokommunikation vor (siehe [ITU H320-2002]). H.320 umfasst entsprechende Spezifikationen für die Kommunikation von Audio, Video, Daten und Signalisierung sowie für die Steuerung. H.320 basiert auf einer Leitungsvermittlung (circuit-switched), im Gegensatz zu paketvermittelnden Protokollen (packet-switched) wie TCP/IP im Internet. Die Audio-Signale und die Video-Signale der Konferenzteilnehmer werden zum Senden digitalisiert und auf die verfügbare Bandbreite (n-mal 64 kbit/s) durch sogenannte Codecs (engl. Coder/Decoder, deutsch Kodierer/Dekodierer) verlustbehaftet komprimiert. H.320 definiert für die Übertragung von Audio-Daten die Protokolle G.711, G.722 sowie G.728 und für die Übertragung von Video-Daten die Protokolle H.261, H.263 und H.264. Die Datenübertragung erfolgt über die Standards T.120 und H.239.

Weitere Details zu H.323 können dem BSI-Dokument [BSI TLSTK-2014] entnommen werden.

Übertragung von Nutzdaten

Das Real-Time Transport Protocol (RTP) dient der Übertragung echtzeitsensitiver Daten für Unicast- und Multicast-Anwendungen (siehe [IETF RFC3550-2003]). Vornehmlich wird RTP für die Übertragung von Echtzeitdaten in Form von Sprach- und Videodaten, d. h. den Mediendaten, eingesetzt. RTP setzt auf dem User Datagram Protocol (UDP) auf. Im Gegensatz zu anderen Anwendungsprotokollen, die UDP verwenden, z. B. RADIUS (Remote Authentication Dial-In User Service), werden bei RTP-Sitzungen im Fall

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

RTP-Pakete enthalten eine Sequenznummer, um eventuell Datenverluste im Empfänger detektieren zu können. Zur Wahrung der Synchronizität enthalten RTP-Pakete einen Zeitstempel auf Basis eines Grundtaktes in Sender und Empfänger. Dabei bezieht sich dieser Zeitstempel auf den Moment, an welchem das erste Byte der RTP-Payload generiert wurde. Über diesen Zeitstempel lässt sich neben Synchronisation auch der Jitter ermitteln.

RTP besitzt keine Mechanismen, um dem Sender über empfangene Daten und eventuelle Verluste sowie über die Qualität der Übertragung (Jitter) Bericht zu erstatten. Darum wurde als Zusatzprotokoll zum RTP das Real-Time Control Protocol (RTCP) entwickelt. Es dient der Rückmeldung sowie der Aushandlung von Übertragungsparametern. Teilnehmer geben sich über RTCP periodisch eine Rückmeldung über die Qualität der empfangenen Daten, um eine flexible Anpassung des Datenstroms an die Netzqualität zu ermöglichen. Um die Bandbreite für RTP nicht durch Verwendung von RTCP einzuschränken, regulieren die Stationen auch die Frequenz der RTCP-Datenpakete.

Da bei RTP und RTCP die Daten im Klartext übertragen werden, kann die Kommunikation durch Mitschneiden der Nachrichten mitgehört werden. Daneben kann aber auch der Inhalt gezielt gefälscht werden oder durch Manipulation der Steuerinformationen ein Denial of Service (DoS) erreicht werden.

Zur Erhöhung der Sicherheit beim Real-Time Transport Protocol (RTP) wurde daher das Secure Real-Time Transport Protocol (SRTP) entwickelt und im [IETF RFC3711-2004] der IETF spezifiziert. SRTP verwendet ein symmetrisches Verschlüsselungsverfahren mit einer Schlüssellänge von mindestens 128 Bit, das auf AES basiert. Die Verwendung von AES mit Schlüssellängen 192 Bit und 256 Bit ist in [IETF RFC6188-2011] beschrieben. SRTP wird im BSI-Dokument [BSI TLSTK-2014] detailliert beschrieben.

Videokonferenzen über Webbrowser

Die Einbindung von externen Videokonferenz-Teilnehmern erfolgt häufig über einen marktüblichen Webbrowser. Die erforderliche Multimedia-Kommunikation in Echtzeit nutzt meist das Protokoll Web Real-Time Communication (WebRTC), das von allen am Markt verfügbaren Browser unterstützt wird und keine Plug-ins, Add-ons oder Client-Installationen erfordert.

WebRTC basiert auf Javascript und HTML5 und erfordert immer einen aktiven Web-Server. Die aktuell meist unterstützten Codecs bei WebRTC sind Opus für Audio- und VP8 für Videoübertragungen. WebRTC wird beim World Wide Web Consortium (W3C) als offener Standard spezifiziert (siehe [W3C RTC-2018]).

Die Spezifikation schreibt die Signalisierung für WebRTC-Verbindungen nicht verbindlich vor. Mögliche Signalisierung-Verfahren sind XMLhttpRequest (XHR), WebSocket, Server Sent Event (SSE) oder aber auch SIP über HTTPS. Alle genannten Verfahren sind verbindlich mittels TLS bzw. DTLS zu verschlüsseln. Der Transport der Mediendaten wird grundsätzlich über SRTP abgesichert.

WebRTC erfragt per Default eine Freigabe für Mikrofon und Kamera vor Beginn einer Konferenz. Dies kann jedoch individuell auch für einen generellen Zugriff konfiguriert werden.

Codecs

Zur Übertragung von Mediendaten kommen bei Videokonferenzlösungen unterschiedliche Codecs zum Einsatz. Sie werden dazu genutzt Audio- und Video-Signale zu digitalisieren. Um Bandbreite zu sparen, werden die Daten meist komprimiert. Im Zusammenhang mit Videokonferenzen werden hauptsächlich Codecs genutzt, die robust gegen Verzögerung und Datenverlust während der Übertragung sind. Wenn die Teilnehmer einer Videokonferenz unterschiedliche Codecs verwenden, müssen die Mediendaten zwischen den Teilnehmern transkodiert werden. Diese Aufgabe kann z. B. von einer MCU übernommen werden.

Codecs können aufeinander aufbauen und in unterschiedlichen Variationen, z. B. mit verschiedenen Bandbreiten, auftreten. Sie werden von verschiedenen Organisationen entwickelt und sind sowohl unter freien als auch unter proprietären Lizenzen verfügbar. Eine Übersicht der gängigsten Audio-Codecs wird in Tabelle 1 dargestellt. In Tabelle 2 sind weit verbreitete Video-Codecs aufgeführt.

Codec	Organisation	Lizenz
G.711	ITU-T	Frei
G.723.1	ITU-T	Proprietäre Implementierungen
G.726	ITU-T	Freie / proprietäre Implementierungen
G.729	ITU-T	Lizenziert von Sipro Lab Telecom
G.722	ITU-T	Frei
G.722.1	ITU-T	Royalty-Free Lizenz von Polycom
G.722.2 (AMR-WB)	ITU-T / 3GPP	Lizenziert von VoiceAge
AMR-WB+	n/a	Lizenziert von VoiceAge
Opus	IETF	3-clause BSD License
Speex	n/a	Revised BSD
iLBC	IETF	3-clause BSD
iSAC	n/a	3-clause BSD
EVS	3GPP	proprietär
AAC-ELD	n/a	proprietär

Tabelle 1: Übersicht verfügbarer Audio-Codecs

Codec	Level	Max. Auflösung	Bild-Rate	Max. Bit Rate
H.263	10	QCIF (176 x 144)	15	64 kbps
	20	CIF (352 x 288)	30	384 kbps
	60	720 x 480	60	16 Mbps
H.264 AVC	1b	QCIF (176 x 144)	15	128 kbps
	2	CIF (352 x 288)	30	2 Mbps
	3	720x480	30	10 Mbps
	3.1	720x1280 (720p, HD)	30	14 Mbps
	3.2	720x1280 (720p, HD)	60	20 Mbps
	4	1080x1920 (1080p, Full HD)	30	20 Mbps
	4.2	1080x1920 (1080p, Full HD)	64	50 Mbps
H.264 SVC	bei Berücksichtigung eines Layer ca. 10% höhere Bitrate als H.264 AVC			
	bei Berücksichtigung aller Layer ca. 30% höhere Bitrate als H.264 AVC			
H.265	1	QCIF (176 x 144)	15	128 kbps
	2	CIF (352 x 288)	30	1,5 Mbps
	3	720 x 576	37,5	6 Mbps
	3.1	720x1280 (720p, HD)	33,7	10 Mbps
	4	720x1280 (720p, HD)	68	12 Mbps
	4	1080x1920 (1080p, Full HD)	32	12 Mbps
	4.1	1080x1920 (1080p, Full HD)	64	20 Mbps
VP 8	-	720x1280 (720p, HD)	30	17 Mbps
	-	1080x1920 (1080p, Full HD)	30	23 Mbps
VP 9	-	720x1280 (720p, HD)	30	15 Mbps
	-	1080x1920 (1080p, Full HD)	30	21 Mbps
AV1	2.0 – 6.3 (vorl.)	426x240 bis 7680x4320	30 - 120	bis zu 800 Mbps

Tabelle 2: Übersicht verfügbarer Video-Codecs

4 Operative Aspekte

Die operativen Aspekte von Videokonferenzsystemen umfassen Aspekte der Planung, der Nutzung und des Betriebs, die im Folgenden betrachtet werden.

4.1 Planungsaspekte

Um die Potenziale von Videokonferenzlösungen auszuschöpfen und einen möglichst sicheren und störungsfreien Betrieb der Videokonferenzlösung zu ermöglichen, müssen bestimmte Voraussetzungen und Rahmenbedingungen geschaffen werden. Insbesondere sollten die folgenden Aspekte berücksichtigt werden.

Abstimmung der Lösung auf die vorgesehene Nutzung

Anzahl und Art der Komponenten sollten möglichst gut auf die konkret vorgesehene Nutzung und die Institution abgestimmt werden und eine geeignete technische Ausstattung bieten. Im Rahmen einer Bedarfsanalyse sollten dazu Kriterien definiert werden, die eine Videokonferenzlösung erfüllen muss. Dies betrifft auch die Ausgestaltung der Komponenten, beispielsweise den Einsatz von virtualisierten Servern und Clients.

Zudem sollte auch sichergestellt werden, dass alle für unterschiedliche Nutzungssituationen erforderlichen Komponenten in einer Lösung geeignet unterstützt werden oder zumindest miteinander kompatibel sind. Insbesondere sollten auch standortübergreifende Videokonferenzen innerhalb einer Institution sowie Videokonferenzen über Vertrauensgrenzen hinweg berücksichtigt werden.

Planung einer geeigneten Infrastruktur

Grundlegend ist auch die Planung einer geeigneten Infrastruktur, in die die Videokonferenzlösung eingebunden wird. Insbesondere betrifft dies die Netzinfrastruktur, die eine angemessene Leistung bereitstellen muss, um eine stabile Videoübertragung in hoher Qualität zu ermöglichen.

Darüber hinaus sollten aber auch Rauminfrastruktur und Videokonferenzlösung aufeinander abgestimmt werden. Beispielsweise kann ein Raumsystem nur dann einen optimalen Nutzen bringen, wenn der vorgesehene Raum geeignete akustische Eigenschaften besitzt und flexibel beleuchtet bzw. verdunkelt werden kann. Die Audio- und Videoausstattung des Raumsystems wiederum muss zur Raumgröße passen.

Auswahl und Einbindung von Video-Endpunkten

Die meisten Videokonferenzlösungen erlauben die Einbindung von Teilnehmern mit unterschiedlichen Arten von Endpunkten (siehe Kapitel 2). Wenn eine hohe Flexibilität gefordert ist, sollte die geplante Videokonferenzlösung möglichst viele verschiedenartige Endpunkte einbinden können. Dies setzt eine Unterstützung von entsprechenden Protokollen und Schnittstellen voraus. Zur Wahrung eines angemessenen Kosten-Nutzen-Verhältnisses sind die konkret geplanten Videonutzer und deren Ausstattung zu betrachten, ehe in eine besonders umfassende und hochwertige Ausstattung investiert wird.

Ein PC oder Laptop mit Headset erfüllt dabei für einen einzelnen Videokonferenz-Teilnehmer prinzipiell denselben Zweck wie ein Raumsystem. Pro Gerät verursacht eine solche Ausstattung im Vergleich zu einem Raumsystem mit spezieller audiovisueller Technik deutlich geringere Anschaffungskosten, bietet jedoch aus Sicht des Nutzers gegebenenfalls nur eine begrenzte Qualität der Videokonferenz. Außerdem muss bei der Planung berücksichtigt werden, dass im Vergleich zu einem Raumsystem eine Videokonferenz über einen PC oder Laptop gegebenenfalls keine besonders natürliche Gesprächssituation liefert. Wenn Videokonferenzen auch für Besprechungen mit einem formellen Charakter, z. B. im Rahmen

von Vorstandssitzungen eines Unternehmens, genutzt werden sollen, sind meist Raumsysteme, gegebenenfalls sogar Telepräsenzsysteme zu bevorzugen.

Das spezialisierte Raumsystem kann pro Konferenz von mehreren Personen gemeinsam genutzt werden und dies mit wechselnden Gruppen je Konferenztermin. Will man einen ähnlich großen Nutzerkreis mit einer höherwertigen Video-Ausstattung am Arbeitsplatz versorgen, kann das die Anschaffungskosten des spezialisierten Raumsystems schnell übersteigen.

4.2 Nutzungsszenarien

Grundlegende Vorteile sowie Einsatzaspekte nennt bereits die Systembeschreibung in Kapitel 2. Im Folgenden werden spezielle Aspekte betrachtet, die bei der Nutzung der Videokonferenzlösung am Arbeitsplatz, in dedizierten Besprechungsräumen und für die mobile Nutzung beachtet werden müssen.

Basis jeder Nutzung sind die entsprechenden Regelungen der Institution, die insbesondere Vorgaben hinsichtlich interner oder standortübergreifender Konferenzen innerhalb einer Institution sowie hinsichtlich Videokonferenzen über Vertrauensgrenzen hinweg spezifizieren.

Abbildung 11: Aspekte bei Nutzungsszenarien

4.2.1 Nutzung am Arbeitsplatz

Die in Kapitel 2 beschriebenen Vorteile und Einsatzmöglichkeiten können bis zu einem gewissen Grad auch mit PCs und Laptops erreicht werden. Im Vergleich mit speziell für den Videokonferenzeinsatz vorgesehenen Endgeräten haben PCs oder Laptops aber ihre Grenzen. So ist eine einfache Endgerätekamera ungeeignet, um mehrere Teilnehmer zu erfassen. Ähnliches gilt für Mikrofon und Lautsprecher, selbst wenn eine Freisprecheinrichtung an das Endgerät angeschlossen wird. Will man die qualitativen Einschränkungen mit einer optimierten Zusatzausrüstung aufheben, z. B. durch hochwertige Kameras und größere Monitore, muss man dies gegebenenfalls an vielen Arbeitsplätzen tun.

Alternativ können je nach Art und Anspruch der Videokonferenz transportable Raumsysteme bzw. Videotelefone genutzt werden.

Sofern es sich beim Arbeitsplatz nicht um ein Einzelbüro handelt, können ähnlich wie bei Telefonaten störende Einflüsse dieser Umgebung die Teilnahme an einer Videokonferenz erschweren bzw. verhindern. Darüber hinaus werden die weiteren Mitarbeiter im Büro in ihrer Tätigkeit behindert.

Diese Aspekte gelten grundsätzlich auch für Heimarbeitsplätze.

4.2.2 Nutzung dedizierter Besprechungsräume

Stehen für Videokonferenzen separate Räume zur Verfügung, wird einerseits durch die räumliche Trennung die Störung durch andere Personen vermieden und anderseits müssen die Teilnehmer der Videokonferenz nicht auf andere Anwesende im selben Raum Rücksicht nehmen.

Darüber hinaus bietet ein dedizierter Besprechungsraum die Möglichkeit, spezielle Komponenten zu nutzen:

Wird ein Raumsystem oder eine Telepräsenzlösung installiert, kann prinzipiell eine hohe Qualität für die Videokonferenz erreicht werden. Solche Lösungen sind auf die gemeinsame Teilnahme einer größeren Anzahl von Personen ausgelegt, sodass eine realitätsnahe Dialogsituation geschaffen werden kann.

Eine Zusatzausstattung wie etwa digitale, vernetzte Whiteboards kann gemeinschaftlich genutzt und flexibel in Konferenzen eingebunden werden.

Auch die Teilnahme an Videokonferenzen kann durch die Nutzung eines dedizierten Besprechungsraums mit Raumsystem flexibel gestaltet werden. Der Teilnehmerkreis der Videokonferenz kann in diesem Fall durch Hinzukommen in den Besprechungsraum einfach erweitert werden, ohne dass weitere Video-Endpunkte eingebunden werden müssen.

Solche separaten Räume oder dedizierte Besprechungsräume stellt eine Institution allerdings nur in geringer Anzahl bereit, sodass eine spontane Nutzung nicht gesichert möglich ist.

4.2.3 Mobile Nutzung

Die mobile Nutzung von Videokonferenzlösungen erfolgt typischerweise unter ungünstigeren Bedingungen als die stationäre Nutzung am Arbeitsplatz oder in einem Besprechungsraum. Die Gründe dafür sind einerseits die Kameras, Mikrofone und Displays, die auf mobilen Geräten wie zum Beispiel Laptops, Tablets oder Smartphones zur Verfügung stehen, und andererseits die eingeschränkten Netzverbindungen einer mobilen Nutzung. Dabei werden häufig Verbindungen über ein WLAN oder Mobilfunknetz zum Internet und von dort aus zur Videokonferenzlösung aufgebaut. Hierbei steht gegebenenfalls nur eine geringe Bandbreite zur Verfügung, sodass die Bild- und Sprachqualität reduziert ist. Zudem ist bei der mobilen Nutzung typischerweise die Umgebung des mobilen Teilnehmers nicht unter Kontrolle der Institution, sodass Bildbearbeitungstechniken zum Ausblenden des Hintergrundes an Bedeutung gewinnen.

Allerdings stehen bei der mobilen Nutzung von Videokonferenzlösungen nicht der Komfort, die Qualität oder die realitätsgetreue Darstellung der Teilnehmer im Vordergrund. Vielmehr werden diese Einbußen in Kauf genommen, um die Teilnahme an einer Videokonferenz überhaupt zu ermöglichen.

Nichtsdestotrotz sollte bei der Auswahl der mobilen Geräte sowie gegebenenfalls notwendiger Peripherie auf Eignung und ausreichende Qualität der Hardware geachtet werden. Insbesondere bei der Nutzung von privaten Geräten, sofern die Regelungen der Institution dies erlauben, sollte eine entsprechende Absicherung von Videokonferenzen gefordert werden.

4.3 Betriebliche Aspekte

Für den Betrieb einer Videokonferenzlösung sind insbesondere folgende Bereiche zu betrachten:

- Betreuung der Nutzer
- Administration der Komponenten
- Monitoring der Videokonferenzlösung
- Protokollierung von Ereignissen, Zugriffen und Nutzung
- Sicherung von Konfiguration und anderen Daten

Abbildung 12 zeigt exemplarisch die im Folgenden beschriebenen Komponenten, die für die genannten betrieblichen Aspekte eine Rolle spielen. Die Management-Einheit eines Videokonferenzsystems wurde bereits in Kapitel 3.2.4 vorgestellt.

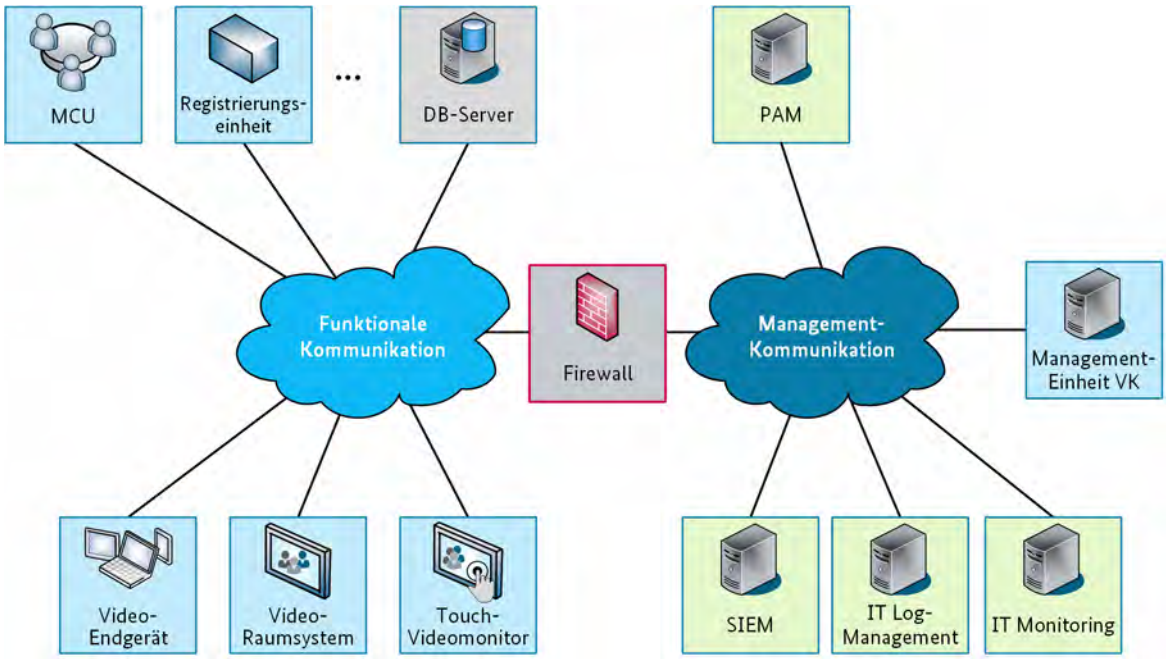

Abbildung 12: Exemplarische Darstellung der am Betrieb beteiligten Komponenten

4.3.1 Nutzerbetreuung

Für den erfolgreichen Betrieb einer Videokonferenzlösung muss diese von den Nutzern angenommen werden. Dabei gilt es vor allem, Einstiegshürden so weit wie möglich abzubauen und eine bequeme, unkomplizierte Nutzung im Alltag zu ermöglichen.

Potenzielle Videokonferenznutzer sollten über Informationsangebote so an die Nutzung der Lösung herangeführt werden, dass ein leichter Einstieg in typische Nutzungsweisen möglich ist bzw. eine erneute Nutzung nach einer längeren Pause leicht fällt. Solche Nutzungshilfen sollten insbesondere am Aufstellort spezialisierter Video-Endpunkte direkt verfügbar sein. So kann z. B. eine Anleitung ausliegen, die die Nutzung einer zur Lösung gehörenden Fernbedienung und die häufigsten Anwendungsfälle in wenigen Schritten erklärt. Aufgrund des erheblichen Funktionsumfangs moderner Videokonferenzlösungen können auch Nutzer-Schulungen, z. B. als Webinar, die Akzeptanz und Informationssicherheit erheblich erhöhen.

Außerdem ist wichtig, dass die Nutzer ausreichend Kenntnis über Richtlinien und Regularien haben, die auch für Videokonferenzen zu beachten sind. Hier ist es sinnvoll, diese Informationen bzw. einen Verweis darauf unmittelbar an einem Video-Endpunkt bzw. im Graphical User Interface (GUI) des Video-Endpunkts bereitzustellen. Ein Beispiel ist der Austausch von Informationen mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit. An einem Video-Endpunkt könnte ein Hinweis angebracht werden, der etwa folgendes besagen könnte: „Dieses System ist für Videokonferenzen mit hohem Schutzbedarf hinsichtlich Vertraulichkeit zugelassen. Werden Videokonferenzen mit hohem Schutzbedarf hinsichtlich Vertraulichkeit durchgeführt, muss der Nutzer die folgenden Punkte berücksichtigen...“ oder „Dieses System ist nur für Videokonferenzen mit normalem Schutzbedarf hinsichtlich Vertraulichkeit zugelassen.“

Im Rahmen der Möglichkeiten der jeweiligen Lösung können Auswahlmöglichkeiten aus vorbereiteten Konferenzeinstellungen für typische Nutzungssituationen, oft in Form von Konferenzprofilen, bereitgestellt werden. Nutzer können so schnell Zugang zur Nutzung der Anlage finden, ohne alle Einstellungsmöglichkeiten im Detail kennen zu müssen.

Im Rahmen der Funktionalitäten einer konkreten Lösung können Bedienkomfort und Unterstützung der Nutzer z. B. durch Chat Bots und Sprachassistenten weiter erhöht werden. Dies ist als Teil der Nutzerbetreuung entsprechend vorzubereiten.

Ergänzend zu solchen Hilfen für die eigenständige Nutzung von Videokonferenz-Angeboten sollte bei Bedarf eine persönliche Unterstützung bei der korrekten und erfolgreichen Bedienung zugänglich sein. Mindestlösung ist die Kontaktmöglichkeit zu einem kundigen Ansprechpartner oder einer entsprechenden Service Hotline. Auf solche Möglichkeiten sollte unter Angabe der Kontaktinformationen am Aufstellort eines spezialisierten Video-Endpunkts hingewiesen werden. Ein solches Betreuungsangebot muss dabei gezielt organisiert werden. Das unterstützende Personal muss die Videokonferenzausstattung sicher beherrschen und bei Bedarf zügig verfügbar sein.

Bei größeren Veranstaltungen oder bei besonders wichtigen Videokonferenzen kann eine Möglichkeit zur Buchung bzw. zum kurzfristigen Abruf von Bedien- oder Betreuungspersonal, z. B. Medientechnikern, sinnvoll sein. Dies gilt insbesondere auch für Videokonferenzen, bei denen ein komplexer Funktionsumfang genutzt werden soll, sodass auf Expertenwissen zurückgegriffen werden muss.

Spezialisierte, in Besprechungsräumen bereitgestellte Video-Endpunkte stehen wechselnden Nutzern zur Verfügung, schon um über eine möglichst gute Auslastung einen hohen Nutzwert der Anlage zu erzielen. Entsprechend müssen Raum und Video-Endpunkte als Ressource reserviert, also gebucht werden können. Um auch hier den Zugang für potenzielle Nutzer möglichst leicht zu machen, sollte eine Buchung von Raum und Video-Endpunkten in einem Vorgang möglich sein. Der Lösungsweg sollte dem der einfachen Besprechungsraumbuchung möglichst ähnlich sein, sodass Videokonferenznutzer auf bereits bekannte Wege zur Reservierung zurückgreifen können.

4.3.2 Administration

Videokonferenzlösungen und deren Zusatzausstattung sollten zentral administriert werden, damit typische Betriebsaufgaben möglichst effizient wahrgenommen werden können. Dies betrifft sowohl zentrale Komponenten einer Videokonferenzlösung, als auch zweckgebundene, für eine Videokonferenzteilnahme optimierte Endpunkte. Durch derartige netzbasierte Administration, auch von Endpunkten, können Wegezeiten im Betrieb reduziert werden. Dies setzt entsprechende Schnittstellen an den Komponenten voraus.

Alle Komponenten sollten unter Beachtung ihrer technischen Eigenarten kontinuierlich gepflegt werden. Dabei sollten stets möglichst einheitliche und auf die Komponenten abgestimmte Software- und Konfigurationsstände gehalten werden. Hierzu ist es ideal, wenn die Videokonferenzlösung in das allgemeine Configuration Management und Change Management der IT aufgenommen wird.

Ziel der Administration sollte ebenfalls sein, die Benutzung von Videokonferenzlösungen zu vereinfachen. Dies kann z. B. durch eine geeignete Vorkonfiguration erreicht werden, wie zweckmäßige Standard-Einstellungen, vorbereitete Auswahlmöglichkeiten für typische Konferenzfälle (siehe Kapitel 4.3.1). Entsprechende Festlegungen setzen eine Analyse voraus, was die konkret anfallenden Nutzungsszenarien der Videokonferenzlösung sind.

Weitere administrative Aufgaben ergeben sich über die notwendige Nutzerverwaltung. Eine solche ist zum Beispiel nötig, um Video-Endpunkte gegen missbräuchliche Nutzung oder unbefugtes Auslesen von lokalen Informationen zu schützen. Die für beliebige IT-Lösungen typische Unterscheidung zwischen produktiven Nutzern, d. h. Konferenzteilnehmern, und Administratoren mit erweiterten Berechtigungen ist auch hier notwendig. Außerdem ergeben sich Aspekte der Nutzerverwaltung über die Lösung zum Buchen spezieller Video-Endpunkte. Die Administration zur Videokonferenzlösung umfasst aus solchen Gründen auch die Verwaltung personenbezogener Nutzerkonten. Der Aufwand wird somit unter anderem von der Anzahl potenzieller Videokonferenznutzer mitbestimmt.

Ideal für Nutzerkomfort und Betrieb ist dabei die Abstützung auf bereits vorhandene Lösungen auch für die Nutzerverwaltung zur Videokonferenzlösung. Die Einrichtung und Anpassung entsprechender Kopplungen und Einbindungen ist Teil der administrativen Aufgaben zur Videokonferenzlösung. Ein Beispiel ist die Anbindung der Videokonferenzlösung an einen bereits existierenden Verzeichnisdienst.

Weitere administrative Aufgaben kommen je nach Gestaltung der Lösung hinzu. So können besondere Aufgaben zur Lizenzverwaltung für Komponenten einer Videokonferenzlösung anfallen. Werden Teile einer Videokonferenzlösung als Cloud-Dienste realisiert, ergeben sich Aufgabenpunkte zum Vertrags- und Servicemanagement. Es ist wichtig, dass für solche Aufgaben notwendige Regelungen festgelegt werden und zuständiges Personal geeignet vorgesehen wird.

Administrative Zugriffe auf IT-Komponenten werden häufig im Rahmen des Privileged Access Management (PAM) durch spezielle Werkzeuge kontrolliert. Dabei erfolgt der administrative Zugriff über eine PAM-Lösung. Hier kann der Zugriff authentisiert, berechtigt, kontrolliert und auch protokolliert werden (siehe auch Kapitel 4.3.4).

4.3.3 Monitoring

Alle zentralen Komponenten von Videokonferenzlösungen sollten zur kontinuierlichen Überwachung in ein zentrales Monitoring eingebunden werden. Dies gilt selbstverständlich auch für Komponenten, die als Cloud-Dienste realisiert werden. Dabei kann sogar das Monitoring selbst über einen Cloud-Dienst erfolgen. Das Monitoring dient aus betrieblicher Sicht zur Sicherstellung der ordnungsgemäßen und sicheren Funktion aller Geräte und des notwendigen Qualitätsniveaus von Videoübertragungen.

Bei Video-Endpunkten auf Arbeitsplatzrechnern, d. h. PCs oder Laptops, ist eine solche permanente Überwachung wenig sinnvoll und widerspricht auch gängiger Praxis im Betrieb solcher Endgeräte.

Bei spezialisierten, zweckgebundenen Video-Endpunkten bestimmen verschiedene Faktoren, z. B. Nutzungszweck und damit verbundene Betriebs- und Nutzungszeiten, ob eine Einbindung in das Monitoring sinnvoll ist. Eine durchgehende Statusüberwachung inklusive Alarmierung bei Nichtverfügbarkeit ist wenig nützlich bei Geräten, die in längeren Nutzungspausen in einen nicht antwortfähigen Standby-Modus versetzt oder gar zu Energiesparzwecken vollständig ausgeschaltet werden.

Dennoch kann auch hier eine Möglichkeit zum punktuellen Monitoring sinnvoll sein, etwa zur Kontrolle der Übertragungsqualität oder zur Gewinnung von Vergleichsdaten, auf die in Störungsfällen zu Diagnosezwecken zurückgegriffen werden kann.

Bei Video-Endpunkten, die entsprechend ihrem Nutzungszweck nahezu permanent aktiv sind bzw. jederzeit aktivierbar sein müssen, ergibt eine permanente Statusüberwachung durchaus Sinn. Ein Beispiel sind Raumsysteme, die in Leitständen oder ähnlichen Aufgabenbereichen eingesetzt werden und dazu

dienen, sich bei Bedarf zur Behandlung einer besonderen Lage unmittelbar mit weiteren Funktionsträgern abzustimmen.

Zu beachten ist, dass ein Monitoring von Videokonferenzlösungen im Vergleich zu anderer IT Besonderheiten im Detail aufweist. So sind je nach Lösung spezielle Protokolle im Monitoring zu berücksichtigen, etwa zur automatischen Erkennung und Einbindung neuer Komponenten. Auch stellen Video- und Sprachübertragung besondere Anforderungen an Übertragung und Verarbeitung auf den Endpunkten. Monitoring-Lösung und -Einbindung müssen entsprechende Parameter abdecken. Die Monitoring-Lösung oder mit ihr gekoppelte Betriebswerkzeuge müssen entsprechende Auswertungen unterstützen.

Unabhängig von einem zielgerichteten Monitoring auf Ebene der Videokonferenzlösung ist ein Monitoring der Kommunikation, insbesondere der Echtzeit-Kommunikation, auf Netzebene wichtig, um Qualitätseinbußen schnell zu erkennen.

Es ergeben sich also insgesamt spezifische Aspekte zum Monitoring von Videokonferenzlösungen. Der konkrete Monitoring-Bedarf muss geklärt werden und auf Konzeptebene sowie bei der Beschaffung der Lösung berücksichtigt werden. Dies gilt mit Blick auf die ins Monitoring einzubindenden Teile der Videokonferenzlösung und für die Monitoring-Infrastruktur.

4.3.4 Protokollierung

Videokonferenzlösungen können sowohl Informationen zum System selbst als auch solche zu dessen Nutzung erfassen und dabei auch verschiedene Arten von Metadaten und Daten zu Konferenzinhalten aufzeichnen.

Wie die meisten Anwendungen und Systeme protokollieren auch Videokonferenzlösungen Informationen in Log-Dateien. Als Daten zum System bzw. dessen Nutzung werden beispielsweise Fehlermeldungen aufgezeichnet, um Probleme feststellen und ihre Ursachen finden zu können. In diesen Bereich fallen auch Audit-Logs, Zugriffsdaten und andere sicherheitsrelevante Daten. Dabei sind insbesondere Protokolle von Systemen an Vertrauensgrenzen wichtig, die einen Übergang zu externen Partnern ermöglichen. Außerdem sollten auch bei Videokonferenzlösungen administrative Zugriffe protokolliert werden. Hierfür werden allgemein oft PAM-Lösungen eingesetzt (siehe Kapitel 4.3.2).

Umfang und Einstellmöglichkeiten zur Protokollierung können dabei variieren. Entsprechend besteht eine wichtige Aufgabe darin, benötigte und erlaubte Protokollierungsinhalte festzulegen, sodass diese Festlegungen in der Administration (siehe Kapitel 4.3.2) planvoll umgesetzt werden können. Diese Festlegung erfordert bei personenbezogenen Daten, die speziell bei Videokonferenzen häufig auftreten können, auch eine Abstimmung mit dem Datenschutzbeauftragten und dem Betriebs- bzw. Personalrat. Bei der Auswahl von Videokonferenzprodukten bzw. von Cloud-Diensten, die im Rahmen von Videokonferenzlösungen genutzt werden, muss auf entsprechende Umsetzungsmöglichkeiten geachtet werden.

Es sollten zumindest solche Informationen protokolliert werden können, die dabei helfen, allgemeine Probleme und Sicherheitsvorfälle festzustellen und zu analysieren. Über entsprechende Schnittstellen sollten die Daten an das zentrale Monitoring bzw. direkt an eine zentrale Lösung zur Zusammenführung von Protokollierungsdaten weitergeleitet werden. Letzteres kann zunächst ein zentrales Log-Management sein. Für die automatisierte Erkennung von Anomalien und Sicherheitsvorfällen ist eine Überwachung einer Videokonferenzlösung über ein Security Information and Event Management (SIEM) erforderlich.

Einige Videokonferenzlösungen bieten die Möglichkeit, die Inhalte einer Videokonferenz aufzuzeichnen. Dies kann in Form einer Speicherung von Videos, Sprachaufzeichnungen, automatischer Transkription von Sprache in Text, z. B. durch einen Cloud-Dienst, und Chat-Protokollen erfolgen. Eine solche Form der Protokollierung kann beispielsweise als Arbeitserleichterung nützlich sein: Das Anfertigen von Notizen

und schriftlichen Protokollen zum Konferenzinhalt kann entfallen bzw. erleichtert werden. Nachweisnotwendigkeiten zum Konferenzverlauf können mit optimiertem Aufwand abgedeckt werden.

Sollen die Vorteile einer Protokollierung von Konferenzinhalten genutzt werden können, muss bei der Auswahl der Videokonferenzlösung auf entsprechende Unterstützung geachtet werden. Allerdings ist dann zu beachten, dass bei der Nutzung derartiger Funktionen maßgebliche rechtliche Rahmenbedingungen zu berücksichtigen sind. Aufzeichnungen von Wort und Bild bzw. Bildfolgen als Video setzen im Regelfall eine Einwilligung der betroffenen Personen voraus.

Damit derartige Regelungen nicht verletzt werden, müssen gezielte Vorkehrungen getroffen werden. Zum einen sollte Personal, das die Nutzerbetreuung zu einer Videokonferenzlösung leistet, auch Auskunft über Regelungen zu solchen Nutzungsaspekten geben können (siehe Kapitel 4.3.1). Außerdem sollten Standardeinstellungen vermieden werden, die eine automatische Aktivierung von inhaltlicher Protokollierung umfassen. Dies muss im Aufgabenbereich Administration berücksichtigt werden (siehe Kapitel 4.3.2). Wird die Videokonferenzlösung als Cloud-Dienst genutzt, muss eine entsprechende Vorgabe an den Anbieter erfolgen.

4.3.5 Datensicherung

Auch im Rahmen von Videokonferenzlösungen fallen Daten an, deren Wiederherstellbarkeit über eine Datensicherung ermöglicht werden sollte. Die Videokonferenzlösung muss dann entsprechend in ein bestehendes Datensicherungskonzept aufgenommen werden.

Für die verschiedenen Datenbestände, z. B. Konfigurationsdaten, Metadaten zu Videokonferenzen und mögliche Protokollierungsdaten ist zu klären, ob und wie schnell diese auch im Desaster-Fall wiederherstellbar sein müssen. Weiterhin muss geklärt werden, wie lange solche Datensicherungen zurückreichen müssen bzw. dürfen. Einzelheiten können sich aus Regelungen für den jeweiligen Datentyp ergeben, zum Beispiel Regelungen zur Aufbewahrung von Protokollierungsdaten.

Für besonders vertraulich zu behandelnde Daten, z. B. Aufzeichnungen zu Konferenzen, muss außerdem geklärt werden, inwieweit der Aspekt „Zugriff nur für Befugte“ im Rahmen der Datensicherung besonders zu behandeln ist. Darüber hinaus muss für personenbezogene Daten die Löschung gemäß DSGVO auch für die Datensicherung beachtet werden.

Soweit Daten gesichert werden sollen, die auf Video-Endpunkten anfallen, ist zu klären, wie mit Geräten umzugehen ist, die bei längeren Nutzungspausen abgeschaltet werden.

5 Gefährdungslage

Im Folgenden werden Bedrohungen und Schwachstellen spezifiziert, die für Videokonferenzsysteme und deren Betrieb und Nutzung von besonderer Bedeutung sind. Zunächst werden in Kapitel 5.1 Bausteine des IT-Grundschutz-Kompendiums genannt, deren Gefährdungen generell für eine Videokonferenzlösung gelten. Im Anschluss werden in Kapitel 5.2 spezifische Gefährdungen für Videokonferenzen genannt. Abschließend betrachtet Kapitel 5.3 allgemeingültige, elementare Gefährdungen, die im IT-Grundschutz-Kompendium spezifiziert sind und auch für Videokonferenzlösungen gelten.

5.1 Bezug zu Bausteinen des IT-Grundschutz-Kompendiums

Im Allgemeinen gelten für Videokonferenzlösung die Gefährdungen aus folgenden Bausteinen des IT-Grundschutz-Kompendiums (siehe [BSI GSK-2019]):

- *NET.4.1 TK-Anlagen*: Insbesondere klassische Videokonferenzsysteme beinhalten typische Funktionen von TK-Anlagen und die Gefährdungslage vererbt sich daher.
- *NET.4.2 VoIP*: Da moderne Videokonferenzsysteme die Signalisierung und die Medienströme mit ähnlichen Mitteln übertragen, wie es bei Voice over IP (VoIP) der Fall ist, vererbt sich auch hier die Gefährdungslage.
- *SYS.4.4 Allgemeines IoT-Gerät*: Die Gefährdungen dieses Bausteins sind insbesondere relevant für mit dem Internet verbundene Komponenten eines Videokonferenzsystems, z. B. eine Sprachsteuerung.

Weiterhin überträgt sich durch die Verwendung von IT-Techniken in Videokonferenzlösungen, wie z. B. Virtualisierung und Cloud, generell auch deren Gefährdungslage. Sofern hier jedoch spezifische Aspekte für Videokonferenzen zu beachten sind, werden diese im Folgenden beschrieben. Ansonsten sind die Gefährdungen in den entsprechenden Bausteinen des IT-Grundschutz-Kompendiums zu beachten, beispielsweise *SYS.1.5 Virtualisierung* und *OPS.2.2 Cloud-Nutzung*.

5.2 Spezifische Gefährdungslage

5.2.1 Abhören von Videokonferenzen

Wenn Medienströme oder Signalisierung in Videokonferenzen oder sonstige in der Konferenz übertragene Daten, z. B. Chats oder Dateien, unverschlüsselt übertragen werden, können Angreifer Informationen abhören. Dies galt grundsätzlich bereits für über ISDN übertragene Videokonferenzen, jedoch ist eine IP-basierte Übertragung wesentlich leichter abhörbar. Dies gilt nicht nur bei der Übertragung einer Videokonferenz über eingeschränkt oder nicht vertrauenswürdige Netze wie das Internet, sondern auch in einem vermeintlich geschützten LAN an einem Standort einer Institution.

Bei solchen Angriffen auf die Vertraulichkeit ist ein mehrstufiger Ansatz typisch: Als erster Schritt wird die Umgebung ausspioniert, um Identitäten im Netz zu identifizieren, auf die bzw. über die der angestrebte Abhörangriff erfolgen kann. Danach wird missbräuchlich vom Angreifer eine Identität bzw. Rolle angenommen, über die er in die Videokonferenz bzw. den zugehörigen Datentransfer eingebunden wird, ohne dass dies auffällt. Schließlich übt der Angreifer die unberechtigt übernommene Rolle aus und gelangt so in die Position, Video- und Sprachdaten sowie gegebenenfalls weitere Daten mitzulesen und zur Abhörung aufzubereiten.

Ein Beispiel für einen solchen Angriff ist seit vielen Jahren und noch bis heute das Address Resolution Protocol Spoofing (ARP Spoofing, siehe Gefährdung *2 9 GARP-Attacken* im Baustein *NET.3.1 Router und Switches* des IT-Grundschutz-Kompendiums, [BSI GSK-2019]). Dieser Angriff gestattet es, jegliche Kommunikation eines Endgeräts über das Gerät des Angreifers zu leiten. Dabei muss sich der eigentliche Angreifer nicht notwendigerweise im LAN des angegriffenen Systems befinden (siehe [BSI TLSTK-2014]).

Im einfachsten Fall reicht zum Abhören der Informationen auch der Zutritt zum LAN-Anschluss des Videokonferenzendgeräts, um durch eine angeschlossene transparente Zusatzkomponente, z. B. einen Splitter, die Kommunikation abzugreifen.

Unzureichend abgesicherte Telefone, die für eine reine Audio-Teilnahme an einer Videokonferenz eingesetzt werden, stellen ein besonderes Gefährdungspotenzial für die gesamte Videokonferenzlösung dar. Diese Geräte unterstützen gegebenenfalls nicht die vom Videokonferenzsystem genutzten Verschlüsselungsverfahren, sodass die Kommunikation leicht von einem Angreifer abgehört werden kann, auch wenn an anderen Stellen ordnungsgemäß verschlüsselt wird.

5.2.2 Manipulation der Signalisierung

Ein Videokonferenzsystem kann über einen unzureichend gesicherten Signalisierungskanal angegriffen werden. Ein Angreifer kann dazu eine manipulierte Signalisierungssequenz an das System übertragen, um ein bestimmtes Verhalten hervorzurufen. Auf diese Weise können Befehle gesendet werden, die auf dem Videokonferenzsystem ausgeführt werden. Denkbar ist auch, dass so undokumentierte Funktionen aktiviert werden. Die Signalisierung kann beispielsweise derart manipuliert werden, dass Fehler hervorgerufen werden, durch die gegebenenfalls das ganze System zum Absturz gebracht wird. Eine Manipulation der Signalisierung kann auch eine vorbereitende Aktivität für den eigentlichen Angriff, z. B. eine Lauschattacke, sein.

5.2.3 Ungeschützte oder unkontrollierte Verschlüsselungsendpunkte

Wird innerhalb einer Videokonferenz verschlüsselt kommuniziert, gibt es in vielen Fällen zwischen den Konferenzteilnehmern zusätzliche Zwischenstationen, die Verschlüsselungsendpunkte realisieren. Beispiele hierfür sind eine MCU oder ein SBC, welche die Verschlüsselung von Medienströmen terminieren, um auf deren Inhalt zugreifen zu können, um z. B. Bildanpassungen vorzunehmen. Werden solche Verschlüsselungsendpunkte nicht ausreichend geschützt, bieten sie Angreifern eine Möglichkeit, verschlüsselte Konferenzen abzuhören. Solche Verschlüsselungsendpunkte können sich auch in einer Cloud befinden, wenn z. B. die MCU in einer Cloud realisiert wird. Dadurch sind diese Verschlüsselungsendpunkte prinzipiell schwerer oder schlimmstenfalls gar nicht kontrollierbar.

5.2.4 Unzureichend abgesicherte Cloud-Dienste

Wenn zentrale Komponenten der Videokonferenzlösung durch Cloud-Dienste realisiert werden, besteht allgemein die Gefahr, dass durch eine unzureichende Absicherung seitens des Cloud-Anbieters ein unberechtigter Zugriff auf Daten von Videokonferenzen und integrierten UCC-Diensten erfolgt. Bei Videokonferenzen ist diese Gefährdung besonders kritisch, wenn personenbezogene oder vertrauliche Daten betroffen sind.

Weiterhin besteht die Gefahr einer unzureichenden Verfügbarkeit eines Cloud-Dienstes bzw. der Cloud-Anbindung, was gegebenenfalls die Verfügbarkeit der gesamten Videokonferenzlösung signifikant beeinträchtigen kann, falls beispielsweise die Anmeldung an einer Videokonferenz über einen Cloud-Dienst erfolgt. Werden Daten einer Videokonferenz, z. B. Protokolle oder bearbeitete Dokumente, über einen Cloud-Dienst gespeichert, besteht auch die grundsätzliche Gefahr des Verlusts der Daten beim Cloud-Dienstleister.

Außerdem besteht eine Gefahr durch Nachlässigkeiten in der Cloud-Nutzung, speziell durch eine unzureichende Nutzung von möglichen Sicherheitsfunktionen. Dies betrifft beispielsweise den Umgang mit Passwörtern.

5.2.5 Qualitätseinbußen durch unzureichende Dimensionierung

Für die Übertragung der Medienströme einer laufenden Videokonferenz wird eine hohe Bandbreite und Performance benötigt. Die Datenmenge übersteigt die einer Telefonkonferenz um ein Vielfaches. Sind die Ressourcen für ein Videokonferenzsystem, z. B. zentrale Komponenten wie MCU oder Netzkomponenten, unzureichend dimensioniert, führt dies zu Problemen bei der Kommunikation. Solche Probleme reichen von einer schlechten Bild- und Tonqualität mit kürzeren Aussetzern bis hin zu Ausfällen für einzelne oder mehrere Nutzer. Diese Symptome können sich auch auf andere Datenströme und Dienste übertragen, die dieselben Ressourcen nutzen. Die Gefährdung ist insbesondere für Bereiche relevant, in denen der Nutzer keine oder nur einen eingeschränkten Einfluss auf die Qualität hat, z. B. bei der Nutzung von Cloud- und anderen Provider-Diensten.

5.2.6 Fehlerhafte Bedienung und Nutzung

Videokonferenzsysteme bieten häufig eine Vielzahl von Funktionen, die für Anwender nicht immer überschaubar und beherrschbar sind. Hierdurch entsteht die Gefahr einer fehlerhaften Bedienung, Nutzung und Konfiguration, die sogar einen unbeabsichtigten Datenabfluss zur Folge haben kann.

Ein besonderes Gefahrenpotenzial entsteht vor allem bei der Vernetzung eines Videokonferenzsystems mit weiteren Diensten. Hier ist die Komplexität des so entstehenden Gesamtsystems für den Nutzer oft nicht mehr überschaubar. Das System kann beispielsweise so eingestellt werden, dass Konferenzteilnehmer auf Dateiablagen zugreifen können. Dieser Zugriff könnte versehentlich auch unbefugten Teilnehmern gestattet werden, die so an vertrauliche Daten gelangen könnten.

Bei einem unangemessenen Berechtigungsmodell, das den Nutzern unnötig viele Rechte einräumt, ist mit einem erhöhten Gefährdungspotenzial durch eine fehlerhafte Bedienung zu rechnen. So können durch nicht ordnungsgemäße Beendigung einer Videokonferenz Raumgespräche abgehört werden.

5.2.7 Automatische Annahme von eingehenden Verbindungsanfragen

Endgeräte einer Videokonferenzlösung können so konfiguriert werden, dass eingehende Verbindungsanfragen beispielsweise durch ein Raumsystem automatisch angenommen werden. So können sich neue Teilnehmer sowohl von Video- als auch von reinen Audio-Endpunkten in eine laufende Konferenz einwählen, ohne dass ein Nutzer dies durch eine Interaktion explizit gestatten muss. Dieser Umstand kann jedoch auch dazu führen, dass sich Teilnehmer einwählen, denen dies eigentlich nicht gestattet ist. Dies kann sogar geschehen, ohne dass der unberechtigte Teilnehmer bemerkt wirkt. Angreifern bietet sich so die Möglichkeit, Konferenzen unbemerkt abzuhören. Weiterhin können hierdurch Gespräche in der Nähe des Videokonferenzsystems mitgehört werden, ohne dass von dort aus eine Konferenz gestartet worden ist (siehe Gefährdung 5.2.9).

5.2.8 Gezieltes Ausspähen von Räumen

Ein Videokonferenzsystem kann durch Angreifer genutzt werden, um einen Raum bzw. Raumgespräche auszuspähen. Dies kann sowohl akustisch als auch visuell durch die Nutzung von Mikrofon und Kamera erfolgen. Auch ein Ausspähen eines im Sichtfeld befindlichen Monitors ist möglich. Ein Angreifer kann die Raumgespräche beispielsweise abhören, wenn ein Nutzer bei der Bedienung nachlässig ist (siehe Gefährdung 5.2.6). Auch Konfigurationsfehler können genutzt werden, um Raumgespräche abzuhören

(siehe Gefährdung 5.2.16). Darüber hinaus kann ein Angreifer vorliegende Schwachstellen eines Videokonferenzsystems möglicherweise ausnutzen, um Raumgespräche abzuhören. Ein zusätzliches Gefährdungspotenzial stellen Komfortfunktionen von modernen Videokonferenzsystemen dar. Hierbei besteht beispielsweise die Möglichkeit, das Raumsystem bei Anwesenheit von Personen unbemerkt zu starten und so den Raum auszuspähen.

5.2.9 Verlust der Vertraulichkeit durch Kompromittierung von Video-Endpunkten

Verschaffen sich Angreifer Zugang zu einem Videokonferenzsystem, können angeschlossene Kameras als Überwachungskameras missbraucht und Konferenzräume ausgespäht werden. Prinzipiell muss das Videokonferenzsystem dazu nicht einmal eine Sicherheitslücke aufweisen. Es könnte bereits ausreichen, wenn es zur automatischen Annahme von Verbindungsanfragen konfiguriert ist (siehe Gefährdung 5.2.7).

Endgeräte, die mit einem Videokonferenzsystem verbunden sind, können durch eine Schadsoftware kompromittiert sein. Dabei kann die Vertraulichkeit von Videokonferenzen oder auf dem Video-Endpunkt gespeicherten Daten gefährdet sein. Dieses Risiko besteht vor allem bei Video-Endpunkten mit Standard-Betriebssystemen, da diese allgemein einer größeren Gefährdung durch Malware-Angriffe ausgesetzt sind als Spezialsysteme.

Von besonderer Bedeutung sind dabei auch Videokonferenzsysteme, deren Kameras als Bestandteil des Internet of Things (IoT) über das Internet erreichbar sind. Können hier Schwachstellen ausgenutzt werden, z. B. bekannte Default-Passwörter, ist eine Übernahme der Kamera inklusive Lauschangriff gegebenenfalls sogar sehr leicht möglich. In diesem Zusammenhang muss darauf hingewiesen werden, dass es bereits seit geraumer Zeit im Internet verfügbare Suchmaschinen gibt, die einerseits über das Internet erreichbare IoT-Geräte listen und andererseits bekannte Schwachstellen und deren Ausnutzung beschreiben. Außerdem bieten in die Videokonferenzlösung integrierte, jedoch unzureichend abgesicherte IoT-Geräte wie beispielsweise eine Videokamera eine erhebliche Angriffsfläche.

Prinzipiell können aber auch dedizierte Videosysteme angegriffen werden.

5.2.10 Leistungsüberwachung und Profiling

Ein unbefugter Zugriff auf Kommunikationsströme in Videokonferenzsystemen ermöglicht grundsätzlich auch eine Leistungsüberwachung und ein Profiling der Nutzer dieser Systeme. Ein derartiger Zugriff kann z. B. durch eine Installation einer entsprechenden Überwachungssoftware (einem Trojaner vergleichbar) auf einem Endgerät oder durch eine automatische Annahme von Anrufen durch den Empfänger erfolgen. Ein Gefährdungspotenzial für Leistungsüberwachung und Profiling geht dabei sowohl von Personen innerhalb als auch außerhalb einer Institution aus. Überwacht werden können nicht nur die eigentlichen Nutzer eines Endgeräts, sondern alle Personen in Sicht- und Hörweite der Kamera und des Mikrofons (siehe Gefährdung 5.2.9).

Bei modernen Videokonferenzsystemen geht durch die Integration in andere Kommunikationsdienste diese Gefährdung deutlich über die reine Auswertung der Video- und Sprachinformationen hinaus. Hier ist eine mögliche Korrelation mit der Nutzung von anderen Diensten, insbesondere UCC-Diensten (z. B. Kalender, Kontakte, E-Mail, Chat und Dokumentenaustausch) zu berücksichtigen.

Eine sehr einfache Überwachung ohne Manipulation oder Ausnutzung von Schwachstellen kann über die Erreichbarkeitsanzeige der UCC-Dienste erfolgen.

5.2.11 Kein ordnungsgemäßer Benutzerwechsel für Video-Endpunkte

Gerade fest installierte Video-Endpunkte in Videokonferenzräumen bergen durch wechselnde Benutzer die Gefahr, dass Informationen zu erfolgten Videokonferenzen vom nächsten Nutzer des Video-Endpunkts eingesehen werden können. Dies kann insbesondere der Fall sein, wenn der vorherige Benutzer sich nicht abgemeldet hat. Hierdurch wird zudem ein Identitätsdiebstahl vereinfacht. Bereits der mögliche Zugriff auf Anruflisten kann kritisch sein, wenn hier ein Personenbezug hergestellt werden kann.

Werden statt personenbezogener Nutzerprofile gemeinsame Profile oder Geräteprofile genutzt, können Berechtigungen nicht klar voneinander getrennt werden. Dies gefährdet die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und steigert die Tragweite der Auswirkungen von Fehlverhalten. Weiterhin ist es schwerer zu rekonstruieren, welche Person für einen Vorfall verantwortlich gewesen ist.

5.2.12 Versehentliche Preisgabe von Informationen

Während einer Videokonferenz können im Bildausschnitt der Kamera vertrauliche Informationen zu sehen sein, die sofort an alle anderen Teilnehmer übertragen werden. Hiervon betroffen sind vor allem Wandtafeln, Whiteboards und ähnliches. Auch der Aufenthaltsort eines Teilnehmers kann vertraulich sein und durch den Bildausschnitt preisgegeben werden. Ebenso können Personen, die sich im Hintergrund des Teilnehmers befinden, nun für alle Teilnehmer der Videokonferenz sicht- und hörbar sein.

Wird ein Client für ein Videokonferenzsystem auf einem PC betrieben, kann in vielen Fällen eine Anwendung oder der Inhalt eines Bildschirms geteilt und anderen Konferenzteilnehmern gezeigt werden. Dabei entsteht die Gefahr, dass auf dem Bild oder Bildausschnitt vertrauliche Informationen eingeblendet werden, die sofort für alle Zuschauer zu sehen sind. Beispiele hierfür sind das versehentliche Freigeben des falschen Fensters oder die Einblendung von Pop-up-Fenstern beispielsweise von empfangenen E-Mails, Chats oder eingehenden Anrufen.

Es besteht weiterhin die Gefahr, dass derart offenbarte Informationen gespeichert werden, wenn etwa die laufende Konferenz aufgezeichnet wird oder andere Teilnehmer Screenshots aufnehmen. Dies kann durchaus auch unbemerkt geschehen.

Wird während einer Videokonferenz ein Desktop oder eine Anwendung auf dem Bildschirm geteilt, kann dessen Steuerung an einen anderen Konferenzteilnehmer weitergegeben werden. Dieser Teilnehmer kann unter Umständen diese Steuerung missbräuchlich verwenden. Möglich ist ein Zugriff auf vertrauliche Informationen oder die Herbeiführung von Schäden.

Auch wenn ein Nutzer sich versehentlich nicht ordnungsgemäß aus einer Videokonferenz abmeldet, besteht die Gefährdung, dass unabsichtlich Informationen preisgegeben werden. Unbemerkt kann bei einem Raumsystem der gesamte Raum und bei einem Endgerät, z. B. Laptop, der bisherige Nutzer sowie dessen Umgebung sicht- und hörbar sein.

5.2.13 Unzureichende Prüfung der Identität von Kommunikationspartnern

Bei Telefonaten ist die Gefahr, dass die Identität von Kommunikationspartnern unzureichend überprüft wird, schon lange bekannt. Diese Gefahr besteht aber auch bei Videokonferenzen. Durch die stärkere visuelle Präsenz des Gesprächspartners besteht allgemein eine größere Bereitschaft, diesem zu vertrauen.

Wird einer Person mit betrügerischen Absichten fälschlicherweise vertraut, gefährdet dies die Vertraulichkeit von Daten, die an sie weitergegeben werden. Wird ihr gar in einer Videokonferenz die Kontrolle über Endgeräte oder Anwendungen überlassen, gefährdet dies Vertraulichkeit, Integrität und Verfügbarkeit der jeweiligen Systeme. Denkbar ist auch, dass der Kommunikationspartner einen schadhaften Link übermittelt, durch den z. B. eine Malware-Infektion eingeleitet wird, oder dass ein Bewerber, dessen Bewerbungsgespräch via Videokonferenz geführt wird, hierdurch einen Angriffsversuch startet.

Wenn Teilnehmer nur per Audio-Endpunkt oder per Chat an einer Videokonferenz teilnehmen, besteht die Gefahr, dass die Identität der Teilnehmer schwerer zu prüfen ist und insbesondere, dass eine Identitätsprüfung vollständig entfällt, weil man vielleicht einen neuen Teilnehmer gar nicht bemerkt.

Ebenso kann eine Identität mehrfach genutzt werden, um sich in eine Konferenz einzuwählen. Dabei können auch verschiedene Arten der Einwahl genutzt werden. So kann eine Person an einer Konferenz über einen Video-Endpunkt teilnehmen und vorgeben, sich wegen besserer Audio-Qualität parallel via Telefon einzuwählen. Diese Telefonverbindung kann jedoch von einer weiteren Person genutzt werden, die so die Konferenz abhört. Diese Gefährdung ist von besonderer Bedeutung, da meist zusätzliche Telefonkanäle nicht hinterfragt werden.

5.2.14 Fehlverhalten und Missbrauch von Sprachsteuerung und KI-Funktionen

Nutzt ein Videokonferenzsystem Sprachsteuerung und Funktionen der Künstlichen Intelligenz (KI), bergen diese ein erhöhtes Potenzial für Fehlverhalten und Missbrauch. Eingaben können durch die KI einer Sprachsteuerung falsch interpretiert werden, sodass Fehler auftreten oder ungewollte Aktionen ausgelöst werden. Diese Fehleranfälligkeit gilt für viele KI-basierte Systeme und kann von Angreifern bewusst ausgenutzt werden, um eine KI zielgerichtet zu einer Fehlprognose zu bewegen. Dies gilt grundsätzlich auch für andere KI-basierte Funktionen in Videokonferenzen wie Gesichtserkennung, Erkennung eines Sprechers, Bilderkennung und Erkennung von Konferenzinhalten.

Außerdem kann eine Sprachschnittstelle derart missbraucht werden, dass ein Angreifer für andere Konferenzteilnehmer unhörbare Sprachbefehle absetzt, mit denen er das System selbst oder weitere angeschlossene Systeme unbemerkt kompromittiert, zum Absturz bringt oder unberechtigt auf Daten zugreift. Beispielsweise kann man auch über unhörbare Aussagen Änderungen am späteren Protokoll bzw. Transkript erzeugen.

5.2.15 Übergreifende Wirkung eines Sicherheitsvorfalls

Videokonferenzlösungen bieten oft mehrere Kommunikationsmöglichkeiten. Dabei werden neben Videokonferenzen auch Dienste wie Chat und Dokumentenzugriff in die Lösung integriert. Die Integration dieser Kommunikationskanäle birgt zunächst das Risiko, dass Informationen über den eigentlichen Adressaten oder Kommunikationskanal hinaus verbreitet werden. Die Weitergabe kann auch automatisch und damit eventuell unbeabsichtigt geschehen. Prinzipiell kann sie in beide Richtungen erfolgen, d. h. zum Videokonferenzsystem hin oder davon ausgehend. Dabei können auch vertrauliche und personenbezogene Daten betroffen sein, deren Schutz durch die Übertragung gefährdet werden kann, z. B. Kontaktdaten von Kommunikationspartnern.

Hervorgerufen werden kann dies sowohl durch Fehlnutzung oder -konfiguration des Systems als auch durch eine absichtliche Kompromittierung oder Malware. Durch die Konnektivität und weitergehende Integration bzw. Verschmelzung von Videokonferenzsystemen mit anderen Systemen wächst das Potenzial, Schwachstellen system- und anwendungsübergreifend auszunutzen. Die Videokonferenzlösung ist hier quasi in der Rolle einer Spinne in der Mitte eines großen Netzes von Anwendungen und Systemen. Ein Sicherheitsvorfall kann so über die reine Videokonferenzlösung hinaus eine Wirkung entfalten und beispielsweise kann ein Angreifer ausgehend von der Videokonferenzlösung über die verfügbaren Schnittstellen andere Anwendungen angreifen.

Hiervon betroffen sind vor allem Meeting Solutions und UC/UCC-Lösungen, die Videokonferenzen mit zahlreichen anderen Diensten vereinen. An das System kann beispielsweise eine Dateiablage angebunden sein, bei der eine Schwachstelle dazu führt, dass Angreifer ihre Zugriffsberechtigungen ausweiten können. Auf diese Weise kann ein Konferenzteilnehmer bzw. ein Angreifer dann auf vertrauliche Daten zugreifen oder sie löschen.

5.2.16 Konfigurationsfehler bei Videokonferenzlösungen

Konfigurationsfehler an MCUs, Gateways und ähnlichen zentralen Komponenten einer Videokonferenzlösung können zu Fehlfunktionen, Vertraulichkeitsverlust, Nicht-Verfügbarkeit von Leistungsmerkmalen oder Absturz anderer zentraler Komponenten und damit zu einer Nicht-Verfügbarkeit des Videokonferenzdienstes als Ganzes führen. Dies wiegt umso schwerer, als moderne Videokonferenzsysteme eine große Verzahnung mit anderen Diensten realisieren und sich so Konfigurationsfehler dienstübergreifend auswirken können.

Auch können Konfigurationsfehler auf Netzelementen wie Switches und auf Sicherheitselementen wie Firewalls zu Nutzungseinbußen der Videokonferenzlösung führen.

5.2.17 Missbrauch von Administrations- und Wartungszugängen

Administrations- und Wartungszugänge bieten Möglichkeiten, tief in ein Videokonferenzsystem eingreifen zu können. Durch Missbrauch dieser Zugänge können schwere Schäden entstehen, die die Vertraulichkeit, Integrität und Verfügbarkeit des Systems sowie der darauf gespeicherter Daten betreffen. Das Risiko eines Missbrauchs von Administrations- und Wartungszugängen steigt signifikant mit der Vielzahl der integrierten Dienste bei modernen Videokonferenzlösungen. Vor allem gilt auch hier der Trend, dass Videokonferenzlösungen über Cloud-Dienste administriert und gewartet werden. Dies führt zu einer erheblich komplexeren Gefährdungslage als bei klassischen Administrations- und Wartungszugängen, z. B. via VPN.

5.2.18 Unzureichende Organisation des Betriebs eines Videokonferenzsystems

Die vielfältigen Schnittstellen von modernen Videokonferenzsystemen zu anderen Anwendungen und Diensten wie z. B. zu Web-Konferenzen und UCC-Diensten erschwert die Organisation des Betriebs. Sind für das Videokonferenzsystem und angebundene Systeme unterschiedliche Organisationseinheiten oder Dienstleister zuständig, können bei der Koordination, insbesondere durch ungeregelte Zuständigkeiten, Fehler und Versäumnisse entstehen. Dies kann dazu führen, dass Funktionalitäten zeitweilig nicht oder nur unzureichend genutzt werden können. Ein Grund hierfür kann beispielsweise sein, dass ein Change, z. B. ein Software-Update, an einem angebundenen System vorgenommen wird, der zu Inkompatibilität mit dem Videokonferenzsystem führt. Unter Umständen kann auch die Verfügbarkeit des gesamten Videokonferenzsystems gefährdet werden.

5.2.19 Unzureichendes Identitäts- und Berechtigungskonzept

Für moderne Videokonferenzlösungen bestehen besondere Gefährdungen durch ein unzureichendes Management von Identitäten, Rollen und Berechtigungen. Wenn beispielsweise die Berechtigungen für die normalen Nutzer und für die Moderatoren einer Videokonferenz nicht angemessen geplant sind, besteht die Gefahr, dass beispielsweise den normalen Nutzern zu viele Rechte eingeräumt werden. So steigen einerseits die Angriffsmöglichkeiten durch Dritte und andererseits die potenziellen Auswirkungen einer fehlerhaften Nutzung.

Wenn einem Nutzer z. B. nach Ausscheiden aus einer Institution nicht unmittelbar auch die Konten und zugehörigen Berechtigungen für die Verwendung einer Videokonferenz und weiterer integrierter Dienste entzogen werden, besteht die Gefahr eines unberechtigten Zugriffs.

5.2.20 Unzureichend abgesicherte Aufzeichnung, Protokollierung und Dateiablage

Videokonferenzsysteme können in unterschiedlichem Maß Daten aufzeichnen (persistente Daten). Hierzu zählen beispielsweise Metadaten in Form von protokollierten Kommunikationsdaten oder ganze Konferenzen in Video-, Audio- oder Transkriptions-Form. Solche Daten sind in der Regel personenbezogen und häufig vertraulich. Bei unzureichender Absicherung der Aufzeichnung können Vertraulichkeit, Integrität und Verfügbarkeit gefährdet sein. Bei unrechtmäßiger Aufzeichnung oder unzureichendem Schutz der Aufzeichnung drohen Verstöße gegen verschiedene Gesetze, z. B. die Datenschutz-Grundverordnung, oder gegen Betriebsvereinbarungen mit unter Umständen empfindlichen Folgen.

Außerdem greifen Videokonferenzlösungen meist parallel auf verschiedene Formen von Dateiablagen zu (siehe Abbildung 13). Diese können als Dienst der Videokonferenzlösung über die interne Dateiablage des Videokonferenzsystems, z. B. für Konfigurationsdaten, realisiert sein. Ebenso kann die Dateiablage als externer Dienst, z. B. als Cloud-Speicher, mit einer Schnittstelle zur Videokonferenzlösung zur Verfügung gestellt werden. Alle Formen einer Dateiablage enthalten in der Regel persistente Daten, die oft personenbezogen und vertraulich sind. Bei unzureichender Absicherung der Dateiablage kann ein Nutzer der Videokonferenz unautorisiert und unbemerkt auf die Dateien zugreifen und so Vertraulichkeit, Integrität und Verfügbarkeit der Daten gefährden.

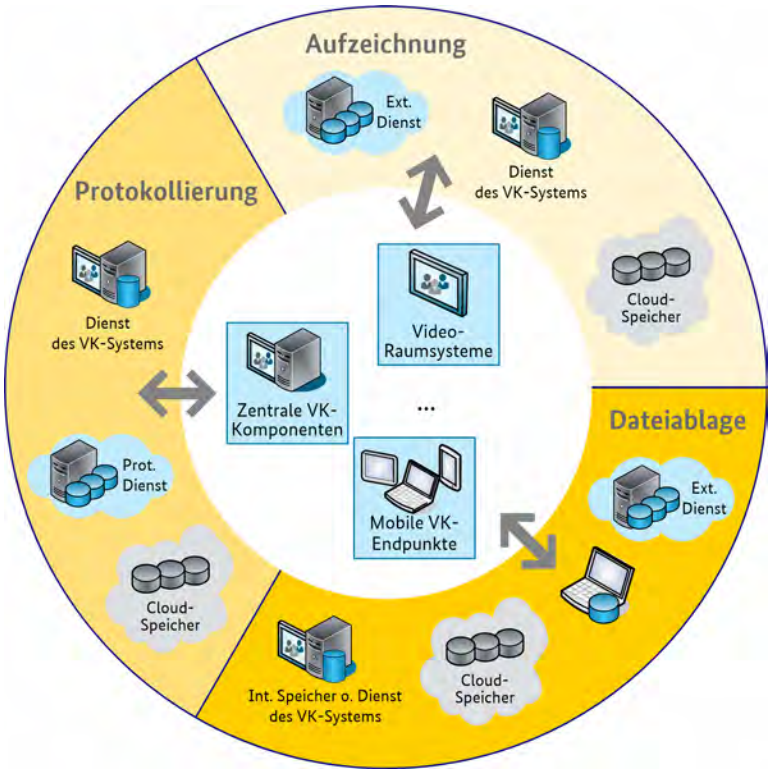

Abbildung 13: Varianten von Aufzeichnung, Protokollierung und Dateiablage

5.2.21 Unzureichende Kenntnis von Technik und Regelungen

Aufgrund von gesetzlichen Regelungen oder internen Betriebsvereinbarungen sind Videokonferenzen in bestimmten Situationen oder zu kritischen Themen nicht erlaubt oder bestimmte Funktionen dürfen nicht genutzt werden, z. B. zur Beschlussfassung in Gremien oder Aufzeichnung von kritischen Informationen. Falls die Nutzer hierüber nicht ausreichend geschult sind, erfolgt gegebenenfalls eine unzulässige Nutzung mit rechtlichen Folgen für die Institution. Ebenso können unzureichende oder fehlende Regelungen dazu führen, dass die Nutzung der Videokonferenzlösung nicht den Sicherheitsrichtlinien der Institution entsprechen.

Auch ergibt sich ein hohes Potenzial an fehlerhafter Bedienung durch die Nutzer, wenn diese Technik und Funktionen der Videokonferenzlösung nur unzureichend beherrschen oder keine ausreichende Unterstützung zur Verfügung steht. Insbesondere bei modernen Videokonferenzlösungen mit vielfältig integrierten Diensten kann nicht davon ausgegangen werden, dass diese Systeme selbsterklärend sind. Eine unzureichende Unterstützung und Anleitung zur Bedienung kann auch dazu führen, dass Videokonferenzlösungen nur wenig genutzt werden. Eine hochwertige Ausstattung kann so zur Fehlinvestition werden.

5.3 Elementare Gefährdungen

Im IT-Grundschutz-Kompendium sind allgemeingültige, elementare Gefährdungen definiert, die übergreifend für viele Systeme zutreffen. Die folgenden elementaren Gefährdungen des IT-Grundschutz-Kompendiums gelten auch für Videokonferenzsysteme:

G 0.8 Ausfall oder Störung der Stromversorgung

G 0.9 Ausfall oder Störung von Kommunikationsnetzen

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.14 Ausspähen von Informationen (Spionage)

G 0.15 Abhören

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.19 Offenlegung schützenswerter Informationen

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

G 0.21 Manipulation von Hard- oder Software

G 0.23 Unbefugtes Eindringen in IT-Systeme

G 0.25 Ausfall von Geräten oder Systemen

G 0.26 Fehlfunktionen von Geräten oder Systemen

G 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.36 Identitätsdiebstahl

G 0.38 Missbrauch personenbezogener Daten

G 0.39 Schadprogramm

G 0.40 Verhinderung von Diensten (Denial of Service)

G 0.42 Social Engineering

G 0.43 Einspielen von Nachrichten

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

6 Sicherheitsanforderungen

Die in diesem Kapitel spezifizierten Sicherheitsforderungen berücksichtigen den Inhalt der Edition 2019 des IT-Grundschutz-Kompendiums des BSI (siehe [BSI GSK-2019]). Weiterhin orientiert sich das vorliegende Kompendium Videokonferenzsysteme an der Struktur der Bausteine des IT-Grundschutz-Kompendiums.

Die Sicherheitsanforderungen sind daher wie folgt gegliedert:

- Zunächst werden in Kapitel 6.1 generell die für die Absicherung der zugrundeliegenden Techniken von Videokonferenzsystemen zu beachtenden Bausteine des IT-Grundschutz-Kompendiums genannt. Diese enthalten jeweils Basis-Anforderungen, die vorrangig umgesetzt werden müssen, Standard-Anforderungen, die grundsätzlich umgesetzt werden sollten, weil sie dem Stand der Technik entsprechen, und Anforderungen, die bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten.
- In Kapitel 6.2, Kapitel 6.3 und Kapitel 6.4 werden dann für Videokonferenzsysteme spezifische Basis-Anforderungen, Standard-Anforderungen und Anforderungen bei erhöhtem Schutzbedarf aufgeführt.

6.1 Absicherung der zugrundeliegenden Techniken

Für die Absicherung von Videokonferenzsystemen gilt zunächst einmal all das, was auch für die sonstige IT gilt. Generell sind für Videokonferenzsysteme verschiedene Bausteine des IT-Grundschutz-Kompendiums anzuwenden, die jedoch keine für Videokonferenzen spezifischen Anforderungen definieren, sondern die zugrundeliegenden Techniken der Videokonferenzlösung adressieren. Auf diese Bausteine wird im Folgenden nur verwiesen und ein Zusammenhang zu Videokonferenzsystemen hergestellt. Hierbei besteht aufgrund der vielfältigen Ausprägungen von Videokonferenzlösungen aber keine Garantie auf Vollständigkeit der genannten Bausteine. Je nach Videokonferenzlösung sind gegebenenfalls weitere Bausteine zu berücksichtigen.

Bei Bedarf werden in den folgenden Kapiteln auch Anforderungen einzelner Bausteine für Videokonferenzsysteme konkretisiert, wenn im Fall eines Videokonferenzsystems über die grundsätzlichen Anforderungen hinaus weitere Aspekte berücksichtigt werden müssen.

Grundsätzlich müssen für alle Komponenten einer Videokonferenzlösung die relevanten Infrastruktur-Bausteine, beispielsweise *INF.2 Rechenzentrum sowie Serverraum* für zentrale Komponenten und *INF.10 Besprechungs-, Veranstaltungs- und Schulungsraum* für Raumsysteme, angewendet werden.

Zentrale Komponenten

Für alle zentralen Komponenten eines Videokonferenzsystems muss der Baustein *SYS.1.1 Allgemeiner Server* angewendet werden. Falls es sich bei einer zentralen Komponente um eine Software auf einem Standardbetriebssystem der Form Windows, Linux oder Unix handelt, ist zur Absicherung des Betriebssystems ebenfalls der Baustein *SYS.1.2 Windows Server 2012* oder der Baustein *SYS.1.3 Server unter Unix* zu beachten.

Bei Nutzung virtualisierter zentraler Komponenten des Videokonferenzsystems muss der Baustein *SYS.1.5 Virtualisierung* zum Schutz der Virtualisierungslösung und der Virtuellen Maschinen (VMs) angewendet werden.

Werden zentrale Komponenten des Videokonferenzsystems in einer Cloud realisiert und beispielsweise als Software as a Service (SaaS) oder Infrastructure as a Service (IaaS) bereitgestellt, sind die Anforderungen des Bausteins *OPS.2.2 Cloud-Nutzung* relevant.

Da insbesondere klassische Videokonferenzsysteme typische Funktionen von TK-Anlagen beinhalten, muss auch der Baustein *NET.4.1 TK-Anlagen* beachtet werden.

Ebenso ist der Baustein *NET.4.2 VoIP* relevant, weil moderne Videokonferenzsysteme die Signalisierung und die Medienströme mit ähnlichen Mitteln übertragen, wie es bei Voice over IP (VoIP) der Fall ist.

Video-Endpunkte

Für die Video-Endpunkte im Sinne von Client-Systemen des Videokonferenzsystems gilt zunächst der Baustein *SYS.2.1 Allgemeiner Client*. Je nach Art des Client-Systems und vorliegendem Betriebssystem müssen darüber hinaus auch die folgenden Bausteine beachtet werden:

- *SYS.2.2.2 Clients unter Windows 8.1*
- *SYS.2.2.3 Clients unter Windows 10*
- *SYS.2.3 Clients unter Unix*
- *SYS.2.4 Clients unter macOS*
- *SYS.3.1 Laptops*
- *SYS.3.2.1 Allgemeine Smartphones und Tablets*
- *SYS.3.2.3 iOS (for Enterprise)*
- *SYS.3.2.4 Android*
- *SYS.3.3 Mobiltelefon*

Die Client-Systeme können durch IoT-Geräte wie z. B. Sprachsteuerungen ergänzt werden. Hierfür ist der Baustein *SYS.4.4 Allgemeines IoT-Gerät* zu beachten.

Netzwerk

Für Videokonferenzen ist außerdem der Baustein *NET.1.1 Netzarchitektur und -design* von besonderer Bedeutung, da hier unter anderem auch eine Segmentierung des Netzes in unterschiedliche Sicherheitssegmente spezifiziert wird, zwischen denen der Verkehr über Firewalls kontrolliert wird.

6.2 Basis-Anforderungen

Die folgenden Anforderungen müssen beim Einsatz einer Videokonferenzlösung vorrangig umgesetzt werden.

6.2.1 Anwendungen und zentrale Komponenten

A-1 Sicherer Umgang mit Videokonferenzdaten

Teilnehmerdaten, Zugangsdaten und andere kritische Videokonferenzdaten, wie z. B. Konferenzprofile, nutzerspezifische Einstellungen sowie PINs und Passwörter zur Freischaltung von Diensten und zum Zugang zu Konferenzräumen, müssen sicher gespeichert werden.

PINs, Passwörter und sonstige Daten mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit und Integrität müssen dabei verschlüsselt hinterlegt werden. Die Berechtigungen für den Zugriff auf Videokonferenzdaten müssen so eingestellt sein, dass nur die notwendigen Zugriffe für autorisierte Teilnehmer gestattet sind.

Somit erfordert der Zugriff auf Videokonferenzdaten eine erfolgreiche Authentisierung und muss verschlüsselt erfolgen. Die Protokolle für den Zugang auf Videokonferenzdaten müssen hinsichtlich Vertraulichkeit und Integrität abgesichert sein.

A-2 Unterschiedliche Profile für Videokonferenzen

Da Sicherheitseinstellungen von Videokonferenzlösungen oft sehr flexibel konfiguriert werden können und je nach Konferenz unterschiedliche Sicherheitsanforderungen bestehen, müssen unterschiedliche Profile für Videokonferenzen auf Basis der grundlegenden Sicherheits-einstellungen bereitgestellt und genutzt werden. Beispielsweise sollte ein spezifisches Profil für Videokonferenzen mit vertraulichem Inhalt erstellt werden.

A-3 Sicherer Umgang mit Metadaten

Metadaten von Videokonferenzen, z. B. Teilnehmer sowie Anfang und Ende der Konferenz, müssen verschlüsselt gespeichert oder mit vergleichbaren Sicherheitsmaßnahmen geschützt werden.

Die Berechtigungen für den Zugriff auf Metadaten müssen so eingestellt sein, dass nur die notwendigen Zugriffe für autorisierte Teilnehmer gestattet sind. Der Zugriff auf Metadaten erfordert eine erfolgreiche Authentisierung und muss verschlüsselt erfolgen, d. h. die Protokolle für den Zugriff auf Metadaten müssen hinsichtlich Vertraulichkeit und Integrität abgesichert sein.

A-4 Sicherer Umgang mit Konferenzaufzeichnungen

Die Aufzeichnung von Videokonferenzen und deren Nutzungszweck muss den teilnehmenden Parteien im Vorfeld bekannt gegeben und nachvollziehbar eine Zustimmung eingeholt werden.

Aufzeichnungen von Videokonferenzen müssen verschlüsselt übertragen und sicher gespeichert sowie gegen Manipulation geschützt werden. Werden dabei Teile der Videokonferenzlösung in einer Cloud realisiert, findet *OPS.2.2 Cloud-Nutzung* Anwendung.

Der Zugriff auf die Aufzeichnung von Videokonferenzen muss restriktiv geregelt sein. Je nach Schutzbedarf der Daten sollte hier ein Vier-Augen-Prinzip in Betracht gezogen werden. Diese Regelungen müssen auch die Weiterverarbeitung, z. B. Transkription, siehe A-21, sowie die Weitergabe an Dritte umfassen.

Die Verschlüsselung und der Schutz gegen Manipulationen der Videokonferenz-Aufzeichnung muss auch bei einer Archivierung der Aufzeichnung erhalten bleiben.

A-5 Absicherung von Dateiablagen

Videokonferenzlösungen können sowohl interne Dateiablagen des Videokonferenzsystems als auch externe Dateiablagen, die als Dienst über eine Schnittstelle erreichbar sind, nutzen. Beide Formen der Dateiablage müssen angemessen gegen unberechtigten Zugriff abgesichert werden, da hier in der Regel persistente Daten enthalten sind, die oft personenbezogen und vertraulich sind.

Insbesondere muss die Dateiablage selbst angemessen abgesichert und bei Aussonderung oder bei Weitergabe an Dritte sicher gelöscht werden.

6.2.2 Endgeräte und Clients

A-6 Absicherung von frei zugänglichen Video-Endpunkten

Video-Endpunkte, die frei zugänglich sind, insbesondere Raumsysteme und Videotelefone, müssen angemessen gegen unberechtigte Zugriffe geschützt sein. Dies gilt auch für Smartphones und Mobiltelefone, die aufgrund ihrer Mobilität und Größe leicht entwendet und dann unberechtigt genutzt werden können.

Ein nicht genutzter dedizierter, frei zugänglicher Video-Endpunkt muss deaktiviert werden, um eine missbräuchliche Nutzung zu verhindern.

A-7 Beenden von Sitzungen und Anmeldungen an Video-Endpunkten

Nach Beendigung einer Videokonferenz muss die Videokonferenzsitzung beendet werden. Bei gemeinsam genutzten Geräten, z. B. Raumsystemen, muss auch zusätzlich ein Abmelden des Nutzers am Gerät erfolgen.

A-8 Absicherung der internen Dateiablage des Video-Endpunkts

Videokonferenzlösungen können auch die interne Dateiablage des Video-Endpunkts nutzen. Daher muss diese angemessen gegen unberechtigten Zugriff abgesichert werden, da hier in der Regel persistente Daten enthalten sind, die oft personenbezogen und vertraulich sind. Bei Aussonderung oder Weitergabe des Endpunktes muss die interne Dateiablage eines Video-Endpunkts sicher gelöscht werden.

6.2.3 Netzwerk

A-9 Dediziertes Sicherheitssegment für frei zugängliche Video-Endpunkte

Frei zugängliche Video-Endpunkte, insbesondere Raumsysteme und Videotelefone, müssen in dedizierten Sicherheitssegmenten lokalisiert werden. Dabei sind die Vorgaben der Anforderung *NET.1.1.A5 Client-Server-Segmentierung* im Baustein *NET.1.1 Netzarchitektur und -design* zu berücksichtigen (siehe [BSI GSK-2019]).

A-10 Positionierung von Cloud Connector und Video Edge Server in einer DMZ

Ein Cloud Connector muss grundsätzlich in einer DMZ positioniert werden.

Eine besondere Rolle spielt dabei der Video Edge Server. Ein lokaler Video Edge Server ist als Cloud-Komponente zu sehen, auf die die jeweilige Institution, die den Video Edge Server einsetzt, nur einen eingeschränkten administrativen Zugriff hat. Daher muss ein Video Edge Server in einer DMZ am Internet-Zugang unter besonderer Berücksichtigung des Bausteins *NET.1.1 Netzarchitektur und -design* realisiert werden. Jegliche Kommunikation muss mit Firewall-Techniken kontrolliert werden. Dies gilt insbesondere für die administrative Kommunikation des Cloud-Providers mit dem Video Edge Server. Dabei sollten speziell die Vorgaben von *NET1.1.A21 Separierung des Management-Bereichs* beachtet werden.

6.2.4 Planung und Betrieb

A-11 Planung und Beschaffung der Videokonferenzlösung

Jede Videokonferenzlösung muss geeignet geplant werden, dabei sind mindestens folgende Punkte zu berücksichtigen:

- Anforderungsanalyse inklusive Sicherheitsanforderungen
- Analyse der verbundenen bzw. integrierten Systeme, Schnittstellen und Dienste
- Grobkonzept inklusive
  - Berücksichtigung von Architekturvorgaben der Institution (Enterprise Architecture)
  - Entscheidungen bezüglich der Architektur, z. B. ob Cloud-Dienste, KI-Funktionen oder Virtualisierung genutzt werden sollen
  - Festlegung der geforderten Verfügbarkeit
  - Festlegung zur Verschlüsselung bei Transport und Speicherung
  - Festlegung zur Authentisierung inklusive erlaubter Authentisierungsverfahren

  - Festlegung zur Protokollierung, insbesondere benötigte und erlaubte Protokollierungsinhalte und Umgang mit diesen
  - Festlegung zum Monitoring, insbesondere Integration in eine zentrale Monitoring-Lösung der Institution
- Dimensionierung der Lösung und gegebenenfalls Anpassung der Dimensionierung des genutzten Netzes, damit es den anfallenden Datenverkehr der Videokonferenzen verarbeiten kann.

A-12 Erstellung eines Rollen- und Berechtigungskonzepts

Für die Videokonferenzlösung muss ein Rollen- und Berechtigungskonzept erstellt werden, das die Rollen und deren Berechtigungen für die Videokonferenzlösung im minimal notwendigen Umfang festlegt. Dabei sind die Rollen und Berechtigungen mit den Profilen gemäß A-2 „Unterschiedliche Profile für Videokonferenzen“ abzustimmen.

Hierbei ist zu berücksichtigen, dass gemäß *SYS.1.1.A6 Deaktivierung nicht benötigter Dienste und Kennungen* vorhandene Standard- bzw. Default-Nutzer soweit wie möglich geändert oder deaktiviert sowie voreingestellte Passwörter von Standard-Nutzern geändert werden müssen.

A-13 Bereitstellung von Informationen zur sicheren Nutzung von Videokonferenzen

Um allen Nutzern der Videokonferenzlösung eine sichere Nutzung der Lösung zu ermöglichen, muss ein Handbuch für den Nutzer erstellt werden, das insbesondere auch Anweisungen bezüglich Informationssicherheit sowie die zu beachtenden Richtlinien und Regularien umfasst. Dieses Handbuch muss allen Nutzern der Videokonferenzlösung zugänglich sein.

Darüber hinaus müssen Regelungen für die Nutzung der Videokonferenzlösung getroffen werden, die auch Themen wie Datenschutz und die Nutzung von KI-Funktionen beinhalten und für alle Nutzer der Videokonferenzlösung verbindlich sind.

A-14 Integration in das Schwachstellen- und Patch-Management

Alle Elemente des Videokonferenzsystems müssen insbesondere aufgrund der bestehenden Verzahnung mit anderen Systemen und Diensten in das Schwachstellen- und Patch-Management der Institution integriert werden. Mindestens muss die Durchführung von Patches auf allen beteiligten und integrierten Elementen geplant und im Vorfeld der Nutzung getestet werden.

6.3 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Standard-Anforderungen dem Stand der Technik für die Absicherung von Videokonferenzsystemen. Sie sollten grundsätzlich umgesetzt werden.

6.3.1 Anwendungen und zentrale Komponenten

A-15 Verschlüsselung der mit IP übertragenen Daten der Videokonferenz auf nicht vertrauenswürdigen Übertragungsstrecken

Erfolgt eine Kommunikation über nicht oder nur eingeschränkt vertrauenswürdige Netze oder Übertragungsstrecken, sollten die Medienströme und die Signalisierung verschlüsselt werden.

Werden weitere Daten in separaten Verbindungen übertragen, z. B. Chat oder Dateitransfer, sollte auch diese Kommunikation verschlüsselt erfolgen, falls die Kommunikation über nicht oder nur eingeschränkt vertrauenswürdige Netze oder Übertragungsstrecken erfolgt.

Dabei muss die Verschlüsselung unter Berücksichtigung der Vorgaben von [BSI TR02102-2019] erfolgen.

Die Nutzer der Videokonferenz sollten über den Status der Verschlüsselung informiert werden.

A-16 Deaktivierung nicht benötigter Dienste und Leistungsmerkmale

Über die Umsetzung der Anforderung *SYS.1.1.A6 Deaktivierung nicht benötigter Dienste und Kennungen* hinaus sollten auch alle nicht benötigten bzw. nicht zulässigen Dienste und Leistungsmerkmale der Videokonferenzlösung deaktiviert oder deinstalliert werden. Sind beispielsweise Komfortfunktionen wie eine Raumprüfung nicht erlaubt, sollte die selbstständige Aktivierung eines Raumsystems unterbunden werden.

Auch hier sollten die getroffenen Entscheidungen so dokumentiert werden, dass nachvollzogen werden kann, welche Konfiguration für die Anwendungen und zentralen Komponenten der Videokonferenzlösung gewählt wurden.

A-17 Sichere Nutzerverwaltung

Für die Videokonferenzlösung sollte die Nutzerverwaltung angemessen abgesichert werden.

Erfolgt eine Nutzerverwaltung innerhalb der Videokonferenzlösung, gilt der Baustein *APP.2.1 Allgemeiner Verzeichnisdienst*.

Erfolgt die Nutzerverwaltung über einen externen Verzeichnisdienst, so ist auch hier der Baustein *APP.2.1 Allgemeiner Verzeichnisdienst* anzuwenden. Bei Bedarf sind ebenfalls die Bausteine *APP.2.2 Active Directory* und *APP.2.3 OpenLDAP* zu berücksichtigen. Für die Integration von Videokonferenzlösungen gelten dabei insbesondere die folgenden Maßnahmen:

- *APP.2.1.A13 Absicherung der Kommunikation mit Verzeichnisdiensten*
- *APP.2.2.A8 Konfiguration des sicheren Kanals unter Windows*
- *APP.2.3.A6 Sichere Authentisierung gegenüber OpenLDAP*

A-18 Sichere Konfiguration von geplanten Videokonferenzen

Werden Videokonferenzen z. B. über Groupware-Lösungen geplant, sollte der Zugang zur Konferenz so abgesichert werden, dass ein unautorisierter Zugriff auf die Konferenz vermieden wird. Beispiele hierzu sind die Vergabe eines Passworts bzw. einer PIN gemäß den Vorgaben der jeweiligen Institution oder die Erzwingung eines Wartebereichs, aus dem ein Teilnehmer erst entlassen wird, wenn der Moderator der Konferenz sich ebenfalls eingewählt und den Teilnehmer zugelassen hat.

A-19 Sichere Anbindung der Videokonferenzlösung an Systeme des Gebäudemanagements

Werden Funktionen des Gebäudemanagements durch ein Videokonferenzsystem genutzt, z. B. zur Verdunklung des Konferenzraums, sollte diese Anbindung angemessen abgesichert werden. Dies beinhaltet sowohl die missbräuchliche Nutzung der Gebäudetechnik über die Videokonferenzlösung als auch die Kompromittierung einer Videokonferenz durch unzureichend abgesicherte Gebäudetechnik.

A-20 Absicherung von Konferenzräumen

Virtuelle Konferenzräume von Videokonferenzen sollten unter Berücksichtigung integrierter Dienste, wie z. B. UC- und UCC-Dienste, vor unberechtigtem Zugriff und der unbemerkten Anwesenheit von Teilnehmern und insbesondere Angreifern bzw. Lauschern geschützt werden.

Teilnehmer einer Videokonferenz sollten angemessen authentisiert werden und der Moderator der Videokonferenz sollte die Identität aller Teilnehmer prüfen. Insbesondere wenn Teilnehmer

über eine reine Audio-Einwahl an einer Videokonferenz teilnehmen, sollte der Moderator zumindest einen Plausibilitäts-Check von Stimme und Telefonnummer durchführen.

Hierzu gehört auch, dass innerhalb der Anzeige des Video-Endpunkts die übrigen Teilnehmer der Videokonferenz angezeigt werden. Treten der Videokonferenz neue Teilnehmer bei oder treten Teilnehmer aus, so sollte dieser Vorgang allen in der Videokonferenz befindlichen Teilnehmern signalisiert werden.

A-21 Absicherung und Einschränkung von Auswertungen von Videokonferenzinhalten

Mit Hilfe von Künstlicher Intelligenz können Videokonferenzinhalte ausgewertet werden. Dies ist sowohl während der Konferenz, z. B. durch Einblenden von Namen aufgrund einer Gesichtserkennung, als auch im Nachhinein anhand von Aufzeichnungen einer Videokonferenz (siehe A-4) möglich.

Soll eine Videokonferenz aufgezeichnet und hieraus die Videokonferenzinhalte ausgewertet werden, muss nachvollziehbar eine Zustimmung der teilnehmenden Parteien eingeholt und diese dauerhaft dokumentiert werden (siehe A-4).

Für Auswertungen während einer Videokonferenz sollte sichergestellt werden, dass nur solche Auswertungen möglich sind, die den Richtlinien der Institution und der geltenden Gesetzeslage entsprechen. Sobald eine Auswertung erfolgt, die nicht dem Zweck oder Komfort der Videokonferenz dient, beispielsweise die Analyse des Verhaltens eines Teilnehmer zur Einschätzung des emotionalen Zustands, erfordert dies grundsätzlich die Zustimmung der Teilnehmer.

Bedingen die Auswertungen die Aufbewahrung von weiteren Dokumenten, beispielsweise die Transkription von Videokonferenzen, so gilt die Anforderung A-5.

A-22 Festlegung des Speicherortes der Daten bei Outsourcing und Cloud-Nutzung

Bei Outsourcing und Cloud-Nutzung sollte darauf geachtet werden, dass der Ort der Verarbeitung und Speicherung der Daten, insbesondere die Länder bzw. die Region, von vornherein festgelegt werden kann. Dies gilt auch für die Verarbeitung von Daten einer für die Videokonferenz genutzten Sprachsteuerung. Dabei ist auf die Einhaltung der DSGVO (siehe [DSGVO-2018]) zu achten.

A-23 Cloud-Verfügbarkeit

Werden Teile des Videokonferenzsystems in einer Cloud realisiert, sollte die Verfügbarkeit der Cloud und der Cloud-Anbindung in der Planung und der Vertragsgestaltung berücksichtigt und durch ein Monitoring überwacht werden.

Hierbei ist die Cloud-Verfügbarkeit sowohl für die in der Cloud realisierten Komponenten und damit für die Verfügbarkeit der Videokonferenzlösung wichtig als auch für andere integrierte UCC-Dienste wie z. B. gemeinsame Dokumentenablagen und Wikis, da der Zugriff auf diese sonst nicht möglich ist.

6.3.2 Endgeräte und Clients

A-24 Deaktivierung oder zumindest Absicherung eines Web-Servers auf einem Video-Endpunkt

Ist auf einem Video-Endpunkt ein Web-Server realisiert, sollte dieser deaktiviert werden, um einen Missbrauch zu verhindern. Sollte dies nicht umsetzbar sein, weil der Web-Server z. B. für die Administration des Video-Endpunkts benötigt wird, ist für die Webanwendung der Baustein *APP.3.1 Webanwendungen* und für den zugrundeliegenden Web-Server der Baustein *APP.3.2 Webserver* zu beachten.

A-25 Deaktivierung oder zumindest Einschränkung der Sprachsteuerung einer Videokonferenz

Es sollte möglich sein, die Sprachsteuerung eines Video-Endpunkts zu deaktivieren oder zumindest einzuschränken, um eine missbräuchliche Nutzung zu verhindern. Dabei kann es sich um eine Sprachsteuerung handeln, die in einem Video-Endpunkt integriert ist, oder um eine Sprachsteuerung des IoT, die mit dem Video-Endpunkt verbunden ist. Wird die Sprachsteuerung für eine Videokonferenz nicht benötigt, sollte sie deaktiviert werden. Außerhalb der Vorbereitung, Durchführung und Nachbereitung einer Videokonferenz sollte die Sprachsteuerung grundsätzlich deaktiviert sein.

A-26 Einschränkung des lokalen Zugriffs auf die Konfiguration von dedizierten Video-Endpunkten

Der lokale Zugriff auf die Konfiguration eines dedizierten Video-Endpunkts, beispielsweise ein Raumsystem, sollte eingeschränkt werden, um unberechtigte oder ungewollte Änderungen der Konfiguration zu vermeiden.

A-27 Deaktivierung der automatischen Annahme eines Video-Anrufs

Video-Endpunkte bieten in der Regel die Möglichkeit der automatischen Annahme eines Video-Anrufs. Damit ist es möglich, zu jeder Zeit einen Anruf auf eine bekannte Adresse eines Video-Endpunkts zu initiieren und über die automatische Annahme des Video-Anrufs sowohl Bild als auch Ton zu aktivieren.

Funktionen zur automatischen Annahme eines Video-Anrufs sollten im Video-Endpunkt deaktiviert werden, um eine unbemerkte Überwachung oder ein Abhören zu verhindern. Zumindest sollte sichtbar angezeigt werden, ob ein Video-Endpunkt aktiv ist oder nicht.

A-28 Signalisierung der Kamera- und Mikrofonaktivität

Damit eine Leistungsüberwachung oder das Ausspähen von Personen und Räumlichkeiten erkannt werden kann, sollten Endgeräte mit optischer Signalisierung der Kamera- und Mikrofonaktivität eingesetzt werden.

A-29 Geeignete Standortwahl

Für Video-Endpunkte, insbesondere für mobile Endgeräte wie PCs und Laptops, sollte auf eine geeignete Standortwahl geachtet werden, um die Gefährdung durch einen versehentlichen Informationsabfluss in Bild und Ton zu minimieren. Außerdem ist darauf zu achten, dass unbeteiligte Personen durch die Videoübertragung nicht erfasst werden, da hierdurch gegen den Datenschutz verstoßen wird und sogar eine unbemerkte Leistungsüberwachung ermöglicht wird.

A-30 Ausblenden des Hintergrunds bei Videokonferenzen

Einige Videokonferenzlösungen bieten die Möglichkeit, den Hintergrund von Videokonferenz-übertragungen unkenntlich zu machen und somit nur das Bild des Sprechers zu übertragen. Diese Funktion sollte insbesondere bei PCs oder Laptops mit Videokamera eingesetzt werden, um einen versehentlichen Abfluss von Informationen oder eine Bilderfassung unbeteiligter Personen zu vermeiden.

A-31 Absicherung der direkten Kommunikation zwischen Standard-Client und Raumsystem

Wird ein Standard-Client direkt mit einem Raumsystem verbunden, um z. B. Dokumente vom Standard-Client in einer Videokonferenz anzuzeigen, sollte die Kommunikation zwischen den beiden Clients abgesichert werden. Erfolgt die Kommunikation drahtlos, z. B. über Bluetooth, ist eine angemessene Authentisierung und Verschlüsselung erforderlich.

6.3.3 Netzwerk

A-32 Dediziertes Sicherheitssegment für zentrale Komponenten des Videokonferenzsystems

Falls die zentralen Komponenten des Videokonferenzsystems nicht angemessen abgesichert werden können, sollten zumindest die betroffenen Komponenten einem oder mehreren eigenen Sicherheitssegmenten unter Berücksichtigungen der Anforderungen in Baustein *NET.1.1 Netzarchitektur und -design* des IT-Grundschutz-Kompendiums, insbesondere der Anforderung *NET.1.1.A22 Spezifikation des Segmentierungskonzepts*, zugeordnet werden.

Hierbei ist ein Sicherheitssegment eine Separierung von Netzbereichen, zwischen denen die Kommunikation mit Firewall-Techniken kontrolliert wird. Sicherheitssegmente können logisch voneinander getrennt werden.

A-33 Absicherung des lokalen Netzzugangs

Falls eine vertrauliche Kommunikation, insbesondere Signalisierung und Medienströme, zwischen den Endpunkten einer Videokonferenzlösung nicht angemessen verschlüsselt werden kann, sollten die Endgeräte der Videokonferenzlösung auf Ebene des Netzwerks über eine Netzzugangskontrolle (Network Access Control, NAC) authentisiert werden und die LAN-Switches so konfiguriert werden, dass Lauschattacken beispielsweise mittels ARP Spoofing unterbunden werden.

A-34 Einsatz eines SBC am Internet-Übergang

Für Videokonferenzen über das Internet bzw. allgemein über eingeschränkt vertrauenswürdige Netze sollte ein Session Border Controller (SBC) in einer DMZ unter besonderer Berücksichtigung des Bausteins *NET.1.1 Netzarchitektur und -design* des IT-Grundschutz-Kompendiums realisiert werden. Dieser SBC sollte als Verschlüsselungsendpunkt die Signalisierung und die Medienströme terminieren. Der SBC sollte für die Signalisierung und die Medienströme Filterfunktionen unterstützen, die zur weiteren Absicherung der Kommunikation genutzt werden sollten.

6.3.4 Planung und Betrieb

A-35 Erstellung von Fein- und Betriebskonzept für die Videokonferenzlösung

Eine Feinplanung für die Videokonferenzlösung sollte durchgeführt, in einem Feinkonzept dokumentiert, regelmäßig geprüft und nachhaltig gepflegt werden.

Für die Videokonferenzlösung sollte ein erweitertes Betriebskonzept erstellt werden. Hierbei bildet die durch die Integration von anderen Diensten bedingte Verzahnung mit anderen Betriebskonzepten eine besondere Herausforderung.

Insbesondere sollten mit einem solchen Betriebskonzept der Betrieb zwischen Videokonferenzlösung und integrierten Diensten harmonisiert und klare Zuständigkeiten festgelegt werden. Hierdurch werden bei der Durchführung von Administrations- und Betriebsaufgaben sowie der Fehlerbehebung Verzögerungen durch eine ungeklärte Organisation des Betriebs vermieden.

A-36 Einbindung der Videokonferenzlösung in Datensicherungs- und Archivierungskonzept

Werden im Rahmen der Videokonferenz Daten aufgezeichnet, sollten diese Dateiablagen bzw. Datenbanken sowohl im Datensicherungskonzept als auch im Archivierungskonzept angemessen berücksichtigt werden. Außerdem sollten insbesondere bei der Nutzung von Cloud-Diensten alle Speicherorte der Videokonferenzlösung einbezogen werden.

A-37 Penetrationstest der Videokonferenzlösung

Die Videokonferenzlösung, alle integrierten Dienste und alle Administrations-Schnittstellen sollten regelmäßig einem Penetrationstest unterzogen werden. Hierbei sollten auch gegebenenfalls genutzte KI-Funktionen berücksichtigt werden.

A-38 Schulungen zur sicheren Nutzung von Videokonferenzen

Zusätzlich zur Bereitstellung von Informationen zur sicheren Nutzung von Videokonferenzen sollten Nutzer entsprechende Schulungen erhalten, die auch alle integrierten Dienste umfassen. Außerdem sollten diese Schulungen auch eine Sensibilisierung bezüglich der Informationssicherheit bei der Nutzung der Videokonferenzlösung beinhalten. Dies sollte insbesondere auch Themen wie Cloud und KI sowie die zu beachtenden Richtlinien und Regularien einschließen.

A-39 Aufnahme der Videokonferenzlösung in die Prozesse zur Behandlung von Schwachstellen und Sicherheitsvorfällen

Die zentralen Komponenten der Videokonferenzlösung inklusive etwaiger Cloud-Komponenten sollten in das Schwachstellen-Management aufgenommen werden, um Sicherheitslücken zu vermeiden und Angriffe zu erschweren (siehe Baustein *DER.1 Detektion von sicherheitsrelevanten Ereignissen* des IT-Grundschutz-Kompendiums). Insbesondere sollten die Anforderungen *DER.1.A9 Einsatz zusätzlicher Detektionssysteme* und *DER.1.A12 Auswertung von Informationen aus externen Quellen* beachtet werden.

Weiterhin sollte die Videokonferenzlösung in den Prozess zur Behandlung von Sicherheitsvorfällen aufgenommen werden (siehe Baustein *DER.2.1 Behandlung von Sicherheitsvorfällen* des IT-Grundschutz-Kompendiums). Dies ist besonders wichtig, da die Videokonferenzlösung hier quasi in der Rolle einer Spinne in der Mitte eines großen Netzes von Anwendungen und Systemen ist. Ein Sicherheitsvorfall kann so über die reine Videokonferenzlösung hinaus eine Wirkung entfalten und beispielsweise kann ein Angreifer ausgehend von der Videokonferenzlösung über die verfügbaren Schnittstellen andere Anwendungen angreifen. Hiervon betroffen sind vor allem Meeting Solutions und UC- bzw. UCC-Lösungen, die Videokonferenzen mit zahlreichen anderen Diensten vereinen.

A-40 Überwachung durch IT-Monitoring

Der konkrete Monitoring-Bedarf sollte geklärt werden und sowohl auf Konzeptebene als auch bei der Beschaffung der Lösung berücksichtigt werden.

Dabei sollten mindestens die zentralen Komponenten des Videokonferenzsystems und wenn möglich auch etwaige Cloud-Komponenten durch das IT-Monitoring überwacht werden. Insbesondere sollte neben Fehlerzuständen auch die Qualität der Videokonferenzen berücksichtigt werden.

A-41 Integration in zentrales Log-Management

Die zentralen Komponenten des Videokonferenzsystems und möglichst auch etwaige Cloud-Komponenten sollten in das zentrale Log-Management integriert werden.

Hierzu ist festzulegen, welche Ereignisse im Log-Management erfasst werden. Die Ereignisprotokolle sollten sicher erzeugt, aufbewahrt und regelmäßig geprüft werden (siehe auch [ISO 27001-2017], Anforderung A.12.4.1).

6.4 Anforderungen bei erhöhtem Schutzbedarf

Die folgenden Sicherheitsanforderungen sollten bei erhöhtem Schutzbedarf in Betracht gezogen werden.

6.4.1 Anwendungen und zentrale Komponenten

A-42 Durchgängige Verschlüsselung der mit IP übertragenen Daten einer Videokonferenz

Ergänzend zu A-15 sollten bei erhöhtem Schutzbedarf die Medienströme und die Signalisierung durchgängig auf der gesamten Übertragungsstrecke verschlüsselt werden. Dabei sollte eine MCU so konfigurierbar sein, dass sie nur verschlüsselte Verbindungen zulässt. Komponenten, die keine geeignete Verschlüsselung unterstützen, sollten nicht eingesetzt werden.

Falls weitere Daten in separaten Verbindungen übertragen werden, z. B. Chat oder Dateitransfer, oder auch eine direkte Kommunikation zwischen Standard-Client und Raumsystem zur Bereitstellung von dort gespeicherten Informationen besteht, sollte auch diese Kommunikation verschlüsselt erfolgen.

Dabei sollte die Verschlüsselung unter Berücksichtigung der Vorgaben von [BSI TR02102-2019] erfolgen.

A-43 Ende-zu-Ende-Verschlüsselung der mit IP übertragenen Daten einer Videokonferenz

Bei erhöhtem Schutzbedarf sollte eine Ende-zu-Ende-Verschlüsselung in Betracht gezogen werden. Hierbei muss berücksichtigt werden, dass dann eine MCU keine Optimierung der erforderlichen Verbindungen mehr vornehmen kann.

Dabei sollte die Verschlüsselung unter Berücksichtigung der Vorgaben von [BSI TR02102-2019] erfolgen.

A-44 Authentisierung zwischen Video-Endpunkten und zentralen Komponenten

Für den erhöhten Schutzbedarf sollte zwischen den Video-Endpunkten und den zentralen Komponenten der Videokonferenz-Lösung eine Authentisierung erfolgen. Dabei sollte nach Möglichkeit eine gegenseitige Authentisierung stattfinden. Dies gilt insbesondere, wenn die zentralen Komponenten in einer Cloud realisiert sind.

Komponenten, die keine geeignete Authentisierung unterstützen, sollten nicht eingesetzt werden.

A-45 Zusätzliche Absicherung der Konfiguration von geplanten Videokonferenzen

Werden Videokonferenzen mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit geplant, sollten ergänzend zu Anforderung A-18 Passwörter oder PINs für der Zugang zur Konferenz nur über einen separaten vertrauenswürdigen Kanal übermittelt werden und nicht direkt in der Einladung genannt werden.

Außerdem sollten Passwörter bzw. PINs eine hohe Komplexität aufweisen und die Vorgaben der jeweiligen Institution berücksichtigen.

Darüber hinaus sollte die Anzahl der Vertreter des Moderators in der Einladung auf die Notwendigkeit gemäß den Verfügbarkeitsanforderungen beschränkt werden. Bei Videokonferenzen mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit und Integrität sollte die Vertreterrolle nur an angemessen vertrauenswürdige Teilnehmer vergeben werden.

A-46 Protokollierung der Tätigkeit von Systembedienern

Bei erhöhtem Schutzbedarf sollten alle Tätigkeiten von Systembedienern aufgezeichnet werden und diese Aufzeichnungen geschützt und regelmäßig geprüft werden (siehe [ISO 27001-2017], Anforderung A.12.4.3).

A-47 Zusätzliche Datensicherung

Werden Dokumente z. B. für die Bearbeitung während Videokonferenzen in einer Cloud abgelegt, sollten diese bei erhöhtem Schutzbedarf ergänzend zu Anforderung A-36 lokal oder mindestens bei einem anderen Cloud-Dienst gesichert werden, um ihre Verfügbarkeit sicherzustellen.

A-48 Zertifizierung nach Common Criteria für zentrale Komponenten des Videokonferenzsystems

Eine wichtige Grundlage zur effektiven Härtung der zentralen Systeme des Videokonferenzsystems ist die Vertrauenswürdigkeit der verwendeten Server-Plattform bzw. des Server-Betriebssystems. Hierzu sollte eine Zertifizierung nach Common Criteria (mindestens gemäß einem Protection Profile) oder vergleichbar vorliegen. Bei erhöhtem Schutzbedarf sollte eine Zertifizierung nach Evaluation Assurance Level (EAL) mindestens mit Stufe EAL2 nachgewiesen werden. Wünschenswert ist jedoch Stufe EAL4 oder besser EAL4+.

A-49 Vermeidung von Verschlüsselungsendpunkten in einer Cloud

Bei erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit oder Integrität sollte eine Verschlüsslung der Daten so erfolgen, dass kein Verschlüsselungsendpunkt in einer Cloud vorliegt. Wenn dies aus technischen Gründen unumgänglich ist, muss zumindest das Schlüsselmanagement auf Seiten des Cloud-Nutzers oder eines entsprechend vertrauenswürdigen weiteren Cloud-Dienstleisters liegen. Andernfalls sind Dienste aus der Public Cloud oder der Virtual Private Cloud bei dem aktuellen Stand der Technik für die Verarbeitung von Daten mit erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit oder Integrität nicht geeignet.

A-50 Keine Aufzeichnung von Videokonferenzinhalten

Bei erhöhtem Schutzbedarf sollte organisatorisch geregelt werden, ob überhaupt, in welchem Umfang und unter welchen Rahmenbedingungen Aufzeichnungen von Videokonferenzen zulässig sind (siehe Anforderung A-4).

Grundsätzlich sollten bei erhöhtem Schutzbedarf Videokonferenzinhalte nicht aufgezeichnet werden, wenn sich ein Verschlüsselungsendpunkt in der Cloud befindet.

A-51 Einsatz von Host-basierten DLP-Systemen

Um einen unberechtigten Abfluss von Daten insbesondere in eine Cloud zu verhindern, sollten Host-basierte Data-Loss-Prevention-Systeme (DLP-Systeme) eingesetzt werden. Diese Systeme stellen sicher, dass kritische Daten nicht über Internet oder Weitverkehrsnetze an unberechtigte Empfänger oder beispielsweise in eine Cloud übertragen werden.

A-52 Einschränkung von KI-Funktionen

Bei erhöhtem Schutzbedarf sollte die Nutzung von KI-Funktionen nach Möglichkeit deaktiviert, zumindest aber auf ein Minimum reduziert werden. Ist eine permanente Deaktivierung nicht möglich oder erwünscht, muss ein Prozess etabliert werden, der sicherstellt, dass der Nutzer einer Videokonferenzlösung vor einer Konferenz zielgerichtet KI-Funktionen deaktiviert.

6.4.2 Endgeräte und Clients

A-53 Ausschließliche Nutzung von verschlüsselter Kommunikation

Die Medienströme sollten durchgängig auf der gesamten Übertragungsstrecke unter Berücksichtigung von [BSI TR02102-2019] verschlüsselt werden (siehe A-42 bzw. A-43). Video-Endpunkte, die keine geeignete Verschlüsselung unterstützen, sollten bei erhöhtem Schutzbedarf nicht eingesetzt werden.

Hierzu gehört auch die direkte Kommunikation zwischen Standard-Client und Raumsystem zur Bereitstellung von dort gespeicherten Informationen.

A-54 Verzicht auf Videokonferenzen in Großraumbüros

Ergänzend zu A-29 sollten bei erhöhtem Schutzbedarf Videokonferenzen ausschließlich in sicheren Umgebungen durchgeführt werden. Insbesondere sind Büros mit mehreren Arbeitsplätzen zu meiden. Ansonsten ist zumindest die Hörbarkeit von Informationen mit erhöhtem Schutzbedarf nicht gesichert vermeidbar.

A-55 Verzicht auf Sprachsteuerung

Bei erhöhtem Schutzbedarf sollte auf die Nutzung von Sprachsteuerung verzichtet werden, da nicht auszuschließen ist, dass die Analyse der Sprachdaten zur Erkennung von Kommandos an die Videokonferenzlösung außerhalb der Europäischen Union erfolgt.

6.4.3 Netzwerk

A-56 Einsatz eines SBC am WAN-Übergang

Ergänzend zu A-34 erfolgt in vielen Fällen auch am WAN-Übergang eine Kontrolle der WAN-Kommunikation mit Firewall-Techniken. Bei erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit oder Integrität sollte am WAN-Zugang für Videokonferenzen zusätzlich einen SBC eingesetzt werden.

A-57 Einsatz von Netz-basierten DLP-Systemen

Zur Verhinderung von unberechtigten Bewegungen von Daten, insbesondere zu externen Netzen, sollten zusätzlich zu A-51 „Einsatz von Host-basierten DLP-Systemen“ ebenfalls Netz-basierte DLP-Systeme eingesetzt werden. Hiermit wird auf Netzebene der Datenverkehr entsprechend kontrolliert, sodass Daten mit erhöhtem Schutzbedarf weder unbeabsichtigt noch vorsätzlich die Institution verlassen können.

6.4.4 Planung und Betrieb

A-58 Sichere Administration

Bei erhöhtem Schutzbedarf sollten die zentralen Komponenten der Videokonferenzlösung über separate Interfaces administriert werden, die an ein separates Administrationsnetz angebunden werden. Die Administration sollte dann über einen Managementbereich kompatibel zur Anforderung *NET.1.1 A21 Separierung des Managementbereichs* erfolgen.

Bei erhöhtem Schutzbedarf sollten die Tätigkeiten von Systemadministratoren aufgezeichnet werden und diese Aufzeichnungen geschützt und regelmäßig überprüft werden (siehe [ISO 27001-2017], Anforderung A.12.4.3).

A-59 Ausschließliche Datenablage innerhalb der Europäischen Union (EU)

Bei erhöhtem Schutzbedarf sollten alle Konferenzdaten und während einer Videokonferenz genutzten Dokumente ausschließlich innerhalb der EU unter Beachtung der DSGVO (siehe [DSGVO-2018]) transportiert und gespeichert werden. Wenn dies bedingt durch die Teilnahme von Nutzern außerhalb der EU nicht möglich ist, sollte sichergestellt werden, dass eine Übertragung und Speicherung auch hier konform zur DSGVO erfolgt.

A-60 Überwachung durch ein Security Information and Event Management (SIEM)

Die zentralen Komponenten der Videokonferenzlösung sollten bei erhöhtem Schutzbedarf durch ein SIEM überwacht werden. Dies sollte zumindest für Komponenten, die Verschlüsselungsendpunkte realisieren, z. B. MCUs, oder die an Vertrauensgrenzen positioniert sind, z. B. SBCs, umgesetzt werden.

A-61 Aufnahme der Videokonferenzlösung in die Notfallvorsorge

Die zentralen Komponenten des Videokonferenzsystems inklusive etwaiger Cloud-Komponenten sollten bei erhöhtem Schutzbedarf hinsichtlich der Verfügbarkeit in die Notfallvorsorge aufgenommen werden. Hierzu gehört bei erhöhten Verfügbarkeitsanforderungen auch die Verfügbarkeit von Redundanzen, Ersatzteilen oder Ersatzgeräten.

A-62 Lesender Zugriff auf von einem Dienstleister betriebene Komponenten

Der Dienstleister sollte der Institution lesenden Zugriff auf die bereitgestellten und vom Dienstleister betriebenen Komponenten der Videokonferenzlösung gewähren, damit diese hinsichtlich ihrer ordnungsgemäßen Funktionalität überprüft werden können. Außerdem ist nur so eine lückenlose Überwachung der Komponenten möglich.

7 Umsetzungshinweise

Die in diesem Kapitel spezifizierten Umsetzungshinweise geben Hilfestellung für die Erfüllung der in Kapitel 6 genannten Anforderungen an Videokonferenzlösungen. Hierfür wird zunächst der Lebenszyklus einer Videokonferenzlösung betrachtet und anschließend für jede in Kapitel 6 genannte Anforderung eine Maßnahme zur Erfüllung dieser Anforderung spezifiziert.

7.1 Lebenszyklus

Im Folgenden wird der Lebenszyklus für eine Videokonferenzlösung von der Planung und Konzeption bis zur Aussonderung dargestellt (siehe Abbildung 14).

Abbildung 14: Lebenszyklus einer Videokonferenzlösung

7.1.1 Planung und Konzeption

Im Vorfeld der eigentlichen Planung ist eine Anforderungsanalyse durchzuführen, aus der sich auch Vorgaben für die einzusetzenden zentralen Systeme bzw. die Cloud-Lösung und die Video-Endpunkte ergeben. Insbesondere sind die voraussichtlichen Einsatzszenarien zu beschreiben, die Nutzungsformen zu definieren und die Rahmenbedingungen für die Nutzung zu spezifizieren. Hieraus ergibt sich die generelle Architektur der Videokonferenz-Infrastruktur.

In einem weiteren Schritt folgt die Festlegung der zugrundeliegenden Technik für Netz, Server und Endpunkte und gegebenenfalls auch die Auswahl spezifischer Varianten, z. B. Standard-Server oder herstellerspezifische Lösungen. Für eine Cloud-basierte Lösung sollten die relevanten technischen und organisatorischen Anforderungen sowie sicherheitsrelevante Aspekte in einer Cloud-Strategie erfasst werden (siehe auch *OPS.2.2 Cloud-Nutzung*).

Danach müssen Anzahl und Integration der vorgesehenen Komponenten der Videokonferenzlösung festgelegt werden und alle betroffenen Umsysteme identifiziert werden. Anhand der Anforderungen an die Verfügbarkeit muss festgelegt werden, bis zu welchem Grad redundante Strukturen innerhalb der Lösung vorzusehen sind, z. B. redundante Anbindung an den Cloud-Anbieter. Hier sind auch für die zentralen Systeme die notwendigen Vorgaben bezüglich der Infrastruktur, insbesondere Klimatisierung und Stromversorgung, festzulegen.

Schon vor der Beschaffung der zentralen Systeme und Endpunkte sollte eine Sicherheitsrichtlinie für die gesamte Videokonferenzlösung erstellt werden

7.1.2 Beschaffung

Im nächsten Schritt muss die Beschaffung der Hardware und eventuell zusätzlich benötigter Software oder Cloud-Dienste erfolgen. Grundsätzlich bilden die Architekturplanung und die Ergebnisse der Anforderungsanalyse die Basis für eine Beschaffung. Generelle Informationen zur Beschaffung sind im Baustein *OPS.1.2.6 Beschaffung, Ausschreibung und Einkauf* zu finden.

Für die Beschaffung der Video-Endpunkte müssen ausgehend von den Einsatzszenarien spezifische Auswahlkriterien für jede Art von Video-Endpunkten formuliert werden. Bei der Beschaffung von speziellen Einzelsystemen, beispielsweise Raumsystemen, ist es wichtig, dass der Endpunkt zu der vorhandenen Infrastruktur passt.

Um geeignete Lösungen und Endpunkte auswählen zu können, müssen diese bezüglich der relevanten Sicherheitskriterien, z. B. Update-Funktionen, Update-Prozess oder Authentisierung-Varianten, gesichtet und bewertet werden.

7.1.3 Umsetzung

Aufbauend auf den organisatorischen und planerischen Vorarbeiten kann die Installation und Inbetriebnahme der Videokonferenzlösung erfolgen. Dabei sind die folgenden Empfehlungen zu beachten:

- Wird eine Cloud-Lösung ausgewählt, sollten alle relevanten Aspekte und Anforderungen vertraglich geregelt werden.
- Die grundlegende Installation und Konfiguration der zentralen Komponenten der Videokonferenzlösung muss sorgfältig durchgeführt werden, um schwer reparierbare Fehler von vornherein zu vermeiden. Neben den spezifischen Maßnahmen für Videokonferenzsysteme sind sowohl die allgemeinen Hinweise in *SYS.1.1.M16 Sichere Installation* als auch die Anforderungen, die in den betreffenden Bausteinen für die zugrundeliegende Technik spezifiziert sind, umzusetzen.
- Auch für die Video-Endpunkte ist eine sorgfältige Installation und Konfiguration essenziell, da diese oft von mehreren Nutzern verwendet werden oder gar frei zugänglich sind.
- Nachdem die Installation und Grundkonfiguration der Komponenten abgeschlossen ist, kann die eigentliche Software der Videokonferenzlösung installiert und konfiguriert werden. Die dafür notwendigen Schritte unterscheiden sich je nach Art und Einsatzzweck der Software teilweise erheblich. Prinzipiell wird empfohlen, die Installation und Konfiguration der Software analog zu der Konfiguration der zugrundeliegenden Technik durchzuführen:
  - Erstellung eines Installationskonzepts
  - Falls mehrere Systeme mit ähnlichen Einsatzgebieten und Konfiguration installiert werden sollen: Erstellen einer Referenzinstallation
  - Installation, Grundkonfiguration, Aktualisierung und Härtung
  - Test und optionaler Penetrationstest bei erhöhtem Schutzbedarf

- Bei der Installation sind unbedingt die vom Hersteller voreingestellten Rollen und Passwörter zu löschen oder zu ändern, da die Videokonferenzlösung sonst von beliebigen Angreifern manipuliert werden kann.
- Ebenso sind alle Schnittstellen abzusichern und alle nicht benötigten Leistungsmerkmale abzuschalten, weil sie unnötige Risiken mit sich bringen.

Die Nutzer und die Administratoren haben einen wesentlichen Einfluss auf die Sicherheit eines Systems. Vor der tatsächlichen Inbetriebnahme und Nutzung müssen daher sowohl Administratoren als auch Nutzer umfassend eingewiesen werden. Insbesondere für Administratoren von Videokonferenzlösungen empfiehlt sich aufgrund der Komplexität der Systeme und der Vielfalt der integrierten Systeme eine intensive Schulung. Nutzern sollten insbesondere die verfügbaren Sicherheitsmechanismen vermittelt werden. Generell sollten hierfür auch die Anforderungen des Bausteins *ORP.3 Sensibilisierung und Schulung zur Informationssicherheit* herangezogen werden.

7.1.4 Betrieb

Nach der Erstinstallation und einer Testbetriebsphase geht die Videokonferenzlösung in den Regelbetrieb über. Unter Sicherheitsgesichtspunkten sind dabei folgende Aspekte zu beachten:

- Bei jedem Change muss sichergestellt werden, dass die Sicherheit der Gesamtlösung auch nach der Änderung nicht beeinträchtigt wird. Dabei ist zu berücksichtigen, dass auch der Entzug von Berechtigungen sowie das Löschen nicht mehr benötigter Datenbestände so geregelt wird, dass keine Sicherheitslücken entstehen. Eine wesentliche Hilfe ist dabei eine effiziente, umfassende Systemverwaltung, die sich jederzeit auf aktuelle Informationen über den Zustand des Systems und seiner Rechtestrukturen abstützen kann (siehe dazu *SYS.1.1.M3 Restriktive Rechtevergabe und SYS.1.1.M21 Betriebsdokumentation*).
- Für die Video-Endpunkte, insbesondere mobile Endpunkte, ist die Installation und permanente Aktualisierung von Software zur Absicherung gegen Schadsoftware dringend zu empfehlen.
- Alle Komponenten der Videokonferenzlösung sollten stets dem aktuellen Stand der Technik angepasst werden. Wird die Lösung durch externe Dienstleister betreut, sollte dies vertraglich geregelt werden.
- Falls eine Komponente in eine externe Reparaturstelle gegeben wird, muss zuvor sichergestellt werden, dass alle Konferenzdaten, Metadaten und gegebenenfalls Videokonferenzinhalte gesichert wurden und auf der Datenablage der betroffenen Komponente sicher gelöscht sind.
- Ein wesentliches Mittel für einen sicheren Betrieb ist die Überwachung mindestens der zentralen Komponenten und die Protokollierung der Administration. Dies erfolgt optimalerweise durch eine Einbindung in zentrale Lösungen für Monitoring und Protokollierung sowie gegebenenfalls in eine zentrale SIEM-Lösung. Bei Standardsystemen, die meist die Basis für die Videokonferenzlösung darstellen, liegen häufig Sicherheitslücken vor, gegen die sich oft Angriffe richten. Dies fordert von den Administratoren, dass sie permanent über den Sicherheitsstatus der Systeme sowie über neue Bedrohungen informiert sind, um rechtzeitig Gegenmaßnahmen einleiten zu können.
- Die Einhaltung der vertraglichen Vereinbarungen, insbesondere der Sicherheitsanforderungen, bei Einbeziehung eines Cloud-Dienstleisters sollte regelmäßig geprüft werden. Hierfür kann ein gezieltes Audit durchgeführt werden (siehe *OPS.2.2 Cloud-Nutzung*).

7.1.5 Aussonderung

Eine Komponente einer Videokonferenzlösung darf nicht einfach ohne Ankündigung abgeschaltet werden. Wenn ein zentrales System außer Betrieb genommen werden soll, dann müssen, wenn es direkte Auswirkungen für die Anwender hat, diese rechtzeitig informiert werden und es muss eine geeignete Ersatzplanung erfolgen, um Ausfallzeiten und gegebenenfalls Datenverluste zu verhindern.

Es muss sichergestellt werden, dass alle Konferenzdaten, Metadaten und gegebenenfalls Videokonferenzinhalte auf der Komponente gesichert oder auf ein Ersatzsystem übertragen wurden.

Bei der Aussonderung von Teilen der Videokonferenzlösung ist außerdem darauf zu achten, dass auf der jeweiligen Datenablage keine schützenswerten Informationen verbleiben. Dazu genügt es nicht, die Speicherbereiche einfach zu löschen oder neu zu formatieren, sondern diese müssen mehrfach vollständig überschrieben werden. Falls eine defekte Komponente dauerhaft außer Betrieb genommen wird, muss die Datenablage sicher entsorgt werden. Dazu kann ein zertifiziertes Unternehmen beauftragt werden.

Die Aussonderung von zentralen Komponenten oder dedizierten Video-Endpunkten muss dokumentiert werden. Bestandsverzeichnisse sowie Netzpläne müssen aktualisiert werden und sofern sich durch die Aussonderung strukturelle Veränderungen der Videokonferenzlösung ergeben, sollte auch das Sicherheitskonzept entsprechend angepasst werden.

Damit bei Beendigung eines Cloud-Dienstes die Sicherheitsanforderungen gewahrt bleiben, muss festgelegt sein, wie die Daten vom Dienstleister an die Institution zurückgegeben und beim Dienstleister gelöscht werden. Ebenso müssen alle erforderlichen Informationen dokumentiert sein, die für die Weiterführung des Betriebs der Videokonferenzlösung nötig sind.

7.1.6 Notfallvorsorge

Neben der Absicherung im laufenden Betrieb spielt die Notfallvorsorge eine wichtige Rolle, da nur so der Schaden im Notfall verringert werden kann. Im Rahmen der allgemeinen Notfallvorsorge ist zu klären, ob die Systeme der Videokonferenzlösung hohen Anforderungen an die Verfügbarkeit unterliegen.

Allgemeine Hinweise zur Notfallvorsorge finden sich im Baustein *DER.4 Notfallmanagement*. Hierzu gehört auch die Planung des Umgangs mit Sicherheitsvorfällen, die sich auf die Anforderungen des Bausteins *DER.2.1 Incident Management* abstützen sollte.

Darüber hinaus sollte durch eine regelmäßige und umfassende Datensicherung gewährleistet werden, dass alle relevanten Daten, z. B. Konfigurationsdaten für Profile, auch im Falle von Störungen, Ausfällen der Hardware oder (absichtlichen oder unabsichtlichen) Löschungen schnell wiederhergestellt werden können.

Es wird vorausgesetzt, dass alle zentralen Komponenten der Videokonferenzlösung in einem Serverraum (siehe Baustein *INF.12 Serverraum*), einem Serverschrank (siehe Baustein *INF.6 Schutzschränke*) oder in einem Rechenzentrum (siehe Baustein *INF.2 Rechenzentrum*) untergebracht sind und somit angemessen geschützt sind. Bei Einsatz einer Cloud-Lösung sind entsprechende Vertragsinhalte vorzusehen und es sollte abhängig von den Verfügbarkeitsanforderungen eine hochverfügbare Anbindung an den Cloud-Dienst eingerichtet werden.

Die für die zugrundeliegende Technologie umzusetzenden Anforderungen sind den jeweiligen spezifischen Bausteinen, Richtlinien oder Kompendien zu entnehmen. Dies gilt analog auch für die genutzten Video-Endpunkte.

7.2 Maßnahmen

7.2.1 Basis-Maßnahmen

7.2.1.1 Anwendungen und zentrale Komponenten

M-1 Sicherer Umgang mit Videokonferenzdaten

Für die in A-1 geforderte verschlüsselte Speicherung der PINs, Passwörter und sonstigen Daten mit erhöhtem Schutzbedarf können detaillierte Informationen zu geeigneten Verschlüsselungsverfahren [BSI TR02102-2019] entnommen werden. Hierbei ist auch auf ein geeignetes Schlüsselmanagement zu achten. Werden die Videokonferenzdaten auf einer angemessen geschützten Plattform gespeichert, kann gegebenenfalls auf eine Verschlüsselung verzichtet werden.

Auch Cloud- und externe Lösungen, die zur Speicherung dieser Daten eingesetzt werden, müssen durch eine Verschlüsselung abgesichert werden. Je nach Schutzbedarf sollte festgelegt werden, ob in der Cloud gespeicherte Daten zusätzlich gegen einen Zugriff durch den Betreiber geschützt werden müssen.

Die geforderte Autorisierung für den Zugriff auf die Videokonferenzdaten sollte über ein Rollen- und Berechtigungskonzept (siehe M-12) umgesetzt werden, das von der Videokonferenzlösung implementiert wird. Zudem sollten Nutzerkonten personengebunden vergeben werden. Um die Nutzung angemessener Passwörter zu gewährleisten, sollte die Passwortrichtlinie der Institution auch auf die Videokonferenzlösung angewendet werden.

Für den verschlüsselten Zugriff auf Videokonferenzdaten sollten für Protokolle, die bei der Kommunikation mit dem System genutzt werden (z. B. TLS), ein geeignetes Verschlüsselungsverfahren gemäß [BSI TR02102-2019] und eine ausreichende Schlüssellänge gewählt werden. Sollte keine Verschlüsselung oder nur zu schwache Verfahren möglich sein, muss der Schutz auf andere Weise umgesetzt werden. Dabei kann die Videokonferenzlösung in einem dedizierten, besonders geschützten Netzsegment positioniert werden (siehe M-9). Der Zugriff auf Videokonferenzdaten erfolgt dann ausschließlich entkoppelt, beispielsweise über Terminal Server (siehe M-58).

Mindestens sollte für den Zugriff auf die Videokonferenzdaten eine angemessene Authentisierung stattfinden, die neben dem Schutzbedarf der Videokonferenzdaten auch den Schutzbedarf der durchzuführenden Videokonferenzen und die Institutionsrichtlinie für Fernzugriffe entsprechend berücksichtigt. Insbesondere sollte bei hohem Schutzbedarf der Videokonferenzdaten und der durchzuführenden Videokonferenzen eine starke Authentisierung in Erwägung gezogen werden.

Es ist zudem empfehlenswert, die Videokonferenzlösung bestmöglich zu überwachen. Dabei sollten vor allem Zugriffe auf sicherheitsrelevante Daten in die Überwachung einbezogen werden.

M-2 Unterschiedliche Profile für Videokonferenzen

Für Videokonferenzen können unterschiedliche Sicherheitseinstellungen erforderlich sein, die z. B. dem Schutzbedarf der Gesprächsinhalte entsprechen. Um hierbei fehlerhafte Sicherheitseinstellungen zu vermeiden, werden in A-2 vorgefertigte Profile gefordert. Diese Profile fassen die Sicherheitseinstellungen zusammen und erleichtern so den Wechsel zwischen verschiedenen Sicherheitsanforderungen.

Sinnvoll sind verschiedene Profile für unterschiedliche Teilnehmergruppen, z. B. nur interne Teilnehmer der Institution an einem Standort, nur interne Teilnehmer der Institution an verschiedenen Standorten oder ein gemischter Teilnehmerkreis mit sowohl internen als auch

externen Teilnehmern. Weiterhin sollten Konferenzprofile für Gesprächsinhalte mit normalem Schutzbedarf und mit erhöhtem Schutzbedarf bereitgestellt werden.

Beispielsweise kann ein Profil erstellt werden, das eine Videokonferenz ohne Kommunikationsverschlüsselung ermöglicht. Dieses Profil kann dann für interne Videokonferenzen mit normalem Schutzbedarf genutzt werden, wenn die Kommunikation ausschließlich in einem LAN erfolgt, welches z. B. durch Segmentierung und Netzzugangskontrolle gut geschützt ist. Werden jedoch auch Teilnehmer eingebunden, die z. B. über ein WAN angebunden sind, sollte ein anderes Profil bereitgestellt und genutzt werden, welches die Verschlüsselung der Kommunikation sicherstellt.

Für Videokonferenzen mit hoher Vertraulichkeit kann ergänzend im Profil ein potenzieller Teilnehmerkreis festgelegt werden, über welchen hinaus kein Beitritt möglich sein darf. Hierzu kann im Vorhinein ein Passwort definiert werden, welches an die potenziellen Teilnehmer verschickt wird und zum Beitritt eingegeben werden muss. Eine sicherere Alternative ist die Beschränkung der Teilnahme auf einzelne Nutzerkonten, deren Besitzer sich zunächst authentisieren müssen.

M-3 Sicherer Umgang mit Metadaten

Für die in A-3 geforderte verschlüsselte Speicherung der Metadaten können detaillierte Informationen zu geeigneten Verschlüsselungsverfahren [BSI TR02102-2019] entnommen werden. Hierbei ist auch auf ein geeignetes Schlüsselmanagement zu achten.

Werden die Metadaten auf einer angemessen geschützten Plattform gespeichert oder nur gesichert pseudonymisiert gespeichert, kann gegebenenfalls auf eine Verschlüsselung verzichtet werden.

Auch Cloud- und externe Lösungen, die zur Speicherung dieser Daten eingesetzt werden, müssen durch Verschlüsselung abgesichert werden. Je nach Schutzbedarf sollte festgelegt werden, ob in der Cloud gespeicherte Daten zusätzlich gegen Zugriff durch den Betreiber geschützt werden müssen.

Ansonsten gelten für den sicheren Zugriff auf Metadaten alle Festlegungen in M-1.

M-4 Sicherer Umgang mit Konferenzaufzeichnungen

Mit aufgezeichneten Videokonferenzen oder Teilen davon muss gemäß A-4 sicher umgegangen werden. Dies gilt nicht nur dann, wenn die Gesprächsinhalte vertraulich sind. Konferenzaufzeichnungen sind prinzipiell personenbezogen, da die Identität der Teilnehmer meist erkennbar ist.

Es muss sichergestellt werden, dass eine Aufzeichnung nur dann stattfindet, wenn dies gemäß rechtlichen Vorgaben zulässig ist, alle Teilnehmer dem zugestimmt haben und mit den aufgezeichneten Inhalten ausschließlich in einer Weise umgegangen wird, der die Teilnehmer zugestimmt haben.

Beim Einholen des Einverständnisses zur Aufnahme der Konferenz müssen die Teilnehmer auch über Nutzungszweck und Weiterverarbeitung der aufgezeichneten Daten aufgeklärt werden. Beispielsweise kann von Videokonferenzen nachträglich eine Transkription erstellt werden oder die Gespräche können mittels KI-Funktionen analysiert werden. Die Zustimmung muss für zukünftige Nachweise gespeichert werden. Optimal ist hier ein schriftlicher Nachweis, der prinzipiell auch auf technischer Ebene durch die Videokonferenzlösung selbst erfolgen kann. Die Teilnehmer können dazu beispielsweise eine eingeblendete Dialogmeldung bestätigen. Falls keine Möglichkeit auf technischer Ebene besteht, kann das Einverständnis vor Beginn der Aufnahme schriftlich oder mündlich eingeholt werden.

Die Aufzeichnung von Konferenzen sollte den Teilnehmern signalisiert werden. Hier ist eine Information in Form einer Ansage, eines Aufmerksamkeitstons zu Beginn der Aufzeichnung oder einer dauerhaft eingeblendeten Benachrichtigung während der Konferenz zu erwägen.

Die Aufzeichnung von Konferenzen kann am Video-Endgerät oder auf einem zentralen System der Videokonferenzlösung erfolgen. Wie in Abbildung 13 visualisiert, werden diese Aufzeichnungen dann lokal im Video-Endpunkt (siehe M-8), lokal im zentralen System oder in einer angebundenen Speicherlösung, gegebenenfalls auch in einer Cloud (siehe M-5), gespeichert.

Geeignete kryptografische Verfahren für die in A-4 geforderte verschlüsselte und manipulationssichere Speicherung von Konferenzaufzeichnungen werden in [BSI TR02102-2019] genannt. Werden die Konferenzaufzeichnungen auf einer angemessen geschützten Plattform gespeichert, kann gegebenenfalls auf eine verschlüsselte Speicherung verzichtet werden. In jedem Fall müssen die Aufzeichnungen mit einer digitalen Signatur oder einem vergleichbaren Verfahren gegen Manipulationen geschützt werden.

Die Videokonferenzlösung sollte nach Möglichkeit so konfiguriert werden, dass Konferenzaufzeichnungen nur im gesicherten und vorgegebenen Umfeld gespeichert werden können, beispielsweise ist die Unterbindung einer lokalen Speicherung auf einem Video-Endpunkt in Erwägung zu ziehen.

Der Speicherort kann prinzipiell auch in der Cloud liegen. In diesem Fall muss der Betreiber insbesondere für eine korrekte Mandantentrennung sorgen. Außerdem sollte in diesem Fall festgelegt werden, ob in der Cloud gespeicherte Konferenzaufzeichnungen zusätzlich gegen Zugriff durch den Betreiber geschützt werden müssen.

Werden Aufzeichnungen archiviert, ist darauf zu achten, dass ein Zugriff auf die Konferenzaufzeichnung und damit ein Entschlüsseln der verschlüsselten und manipulationssicheren Archivierung während der gesamten Archivierungsfrist möglich sein muss (siehe auch [BSI TR03125-2018]).

In den meisten Fällen müssen auch für die Weiterverarbeitung von Aufzeichnungen geeignete Schutzmaßnahmen umgesetzt werden, insbesondere wenn hieraus weitere persistente Daten entstehen. Der Schutzbedarf der Weiterverarbeitung entspricht dabei den inhaltlichen Informationen der aufgezeichneten Konferenz, die nach der Verarbeitung erhalten bleiben oder rekonstruiert werden könnten. Auch hier sollten ein angemessener Zugriffsschutz und Verschlüsselung eingesetzt werden (siehe auch M-5).

Der Zugriff auf gespeicherte Konferenzaufzeichnungen umfasst sowohl den Zugriff über die Videokonferenzlösung als auch den direkten Zugriff über das Dateisystem. Der Zugriff darf nur nach erfolgreicher Authentisierung möglich sein und setzt eine entsprechende Autorisierung voraus. Die Berechtigungen sollten sich am Schutzbedarf der aufgezeichneten Konferenz orientieren (siehe M-50).

Konferenzaufzeichnungen dürfen nur an Dritte zur Nutzung weitergegeben werden, wenn dies von allen Teilnehmern erlaubt wurde, mit dem Schutzbedarf vereinbar ist und die Wirksamkeit von Schutzmaßnahmen beibehalten wird. Dritte sollten Auskunft über die Art der Schutzmaßnahmen und die wichtigsten Parameter der Maßnahmen geben. Darüber hinaus sollte eine schriftliche Bestätigung eingeholt werden, dass die Daten durch Maßnahmen geschützt werden, die dem geforderten Schutzbedarf und der erlaubten Nutzung entsprechen.

M-5 Absicherung von Dateiablagen

Während einer Videokonferenz kann potenziell auf Dateiablagen im Video-Endgerät, auf einem zentralen System der Videokonferenzlösung oder auf eine externe Speicherlösung, auch in einer Cloud, zugegriffen werden (siehe Abbildung 13).

Der in A-5 geforderte sichere Zugriff auf die Dateiablagen kann über geeignete Berechtigungen im Rahmen eines Rollen- und Berechtigungskonzepts für die Videokonferenzlösung realisiert werden (siehe M-12). Hierbei ist darauf zu achten, dass alle Dateiablagen im Rollen- und Berechtigungskonzept angemessen berücksichtigt werden. Hierzu gehören sowohl lokale Dateiablagen im Video-Endpunkt (siehe M-8), interne Dateiablagen im Videokonferenzsystem, z. B. für Aufnahmen von Whiteboard-Zeichnungen, und auch externe Dateiablagen, z. B. ein Datenbank-Server mit gescannten Unterlagen.

Darüber hinaus sollte auch ein direkter Zugriff auf die Dateiablagen auf die notwendigen Zugriffe beschränkt sowie geeignet autorisiert und authentisiert werden (siehe M-1). Ergänzend sollte für die externen Dateiablagen ein dediziertes Netzsegment erwogen werden.

Ein effektiver Schutz für Daten mit erhöhtem Schutzbedarf wird durch eine Verschlüsselung der Dateiablage erreicht. Detaillierte Informationen zu geeigneten Verschlüsselungsverfahren können dem BSI-Dokument [BSI TR02102-2019] entnommen werden. Die Verschlüsselung der abgelegten Daten muss auch bei der Übertragung der Daten und insbesondere bei der Datensicherung erhalten bleiben. Sind die Daten auf einer angemessen geschützten Plattform gespeichert, kann gegebenenfalls auf eine verschlüsselte Speicherung verzichtet werden.

Bei der Aussonderung oder auch Weitergabe von Komponenten der Videokonferenzlösung muss sichergestellt werden, dass jegliche personenbezogene oder schützenswerte Information von der Datenablage entfernt wurde. Hierzu müssen die Speicherbereiche mehrfach vollständig durch Fülldaten überschrieben werden. Ein einfaches Löschen oder eine Neuformatierung eines Datenträgers ist nicht ausreichend, da die Daten in diesem Fall leicht zu rekonstruieren sind. Falls eine defekte Komponente dauerhaft außer Betrieb genommen wird, sollte die Datenablage physisch sicher zerstört werden. Mindestens müssen die Daten sicher gelöscht sein.

7.2.1.2 Endgeräte und Clients

M-6 Absicherung von frei zugänglichen Video-Endpunkten

Frei zugängliche Video-Endpunkte, z. B. Raumsysteme, können leichter manipuliert oder für Angriffe genutzt werden, da der zugreifende Personenkreis nicht angemessen kontrolliert werden kann. Aus diesem Grund sind hier ergänzende Schutzmaßnahmen erforderlich.

Der in A-6 geforderte Zugriffsschutz für den Endpunkt kann durch die Abfrage eines Passworts oder einer PIN beim Systemstart erfolgen. Alternativ oder ergänzend können weitergehende Erkennungsmechanismen wie beispielsweise Smartcard, Fingerabdruck- oder Gesichtserkennung oder eine Gerätekopplung via Ultraschall in Betracht kommen. Empfehlenswert ist darüber hinaus die Authentisierung mit einem personengebundenen Nutzerkonto zur Anmeldung am Endpunkt. Die Eingabemöglichkeit sollte so gestaltet sein, dass sie möglichst nicht von Dritten eingesehen werden kann.

Es muss sichergestellt werden, dass alle Mechanismen sicher konfiguriert sind. Nicht genutzte Mechanismen sollten deaktiviert werden. Beispielsweise sollte das Default-Passwort gesperrt werden, wenn andere Mechanismen genutzt werden. Ebenso sollten, falls der Endpunkt verschiedene Konten vorsieht, die Default-Benutzer gelöscht oder deaktiviert und der Video-Endpunkt in ein Rollen- und Berechtigungskonzept (siehe M-12) eingebunden werden.

Eine Manipulation von Video-Endpunkten kann auch hardwareseitig erfolgen, indem z. B. ein zusätzliches Gerät angeschlossen oder der Geräteanschluss manipuliert wird.

- Nicht genutzte Anschlüsse des Endpunkts sollten daher nach Möglichkeit entfernt, deaktiviert oder physisch geschützt werden. Auch das Gehäuse sollte einen angemessenen Schutz bieten, sodass es möglichst nicht von Unbefugten geöffnet werden kann.

- Die genutzten Anschlüsse für frei zugängliche Video-Endpunkte sollten derart abgesichert werden, dass ein unbemerktes Anschließen von Komponenten zum Abgreifen von Informationen, z. B. durch Anschluss eines Splitters, verhindert wird.

Insbesondere sollte vor Beginn einer vertraulichen Videokonferenz eine Sichtkontrolle des Video-Endpunkts inklusive aller Anschlüsse erfolgen.

Frei zugängliche Video-Endpunkte sollten nach beendeter Videokonferenz deaktiviert werden, damit der Zugriffsschutz bei einer erneuten Nutzung aktiviert ist. Bevorzugt sollte das Gerät ausgeschaltet werden, gegebenenfalls sogar stromfrei geschaltet werden. Der Endpunkt sollte so konfiguriert werden, dass er sich bei Inaktivität oder nach Abmelden des Nutzers automatisch deaktiviert. Hierbei sollte darauf geachtet werden, dass möglichst nicht nur in den Stand-by-Modus gewechselt wird, sondern der Video-Endpunkt vollständig ausgeschaltet wird.

Ein physisches Ausschalten ist nur dann möglich, wenn Komfortfunktionen wie ein automatischer Start bei Anwesenheit von Personen oder Wake-on-LAN (WoL) nicht genutzt werden sollen.

Die Absicherung sollte auch Zusatzkomponenten wie digitale Whiteboards abdecken. Hierbei sind individuelle technische Eigenschaften der Geräte zu berücksichtigen.

Mobile Endgeräte, die häufiger unbeaufsichtigt sind und leicht entwendet werden können, stellen ebenfalls frei zugängliche Endgeräte dar. Somit sollten auch mobile Endgeräte und insbesondere die Videokonferenz-App gegen unberechtigte Zugriffe geschützt werden und die Datenablagen für Daten mit Bezug zur Videokonferenz verschlüsselt erfolgen. Hierdurch wird der Zugriff auf die Videokonferenz-App erschwert und die gespeicherten Daten sind im Fall eines Verlustes oder Diebstahls geschützt. Weiterhin kann für mobile Endgeräte ein Mobile Device Management (siehe Baustein *SYS.3.2.2 Mobile Device Management (MDM)* des IT-Grundschutz-Kompendiums) genutzt werden, mit dem die Daten auf dem Gerät aus der Ferne gelöscht werden können.

M-7 Beenden von Sitzungen und Anmeldungen an Video-Endpunkten

Mechanismen zur Authentisierung können besonders leicht von Angreifern umgangen werden, wenn aktive Sitzungen von bereits authentisierten Nutzern aufgegriffen werden können.

Wie in A-7 gefordert, sollten daher Sitzung nach einer Videokonferenz aktiv beendet werden und alle Teilnehmer sich vergewissern, dass die Verbindung geschlossen wurde. Unterstützend kann die Videokonferenzlösung eventuell so konfiguriert werden, dass sie automatisch die Verbindung beendet, wenn alle anderen Konferenzteilnehmer dies bereits getan haben.

Auch das geforderte Abmelden eines Nutzers an gemeinschaftlich genutzten Video-Endpunkten kann gegebenenfalls dadurch unterstützt werden, dass Benutzer bei Inaktivität automatisch abgemeldet werden. Dabei ist für die Dauer der Inaktivität ein angemessener Zeitraum zu wählen.

Wird ein dedizierter Video-Endpunkt, z. B. ein Raumsystem oder Videotelefon, nicht mehr verwendet, sollte er ausgeschaltet werden bzw. so deaktiviert werden, dass ein erneuter Zugriffsschutz aktiviert ist (siehe M-6).

M-8 Absicherung der internen Dateiablage des Video-Endpunkts

Die Umsetzung von A-8 kann über die in M-5 beschriebenen Maßnahmen sichergestellt werden. Auch hier muss sowohl der Zugriff über die Videokonferenzlösung als auch der direkte Zugriff auf das Dateisystem berücksichtigt werden.

Daten mit erhöhtem Schutzbedarf, z. B. Aufzeichnungen von Videokonferenzen, müssen auf einem Video-Endpunkt verschlüsselt gespeichert werden. Detaillierte Informationen zu geeigneten Verschlüsselungsverfahren können dem Dokument [BSI TR02102-2019] entnommen werden.

Der in A-8 geforderte sichere Zugriff auf die interne Dateiablage des Video-Endpunkts sollte über geeignete Berechtigungen realisiert werden. Alle Video-Endpunkte sollten im Rollen- und Berechtigungskonzept berücksichtigt werden (siehe M-12), das für Video-Endpunkte möglichst nutzerbezogene Konten nutzt. Konten für mehrere Nutzer, z. B. ein Nutzer „Videokonferenz“ auf einem Raumsystem sollten vermieden werden.

Auch für Video-Endpunkte, insbesondere für mobile Endpunkte, die ausgesondert oder an Dritte weitergegeben werden, muss analog zu M-5 sichergestellt werden, dass personenbezogene oder schützenswerte Informationen von der internen Datenablage entfernt wurden.

7.2.1.3 Netzwerk

M-9 Dediziertes Sicherheitssegment für frei zugängliche Video-Endpunkte

Bei der Umsetzung von A-9 ist zu berücksichtigen, dass am Zonenübergang Medienströme von Videokonferenzen durch eine Firewall geleitet werden müssen. Hieraus entsteht bei der Firewall eine hohe Rechenlast. Kann diese nicht bewältigt werden, kann die Qualität der Medienströme beeinträchtigt werden. Liegen Video-Endpunkte in verschiedenen Sicherheitssegmenten, erhöht sich die Anzahl der zu passierenden Netzübergänge auch bei direkten Verbindungen zwischen den Endpunkten.

Bei einer Ende-zu-Ende-Verschlüsselung der Kommunikation kann eine Firewall nicht auf die Nutzdaten der Verbindung zugreifen, sofern sie keinen Verschlüsselungsendpunkt bilden soll. In diesem Fall ist daher eine Kontrolle der Medienströme nicht sinnvoll möglich.

M-10 Positionierung von Cloud Connector und Video Edge Server in einer DMZ

Komponenten wie Cloud Connector und Video Edge Server sind meist Eigentum des Cloud-Providers und können somit nur eingeschränkt durch die Institution administriert werden. Häufig sind diese Komponenten vollständig außerhalb der Kontrolle der Institution. Aus diesem Grund wird in A-10 die Positionierung in einer DMZ gefordert. Dabei kann die Trennung durch Mikrosegmentierung über ACLs oder Firewalls auf Ebene der Virtualisierungslösungen umgesetzt werden. Alternativ kann jeder Cloud Connector oder Video Edge Server in einer eigenen DMZ betrieben werden.

Der Zugang zu den Administrationsschnittstellen sollte besonders geschützt werden. Administrative Kommunikation mit den Geräten kann dazu z. B. über ein IDPS geführt werden.

7.2.1.4 Planung und Betrieb

M-11 Planung und Beschaffung der Videokonferenzlösung

Bei der in A-11 geforderten Planung sollte zunächst eine konkrete Architektur mit Einsatzszenarien entworfen werden, die sich möglichst nah an der tatsächlichen Nutzung orientieren. Dabei sollten von Anfang an Sicherheitsaspekte und geltende Gesetze, Regelungen und Vorschriften berücksichtigt werden. Hieraus kann eine Lösungsarchitektur und eine grobe Betriebskonzeption abgeleitet werden.

Über eine Anforderungsanalyse wird im Detail geklärt, welche Anforderungen an die Videokonferenzlösung gestellt werden und welche Anwendungsszenarien zu berücksichtigen sind. Um zusätzlich Prioritäten hervorzuheben, können Anforderungen mit individuellen Gewichten versehen werden. Die Analyse sollte sowohl funktionale als auch sicherheitstechnische Anforderungen abdecken. Dabei sollten möglichst alle Aspekte der geplanten Nutzung und des Schutzbedarfs von Inhalt und Teilnehmern betrachtet werden.

Insbesondere sollte bereits während der Planungsphase die für die absehbaren Einsatzszenarien erforderlichen Maßnahmen hinsichtlich Verschlüsselung und Authentisierung bestimmt werden.

Wird die Beschaffung einer Cloud-Lösung angestrebt, sollte sichergestellt werden, dass der Cloud Service Provider Cloud-Computing-Dienst angemessen schützt. Ein wesentlicher Bestandteil dieses Schutzes ist die Verschlüsselung der Kommunikation mit dem Dienst und der persistenten Daten. Für weitere Details wird auf [ISO 27017-2015] und [ISO 27018-2019] sowie auf das BSI-Dokument Cloud Computing Compliance Controls Catalogue (C5, siehe [BSI C5-2017]) verwiesen.

In der Planung sind ebenfalls Systeme, Schnittstellen und Dienste, die mit der Videokonferenzlösung verbunden werden sollen, zu berücksichtigen. Idealerweise wird die benötigte Konnektivität standardmäßig unterstützt. Ist dies nicht der Fall, muss an den entsprechenden Stellen zusätzlicher Aufwand investiert werden. Zur besseren Vergleichbarkeit ist es sinnvoll, diesen Aufwand grob abzuschätzen.

Bereits im Rahmen der Planung sollte geprüft werden, ob die Videokonferenzlösung in den bereits vorhandene Richtlinien angemessen berücksichtigt ist. Gegebenenfalls müssen die internen Richtlinien der Institution angepasst werden.

Aufgrund der Komplexität einer Videokonferenzlösung sollte die Beschaffung mit einem Abnahmetest abgeschlossen werden, der alle Szenarien sowie alle integrierten Dienste, z. B. Funktionen der Künstlichen Intelligenz (KI), und Schnittstellen, z. B. zu externen Dateiablagen, berücksichtigt. Während des Beschaffungsvorgangs sollten in angemessenem Umfang Produkttests zur Sicherstellung der Funktionalität und ein Proof of Concept (PoC) zur Absicherung der Architektur geplant werden. Hierfür sollten angemessene Zeiträume eingeplant werden.

M-12 Erstellung eines Rollen- und Berechtigungskonzepts

Die Basis des in A-12 geforderten Konzepts kann sich an der Rollenaufteilung in Administrator, Moderator und Teilnehmer orientieren. Diesen Rollen sollten Berechtigungen zugeteilt werden, die dem Aufgabenbereich, d. h. den individuellen Aufgaben und Verantwortlichkeiten der Personen, entsprechen. Berechtigungen werden am besten nach dem Least-Privilege-Prinzip vergeben. Dabei wird der Umfang der Berechtigungen auf das notwendige Minimum begrenzt. In jedem Fall sollte das Rollen- und Berechtigungskonzept auch den Zugriff auf Dateiablagen berücksichtigen und eine Trennung zwischen produktiven und administrativen Tätigkeiten vorsehen. Beispielsweise können folgende Rollen eingerichtet werden:

- Administrator

  Administratoren benötigen weitreichende Berechtigungen, um ihre Aufgaben wahrnehmen zu können. Sie müssen in der Lage sein, alle erforderlichen Einstellungen vorzunehmen. Weiterhin sind sie für die Verwaltung von Nutzerkonten zuständig und müssen solche Konten anlegen und löschen sowie Passwörter und Berechtigungen ändern können.

  Für alle Rollen, mindestens jedoch für die Administrator-Rolle, sollten nicht-triviale Namen für die Rolle bzw. den Nutzer verwendet werden. Vom Hersteller vorgegebene Standard- bzw. Default-Nutzer, z. B. Nutzer „Administrator“ mit Passwort „123456“ sollten gelöscht oder deaktiviert werden.

- Moderator

  Moderatoren sind für den reibungslosen Ablauf von Videokonferenzen verantwortlich. Sie benötigen erweiterte Berechtigungen zur Steuerung von Videokonferenzen, z. B. das Ein- und Ausladen von Teilnehmern. Moderatoren sind jedoch nicht für die Konfiguration der Videokonferenzlösung zuständig. Ihre Berechtigungen sollten daher über den genannten Aufgabenbereich nicht hinausgehen.

- Teilnehmer

  Nutzer, die über die bloße Teilnahme an Videokonferenzen hinaus keine weiteren Aufgaben erfüllen, sollten nur minimale Berechtigungen zugewiesen bekommen. Sie sollten daher lediglich zu elementaren Operationen berechtigt sein, z. B. um Einstellungen im Rahmen ihres Nutzerprofils zu ändern.

M-13 Bereitstellung von Informationen zur sicheren Nutzung von Videokonferenzen

Jeder einzelne Nutzer ist ein wichtiger Faktor für die Sicherheit von Videokonferenzen. Daher sollten die in A-13 geforderten Informationen zur sicheren Nutzung umfassend erstellt und den Nutzern zur Kenntnis gebracht werden.

In den sicherheitsrelevanten Aspekten des Nutzerhandbuchs sollten alle grundlegenden Voraussetzungen für eine möglichst sichere Nutzung der Videokonferenzlösung erklärt werden. Die Informationen sollten sowohl die sichere Bedienung der Lösung selbst als auch das Verhalten der Nutzer und zuständige Ansprechpartner abdecken. Wichtig ist eine Anleitung, die konkret auf die vorhandenen Sicherheitseinstellungen der Videokonferenzlösung eingeht und festlegt, wann diese zu verwenden sind.

Über konkrete Sicherheitseinstellungen hinaus sollten Nutzer für bestehende Sicherheitsrisiken sensibilisiert werden, z. B. sollten Einladungen mit Zugangsdaten nicht ausgedruckt und offen gelagert werden. In diesem Zusammenhang sollte insbesondere auf die Gefahren von Social Engineering und die Nutzung von KI-Funktionen hingewiesen werden. Bestehende Gesetze, Richtlinien und Regelungen zu diesen Themen müssen den Nutzern der Videokonferenzlösung bekannt gemacht werden und zugänglich sein. Zudem sollte über die Aspekte des Datenschutzes aufgeklärt und Nutzer zu dessen Einhaltung verpflichtet werden.

Ergänzend zum Handbuch kann es sinnvoll sein, zu Beginn des Betriebs der Videokonferenzlösung eine Einführungsveranstaltung zu halten. Im Anschluss an die allgemeine Vorstellung des Produkts und der Einführung der wichtigsten Funktionen kann dabei auch auf die sichere Nutzung eingegangen werden. Um das Bewusstsein für einen verantwortungsvollen Umgang mit dem System zu stärken, können während der Veranstaltung Sicherheitsrisiken effektiv und einprägsam veranschaulicht werden. Hierbei sollte auch auf das bestehende Handbuch und weitere bestehende Regelungen hingewiesen werden.

M-14 Integration in das Schwachstellen- und Patch-Management

Bei der in A-14 geforderten Integration der Videokonferenzlösung in das Schwachstellen- und Patch-Management sollten Komponenten nach Möglichkeit automatisch über Protokolle wie LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Devices) inventarisiert werden.

Das Schwachstellen- und Patch-Management sollte sämtliche Zuständigkeiten eindeutig regeln. Dabei sollten allen Komponenten und Prozessen jeweils Verantwortliche zugewiesen werden. Insbesondere sollte Personal benannt werden, welches in Notfällen den Betrieb der Videokonferenzlösung aufrechterhält oder wiederherstellt. Existiert ein Computer Emergency Response Team (CERT), sollte dessen Zuständigkeitsbereich auf die Videokonferenzlösung erweitert werden. Sinnvoll ist auch die Benennung eines Verantwortlichen für den Kontakt mit Herstellern.

Die Videokonferenzlösung sollte in vollem Umfang und in regelmäßigen Abständen auf Schwachstellen untersucht werden. Der genutzte Schwachstellen-Scanner muss dabei stets die aktuellsten Schwachstellen berücksichtigen. Hierzu ist es empfehlenswert, regelmäßig aktuelle Meldungen von Warndiensten abzurufen. Bei Bekanntwerden einer schwerwiegenden Sicherheitslücke ist eine anlassbezogene Untersuchung durchzuführen. Aufgrund des entstehenden Netzverkehrs kann es sinnvoll sein, die Untersuchung außerhalb der üblichen Geschäftszeiten durchzuführen.

Patches sollten auf einem internen Repository gespeichert und von dort aus installiert werden. Die Quelle der Patches sollte zuvor hinreichend auf Authentizität überprüft werden und die Patches auf Schadsoftware und Integrität geprüft werden. Dies gilt besonders dann, wenn die Patches aus dem Internet heruntergeladen werden.

Das Patch-Management sollte alle Komponenten einer Videokonferenzlösung umfassen und regeln, wie und wie oft Patches ausgerollt werden. Patches zur Behebung von Sicherheitslücken sollten möglichst zeitnah installiert werden. Allgemein kann es sinnvoll sein, ein Wartungsfenster festzulegen. Um den produktiven Betrieb nicht zu stören, kann hierfür ein Zeitraum außerhalb der Geschäftszeiten gewählt werden.

Es sollte sichergestellt werden, dass die Videokonferenzlösung nach der Installation von Patches weiterhin fehlerfrei funktioniert.

- Dazu können Patches für zentrale Komponenten beispielsweise auf Testgeräten installiert werden, welche anschließend analysiert werden. Insbesondere sollte im Testbetrieb auch die fehlerfreie Integration aller beteiligten Komponenten nachgewiesen werden. Diese Analyse sollte auch durchgeführt werden, wenn für Umsysteme der Videokonferenz, z. B. eingebundene Datenbank-Systeme, ein Patch installiert wurde.
- Es kann sinnvoll sein, den Rollout eines Patches für mehrere gleichartige Komponenten zeitlich zu verteilen. Auf diese Weise wirken sich Probleme, die im Testbetrieb nicht erkannt wurden, nicht auf den gesamten Produktivbetrieb aus. Hierbei sollte jedoch ein Termin festgelegt werden, bis zu dem die Installation auf allen Geräten durchgeführt ist.
- Für den Fall, dass beim Rollout eines Patches Fehler auftreten, muss das Patch-Management auch einen Prozess für einen geordneten Rollback festlegen.

7.2.2 Standard-Maßnahmen

7.2.2.1 Anwendungen und zentrale Komponenten

M-15 Verschlüsselung der mit IP übertragenen Daten der Videokonferenz auf nicht vertrauenswürdigen Übertragungsstrecken

Auf nicht vertrauenswürdigen Übertragungsstrecken, beispielsweise im Internet oder in WANs, die die von mehreren Kunden eines WAN-Providers gemeinsam genutzt werden, besteht eine erhöhte Gefahr, dass Videokonferenzen durch Angreifer abgehört werden. Daher wird für diese Strecken in A-15 eine Verschlüsselung aller Daten der Videokonferenz gefordert. Diese Verschlüsselung kann auf Ebene der Videokonferenz oder auf Ebene des Netze beispielsweise mit VPN-Techniken realisiert werden. Typischerweise können Mediendaten von Videokonferenzen mit SRTP und Signalisierungsdaten mit TLS/DTLS verschlüsselt werden. Detaillierte Informationen zu geeigneten Verschlüsselungsverfahren spezifiziert [BSI TR02102-2019].

Um einen effektiven Schutz zu gewährleisten, sollte darauf geachtet werden, dass Verschlüsselungsendpunkte ausschließlich in vertrauenswürdigen Netzen positioniert sind und dass die Datenpakete der Videokonferenz auch von einer Firewall kontrolliert werden können.

M-16 Deaktivierung nicht benötigter Dienste und Leistungsmerkmale

Die allgemeine Vorgehensweise zur Umsetzung von A-16 entspricht den Umsetzungshinweisen zu Baustein *SYS.1.1.A6 Deaktivierung nicht benötigter Dienste und Kennungen*. Für alle Funktionen sollten die Sicherheitsrisiken gegen den Komfortgewinn abgewogen werden. Beispielsweise ist für die Nutzung der Komfortfunktion, mit der ein Raumsystem bei Anwesenheit von Personen gestartet werden kann, abzuwägen, ob die Gefährdung einer Raumüberwachung die Nutzung ausschließt.

Ergänzend sollten nur Plug-ins und Add-ons für die Videokonferenzlösung installiert werden, die erforderlich sind und die keine Sicherheitsrisiken bergen oder den Betrieb des Systems anderweitig gefährden können. In einigen Fällen stellen Hersteller entsprechende Härtungsrichtlinien zur Verfügung, die als Hilfestellung verwendet werden können.

Die getroffenen Entscheidungen müssen dokumentiert werden. Im Rahmen dessen sollte dies in den Profilen (siehe M-2) abgebildet und den Nutzern bekannt gemacht werden (siehe M-13).

M-17 Sichere Nutzerverwaltung

Die Nutzerverwaltung kann gemäß A-17 entweder innerhalb der Videokonferenzlösung oder über einen externen Verzeichnisdienst erfolgen. Beide Varianten zur Nutzerverwaltung müssen gegen einen unrechtmäßigen Zugriff abgesichert sein.

Erfolgt die Nutzerverwaltung innerhalb der Videokonferenzlösung, müssen diese Daten mit der Nutzerverwaltung von angebundenen Systemen und Lösungen, z. B. Datenbank-Server, sowie einem zentralen externen Verzeichnisdienst abgestimmt werden.

M-18 Sichere Konfiguration von geplanten Videokonferenzen

Geplante Konferenzen können durch geeignete Voreinstellungen abgesichert werden. Die Sicherheitsmaßnahmen zur Umsetzung von A-18 dürfen nicht durch Benutzer abgeschwächt, sondern bei Bedarf lediglich erhöht werden können. Grundsätzlich sollte eine Balance zwischen Bedienbarkeit und Sicherheitsniveau erreicht werden. Hierfür sollten sich die Konfigurationseinstellungen an der Vertraulichkeit der Gesprächsinhalte und dem Teilnehmerkreis der jeweiligen Videokonferenz orientieren. Beispiele für potenzielle Sicherheitsmaßnahmen, die gegebenenfalls auch in Konferenzprofilen (siehe M-2) abgebildet werden können, sind:

- Authentisierung vor Teilnahme an Videokonferenzen

  Um einer Videokonferenz beitreten zu können, kann die Eingabe eines gültigen Passwortes gefordert werden. Dieses sollte unabhängig von der Einladung an die geplanten Gesprächsteilnehmer verteilt werden. Alternativ kann die erfolgreiche Authentisierung mit einem personengebundenen Nutzerkonto gefordert werden.

- Einrichtung eines Wartebereichs

  Bevor Teilnehmer einer Konferenz beitreten können, verbleiben sie in einem virtuellen Wartebereich. Von dort können sie ausschließlich durch einen Moderator der Konferenz hinzugefügt werden.

- Einschränkung von erlaubten Kanälen

  Teilnehmer dürfen nur mit einem Videokanal beitreten. Reine Sprachkanäle, d. h. die Einwahl über Telefon, und die damit erschwerte Erkennung des Teilnehmers werden ausgeschlossen.

- Schutz bzw. Verhinderung der Weiterleitung von Einladungen und Terminen

  Die Weiterleitung von Einladungen kann abgesichert oder unterbunden werden. Eine Form der Absicherung könnte vorsehen, dass der Adressat der Weiterleitung von einem Moderator eine individuelle Teilnahmeerlaubnis erhalten muss. Erst danach können Details zur Konferenz, z. B. Titel oder Teilnehmerliste, abgerufen werden.

- Keine Eintragung von Konferenzen in entsprechenden Kalendern

  Eine einfache Schutzmaßnahme besteht darin, den Termin einer Konferenz nicht öffentlich bekannt zu geben. Dazu ist es sinnvoll, entsprechende Termine nicht in solche Kalender einzutragen, auf die über die Kommunikationspartner hinaus weitere Personen lesenden Zugriff haben. Zumindest sollte im Eintrag auf Angaben verzichtet werden, die Rückschlüsse auf die geplante Videokonferenz ermöglichen.

Ebenso sollte eine Einladung zu einer Konferenz, in der eventuell sogar Zugangsdaten enthalten sind, nicht öffentlich bekannt gegeben werden, z. B. durch einen Ausdruck.

- Verschlüsselung der Kommunikation

  Durch Verschlüsselung kann die Kommunikation gegen Abhörversuche geschützt werden. Der Einsatz einer Ende-zu-Ende-Verschlüsselung sollte jedoch wegen des technischen Aufwands nur bei hohem Schutzbedarf erwogen werden (siehe M-43).

M-19 Sichere Anbindung der Videokonferenzlösung an Systeme des Gebäudemanagements

Die Verbindung zu Systemen des Gebäudemanagements sollte so realisiert werden, dass gemäß A-19 eine gegenseitige missbräuchliche Nutzung oder Kompromittierung verhindert wird. Hierfür sollte die Gebäudetechnik und Videokonferenzlösung in separaten Netzen bzw. Sicherheitssegmenten betrieben werden (siehe Baustein *SYS.4.4 Allgemeines IoT-Gerät*). Die dazwischen liegende Firewall sollte so konfiguriert werden, dass nur Zugriffe von wenigen Systemen der Videokonferenzlösung zur Gebäudetechnik zugelassen werden. Zur Kommunikation sollten ausschließlich Protokolle mit Verschlüsselung wie SSL/TLS und SSH erlaubt werden. Unverschlüsselte Verbindungen über unsichere Protokolle sollten blockiert werden.

Der Zugriff vom Videokonferenzsystem auf die Gebäudetechnik sollte auf die notwendigen Zielsysteme beschränkt bleiben. Beispielsweise sollten nur solche Verbindungen zugelassen werden, die einem Raumsystem die Steuerung der Gebäudetechnik im selben Raum ermöglichen. Die Berechtigungen zur Steuerung sollten auf den notwendigen Umfang und autorisierten Personenkreis begrenzt werden. Insbesondere sollte es nicht möglich sein, dass beliebige Teilnehmer einer Konferenz die Raumtechnik steuern können.

M-20 Absicherung von Konferenzräumen

Für die in A-20 empfohlene Authentisierung von Videokonferenzteilnehmern ist generell folgendes zu beachten:

Während im Bereich der Chat- und Webkonferenzen in der Regel eine Teilnehmerauthentisierung anhand von Nutzername und Passwort durchgeführt wird, wird bei Audio- und Videokonferenzen häufig lediglich eine Authentisierung auf Basis einer PIN durchgeführt. Zu beachten ist hierbei, dass die PIN meist nicht personenbezogen ist, sondern für alle Nutzer eines Konferenzraumes identisch ist. Dies kann sogar so weit gehen, dass die PIN nicht nur für eine anberaumte Konferenz gilt, sondern zeitlich unbestimmt für den virtuellen Konferenzraum. Um den Beitritt nicht gewünschter Teilnehmer zu verhindern oder zumindest zu erschweren, können Konferenzsysteme auf folgende Weise gesichert werden.

- Regelmäßige Änderung der PIN zur Absicherung eines Konferenzraumes, um die dauerhafte Kompromittierung einzelner Räume zu vermeiden
- Implementierung von Maßnahmen zum Umgang mit PINs, u. a. Regelung zur Weitergabe von PINs und Festlegung einer minimalen PIN-Komplexität
- Vergabe von individuellen Konferenz-PINs
- Vergabe von persönlichen PINs für jeden Teilnehmer, falls keine Authentisierung zumindest über Nutzername und Passwort möglich ist
- Schließung des Konferenzraums durch den Moderator, sobald alle gewünschten Teilnehmer beigetreten sind
- Beitritt in eine Konferenz nur durch Hinzuschalten eines Teilnehmers durch den Moderator

Um zu verhindern, dass an Gesprächen und Konferenzen unbemerkt Dritte teilnehmen, ist neben dem Schutz durch Verschlüsselung und Authentisierung besonders wichtig, dass die Teilnehmer einer Konferenz über die Teilnahme Dritter informiert werden. Dies kann im Fall von Audio-, Video- und Webkonferenzen beispielsweise über ein akustisches Aufmerksamkeitssignal oder die Nennung des Namens des neuen Teilnehmers erfolgen. Zudem ermöglichen die Endgeräte einer Videokonferenzlösung zur Konferenzsteuerung oft das Einblenden einer Teilnehmerliste. Diese sollte sich zur Kontrolle auf unbemerkte und unbefugte Teilnehmer im Regelfall im Vordergrund des Bildschirms befinden und nicht dauerhaft ausgeblendet werden. Zudem sollte mindestens durch den Moderator die Teilnehmerliste kontrolliert und die Teilnahme anonymer Teilnehmer unterbunden werden.

M-21 Absicherung und Einschränkung von Auswertungen von Videokonferenzinhalten

Um A-21 umzusetzen, sollten die folgenden Punkte berücksichtigt werden:

Inhalte von Videokonferenzen können zum Teil automatisch vom Videokonferenzsystem während der aktiven Konferenz ausgewertet werden, ohne dass den Administratoren oder Nutzern dies bewusst ist. Diese Auswertung kann von den Nutzern unerwünscht sein. Insbesondere sollte auch bei Auswertungen für Komfortfunktionen beachtet werden, dass Menschen die Auswertung ihrer personenbezogenen Daten durch einen Automaten als störend empfinden können.

Besondere Beachtung sollten KI-Funktionen erhalten, mit denen beispielsweise die verbale Kommunikation nach Sprachkommandos abgehört oder auf nonverbale Reaktionen in Sprache und Mimik untersucht wird oder die eine Gesichtserkennung durchführen. Auch Software, die eine textbasierte Auswertung des Chatverlaufs vornimmt, kann bei diesem Aspekt eine Rolle spielen.

Generell sollten die Allgemeinen Geschäftsbedingungen und die Dokumentation des Herstellers auf solche Auswertungsmechanismen geprüft werden. Gleiches gilt, wenn Zusatzfunktionen von Drittherstellern zur Verfügung gestellt werden. Gegebenenfalls sollten direkt beim Hersteller Informationen erfragt werden. Dabei sollte geklärt werden, in welcher Form Inhalte von Videokonferenzen ausgewertet werden.

Es sollte sorgfältig geprüft werden, ob der Art der Auswertung generell durch die Institution zugestimmt werden kann. Eine Verweigerung der Zustimmung kann jedoch dazu führen, dass eine Videokonferenzlösung oder Teile davon nicht genutzt werden können.

Werden Funktionen zur Sprach- und Bildinterpretation verwendet, ist zwischen Nutzen und Vertraulichkeitsniveau abzuwägen. Dies gilt auch für Komfortfunktionen, die eine Übertragung der Daten in eine Cloud bedingen. Zumindest für vertrauliche Videokonferenzen sollte die Möglichkeit bestehen, entsprechende Funktionen zu deaktivieren und eine inhaltliche Auswertung der Kommunikation zu verhindern.

Prinzipiell beschränken sich die genannten Aspekte nicht nur auf technische Formen der Auswertung. Sie kann auch manuell durch Konferenzteilnehmer erfolgen.

Werden Videokonferenzinhalte über den Zweck der Videokonferenz hinausgehend ausgewertet, muss dazu auch eine Zustimmung der Gesprächspartner eingeholt werden. Sie muss sowohl eine Auswertung durch den Hersteller des Videokonferenzsystems und Zusatzmodule während der Videokonferenz als auch eine Weiterverarbeitung von potenziellen Aufzeichnungen abdecken. Die Zustimmung sollte zur zukünftigen Nachweisbarkeit gespeichert werden.

Sofern Videokonferenzinhalte aufgezeichnet werden sollen, gelten die Anforderung A-4 sowie die Umsetzungshinweise hierzu (siehe M-4).

In vielen Fällen werden auch während der Auswertung von Videokonferenzen persistente Daten erzeugt, für die geeignete Schutzmaßnahmen umgesetzt werden müssen. Der Schutzbedarf der

Weiterverarbeitung entspricht dabei den inhaltlichen Informationen der aufgezeichneten Konferenz, die nach der Verarbeitung erhalten bleiben oder rekonstruiert werden könnten. Auch hier sollten ein angemessener Zugriffsschutz und eine Verschlüsselung eingesetzt werden (siehe A-5 und M-5).

M-22 Festlegung des Speicherortes der Daten bei Outsourcing und Cloud-Nutzung

Bei der in A-22 empfohlenen Festlegung des Speicherorts sollte dieser am besten innerhalb der EU liegen oder zumindest in einem Land mit Datenschutzstandards, die mit der DSGVO vergleichbar sind. Dies umfasst alle persistenten Daten einer Videokonferenz, d. h. auch Aufzeichnungen oder Auswertungen der Videokonferenz.

Die Möglichkeit zur Festlegung des Speicherortes sowie vom Videokonferenzsystem intern genutzte Speicherorte, für die keine Konfiguration möglich ist, sollte im Rahmen der Planung und Beschaffung geklärt werden (siehe M-11). Abhängig vom Schutzbedarf der geplanten Videokonferenzen kann dies die Auswahl der Videokonferenzlösung beeinflussen.

Der Speicherort sollte möglichst per einheitlicher Konfiguration für alle Videokonferenzen festgelegt werden. Ist auf technischer Ebene eine Festlegung nicht möglich, sollte eine Richtlinie etabliert werden, die die erlaubten Speicherorte festlegt und auf die alle Nutzer hingewiesen werden.

M-23 Cloud-Verfügbarkeit

Die in A-23 empfohlene Berücksichtigung der Cloud-Verfügbarkeit in der Vertragsgestaltung kann über das Aushandeln ausreichender Service Level Agreements (SLAs) umgesetzt werden.

Das Monitoring der Verfügbarkeit von Cloud-Diensten hängt von der Art des Dienstes ab:

Wird beispielsweise eine Komponente der Videokonferenzlösung als Software as a Service (SaaS) genutzt, so werden häufig entsprechende Informationen zur Verfügbarkeit durch den Provider bereitgestellt. Diese sollte regelmäßig, möglichst automatisiert geprüft werden. Darüber hinaus sollte automatisch eine Fehlermeldung erzeugt werden, wenn eine Videokonferenz aufgrund mangelnder Verfügbarkeit nicht eingerichtet werden kann.

Wird eine Komponente in einer (Virtual) Private Cloud bereitgestellt, sollte diese in das Monitoring der Institution eingebunden werden.

7.2.2.2 Endgeräte und Clients

M-24 Deaktivierung oder zumindest Absicherung eines Web-Servers auf einem Video-Endpunkt

Für die Umsetzung von A-24 sollte zunächst ermittelt werden, ob und auf welchen Video-Endpunkten ein Web-Server in Betrieb ist und für welche Tätigkeiten dieser erforderlich ist. Dies ist beispielsweise bei Raumsystemen oder bei Browser-basierten Endpunkten häufig der Fall.

Zur Überprüfung können die Angaben des Herstellers herangezogen werden. Video-Endpunkte können auch selbst untersucht werden, indem z. B. die aktiven Prozesse analysiert werden oder mit einem Port-Scanner ermittelt wird, welche Ports auf dem Gerät geöffnet sind. Dies lässt Rückschlüsse darauf zu, welche Anwendungen auf dem Endpunkt aktiv sind.

Vor einer Deaktivierung des Web-Servers sollte die Absicherung der alternativen Zugänge geprüft werden. Beispielsweise kommt eine Administration über einen ungesicherten Telnet-Zugang nicht in Betracht.

Um die Deaktivierung oder Absicherung aktiver Web-Server umzusetzen, sollten über die in A-24 genannten Bausteine hinaus auch die Herstellerangaben berücksichtigt werden.

M-25 Deaktivierung oder zumindest Einschränkung bzw. Deaktivierung der Sprachsteuerung

Unterstützt die Videokonferenzlösung Möglichkeiten zur Sprachsteuerung, sollte zur Umsetzung von A-25 zwischen Nutzen und Risiken, die durch Missbrauch oder Fehlfunktion entstehen können, abgewogen werden. In diese Überlegung sollten auch die Aspekte Vertraulichkeit und Datenschutz miteinbezogen werden (siehe M-21).

Führt diese Betrachtung zu dem Ergebnis, dass eine vollständige Deaktivierung der Sprachsteuerung für Videokonferenzen nicht gewünscht ist, sollten die möglichen Steuerungsoptionen auf die notwendigsten begrenzt werden, beispielsweise durch angepasste Profile der Sprachsteuerung. Falls die Sprachsteuerung nicht permanent deaktiviert wird, sollte eine Arbeitsanweisung etabliert werden, die den Umgang mit der Sprachsteuerung regelt. Die Einhaltung der Arbeitsanweisung sollte dann stichprobenartig überprüft werden.

Die angebundene oder integrierte Sprachsteuerung sollte so konfiguriert werden, dass sie nicht versehentlich aktiviert werden kann. Wenn nötig, sollten vorkonfigurierte Befehle und Aktivierungscodes, bei denen diese Gefahr besteht, umkonfiguriert oder deaktiviert werden.

Wird die Videokonferenzlösung ausgeschaltet, sollte auch eine externe Sprachsteuerung ausgeschaltet werden.

M-26 Einschränkung des lokalen Zugriffs auf die Konfiguration von dedizierten Video-Endpunkten

Ein dedizierter Video-Endpunkt, z. B. Raumsystem oder Videotelefon, stellt meist einen Zugang über Bedientasten am Gerät oder über eine Fernbedienung bereit, über die verschiedene Einstellungen vorgenommen und geändert werden können.

Dabei umfasst die in A-26 empfohlene Zugriffseinschränkung nicht die Nutzereinstellungen zu Displayauflösung und Videosignalausgängen, sondern die Netz- und Administrationseinstellungen des Video-Endpunkts. Hier sollten PINs bzw. Kennwörter, die vom Hersteller für administrative Zugriffe voreingestellt wurden, geändert werden. Typischerweise sind leicht zu erratende PINs wie 0000 oder der Herstellername als Default-Kennwort voreingestellt. Die Komplexität von PIN oder Kennwort sollte dabei möglichst hoch gewählt und wenn möglich durch das System geprüft werden.

Hierbei sollte nicht nur eine klassische Fernbedienung berücksichtigt werden, sondern auch Fernbedienungen, die z. B. via App und Bluetooth ein Raumsystem steuern können. In diesem Fall muss die Bluetooth-Kommunikation nach aktuellem Stand der Technik abgesichert erfolgen (siehe [NIST BTS-2017]).

M-27 Deaktivierung der automatischen Annahme eines Video-Anrufs

Zur Unterstützung der in A-27 empfohlenen Deaktivierung der automatischen Annahme eines Video-Anrufs sollte, sofern technisch möglich, bei Inaktivität des Video-Endpunkts die Kamera automatisch so aus dem Raumsichtfeld gedreht werden, dass kein auswertbares Signal übertragen werden kann und die Tonübertragung deaktiviert wird. Hierdurch ist den Nutzern eines Raumes mit Videokonferenzlösung sofort sichtbar, ob ein Video-Endpunkt aktiv oder inaktiv ist.

M-28 Signalisierung der Kamera- und Mikrofonaktivität

Zur Umsetzung von A-28 ist an vielen Endgeräten eine LED angebracht, die bei Betrieb der Kamera aktiviert wird. Eine solche Anzeige stellt den Kamerastatus nicht mit absoluter Verlässlichkeit dar, da prinzipiell eine Deaktivierung der Warn-LED durch einen Angreifer denkbar ist. Sie bietet aber zumindest eine weitere Sicherheitsstufe, die ein Angreifer überwinden muss.

Existiert am Endgerät keine Warn-LED, mit der die Kameraaktivität signalisiert werden kann, sollte eine Kameraabdeckung (z. B. Schutzkappe) als verlässlicher und einfach zu realisierender

Schutz in Betracht gezogen werden. In besonders schützenswerten Umgebungen sollte eine solche Abdeckung grundsätzlich genutzt werden.

Weiterhin sollte die Mikrofonaktivität angezeigt werden. Wünschenswert ist eine Anzeige analog zur Kameraaktivität.

Darüber hinaus sollten die Nutzer informiert werden, ob eine Signalisierung am genutzten Endpunkt erfolgt bzw. welche Maßnahmen zu ergreifen sind.

Erfolgt eine Videokonferenz über eine Webanwendung auf Basis von WebRTC, sollte der Browser so konfiguriert werden, dass die Freigabe zur Nutzung von Mikrofon und Kamera stets vor Beginn einer Konferenz abgefragt wird. Eine generelle Freigabe sollte unterbunden werden.

M-29 Geeignete Standortwahl

Bei der Umsetzung von A-29 sollten folgende Eckpunkte beachtet werden:

- Keine Erfassung von Informationen im Hintergrund (z. B. Whiteboard, Monitor, Pinnwand)
- Keine Erfassung von Durchgangswegen und öffentlichen Räumen, z. B. in Zügen
- Keine Erfassung von Arbeitsplätzen unbeteiligter Dritter
- Monitore u. Ä. nicht durch Fenster einsehbar

Falls der Aufenthaltsort als sensible Information einzustufen ist, sollten Fensterflächen und markante Rauminhalte im Hintergrund nicht erfasst werden.

Wenn diese Punkte durch eine geeignete Positionierung des Endgerätes bzw. der Kamera nicht zu erzielen sind, z. B. in einem Großraumbüro, können Trennwände oder Raumteiler genutzt werden. Führt auch das nicht zum gewünschten Ergebnis und kann A-29 nicht sicher umgesetzt werden, sollte auf einen Einsatz von Videokonferenzen am betreffenden Ort verzichtet werden.

Alternativ sollte, insbesondere bei vertraulichen Gesprächsinhalten, für Videokonferenzen auf dedizierte Besprechungsräume oder Stillarbeitsräume, sogenannte Think Tanks, zurückgegriffen werden (siehe M-54).

M-30 Ausblenden des Hintergrunds bei Videokonferenzen

Beim in A-30 empfohlenen Ausblenden des Hintergrunds ist folgendes zu beachten:

Da Bildverarbeitungsverfahren zum Ausblenden des Hintergrunds häufig fehleranfällig sind, sollte vor der Nutzung in Konferenzen sichergestellt werden, dass der Hintergrund korrekt ausgeblendet wird und auch entsprechende Daten nicht übertragen werden. Prinzipiell können Fehler jedoch auch während laufender Videokonferenzen auftreten, sodass kurzzeitig ein Teil des Hintergrunds zu sehen sein kann. Die Nutzung eines solchen Verfahrens sollte daher mit einer angemessenen Vorsicht geschehen. Besteht die Gefahr, dass vertrauliche Daten preisgegeben werden, sollten alternative Schutzmaßnahmen getroffen werden (siehe M-29).

Nicht alle Videokonferenzlösungen bieten integrierte Funktionen, mit denen der Hintergrund automatisch ausgeblendet werden kann. Ist diese Funktion dennoch gewünscht, muss unter Umständen eine zusätzliche Kamera beschafft werden, die ein derartiges Verfahren unterstützt. In diesem Fall sollte sichergestellt werden, dass alle anderen angeschlossenen Kameras während Konferenzen kein Videosignal übertragen.

Eventuell sind alternative Möglichkeiten vorzuziehen, um einen versehentlichen Abfluss von Informationen oder eine Bilderfassung unbeteiligter Personen zu vermeiden (siehe auch M-29):

- Verzicht auf Bildübertragung
- Aufstellen eines Sichtschutzes

- Verlegung des Video-Endpunkts an einen unproblematischen Standort
- Nutzung eines Besprechungsraums

M-31 Absicherung der direkten Kommunikation zwischen Standard-Client und Raumsystem

Für die Umsetzung von A-31 sollten die folgenden Punkte beachtet werden:

Prinzipiell können auch unzulässige Geräte mit einem Raumsystem verbunden werden. Es sollte daher überprüft werden, ob das Gerät grundsätzlich autorisiert ist, mit dem Raumsystem verbunden zu werden. Dies muss in den Informationen zum Raumsystem dokumentiert sein.

Darüber hinaus muss sich ein Standard-Client gegenüber dem Raumsystem authentisieren. Beispielsweise kann das Raumsystem eine Bestätigung von einem der Konferenzteilnehmer einholen, ob die Verbindung zugelassen werden darf.

Eine drahtlose Kommunikation zwischen Standard-Client und Raumsystem sollte verschlüsselt werden, da sie ansonsten von Angreifern eingesehen oder manipuliert werden könnte. Dies gilt insbesondere für WLAN- und Bluetooth-Kommunikation (siehe Baustein *NET.2.1 WLAN-Betrieb* des IT-Grundschutz-Kompendiums sowie [NIST BTS-2017]). Geeignete Verschlüsselungsverfahren und Schlüssellängen sind in [BSI TR02102-2019] spezifiziert.

7.2.2.3 Netzwerk

M-32 Dediziertes Sicherheitssegment für zentrale Komponenten des Videokonferenzsystems

Der Aufbau von Sicherheitssegmenten mit den Mitteln des Netzes stellt eine sinnvolle Sicherheitsmaßnahme dar, die unter gewissen Rahmenbedingungen in Betracht gezogen werden sollte.

Die in A-32 empfohlene Zuordnung von zentralen Komponenten des Videokonferenzsystems zu dedizierten Sicherheitssegmenten kann analog zu *NET.1.1.A4 Netztrennung in Sicherheitszonen* erfolgen. Als Sicherheitselement zur Kontrolle der Kommunikation kommen üblicherweise eine Firewall und/oder ein Intrusion Prevention System (IPS) in Betracht.

Wenn zentrale Komponenten der Videokonferenzlösung wie beispielsweise eine MCU nicht angemessen dahingehend gehärtet werden können, dass sie mit den anderen zentralen Systemen in einem gemeinsamen Sicherheitssegment positioniert werden können, müssen je nach Sicherheitsanforderungen auch mehrere Sicherheitssegmente eingerichtet werden.

Wenn die zentralen Systeme und die Video-Endpunkte einer Videokonferenzlösung unterschiedlichen Sicherheitssegmenten zugeordnet werden, wird die Kommunikation und damit gegebenenfalls auch die Medienströme durch eine Firewall geleitet, was hinsichtlich Firewall-Durchsatz sowie Delay und Jitter für die Qualität der Übertragung zu berücksichtigen ist. Außerdem ist bei modernen Videokonferenzlösungen, die in Meeting Solutions, UC- oder UCC-Lösungen integriert werden, auf Grund der sehr komplexen Kommunikationsbeziehungen auch mit einem sehr komplexen Firewall-Regelwerk zu rechnen.

M-33 Absicherung des lokalen Netzzugangs

Bei der in A-33 empfohlenen Netzzugangskontrolle (Network Access Control, NAC) werden Video-Endpunkte an NAC-fähige Switches angeschlossen und müssen sich gegenüber einem RADIUS-Server authentisieren, bevor sie mit anderen Endpunkten im Netz kommunizieren können.

Die Sicherheit des Verfahrens hängt maßgeblich davon ab, dass eine sichere Authentisierung eingesetzt wird. Eine Authentisierung anhand der MAC-Adressen der Video-Endpunkte ist relativ unsicher, da diese leicht gefälscht werden können. Empfehlenswert ist eine mit IEEE 802.1X

konforme Authentisierung via Extensible Authentication Protocol (EAP), bei dem Endpunkte ein gültiges Zertifikat oder Passwort vorweisen müssen. Optional kann eine Authentisierung nach IEEE 802.1AE (MACsec) genutzt werden. Dieser Standard wird jedoch zurzeit noch selten von Geräten unterstützt.

Die Unterstützung von NAC und Mechanismen gegen ARP Spoofing oder vergleichbar muss im Vorfeld geklärt werden. Abhängig von den Sicherheitsanforderungen der Videokonferenzlösung sollte ein Austausch der Switches zum Anschluss der Video-Endpunkte in Betracht gezogen werden.

M-34 Einsatz eines SBC am Internet-Übergang

Zum Terminieren von Signalisierung und Medienströmen von Videokonferenzlösungen sollte gemäß A-34 am Internet-Übergang ein SBC in einer DMZ eingesetzt werden (siehe Kapitel 3.2.5). Bei dieser Empfehlung sollte jedoch bedacht werden, dass ein SBC stets ein Verschlüsselungsendpunkt ist.

Falls der lokale Einsatz eines SBC nicht möglich ist, kann ein verschlüsselter Tunnel zu einem anderen vertrauenswürdigen Netz aufgebaut werden, in dem ein SBC betrieben wird. Bei diesem Verfahren ist jedoch mit einer Einschränkung der Performance der Videokonferenzlösung zu rechnen.

7.2.2.4 Planung und Betrieb

M-35 Erstellung von Fein- und Betriebskonzept für die Videokonferenzlösung

In dem in A-35 empfohlenen Feinkonzept sollte für alle Komponenten der Videokonferenzlösung die genaue Ausführung und Konfiguration, insbesondere alle Sicherheitseinstellungen wie Parameter zur Verschlüsselung, festgelegt und dokumentiert werden.

Im Betriebskonzept sollte festgelegt werden, auf welche Weise die Videokonferenzlösung in den bestehenden Betrieb eingebunden wird. Um den Betrieb der Videokonferenzlösung mit dem Betrieb der verbundenen und integrierten Dienste zu harmonisieren, ist eine Abstimmung mit den Betriebseinheiten dieser Dienste und den entsprechenden Betriebskonzepten essenziell.

Das Betriebskonzept sollte klassische administrative Aufgaben im Umgang mit eingesetzten Sicherheitsfunktionalitäten spezifizieren. Dabei sollten sowohl der Umfang der Aufgaben und die Zuständigkeiten als auch Schnittstellen und Zuständigkeiten für die Umsysteme festgelegt werden. Es sollte zudem festgelegt werden, wie Schlüssel verteilt und Zertifikate gehandhabt werden. Insbesondere müssen Abweichungen zwischen dem Betrieb der Videokonferenzlösung und den Umsystemen erkannt und dokumentiert werden.

Die Videokonferenzlösung sollte in Bezug auf verschiedene Aspekte überwacht werden. Der aktuelle Status kann über ein Monitoring der Komponenten in geeignetem Umfang analysiert werden. Dazu sollte im Betriebskonzept festgelegt werden, welche Parameter überwacht werden, wann Alarme ausgegeben werden und inwieweit Präventivwarnungen sinnvoll sind. Aus dem Monitoring können ebenfalls Maßnahmen zur Fehleraufbereitung abgeleitet werden. Diese helfen bei der Rekonstruktion von aufgetretenen Problemen und ihrer zukünftigen Vermeidung.

Über ein Reporting werden einschlägige Daten in regelmäßigen Abständen über einen längeren Zeitraum analysiert. Hierdurch können negative Trends wie beispielsweise anhaltende Verschlechterungen bei der Videoqualität erkannt werden. Auch hierzu sollten die Rahmenparameter im Betriebskonzept festgehalten werden.

M-36 Einbindung der Videokonferenzlösung in Datensicherungs- und Archivierungskonzept

Zu den für die Umsetzung von A-36 relevanten Daten zählen zunächst Konfigurationsdaten, mit denen eine Systemwiederherstellung durchgeführt werden kann, und die vordefinierten Konferenzprofile. Dabei ist es ausreichend, Konfigurationsdaten anlassbezogen dann zu sichern, wenn Changes durchgeführt werden.

Auch protokollierte Daten, die für zukünftige oder statistische Betrachtungen interessant sein können, sollten in die Datensicherung aufgenommen werden. Hierzu zählen z. B. Informationen zur Auslastung und Videoqualität sowie Audit-Logs. Ebenso gilt dies für Kontaktdaten, unter denen Gesprächspartner zu erreichen sind. Die Sicherung sollte hierbei in regelmäßigen Abständen erfolgen. Auch bei der Datensicherung und Archivierung müssen gesetzliche Rahmenbedingungen, besonders in Bezug auf die personenbezogenen Daten bei Videokonferenzen, beachtet werden.

Die Sicherung von Daten kann innerhalb der Videokonferenzlösung selbst erfolgen, sofern diese dazu technische Möglichkeiten bietet. Zu diesem Zweck können jedoch auch externe Lösungen eingesetzt werden. Dies gilt auch für die Datensicherung bei Cloud-Lösungen. Der Aspekt der angemessenen Mandantentrennung überträgt sich dabei auch auf die Sicherung der Daten.

Bedarfsweise können auch Videoaufzeichnungen, Chat-Protokolle, Konferenzauswertungen in die Datensicherung und Archivierung mit eingebunden werden. Auch hierbei müssen gesetzliche Rahmenbedingungen des Datenschutzes berücksichtigt werden.

Daten sollten nur dann von der Sicherung ausgenommen werden, wenn ihr Verlust garantiert ausgeschlossen werden kann, keine Auswirkungen hat oder die Daten mit vertretbarem Aufwand wiederhergestellt werden können. In die Sicherung sind gegebenenfalls auch Daten von integrierten oder vernetzten Systemen miteinzubeziehen.

Das Konzept sollte nicht nur den Umfang der Datensicherung und Archivierung, sondern auch die zeitliche Rahmenbedingungen festlegen. Dies betrifft Recovery Point Objective (RPO), Recovery Time Objective (RTO) und generelle Aufbewahrungsfristen.

Grundsätzlich muss sichergestellt werden, dass die Datensicherung jederzeit wieder in die produktive Lösung eingeladen und entschlüsselt werden kann. Desgleichen muss für die Archivierung sichergestellt werden, dass die archivierten Daten jederzeit, insbesondere auch am Ende der Archivierungsfrist, lesbar sind und entschlüsselt werden können (siehe auch [BSI TR03125-2018]). Hierzu sind regelmäßige Tests für eine Datenwiederherstellung und einen Zugriff auf die Datenarchivierung durchzuführen.

Ergänzend wird auf den Baustein *CON.3 Datensicherungskonzept* und *OPS.1.2.2. Archivierung* des IT-Grundschutz-Kompendiums verwiesen.

M-37 Penetrationstest der Videokonferenzlösung

Bei der Umsetzung der in A-37 empfohlenen Penetrationstests ist folgendes zu beachten:

Ein Penetrationstest kann den Betrieb der Videokonferenzlösung gefährden. Dabei können das vollständige System, Teile davon oder integrierte Dienste funktional beeinträchtigt werden oder ausfallen. Die Beeinträchtigung kann temporär oder längerfristig bestehen, während je nach Schwere ein beträchtlicher Aufwand vonnöten sein kann, um den normalen Betriebszustand wiederherzustellen. Weiterhin kann ein permanenter Verlust von persistenten Daten auftreten.

Bevor ein Penetrationstest am produktiven System durchgeführt wird, sollten daher wichtige Sicherheitsmaßnahmen getroffen werden: Der Rahmen des Penetrationstests sollte exakt festgelegt werden und darf im Verlauf keinesfalls überschritten werden. Dabei sollte definiert werden, welche Komponenten und Schnittstellen welcher Art von Test unterzogen werden. Nach Möglichkeit sollten auch KI-Funktionen miteinbezogen werden. Es sollte zudem bestimmt

werden, wie mit integrierten und angebundenen Systemen zu verfahren ist. Auch der zeitliche Rahmen sollte klar gesetzt werden.

Alle Rahmenbedingungen und Tätigkeiten sollten mit den jeweiligen Verantwortlichen genau abgesprochen werden. Dies gilt besonders dann, wenn für den Penetrationstest ein externer Dienstleister beauftragt wird. Ebenso ist das Personal zu benachrichtigen, das für die Sicherheit der IT-Infrastruktur zuständig ist, sodass es darauf vorbereitet ist, Symptome eines Angriffs wahrzunehmen.

Der Zeitpunkt für den Test sollte so gewählt werden, dass durch Ausfälle entstehende Schäden möglichst gering gehalten werden und ein zeitlicher Puffer besteht, um den normalen Betriebszustand wiederherzustellen. Es kann daher sinnvoll sein, den Zeitpunkt des Tests außerhalb der üblichen Geschäftszeiten zu legen. Alternativ kann festgelegt werden, dass die Videokonferenzlösung während des Tests nicht genutzt werden darf. Zumindest sollte den Nutzern mitgeteilt werden, in welchem Zeitraum mit Beeinträchtigungen oder Ausfällen zu rechnen ist.

Um den produktiven Betrieb nicht zu gefährden, kann der Penetrationstest auch auf einen Teil der Ausstattung begrenzt werden. Hierzu können beispielsweise baugleiche Ersatzgeräte getestet werden, die denselben Versionsstand besitzen. Dabei sollte darauf geachtet werden, dass die Parameter eines solchen Testszenarios mit den realen Gegebenheiten vergleichbar sind.

Vor Beginn des Penetrationstests sollten alle persistenten Daten gesichert werden, um Verlusten vorzubeugen und ihre Integrität gewährleisten zu können (siehe M-36).

Das Testszenario sollte aktuelle Schwachstellen berücksichtigen und wichtige Angriffsarten nachstellen. Einzelne Tests sollten möglichst automatisiert durchgeführt werden. Hierzu können in erheblichem Umfang bereits bestehende Tools und Frameworks genutzt werden. Dabei sollte darauf geachtet werden, dass jede eingesetzte Software auf dem aktuellen Stand ist. Als Basis für das konkrete Vorgehen können die Befunde eines zuvor abgeschlossenen Schwachstellen-Scans genutzt werden. Bestehen Unsicherheiten oder steht kein eigenes fachkundiges Personal zur Verfügung, sollte für die Durchführung ein externer Dienstleister beauftragt werden.

Alle Schritte des Penetrationstests sollten möglichst exakt dokumentiert werden. Einzelne Arbeitsschritte können ohne Aufwand protokolliert werden, indem relevante Log-Daten gespeichert und auf der Kommandozeile abgesetzte Befehle inklusive ihrer Ergebnisse in eine Datei geschrieben werden. In jedem Fall sollte im Anschluss an den Penetrationstest ein Bericht erstellt werden, der alle relevanten Parameter und Ziele, die genaue Durchführung und die konkreten Ergebnisse und Befunde enthält. Der Bericht sollte ein abschließendes Fazit enthalten und Empfehlungen zur Verbesserung der Sicherheit der Videokonferenzlösung liefern. Er sollte als Grundlage für weitere Maßnahmen genutzt werden können.

Penetrationstests sollten in angemessenen, regelmäßigen Abständen durchgeführt werden. Bei Bekanntwerden einer Sicherheitslücke, von der die Videokonferenzlösung betroffen sein könnte, kann ergänzend ein anlassbezogener Test sinnvoll sein.

M-38 Schulungen zur sicheren Nutzung von Videokonferenzen

Wie in A-38 empfohlen, sollten alle potenziellen Nutzer einer Videokonferenzlösung an einer Schulung teilnehmen, in der die sichere Nutzung von Videokonferenzen vermittelt wird. Die Schulung sollte bei erkennbarem Bedarf wiederholt werden, z. B. wenn viele neue Nutzer hinzukommen oder die letzte Veranstaltung schon länger zurückliegt. Eine Wiederholung kann auch anlassbezogen sinnvoll sein, etwa nach Einführung eines neuen Videokonferenzsystems oder neuer Funktionalitäten, einem konkreten Sicherheitsvorfall, der auf mangelnde Information zurückzuführen ist, oder bei Erkennung eines neuen Gefahrenpotenzials, welches ein verändertes Nutzerverhalten bedingt.

Zur Stärkung des Gefahrenbewusstseins ist es förderlich, Sicherheitsvorfälle und mögliche Folgen darzustellen, die durch unsachgemäße Nutzung ausgelöst werden können. Ein Verständnis für die zugrunde liegende Problematik trägt zur besseren Akzeptanz von Regelungen bei. Hierzu kann ein Bezug zu aktuellen oder besonders nennenswerten Vorfällen aus der Praxis hergestellt werden.

Teilnehmer der Schulung sollten dabei jedoch nicht so stark verunsichert werden, dass sie von einer Nutzung von Videokonferenzen absehen. Stattdessen sollte ihnen erklärt werden, wie sie auf einfache Art konstruktiv zur Verbesserung der Sicherheit beitragen können. Es sollte zudem Hemmungen entgegengewirkt werden, einen Sicherheitsvorfall oder einen Verdacht sofort zu melden. Dies gilt insbesondere für Vorfälle, die durch eigenes Verschulden verursacht wurden.

In einem einleitenden Schulungsteil können allgemeine Aspekte behandelt und generelles Gefahrenpotenzial dargestellt werden. Dabei sollte das Bewusstsein für Risiken und Gefahren gestärkt werden. Es sollte ein Verständnis dafür entstehen, welche Umstände zu einem Sicherheitsvorfall führen können und welche Auswirkungen sie nach sich ziehen können. Folgende Aspekte können dazu genannt werden:

- Arten und Auslöser von Sicherheitsvorfällen
- Gängige Angriffsszenarien, Funktionsweise von Abhör-Angriffen
- Auswirkungen von Sicherheitsvorfällen
- Risiken von Datenspeicherung in der Cloud und auf dem Video-Endpunkt
- Social Engineering
- Beispiele aus der Praxis

Anschließend sollte erklärt werden, auf welche Weise Probleme vermieden werden und wie eine möglichst sichere Nutzung von Videokonferenzen erreicht werden kann. Diese sollte sowohl auf technische Aspekte des Systems als auch auf das Verhalten der Nutzer bezogen werden, beispielsweise:

- Sichere Konfigurationen für Video-Endpunkte
- Sichere Passwörter
- Nutzung von Verschlüsselung bzw. von Konferenzprofilen mit Verschlüsselung
- Potenzielle Bedienfehler durch Benutzer, z. B. versehentliche Preisgabe von Informationen
- Abmeldung der Nutzer und Ausschalten des Systems
- Erwartete Maßnahmen der Nutzer, z. B. Prüfung der Identität von Gesprächspartnern
- Mögliche Probleme von Sprachsteuerungen
- Datenschutz und weitere rechtliche Aspekte
- Verhalten bei Sicherheitsvorfällen

Abschließend sollte auf die bestehenden Informationen zur sicheren Nutzung (siehe M-13) als ergänzende Dokumentation verwiesen werden. Ebenfalls sollten konkrete Ansprechpartner und deren Kontaktdaten vermittelt werden, die bei Sicherheitsvorfällen zu benachrichtigen sind und für Fragen zur Verfügung stehen. Von den Teilnehmern sollte eine schriftliche Bestätigung eingeholt werden, dass sie in der sicheren Nutzung von Videokonferenzen unterrichtet worden sind und die vermittelten Verhaltensweisen und Regelungen befolgen werden.

M-39 Aufnahme der Videokonferenzlösung in die Prozesse zur Behandlung von Schwachstellen und Sicherheitsvorfällen

Die in A-39 empfohlene Einbindung in das Schwachstellen-Management beinhaltet die regelmäßige Information über bekannt gewordene Schwachstellen für alle eingesetzten Komponenten der Videokonferenzlösung. Zusätzlich sollten zentrale und Cloud-Komponenten der Videokonferenzlösung in regelmäßigen Abständen auf aktuelle Schwachstellen untersucht werden. Dies erfolgt bei Installationen im eigenen Rechenzentrum oder in einer (Virtual) Private Cloud am besten automatisiert durch Einsatz eines Schwachstellen-Scanners.

Existieren Schwachstellen, die nicht durch Software-Patches beseitigt werden können, sollte abhängig von der Brisanz der Schwachstellen in Erwägung gezogen werden, die betroffenen Komponenten auszutauschen bzw. bis zu einem geeigneten Patch nicht zu nutzen. Dies gilt auch für Video-Endpunkte und zusätzliche Peripherie.

Im Rahmen der Prozesse zur Behandlung von Sicherheitsvorfällen sollte schnellstmöglich verantwortliches Personal benachrichtigt werden, sobald ein Sicherheitsvorfall erkannt wird. Nur so können potenzielle Schäden für die Videokonferenzlösung und die integrierten Systeme minimiert werden. Als Erstmaßnahme sollten betroffene Komponenten isoliert oder vom Netz getrennt werden, sodass die Auswirkungen des Vorfalls begrenzt bleiben. Hierbei sind zentrale Systeme und Video-Endpunkte gleichermaßen zu berücksichtigen. Bei Diebstahl von mobilen Geräten kann es sinnvoll sein, dort gespeicherte Daten aus der Ferne zu löschen.

Falls Teile der Videokonferenzlösung als Cloud-Dienst, z. B. als SaaS, realisiert werden, sollte sichergestellt werden, dass der Provider aktuelle Informationen zu Schwachstellen und Sicherheitsvorfällen bereitstellt. Auch bei der Nutzung von Cloud-Diensten sollten dem Nutzer entsprechende Meldewege bereitgestellt werden, um potenzielle Sicherheitsvorfälle und Schwachstellen dem Provider zu melden.

M-40 Überwachung durch IT-Monitoring

Ein primäres Ziel des in A-40 empfohlenen Monitoring ist es, den fehlerfreien Zustand aller Komponenten zu kontrollieren. Dabei wird kontinuierlich überwacht, ob alle Bestandteile der Lösung in Betrieb sind und ordnungsgemäß arbeiten. Auch die Konfiguration der Komponenten und die Konnektivität zu anderen Systemen sollten dabei mit einbezogen werden.

Viele Lösungen können via SNMP Informationen an das Monitoring übertragen. Zur automatischen Erkennung und Einbindung neuer Komponenten kommt häufig LLDP-MED (Link Layer Discovery Protocol - Media Endpoint Discovery) oder ein proprietäres Protokoll zum Einsatz.

Die Videokonferenzlösung sollte mindestens eine SNMP-Unterstützung bieten, die die wichtigsten Systemparameter und eine Alarmierung beinhaltet. Darüber hinaus sollten möglichst VoIP- und Video-spezifische Parameter unterstützt werden. Die hierzu erforderliche MIBs (Management Information Base) sind meist herstellerspezifisch und sollten bei den in Betracht kommenden Herstellern erfragt werden.

Das Monitoring sollte ebenfalls kontrollieren, ob Anforderungen an die Qualität der Videoübertagung eingehalten werden. Die Qualität kann anhand von Merkmalen wie Verluste und Verzögerungen von Paketen (Delay und Jitter) gemessen werden. Eine hochwertige und stabile Videoübertagung ist entscheidend für die optimale Nutzung der technischen Möglichkeiten und trägt maßgeblich zur Akzeptanz der Lösung durch die Nutzer bei. Sie hilft außerdem bei der Einschätzung, ob die Netzinfrastruktur genügend Ressourcen für die Videokonferenzlösung bereitstellt.

M-41 Integration in zentrales Log-Management

Bei der in A-41 empfohlenen Integration in das zentrale Log-Management können in der Regel nur Systeme berücksichtigt werden, die im eigenen Rechenzentrum, als (Virtual) Private Cloud realisiert werden oder als Infrastructure as a Service (IaaS) im Rahmen eines Cloud-Dienstes genutzt werden.

Im Log-Management sollten zumindest solche Informationen protokolliert werden, die dabei helfen, allgemeine Probleme und Sicherheitsvorfälle festzustellen und genauer zu analysieren. Dazu muss der angemessene Log-Level analysiert und eingestellt werden.

Es ist möglich, dass Systeme nicht ohne weiteres als Datenquellen in das Log-Management integriert werden können, da beispielsweise das Ausgabeformat nicht standardisiert ist. In solchen Fällen muss ein Konnektor genutzt werden, um die Daten aus der Quelle zu verarbeiten. Im Rahmen der Beschaffung sollte geprüft werden, ob für diesen Anwendungsfall ein Konnektor vom Hersteller der Log-Management-Lösung oder Drittentwicklern verfügbar ist. Ist dies nicht der Fall, sollte hierzu eine eigene Lösung entwickelt werden. Hierzu sollten Anleitungen und Werkzeuge genutzt werden, die von Herstellern üblicherweise für Eigenentwicklungen zur Verfügung gestellt werden.

Beispielsweise können folgende Daten zur längerfristigen Speicherung an das Log-Management weitergeleitet werden:

- Leistungsindikatoren
- Systemdaten, insbesondere Fehlermeldungen
- Sicherheitsrelevante Informationen und Audit-Logs

Unter Umständen werden in den Log-Daten der Videokonferenzlösung Nutzungsdaten und Verbindungen zwischen Konferenzteilnehmern protokolliert. Da es sich bei solchen Daten um personenbezogene Daten handelt, müssen gesetzliche Rahmenbedingungen und insbesondere die DSGVO eingehalten werden. Bei der Protokollierung im Cloud-Umfeld muss sichergestellt werden, dass eine ausreichende Mandantentrennung gegeben ist.

7.2.3 Maßnahmen bei erhöhtem Schutzbedarf

7.2.3.1 Anwendungen und zentrale Komponenten

M-42 Durchgängige Verschlüsselung der mit IP übertragenen Daten einer Videokonferenz

Die in A-42 empfohlene Verschlüsselung der Medienströme sollte möglichst über Secure Real-time Transport Protocol (SRTP) respektive Secure RTP Control Protocol (SRTCP) erfolgen. Alternativ kann eine gleichwertige Verschlüsselungstechnik, die beispielsweise auf VPN-Techniken basiert, eingesetzt werden.

Die Verschlüsselung erfolgt zwischen den Endgeräten bzw. zwischen Endgerät und einem Gateway, das die Medienströme terminiert wie z. B. Media Gateway oder SBC, und gegebenenfalls zwischen Gateways. Die an der Verschlüsselung beteiligten Instanzen müssen ein dynamisches Schlüsselmanagement unterstützen, das eine sichere Aushandlung des Schlüsselmaterials erlaubt.

Die Verschlüsselung der Signalisierung sollte mit einer sicheren Variante von TLS erfolgen. Dabei muss beachtet werden, dass gravierende Unterschiede im Sicherheitsniveau zwischen verschiedenen TLS-Varianten bestehen. Alternativ kann eine gleichwertige Verschlüsselungs-technik, die beispielsweise auf IPsec oder auf einer anderen VPN-Technik basiert, eingesetzt werden.

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

Hinweis: Die Übertragung der Medienströme innerhalb einer Videokonferenzanlage eines Herstellers, z. B. zwischen Video-Terminals und MCU, und zwischen einheitlichen Anlagen an verschiedenen Standorten einer Institution kann meist gemäß A-43 abgesichert werden. Jedoch ist dies bei der übergreifenden Kommunikation zwischen unterschiedlichen Institutionen mit Anlagen unterschiedlicher Hersteller nicht immer gewährleistet. Der Grund besteht darin, dass die etablierten Standards gewisse Freiheitsgrade in der Implementierung erlauben. Daher verhindern in dieser Konstellation häufig Inkompatibilitäten eine sichere Verschlüsselung oder aber die jeweiligen Institutionen müssen die Einstellungen für eine sichere Verschlüsselung aufwendig abstimmen.

M-43 Ende-zu-Ende-Verschlüsselung der mit IP übertragenen Daten einer Videokonferenz

Zur Umsetzung von A-43 sollte die Videokonferenzlösung so konfiguriert werden, dass nur Ende-zu-Ende-verschlüsselte Verbindungen zugelassen werden, d. h. die Verschlüsselung muss von den Video-Endpunkten vorgenommen werden und darf im gesamten Übertragungsweg nicht entschlüsselt werden.

Somit muss sichergestellt werden, dass sich keinerlei Verschlüsselungsendpunkte zwischen den Clients befinden. Werden Daten durch eine MCU übertragen, darf diese die Daten nicht entschlüsseln. Dies kann dazu führen, dass einige Funktionen der MCU nicht genutzt werden können, da diese die Medienströme nicht dekodieren kann. Auch SBC und Video Edge Server werden vornehmlich als Verschlüsselungsendpunkte eingesetzt. Aus diesem Grund ist eine echte Ende-zu-Ende für Videokonferenzen in der Regel nicht praktikabel.

Wenn daher auf eine Ende-zu-Ende-Verschlüsselung verzichtet wird, sollten nach Möglichkeit Verschlüsselungsendpunkte genutzt werden, die der eigenen Kontrolle unterliegen. Es sollte jedoch darauf geachtet werden, dass sie angemessen geschützt sind. Verschlüsselungsendpunkte bei einem Provider, insbesondere einem Cloud-Provider, sollten gemäß M-49 vermieden werden.

Alle Endpunkte, die zur Teilnahme an Videokonferenzen mit Ende-zu-Ende-Verschlüsselung genutzt werden sollen, müssen entsprechende Verschlüsselungsmechanismen unterstützen. Gegebenenfalls sind in diesem Fall einige Endpunkte nicht geeignet; beispielsweise kann sich ein Nutzer nicht mehr per Telefon in eine Videokonferenz einwählen.

M-44 Authentisierung zwischen Video-Endpunkten und zentralen Komponenten

Für die in A-44 empfohlene gegenseitige Authentisierung sollte Mutual TLS (MTLS) unter Beachtung der Hinweise für den Einsatz von TLS eingesetzt werden (siehe [BSI TR02102-2019]).

M-45 Zusätzliche Absicherung der Konfiguration von geplanten Videokonferenzen

Für die in A-45 empfohlene separate Übertragung von PIN oder Passwort für den Zugang zu einer Konferenz sollte eine separate vertrauenswürdige Verbindung genutzt werden.

Ergänzend sollte ein Teilnehmer nach erfolgreicher Authentisierung in einem Wartebereich verbleiben, bis einer der Moderatoren über die Zulassung entschieden hat.

Alternativ kann ein Teilnehmer zunächst von der Videokonferenzlösung kontaktiert werden. Der Teilnehmer muss seine Einwahl in die Videokonferenz anschließend bestätigen. Auf diese Weise kann verhindert werden, dass z. B. bei telefonischem Kontakt eine Mailbox einen Teil der Konferenz aufnimmt. Durch diese aktive Einwahl kann von vornherein der Personenkreis kontrolliert werden, für den der Zugang zur Konferenz vorgesehen ist. Allerdings setzt dies auch voraus, dass der kontaktierte Video-Endpunkt gegen einen unbefugten Zugriff abgesichert ist.

M-46 Protokollierung der Tätigkeit von Systembedienern

Bei erhöhtem Schutzbedarf sollte zur Umsetzung von A-46 eine Integration des Videokonferenzsystems in eine Lösung zum Privileged Access Management (PAM) in Betracht gezogen werden. Ebenso sollte eine Entkopplung, beispielsweise über einen Terminal Server, erwogen werden. Bei der Protokollierung muss eine Pseudonymisierung personenbezogener Daten realisiert werden und die Funktion zur Aufhebung der Pseudonymisierung muss besonders geschützt werden. Der Zugriff auf nicht mehr pseudonymisierte Daten sollte ausschließlich im Vier-Augen-Prinzip erfolgen. Dieses sollte von der entsprechenden Protokollierungslösung erzwungen werden.

M-47 Zusätzliche Datensicherung

Die in A-47 empfohlene Sicherung für Dateien, die in der Cloud abgelegt werden, kann einfach realisiert werden, indem der Nutzer, der die Datei zur Verfügung stellt, eine lokale Kopie auf seinem lokalen Video-Endpunkt oder einer internen Dateiablage der Institution sichert. Dies sollte sowohl vor als auch nach der Bearbeitung in der Konferenz erfolgen.

Besteht keine Möglichkeit, eine Sicherungskopie auf einem internen Speicher der Institution anzulegen, kann diese auch in einem separaten Cloud-Speicher angelegt werden. Dieser alternative Cloud-Dienst muss die Anforderungen bezüglich Datensicherheit und Integrität erfüllen (siehe auch M-59). Auf die Sicherungskopie kann so auch dann zugegriffen werden, wenn der ursprüngliche Cloud-Dienst ausgefallen ist.

Bei der Wahl des Speicherorts muss der Schutzbedarf der zu speichernden Daten beachtet werden. Insbesondere sollte die Vertraulichkeit angemessen geschützt und die Datei gegebenenfalls verschlüsselt gespeichert werden (siehe M-5).

M-48 Zertifizierung nach Common Criteria für zentrale Komponenten des Videokonferenzsystems

Die in A-48 empfohlene Zertifizierung nach Common Criteria für die Plattformen der zentralen Komponenten der Videokonferenzlösung sollte bereits während der Planungsphase geprüft und berücksichtigt werden. Es sollte beachtet werden, dass Zertifizierungen immer nur für einen begrenzten Zeitraum ausgestellt werden. Daher sollte sichergestellt werden, dass die erforderliche Zertifizierung weiterhin aktuell ist. Sie muss zudem für alle zentralen Komponenten gelten.

Es kann vorkommen, dass die Informationen, die ein Hersteller über die Common-Criteria-Zertifizierung seines Produkts herausgibt, bereits veraltet ist. Für aktuelle Informationen sollte daher unbedingt die offizielle Website der Common Criteria for Information Technology Security Evaluation als Referenz herangezogen werden (siehe https://www.commoncriteriaportal.org/).

M-49 Vermeidung von Verschlüsselungsendpunkten in einer Cloud

Wenn bei der Umsetzung von A-49 aus technischen Gründen ein Verschlüsselungsendpunkt in einer Cloud nicht vermieden werden kann, sollte der Cloud-Dienstleister einen Dienst anbieten, der es erlaubt, entweder eigenes Schlüsselmaterial zu verwenden oder Schlüsselmaterial zu nutzen, welches ein vertrauenswürdiger zusätzlicher Cloud-Dienstleister bereitstellt.

Hierzu können entweder im eigenen Rechenzentrum oder bei einem Cloud-Dienstleister sogenannte Hardware Security Modules (HSM) genutzt werden (siehe Umsetzungshinweise zu *OPS.2.2.M17 Einsatz von Verschlüsselung bei Cloud-Nutzung*).

M-50 Keine Aufzeichnung von Videokonferenzinhalten

Die in A-50 geforderte Regelung zur Aufzeichnung von Videokonferenzen muss durch technische Maßnahmen flankiert werden. Grundsätzlich darf in der Videokonferenzlösung die Aufzeichnung nicht generell aktiviert sein. Gemäß den erlaubten Rahmenbedingungen muss ein Profil für Videokonferenzen mit erhöhtem Schutzbedarf definiert sein, in dem im Einzelfall die

Aufzeichnung aktiviert werden kann (siehe M-2). Hierbei sind die in M-4 beschriebenen Hinweise bezüglich Zustimmung zur und Umgang mit der Aufzeichnung zu beachten.

Bei hohem Schutzbedarf sollte zur Kontrolle ein Vier-Augen-Prinzip beim Zugriff auf die Videokonferenzinhalte umgesetzt werden, sodass jeder Zugriff durch eine weitere Person überwacht wird.

M-51 Einsatz von Host-basierten DLP-Systemen

Host-basierte DLP-Systeme eignen sich für die Überwachung sowohl institutionsinterner als auch übergreifender Kommunikation und insbesondere für die Peer-to-Peer-Dateiübertragung, wenn deren Ende-zu-Ende-Verschlüsselung nicht aufgebrochen werden soll.

Der in A-51 empfohlenen Einsatz von Host-basierten DLP-Systemen sollte sowohl die zentralen Komponenten als auch möglichst alle Video-Endpunkte abdecken. Auf den jeweiligen Hosts muss hierfür ein DLP-Agent installiert werden. Möglich ist auch eine Kombination von Host- und Netz-basierter DLP (siehe M-57).

Für die zu schützenden Daten muss ein Konzept zur Klassifizierung von Daten entwickelt und umgesetzt werden. Dieses sollte für verschiedene Klassen von Daten ein angemessenes Schutzniveau spezifizieren. Für jedes Schutzniveau muss definiert werden, welche Dateibewegungen zugelassen werden und welche Nutzer bzw. Rollen welche Operationen darauf ausführen dürfen. Das DLP-System sollte kontinuierlich auf Alarme überprüft werden.

Die Verwendung von DLP für interne Videokonferenzen ist nur dann zielführend, wenn Dateien und Daten unterschiedlicher Klassifizierungen zwischen Nutzern mit unterschiedlichen Berechtigungsstufen ausgetauscht werden sollen.

M-52 Einschränkung von KI-Funktionen

Der Einsatz von KI-Funktionen geht häufig mit einer inhaltlichen Analyse von Videokonferenzen einher. Zu diesem Zweck werden oftmals Inhalte oder Metadaten von Videokonferenzen an eine zentrale Analyse-Instanz des Herstellers geleitet. Bei einem erhöhten Schutzbedarf der Videokonferenzen und der dort übertragenen Inhalte muss dieses Verhalten vermieden werden, da Speicherung der Daten und Umfang der Analyse nicht kontrolliert werden können.

KI-Funktionen sollten gezielt deaktiviert werden können, z. B. generell für alle Videokonferenzen oder bedarfsweise für vertrauliche Konferenzen. Die bedarfsweise Deaktivierung sollte möglichst automatisch über ein Konferenzprofil umgesetzt werden (siehe M-2).

Ist die in A-52 empfohlene Deaktivierung von KI-Funktionen nicht möglich oder aufgrund von Komfortfunktionen nicht gewünscht, sollte der Umfang soweit wie möglich begrenzt werden. Mindestens muss darauf geachtet werden, dass keine Daten in Netze geleitet werden, die nicht zur eigenen Institution gehören oder nicht vertrauenswürdig sind.

7.2.3.2 Endgeräte und Clients

M-53 Ausschließliche Nutzung von verschlüsselter Kommunikation

Zur Umsetzung von A-53 sollte die Videokonferenzlösung so konfiguriert werden, dass nur Endpunkte zu Videokonferenzen zugelassen werden, die eine geeignete Verschlüsselung unterstützen. Diese Einstellung kann an zentralen Stellen wie z. B. MCUs vorgenommen werden und muss organisatorisch flankiert werden.

Es sollte bedacht werden, dass einige Endpunkte wie z. B. reine Audiogeräte grundsätzlich keine Verschlüsselung unterstützen. Die Teilnahme an Videokonferenzen mit erhöhtem Schutzbedarf ist von diesen Video-Endpunkten dann nicht mehr zulässig.

Sollen in der Videokonferenz Informationen von einer internen oder externen Dateiablage bereitgestellt werden, z. B. Informationen von einem Standard-Client auf einem Raumsystem, sollte auch diese Kommunikation durch eine geeignete Verschlüsselung gesichert werden.

M-54 Verzicht auf Videokonferenzen in Großraumbüros

Zur Umsetzung von A-54 wird empfohlen, Videokonferenzen mit erhöhtem Schutzbedarf in einem dedizierten Raum durchzuführen, der für einen erhöhten Schutzbedarf geeignet ist. Er sollte angemessen gegen Abhör- und Ausspähversuche und unbefugtes Betreten abgesichert sein.

Insbesondere Nutzer von mobilen Endgeräten sollten Videokonferenzen mit erhöhtem Schutzbedarf nicht in öffentlichen Räumen wie beispielsweise Parks durchführen, da hier ein Abhören oder Ausspähen nicht gesichert unterbunden werden kann und dieses gegebenenfalls auch über große Entfernungen möglich ist.

M-55 Verzicht auf Sprachsteuerung

Beim Einsatz von Sprachsteuerung während Videokonferenzen wird die verbale Kommunikation kontinuierlich analysiert und auf Befehle untersucht. Dieser Umstand kann bei erhöhtem Schutzbedarf problematisch sein, da eine Preisgabe von vertraulichen Informationen nicht ausgeschlossen werden kann. Daher sollte gemäß A-55 bei erhöhtem Schutzbedarf auf eine Sprachsteuerung verzichtet werden.

Hierzu wird empfohlen, die Sprachsteuerung an zentraler Stelle zu deaktivieren bzw. keine Add-ons zu diesem Zweck zu installieren. Falls eine entsprechende Konfiguration nicht zentral vorgenommen werden kann oder soll, muss dies auf den Video-Endpunkten umgesetzt werden. Externe Sprachsteuerungen sollten ausgeschaltet werden, wenn in ihrem Umfeld eine vertrauliche Videokonferenz durchgeführt wird.

7.2.3.3 Netzwerk

M-56 Einsatz eines SBC am WAN-Übergang

Ein gemäß A-56 am WAN-Übergang eingesetzter SBC darf die Firewall nicht umgehen, sondern stellt ein zusätzliches Sicherheitselement dar. Er sollte sowohl Signalisierung als auch Medienströme filtern. Da die Daten zu diesem Zweck entschlüsselt werden müssen, bildet der SBC zwangsläufig einen zusätzlichen Verschlüsselungsendpunkt.

M-57 Einsatz von Netz-basierten DLP-Systemen

Ähnlich zu Host-basierten DLP-Systemen (siehe M-51) kontrollieren auch die in A-57 empfohlenen Netz-basierten DLP-Systeme Dateiübertragungen und -verarbeitungen. Dabei werden die jeweiligen Dateien anhand von Attributen klassifiziert und die Operationen auf Konformität mit den Richtlinien der Institution kontrolliert. Netz-basierte DLP kann mit Host-basierter DLP kombiniert werden.

Netz-basierte DLP-Systeme können überall dort zum Einsatz kommen, wo eine zentrale Kontrolle der Datenströme möglich ist, z. B. bei Dateiübertragung zu externen Teilnehmern. Hierbei muss die verschlüsselte Kommunikation zur Untersuchung durch das DLP-System im Sinne eines „friendly Man-in-the-Middle“ aufgebrochen werden. Das DLP-System muss daher gehärtet und in einer gesicherten Netzzone positioniert werden. Dieser Ansatz eignet sich besonders, wenn nur die institutionsübergreifende Kommunikation mittels DLP gesichert werden soll.

7.2.3.4 Planung und Betrieb

M-58 Sichere Administration

Die in A-58 empfohlenen separaten Administrationsnetze und -schnittstellen sollten nicht direkt über das Internet erreichbar sein. Ein Zugriff aus dem Internet muss entsprechend abgesichert und entkoppelt erfolgen.

Der Zugriff auf administrative Schnittstellen sollte nur nach einer erfolgreichen Authentisierung möglich sein. Standard-Passwörter auf den Geräten sollten bei der Installation und Konfiguration geändert werden und, falls technisch möglich, durch eine Zwei-Faktoren-Authentisierung ersetzt werden.

Bei erhöhtem Schutzbedarf sollte eine Integration des Videokonferenzsystems in eine Lösung zum Privileged Access Management (PAM) in Betracht gezogen werden. Ebenso sollte eine Entkopplung, beispielsweise über einen Terminal Server, erwogen werden. Bei der Protokollierung muss eine Pseudonymisierung personenbezogener Daten realisiert werden und die Funktion zur Aufhebung der Pseudonymisierung muss besonders geschützt werden. Der Zugriff auf nicht mehr pseudonymisierte Daten sollte ausschließlich im Vier-Augen-Prinzip erfolgen. Dieses sollte von der entsprechenden Protokollierungslösung erzwungen werden.

M-59 Ausschließliche Datenablage innerhalb der Europäischen Union (EU)

Insbesondere dann, wenn Speicherorte nicht unter eigener Kontrolle liegen, sollten Standorte und Transportwege eindeutig festgelegt werden. Dabei sollte, wie in A-59 gefordert, möglichst keine Speicherung und Übertragung über die Grenzen der EU hinaus erfolgen.

Nutzer, die außerhalb der EU positioniert sind, dürfen die übertragenen Daten nicht lokal speichern. Dies ist auch organisatorisch zu flankieren.

Werden z. B. im Rahmen von Cloud-Lösungen Auftragsverarbeiter in Anspruch genommen, sollte von ihnen eine entsprechende Zusicherung eingeholt werden. Bei der Verarbeitung der Daten muss die DSGVO berücksichtigt werden. Dies gilt auch für Auftragsverarbeiter.

M-60 Überwachung durch ein Security Information and Event Management (SIEM)

Ziel der in A-60 empfohlenen Überwachung ist die frühzeitige Erkennung von Sicherheitsvorfällen und anderen Problemen. Das SIEM sollte sicherheitsrelevante Log-Daten der Videokonferenzlösung kontinuierlich auswerten und für einen angemessenen Zeitraum archivieren.

Für den erfolgreichen Betrieb sollte das Datenaufkommen, das durch die Videokonferenzlösung anfällt, möglichst genau abgeschätzt werden. Hierzu können auf Basis vorhandener Bestandsdaten Schätzwerte ermittelt, ein temporärer Log-Server für eine Messung genutzt oder der Hersteller des SIEM nach Erfahrungswerten gefragt werden. Der ermittelte Wert sollte in der Wahl der Lizenzgröße für das SIEM und dessen Speicherplatz berücksichtigt werden.

Um die Log-Daten der Videokonferenzlösung analysieren zu können, werden für das SIEM spezielle Konnektoren benötigt. Sollte kein passender Konnektor verfügbar sein, muss hierfür eine eigene Lösung entwickelt werden, für die SIEM-Hersteller häufig Anleitungen und Werkzeuge bereitstellen. Im Kontext von Videokonferenzlösungen ist dieser Mehraufwand wahrscheinlich, da die Einbindung von Videokonferenzlösungen in ein SIEM noch kein typischer Anwendungsfall ist. Es sollte kontinuierlich überprüft werden, ob alle Konnektoren korrekt arbeiten. Insbesondere nach Changes und Updates sollte eine Kontrolle durchgeführt werden.

Zur aussagekräftigen Analyse der Daten muss für das SIEM ein Regelwerk entwickelt werden. Dieses muss individuelle Gegebenheiten der Institution und der Videokonferenzlösung berücksichtigen, um Sicherheitsvorfälle und sonstige Probleme erkennen zu können.

Durch die Überwachung der Videokonferenzlösung übertragen sich Aspekte des Datenschutzes auf das SIEM.

M-61 Aufnahme der Videokonferenzlösung in die Notfallvorsorge

Im Rahmen der in A-61 empfohlenen Notfallvorsorge sollte bei der Schaffung von Redundanzen auch die zugrunde liegende IT-Infrastruktur einbezogen werden, die von der Videokonferenzlösung genutzt wird.

Sind Dienstleister für den Betrieb der Videokonferenzlösung verantwortlich, sollten im Rahmenvertrag Service Level Agreements (SLA) getroffen werden. Dabei sollten angestrebte Ausfallraten und Reaktionszeiten vereinbart und kontrolliert werden, zu deren Einhaltung sich der Dienstleister verpflichtet.

Im Rahmen der Notfallvorsorge der Videokonferenzlösung muss die Zielsetzung für den Wiederanlauf festgelegt werden. Die Prozesse können darauf ausgerichtet werden, den Normalbetrieb mit vollem Funktionsumfang so schnell wie möglich wieder herzustellen. Alternativ kann eine temporäre Notbetriebslösung vorgezogen werden. Diese bietet den Vorteil, dass grundlegende Funktionen schnell wieder zur Verfügung stehen, jedoch vergeht unter Umständen insgesamt mehr Zeit, bis der Normalbetrieb wieder stattfinden kann.

Die Notfallmaßnahmen sollten je nach Zweck priorisiert werden. Dabei sollte die Wiederherstellung der wichtigsten Funktionen und Dienste am höchsten priorisiert werden. Beispielsweise sollten Komponenten, deren Ausfall große Beeinträchtigungen bedingen, z. B. finanzielle Schäden durch mangelnde Abstimmungsmöglichkeiten, mit hoher Priorität wieder gestartet werden.

Soll die Videokonferenzlösung zur Kommunikation in Notfällen genutzt werden, sind Notfallmaßnahmen, die die Funktionsfähigkeit der Videokonferenzlösung adressieren, auch in der allgemeinen Notfallvorsorge hoch zu priorisieren. Auch als kritisch eingestufte Video-Endpunkte sollten hier einbezogen werden, z. B. Video-Endpunkte, die im Notfall vom Krisenstab genutzt werden sollen. Beispielsweise können Ersatzgeräte zur Verfügung gestellt werden oder ein mobiler Video-Endpunkt als Ersatz für ein ausgefallenes Raumsystem vorgehalten werden.

M-62 Lesender Zugriff auf von einem Dienstleister betriebene Komponenten

Zur Umsetzung von A-62 sollte mit dem Dienstleister geklärt werden, inwieweit Zugriffe ermöglicht werden können und welche Voraussetzungen hierfür erforderlich sind. Die Komponenten sollten auf einem angemessenen Niveau kontrolliert werden können, während der Dienstleister nicht beim Betrieb beeinträchtigt werden darf.

Durch den lesenden Zugriff kann die Institution die Komponenten der Videokonferenzlösung durch eigene Mittel auf eine ordnungsgemäße Funktion und auf Hinweise auf Sicherheitsvorfälle überprüfen. Dabei sollten die gelesenen Daten an ein IT-Monitoring (siehe M-40), Log-Management (siehe M-41) oder SIEM (siehe M-60) übertragen werden.

8 Beispiele für Sicherheitskonzepte

Ein Sicherheitskonzept wird gemäß BSI-Standard 200-2 (siehe [BSI S2002-2017]) immer für einen festgelegten Informationsverbund erstellt, der alle Applikationen und Komponenten für einen bestimmten Teilbereich der IT-Infrastruktur einer Institution enthält. Dies kann jedoch auch die gesamte IT-Infrastruktur einer Institution umfassen.

Im Folgenden wird zunächst allgemein das Vorgehen für die Erstellung eines Sicherheitskonzepts zur Standard-Absicherung gemäß BSI erläutert. Anschließend werden exemplarisch drei Sicherheitskonzepte für verschiedene Beispielszenarien einer Videokonferenzlösung vorgestellt.

8.1 Methodik zur Erstellung eines Sicherheitskonzepts gemäß BSI

Im BSI-Standard 200-2 ist das in Abbildung 15 dargestellte Vorgehen für die Erstellung eines Sicherheitskonzepts zur Standard-Absicherung festgelegt:

Zuerst wird der Geltungsbereich ermittelt, d. h. der Informationsverbund definiert, für den die Sicherheitskonzeption erstellt und umgesetzt werden soll. Für diesen Geltungsbereich werden in einer Strukturanalyse die Komponenten des Informationsverbunds systematisch erfasst. Hierzu gehören Applikationen, Systeme, Räume und Verbindungen, aber auch die Prozesse und Interaktionen zwischen den Komponenten.

Im Anschluss an die Strukturanalyse erfolgt eine Schutzbedarfsfeststellung, in der für alle in der Strukturanalyse erfassten Komponenten der Bedarf an Vertraulichkeit, Verfügbarkeit und Integrität bestimmt wird. Dies dient dazu zu ermitteln, ob es reicht, die Basisanforderungen umzusetzen oder ob auch Standard-Anforderungen und gegebenenfalls sogar Anforderungen für den erhöhten Schutzbedarf umgesetzt werden müssen.

Nun müssen im Rahmen der Modellierung des Informationsverbunds die umzusetzenden Anforderungen ausgewählt werden. Diese setzen sich im Fall eines Sicherheitskonzepts für eine Videokonferenzlösung aus passenden Bausteinen des IT-Grundschutz-Kompendiums und den im Kompendium Videokonferenzen festgelegten Sicherheitsanforderungen zusammen.

Für diese wird ein erster IT-Grundschutz-Check durchgeführt, in dem in einem Soll-Ist-Vergleich geprüft wird, wie der Umsetzungsstatus dieser Anforderungen aussieht. Für jede Anforderung wird ermittelt, ob sie bereits vollständig umgesetzt ist oder ob hier noch Handlungsbedarf besteht.

Werden Risiken identifiziert, die durch die ausgewählten Anforderungen nicht behoben werden können, oder wird festgestellt, dass eine Anforderung nicht oder nicht vollständig umgesetzt werden kann, muss eine Risikoanalyse durchgeführt werden. In dieser wird für jedes identifizierte Risiko ermittelt, wie hoch es ist und ob es durch weiterführende Sicherheitsmaßnahmen minimiert werden kann oder ob das Risiko getragen werden muss und kann.

Im Anschluss werden die umzusetzenden Sicherheitsmaßnahmen konsolidiert und durch die Risikoanalyse neu hinzugekommene Maßnahmen ergänzt. Außerdem wird das Zusammenwirken aller Maßnahmen überprüft und gegebenenfalls werden Maßnahmen angepasst.

Danach wird ein zweiter IT-Grundschutz-Check durchgeführt, in dem der Umsetzungsstatus für die neuen und geänderten Maßnahmen geprüft wird.

Abschließend werden die Maßnahmen umgesetzt. Der konkrete Handlungsbedarf kann den IT-Grundschutz-Checks entnommen werden. Grundsätzlich müssen die Aufrechterhaltung der Umsetzung der Maßnahmen und eine mögliche Verbesserung kontinuierlich überprüft werden.

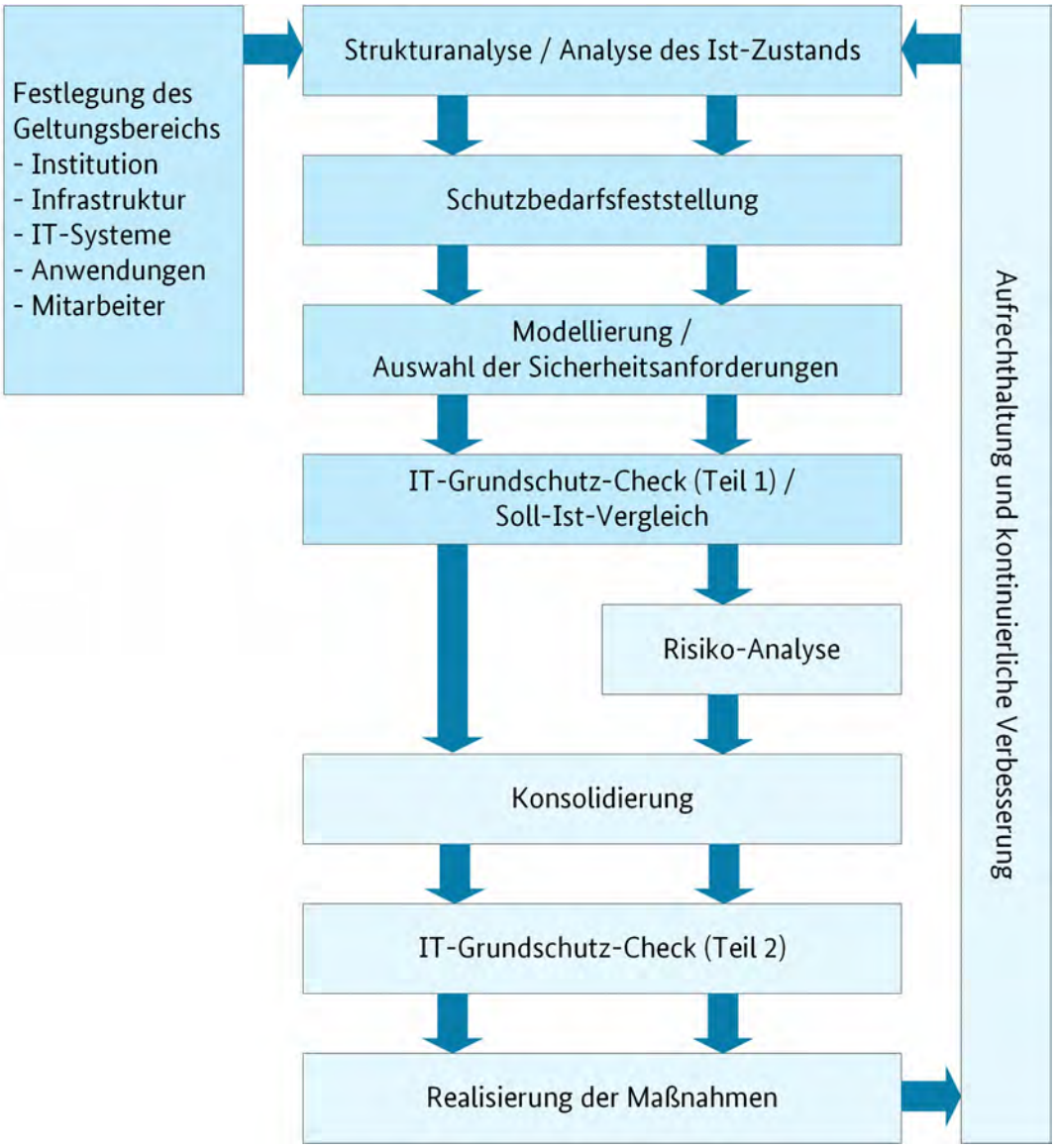

Abbildung 15: Vorgehen beim Erstellen eines Sicherheitskonzepts gemäß BSI (Quelle [BSI S2002-2017])

Im Folgenden wird anhand von drei Beispielszenarien der Aufbau eines Sicherheitskonzepts für eine Videokonferenzlösung dargestellt. Hierbei werden als Szenarien eine reine On-Premises-Lösung, eine reine Cloud-Lösung sowie eine Hybrid-Lösung betrachtet.

Das Verfahren zur Erstellung eines Sicherheitskonzepts wird anhand der Szenarien bis zum ersten IT-Grundschutz-Check durchgeführt. Risiko-Analyse, Konsolidierung und zweiter IT-Grundschutz-Check können für ein Beispielszenario ohne konkrete Details nicht sinnvoll durchgeführt werden.

8.2 Beispiel einer On-Premises-Lösung: Forschungszentrum

Ein mögliches Szenario für eine Videokonferenzlösung bildet eine On-Premises-Lösung. Hier werden die zentralen Komponenten der Videokonferenzlösung vollständig im Rechenzentrum der Institution realisiert. Es wird nicht auf Cloud-Dienste zurückgegriffen. Als Beispiel wird ein Forschungszentrum mit mehreren Instituten betrachtet.

Videokonferenzen werden für die Durchführung von Befragungen im Rahmen von Studien genutzt. Hierbei befindet sich der Interviewer in einem der Institute und weitere Teilnehmer am gleichen Standort oder in anderen Instituten. Insbesondere muss sich der Befragte nicht am gleichen Institut wie der Interviewer befinden. Außerdem werden Videokonferenzen für die Bürokommunikation eingesetzt.

Der Funktionsumfang umfasst neben der Audio- und Video-Übertragung auch die Übertragung von weiteren Inhalten während einer Videokonferenz, z. B. die Übertragung der Ergebnisse der Studien, sowie einen temporären Gruppen-Chat während einer Videokonferenz. Eine Aufzeichnung von Videokonferenz-inhalten ist nicht erforderlich und nicht gewünscht.

Als interne Video-Endpunkte werden sowohl Video-Endpunkte auf Desktop-PCs oder mobilen Endgeräten als auch klassische Raumsysteme eingebunden. Externe Video-Endpunkte sind ein Raumsystem in einem Labor und Software-basierte Video-Endpunkte (Software-Client) und einfache Browser für mobiles Personal.

8.2.1 Geltungsbereich und Strukturanalyse

Das in Abbildung 16 dargestellte Szenario einer On-Premises-Lösung umfasst das Rechenzentrum und die Institute des Forschungszentrums, die über ein dediziertes Glasfasernetz untereinander verbunden sind. Die zentralen Komponenten der Videokonferenzlösung befinden sich im Rechenzentrum des Forschungszentrums. In manchen größeren Instituten ist ebenfalls eine MCU vorhanden. Interne Video-Endpunkte sind sowohl klassische Raumsysteme als auch Software-Clients. Als externe Video-Endpunkte werden Software-Clients oder einfache Browser genutzt. Darüber hinaus wird ein Raumsystem in einem Labor eingebunden. In beiden Fällen erfolgt die Verbindung über das Internet an das Rechenzentrum des Forschungszentrums.

Die genannten Bereiche bilden für das Sicherheitskonzept den Geltungsbereich, d. h. den sogenannten Informationsverbund. Es wird also das gesamte Forschungszentrum mit allen Instituten betrachtet, aber darin nur die zur Videokonferenzlösung gehörenden Systeme.

Im Rahmen der Strukturanalyse sind demnach die folgenden IT-Systeme relevant:

- Zentrale Komponenten der Videokonferenzlösung im Rechenzentrum des Forschungszentrums: MCU, Registrierungseinheit, Routing-Einheit, Management-Einheit, Chat-Server und DB-Server
- DMZ-Systeme im Rechenzentrum des Forschungszentrums: SBC und VPN-Gateway
- MCUs in den Instituten
- Video-Endpunkte in den Instituten: Software-Clients und Raumsysteme
- Video-Endpunkt des externen Labors: Raumsystem
- Video-Endpunkte des mobilen Personals: Software-Clients und einfache Browser

In der Strukturanalyse zu berücksichtigende Räume sind zumindest das Rechenzentrum des Forschungszentrums inklusive der Räume, in denen sich die MCUs der Institute befinden, sowie die Büros und Besprechungsräume, in denen sich die Video-Endpunkte in den Instituten befinden.

Weiterhin ist das externe Labor als potenziell unsicherer Raum zu betrachten. Gegebenenfalls gelten hier vertragliche Vorgaben für die Absicherung der Videokonferenzen, die zu berücksichtigen sind.

Auch die Räume, in denen sich das mobile Personal bei einer Videokonferenz befindet, müssen als unsicher angesehen werden. Hier sind entsprechende organisatorische Vorgaben zu gestalten.

Weiterhin müssen als Verbindungen die internen IP-Netze des Rechenzentrums und der Institute sowie das dedizierte Glasfasernetz und die Internetverbindung betrachtet werden.

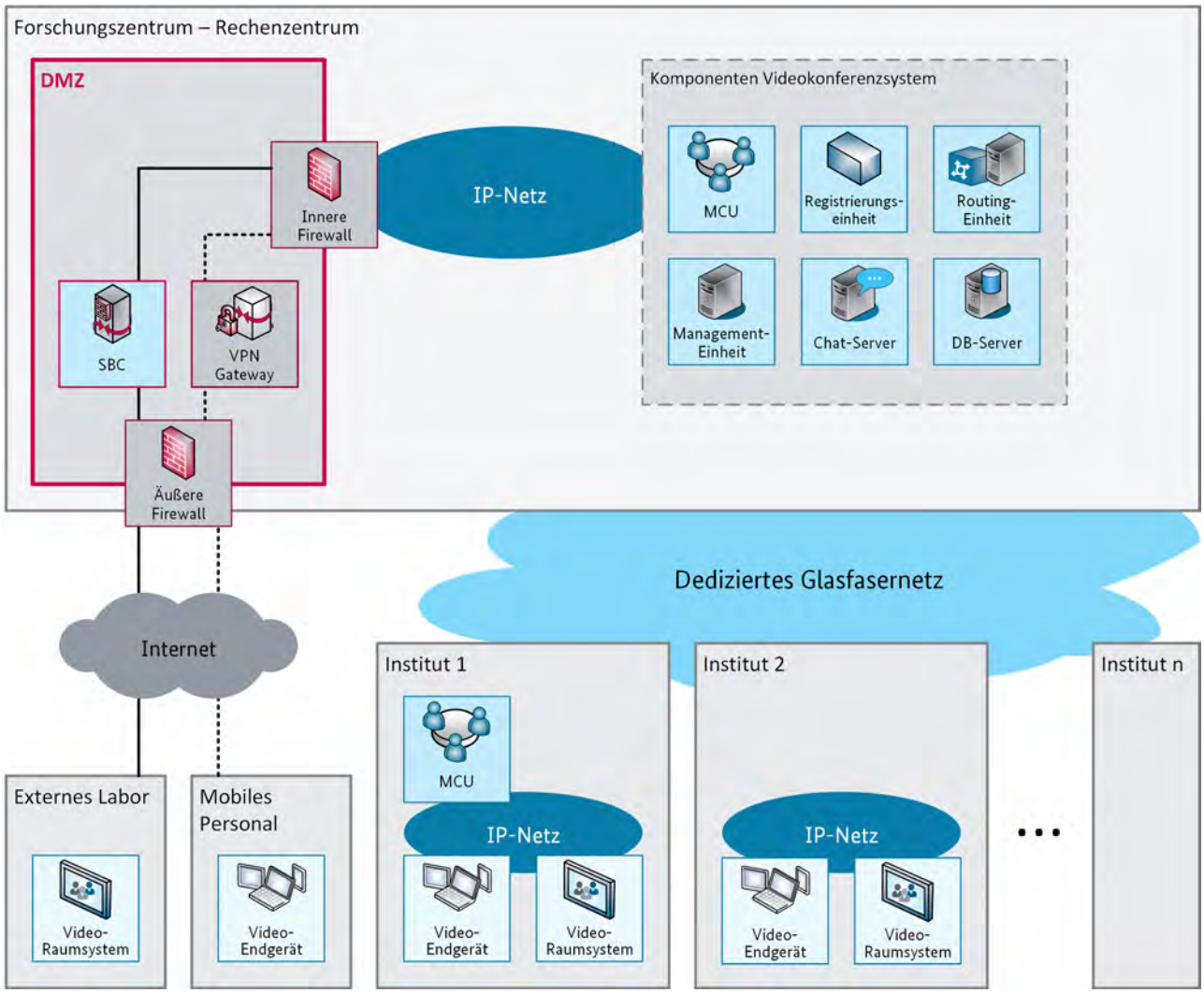

Abbildung 16: On-Premises-Lösung

8.2.2 Schutzbedarfsfeststellung

Bei einer Videokonferenzlösung hängt der Schutzbedarf der Komponenten hauptsächlich vom Inhalt der Videokonferenzen und von den während einer Konferenz übermittelten Daten und Chats ab. Im betrachteten Fall eines Forschungslabors werden Befragungen in klinischen Studien durchgeführt. Es ist davon auszugehen, dass der Inhalt dieser Befragungen einen hohen bis sehr hohen Schutzbedarf hat. Weiterhin können in der normalen Bürokommunikation kritische Forschungsdaten Thema einer Videokonferenz sein oder während einer solchen übermittelt werden. Auch hier sollte von einem hohen bis sehr hohen Schutzbedarf ausgegangen werden.

Dieser hohe bis sehr hohe Schutzbedarf gilt dann für die in der Strukturanalyse erfassten Systeme und vererbt sich von diesen auf die Räume, in denen sie sich befinden und auch auf die Verbindungen, über die sie verbunden sind.

8.2.3 Modellierung

Für die Modellierung des in der Strukturanalyse festgelegten Informationsverbunds muss zunächst die Relevanz der Bausteine des IT-Grundschutz-Kompendiums zur Absicherung der zugrundeliegenden Techniken geprüft werden. Wesentliche Bausteine im Hinblick auf Videokonferenzen nennt Kapitel 6.1. Da in dem hier betrachteten Szenario keine Cloud-Dienste in Anspruch genommen werden, ist beispielsweise der Baustein *OPS.2.2 Cloud-Nutzung* nicht relevant. Ebenso kann auf den Baustein *SYS.4.4 Allgemeines IoT-Gerät* verzichtet werden, weil keine IoT-Geräte eingesetzt werden.

Weiterhin müssen die für Videokonferenzlösungen spezifischen Sicherheitsanforderungen aus Kapitel 6.2 bis Kapitel 6.4 betrachtet werden. Diese sind in Kapitel 8.5 in einer Tabelle zusammengefasst. Hier ist die Relevanz jeder dieser Anforderungen für alle drei betrachteten Beispielszenarien angegeben.

8.2.4 IT-Grundschutz-Check

Im IT-Grundschutz-Check wird für jede Anforderung geprüft, ob sie bereits ausreichend erfüllt ist oder ob noch Handlungsbedarf besteht.

Für das vorliegende Szenario wird angenommen, dass alle relevanten Anforderungen inklusive der Anforderungen in den relevanten Bausteinen des IT-Grundschutz-Kompendiums (siehe [BSI GSK-2019]) ausreichend erfüllt sind. Die Vorgehensweise der Prüfung wird für eine Anforderung exemplarisch dargestellt.

Als Beispiel wird die Anforderung A-42 „Durchgängige Verschlüsselung der mit IP übertragenen Daten einer Videokonferenz“ betrachtet, die bei hohem Schutzbedarf umgesetzt werden sollte und somit für dieses Szenario relevant ist. Nutzt die Videokonferenzlösung zur Übertragung aller Daten TLS bzw. SRTP, so ist diese Anforderung z. B. schon umgesetzt und es ist kein weiterer Handlungsbedarf erforderlich.

8.3 Beispiel einer reinen Cloud-Lösung: Start-up-Unternehmen

In einem weiteren Szenario wird eine reine Cloud-Lösung vorgestellt, in der die zentralen Komponenten der Videokonferenzlösung vollständig in einer Cloud realisiert werden. Als Beispiel wird ein Start-up-Unternehmen mit einer kleinen Außenstelle betrachtet, deren Projektmitarbeiter weltweit unterwegs sind.

Videokonferenzen werden für die Projektarbeit, insbesondere auch unter Einbindung externer Teilnehmer genutzt. Weltweit verteilte Mitarbeiter tauschen sich über Videokonferenzen aus und arbeiten gemeinsam an Dokumenten. Außerdem dienen Videokonferenzen zur Projektabstimmung.

Der Funktionsumfang umfasst neben der Audio- und Video-Übertragung meist auch Screen Sharing und Application bzw. Content Sharing. Hauptsächlich werden Desktop-Konferenzen genutzt.

Als interne Video-Endpunkte werden sowohl Software-basierte Video-Endpunkte als auch moderne Raumsysteme, sogenannte Touch-Videomonitore, eingebunden. Externe Video-Endpunkte sind Software-basierte Video-Endpunkte und einfache Browser von mobilen Projektmitarbeitern.

8.3.1 Geltungsbereich und Strukturanalyse

Das in Abbildung 17 dargestellte Szenario einer reinen Cloud-Lösung umfasst den Hauptstandort des Start-up-Unternehmens mit DMZ-Systemen und Video-Endpunkten, eine kleine Außenstelle mit Video-Endpunkten, Video-Endpunkte von mobilen Projektmitarbeitern und eine Videokonferenz-Cloud.

Die zentralen Komponenten der Videokonferenzlösung werden in der Videokonferenz-Cloud zur Verfügung gestellt. Am Hauptstandort des Start-up-Unternehmens befinden sich lediglich ein Cloud Connector und ein SBC in einer DMZ. Die Video-Endpunkte am Hauptstandort und der Außenstelle des Start-up-Unternehmens verbinden sich über das Internet mit den zentralen Komponenten in der Cloud. Das Gleiche gilt für die Video-Endpunkte der mobilen Projektmitarbeiter.

Die kleine Außenstelle ist hier ohne eigenes IP-Netz dargestellt. Die wenigen hier arbeitenden Projektmitarbeiter werden wie die mobilen Projektmitarbeiter mit Internetzugang über ein WLAN o. ä. betrachtet. Ebenfalls möglich wäre hier ein eigenes kleines IP-Netz, das durch eine Firewall z. B. auf einem Internet-Router, abgesichert wird.

Die genannten Bereiche bilden für das Sicherheitskonzept den Geltungsbereich, d. h. den sogenannten Informationsverbund. Es werden also die Videokonferenz-Cloud sowie alle zur Videokonferenzlösung gehörenden Systeme des gesamten Start-up-Unternehmens mit Außenstelle und mobilen Projektmitarbeitern betrachtet.

Im Rahmen der Strukturanalyse sind die folgenden IT-Systeme relevant:

- Zentrale Komponenten der Videokonferenzlösung in der Cloud nur in Bezug auf die Cloud-Nutzung: MCU, Management-Einheit, Registrierungseinheit, Routing-Einheit, Chat-Server, Präsenz-Server, Datei-Server, DB-Server, SBC und Cloud Connector
- DMZ-Systeme im Hauptstandort: Cloud Connector und SBC
- Video-Endpunkte im Hauptstandort: Software-basierte Video-Endpunkte (Software-Clients) und Touch-Videomonitore
- Video-Endpunkte in der Außenstelle: Software-Clients und Touch-Videomonitore
- Video-Endpunkte der mobilen Projektmitarbeiter: Software-Clients und einfache Browser

In der Strukturanalyse zu berücksichtigende Räume sind zumindest der Raum am Hauptstandort, in dem sich die DMZ-Systeme befinden, sowie die Büros und Konferenzräume, in denen sich die Video-Endpunkte des Hauptstandorts und der Außenstelle befinden.

Die Räume, in denen sich die mobilen Projektmitarbeiter bei einer Videokonferenz befinden, müssen als unsicher angesehen werden. Hier müssen entsprechende organisatorische Vorgaben greifen.

Die Räume des Cloud-Providers, in denen sich die Systeme der Videokonferenz-Cloud befinden, müssen nicht betrachtet werden, da sie über die vertraglichen und organisatorischen Vorgaben an den Cloud-Provider abgedeckt sind.

Weiterhin müssen als Verbindungen die internen IP-Netze des Hauptstandorts sowie die Internetverbindung betrachtet werden.

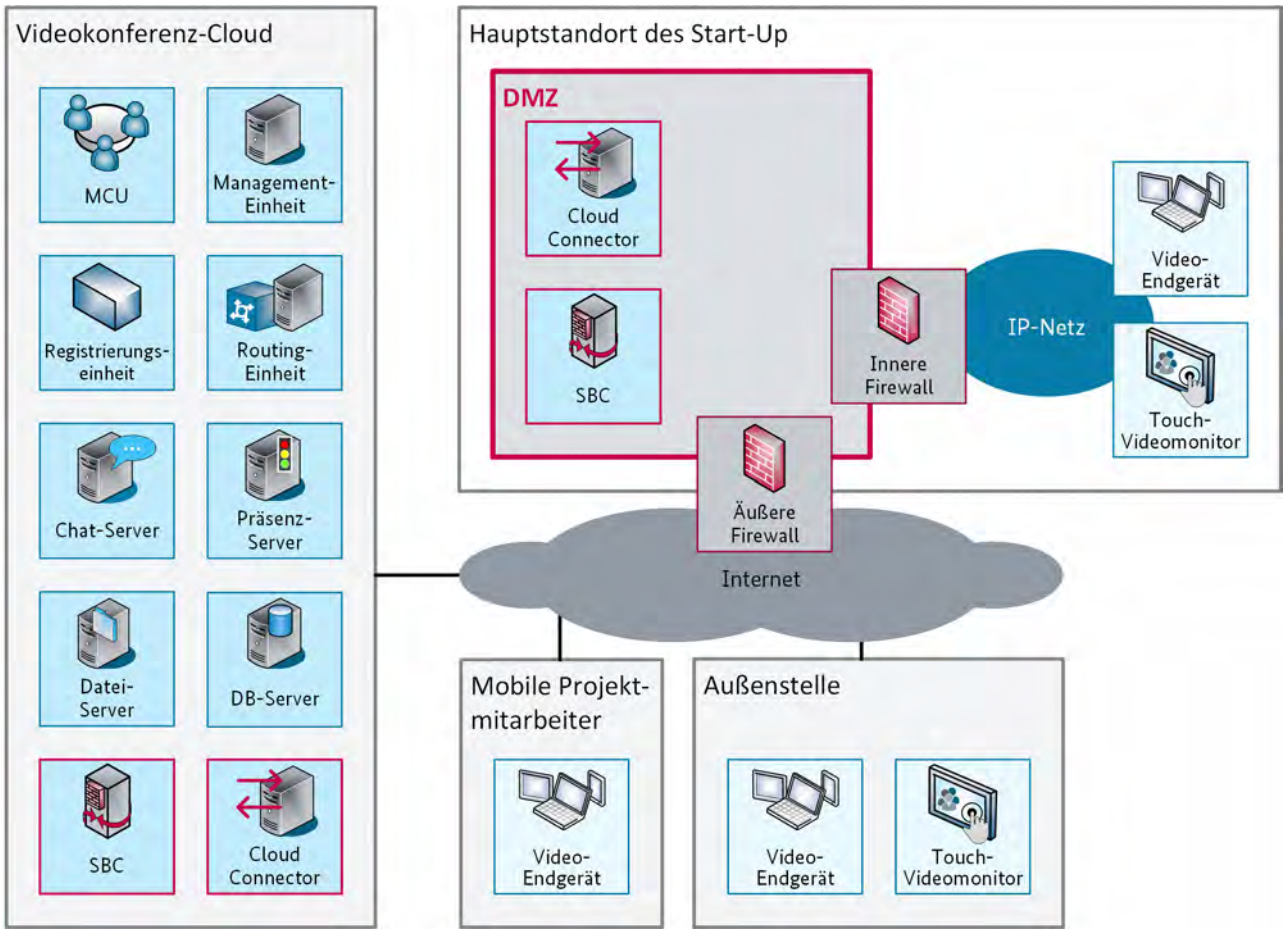

Abbildung 17: Cloud-Lösung

8.3.2 Schutzbedarfsfeststellung

Bei einer Videokonferenzlösung hängt der Schutzbedarf der Komponenten hauptsächlich vom Inhalt der Videokonferenzen und von den während einer Konferenz übermittelten Daten ab. Im betrachteten Fall eines Start-up-Unternehmens wird davon ausgegangen, dass die über Videokonferenzen erfolgende Projektarbeit und Projektabstimmung sowie das Content Sharing keine kritischen Daten beinhalten. Es wird von einem normalen Schutzbedarf ausgegangen.

Dieser normale Schutzbedarf gilt dann für die in der Strukturanalyse erfassten Systeme und vererbt sich von diesen auf die Räume, in denen sie sich befinden und auch auf die Verbindungen, über die sie verbunden sind.

8.3.3 Modellierung

Für die Modellierung des in der Strukturanalyse festgelegten Informationsverbunds muss zunächst die Relevanz der Bausteine des IT-Grundschutz-Kompendiums zur Absicherung der zugrundeliegenden Techniken geprüft werden. Wesentliche Bausteine im Hinblick auf Videokonferenzen nennt Kapitel 6.1. Da in dem hier betrachteten Szenario die zentralen Systeme des Videokonferenzsystems nur in der Cloud realisiert sind, müssen für sie z. B. die Serverbausteine nicht betrachtet werden. Dies wird hier über den Baustein *OPS.2.2 Cloud-Nutzung* abgedeckt. Auf den Baustein *SYS.4.4 Allgemeines IoT-Gerät* kann verzichtet werden, weil keine IoT-Geräte eingesetzt werden.

Weiterhin müssen die für Videokonferenzlösungen spezifischen Sicherheitsanforderungen aus Kapitel 6.2, 6.3 und 6.4 betrachtet werden. Diese sind in Kapitel 8.5 in einer Tabelle zusammengefasst. Hier ist die Relevanz jeder dieser Anforderungen für alle drei betrachteten Beispielszenarien angegeben.

8.3.4 IT-Grundschutz-Check

Im IT-Grundschutz-Check wird für jede Anforderung geprüft, ob sie bereits ausreichend erfüllt ist oder ob noch Handlungsbedarf besteht.

Für das vorliegende Szenario wird angenommen, dass alle relevanten Anforderungen inklusive der Anforderungen in den relevanten Bausteinen des IT-Grundschutz-Kompendiums (siehe [BSI GSK-2019]) ausreichend erfüllt sind. Die Vorgehensweise der Prüfung wird für eine Anforderung exemplarisch dargestellt.

Als Beispiel wird die Anforderung A-10 „Positionierung von Cloud Connector und Video Edge Server in einer DMZ“ betrachtet, die für dieses Szenario relevant ist. Nur am Hauptstandort des Start-up-Unternehmens ist ein Cloud Connector realisiert und dieser befindet sich in einer DMZ. Video Edge Server werden nicht eingesetzt. Damit ist die Anforderung umgesetzt und es besteht hier kein weiterer Handlungsbedarf.

8.4 Beispiel einer Hybrid-Lösung: Groß-Unternehmen

Im letzten Szenario wird eine Hybrid-Lösung betrachtet. Hier wird das Videokonferenzsystem ohne UCC-Funktionen in der Cloud realisiert. Ein UC-System befindet sich im Rechenzentrum der betrachteten Institution. Weitere Cloud-Dienste werden eingebunden. Als Beispiel wird ein Automobilzulieferer betrachtet, der viele verteilte Standorte hat, die über WAN angebunden werden.

Videokonferenzen werden für die Bürokommunikation, für Meetings und für Vorstands-Präsentationen genutzt. Insbesondere werden sie auch in Entwicklungsabteilungen eingesetzt. An den Videokonferenzen können neben den Mitarbeitern an den Standorten auch mobile interne Mitarbeiter und externe Mitarbeiter teilnehmen. Letztere können auch reine Audio-Teilnehmer über Standardtelefone sein.

Der Funktionsumfang umfasst neben der Audio- und Video-Übertragung auch die Einbindung weiterer Medien bzw. Techniken in die Konferenz, wie z. B. IoT-Geräte und KI-Funktionen. Konferenzen werden auch aufgezeichnet und gegebenenfalls weiterverarbeitet.

Als interne Video-Endpunkte werden vielfach Raumsysteme und moderne Touch-Videomonitore genutzt. Teilweise sind hier auch Geräte der technischen Gebäudeausstattung, z. B. zum Verdunkeln des Raumes, angebunden. Vereinzelt werden an den Standorten auch Software-basierte Video-Endpunkte eingesetzt. Die internen mobilen Mitarbeiter nutzen ebenfalls Software-basierte Video-Endpunkte.

Externe Video-Endpunkte können Software-basierte Video-Endpunkte, einfache Browser, Smartphones oder Tablets und Standardtelefone für die reine Audio-Teilnahme an Videokonferenzen sein.

8.4.1 Geltungsbereich und Strukturanalyse

Das in Abbildung 18 dargestellte Szenario einer Hybrid-Lösung umfasst das Rechenzentrum des Automobilzulieferers mit den zentralen Komponenten der UC-Lösung und den DMZ-Systemen sowie die über WAN angebundenen Standorte des Automobilzulieferers mit Video-Endpunkten, eventuell angebundenen IoT-Geräten und gegebenenfalls einem Video Edge Server. Dazu kommen die über das Internet angebundenen Video-Endpunkte der mobilen Mitarbeiter sowie der externen Videokonferenz-teilnehmer und externe Telefonteilnehmer, die über das öffentliche Telekommunikationsnetz angebunden sind. Ergänzt wird das Szenario durch eine Videokonferenz-Cloud mit den zentralen Systemen der Videokonferenzlösung bis auf die UC-Lösung und durch weitere Cloud-Dienste, die ebenfalls von einem Cloud-Provider bereitgestellt werden.

Die genannten Bereiche bilden für das Sicherheitskonzept den Geltungsbereich, d. h. den sogenannten Informationsverbund. Es werden also die Videokonferenz-Cloud, die weiteren Cloud-Dienste sowie alle zur Videokonferenzlösung gehörenden Systeme des gesamten Automobilzulieferers mit allen Standorten, mobilen Mitarbeitern und externen Teilnehmern betrachtet.

Im Rahmen der Strukturanalyse sind dabei die folgenden IT-Systeme relevant:

- Zentrale Komponenten der Videokonferenzlösung in der Cloud: MCU, Management-Einheit, Registrierungseinheit, Routing-Einheit, DB-Server, Cloud-Speicher, Cloud Connector und SBC
- Systeme der weiteren Cloud-Dienste in der Cloud: IoT-Server, Cloud-Speicher, KI-Server, KI-Datenbank Applikations-Server und Cloud Connector
- Zentrale Komponenten der UC-Lösung im Rechenzentrum: UC-System, Chat-Server, Präsenz-Server und Management-Einheit
- DMZ-Systeme im Rechenzentrum: SBC und Cloud Connector
- Video Edge Server an einigen Standorten

- Video-Endpunkte an den Standorten: Video-Endgeräte, Video-Raumsysteme und Touch-Videomonitore
- IoT-Geräte und Systeme des Gebäudemanagements an den Standorten
- Video-Endpunkte der mobilen internen Teilnehmer
- Video-Endpunkte der externen Teilnehmer: Video-Endgeräte, Smartphones und Telefone

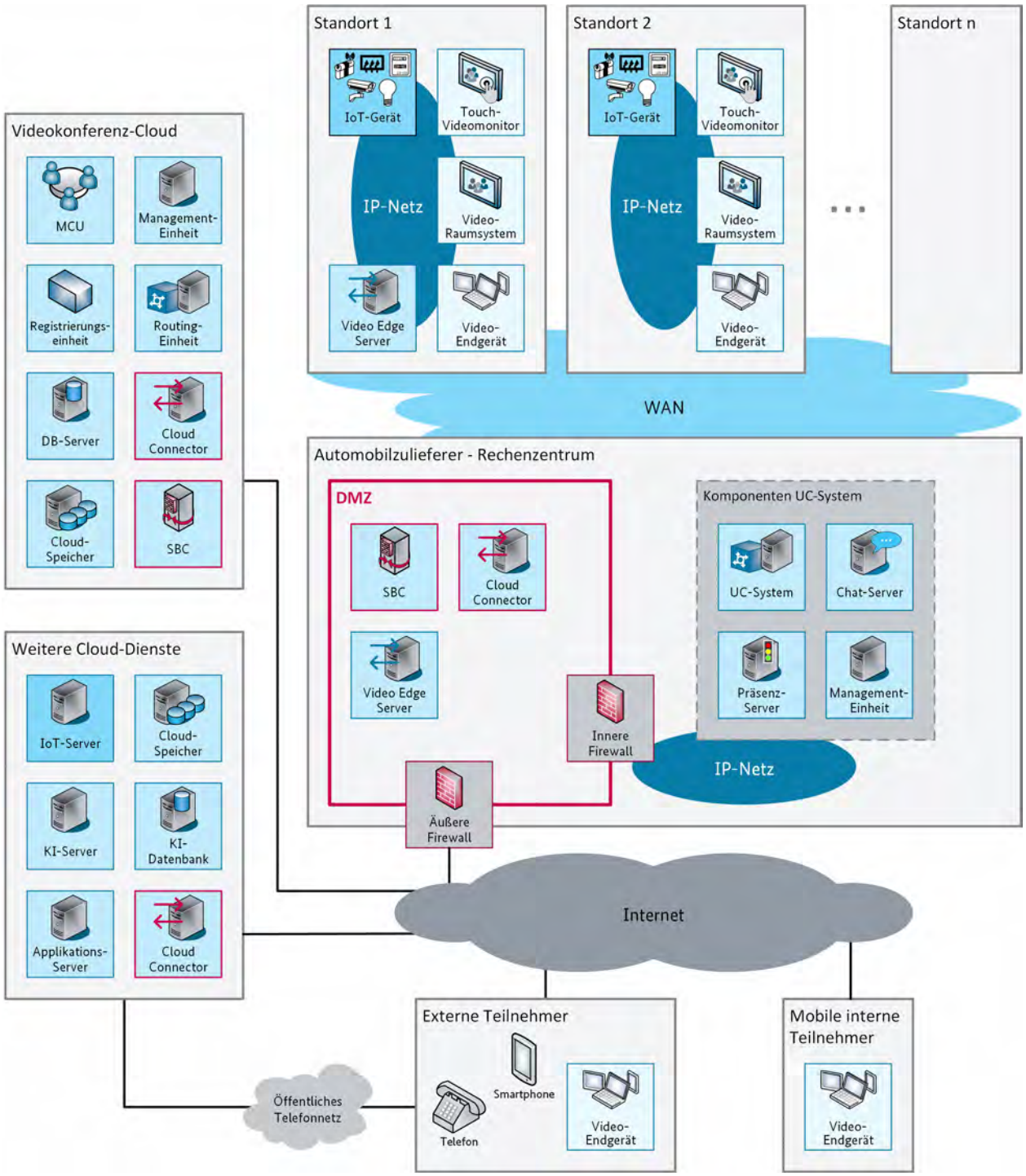

Abbildung 18: Hybrid-Lösung

In der Strukturanalyse zu berücksichtigende Räume sind zumindest das Rechenzentrum, in dem sich die zentralen Komponenten der UC-Lösung und die DMZ-Systeme befinden, die Räume der Standorte, in denen sich die Video Edge Server befinden, sowie die Büros und Konferenzräume, in denen sich die Video-Endpunkte und IoT-Geräte der Standorte befinden.

Die Räume, in denen sich die mobilen internen Teilnehmer bei einer Videokonferenz befinden, müssen als unsicher angesehen werden. Hier müssen entsprechende organisatorische Vorgaben greifen.

Auch die Räume, in denen sich die externen Teilnehmer bei einer Videokonferenz befinden, sind als potenziell unsichere Räume zu betrachten. Bei Bedarf sind hier vertragliche Vorgaben für die Absicherung der Videokonferenzen erforderlich, z. B. keine Videokonferenzen in Großraumbüros.

Die Räume des Cloud-Providers, in denen sich die Systeme der Videokonferenz-Cloud befinden, müssen nicht betrachtet werden, da sie über die vertraglichen und organisatorischen Vorgaben an den Cloud-Provider abgedeckt sind.

Weiterhin müssen als Verbindungen die internen IP-Netze des Rechenzentrums und der Standorte sowie das WAN, die Internetverbindung und das öffentliche Telekommunikationsnetz betrachtet werden.

8.4.2 Schutzbedarfsfeststellung

Bei einer Videokonferenzlösung hängt der Schutzbedarf der Komponenten hauptsächlich vom Inhalt der Videokonferenzen und von den während einer Konferenz übermittelten Daten ab. Im betrachteten Fall eines Automobilzulieferers wird davon ausgegangen, dass teilweise kritische Informationen in den Videokonferenzen genannt werden, wie z. B. projektspezifische Informationen aus der Produktentwicklung oder gegebenenfalls auch Vorstands-Präsentationen. Für diese gilt ein hoher Schutzbedarf. Es gibt aber auch Videokonferenzen mit normalem Schutzbedarf, z. B. die einfache Bürokommunikation. Es muss also ein normaler bis hoher Schutzbedarf abgedeckt werden.

Dieser normale bis hohe Schutzbedarf gilt dann für die in der Strukturanalyse erfassten Systeme und vererbt sich von diesen auf die Räume, in denen sie sich befinden und auch auf die Verbindungen, über die sie verbunden sind.

8.4.3 Modellierung

Für die Modellierung des in der Strukturanalyse festgelegten Informationsverbunds muss zunächst die Relevanz der Bausteine des IT-Grundschutz-Kompendiums zur Absicherung der zugrundeliegenden Techniken geprüft werden. Wesentliche Bausteine im Hinblick auf Videokonferenzen nennt Kapitel 6.1. Dies sind in dem hier betrachteten Szenario einer Hybrid-Lösung voraussichtlich fast alle genannten Bausteine. Gegebenenfalls kann auf einige Server- und Client-Bausteine verzichtet werden, wenn das entsprechende Betriebssystem nicht eingesetzt wird. Für den Fall, dass keine Virtualisierung erfolgt, kann auch auf den Baustein *SYS.1.5 Virtualisierung* verzichtet werden.

Darüber hinaus können weitere Anforderungen für die zugrundeliegenden UC-Systeme zu beachten sein. Eine ausführliche Darstellung der UC-bezogenen Anforderungen gibt [BSI TLSTK-2014].

Weiterhin müssen die für Videokonferenzlösungen spezifischen Sicherheitsanforderungen aus Kapitel 6.2, 6.3 und 6.4 betrachtet werden. Diese sind in Kapitel 8.5 in einer Tabelle zusammengefasst. Hier ist die Relevanz jeder dieser Anforderungen für alle drei betrachteten Beispielszenarien angegeben.

8.4.4 IT-Grundschutz-Check

Im IT-Grundschutz-Check wird für jede Anforderung geprüft, ob sie bereits ausreichend erfüllt ist oder ob noch Handlungsbedarf besteht.

Für das vorliegende Szenario wird angenommen, dass alle relevanten Anforderungen inklusive der Anforderungen in den relevanten Bausteinen des IT-Grundschutz-Kompendiums (siehe [BSI GSK-2019]) und der UC-bezogenen Anforderungen (siehe [BSI TLSTK-2014]) ausreichend erfüllt sind. Die Vorgehensweise der Prüfung wird für eine Anforderung exemplarisch dargestellt.

Als Beispiel wird die Anforderung A-2 „Unterschiedliche Profile für Videokonferenzen" betrachtet, die für dieses Szenario relevant ist, da unterschiedlicher Schutzbedarf für die Videokonferenzen besteht. Gibt es bereits unterschiedliche Profile für normalen und für hohen Schutzbedarf und gegebenenfalls auch unterschiedliche Profile für verschiedene Teilnehmergruppen, so ist die Anforderung umgesetzt. Ansonsten besteht hier Handlungsbedarf.

8.5 Zuordnung der Sicherheitsanforderungen für die Beispielszenarien

Die folgende Tabelle ordnet den zuvor dargestellten drei Beispielszenarien Sicherheitsanforderungen zu, die in Kapitel 6.2 bis Kapitel 6.4 spezifiziert wurden und für das jeweilige Szenario relevant sind.

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

In diesem Zusammenhang ist auch das Ergebnis der Schutzbedarfsfeststellung wesentlich, um festzulegen, ob auch Anforderungen für den erhöhten Schutzbedarf relevant sind.

	Legende: + = relevant; - = nicht relevant; n/a = nicht genutzte Funktion	**Forsch.-zentrum** (On-Prem)	**Start-up-Untern.** (Cloud)	**Groß-Untern.** (Hybrid)
Basis-Anforderungen				
Anwendungen und zentrale Komponenten				
A-1	Sicherer Umgang mit Videokonferenzdaten	**+**	**+**	**+**
A-2	Unterschiedliche Profile für Videokonferenzen	**+**	**+**	**+**
A-3	Sicherer Umgang mit Metadaten	**+**	**+**	**+**
A-4	Sicherer Umgang mit Konferenzaufzeichnungen	**n/a**	**n/a**	**+**
A-5	Absicherung von Dateiablagen	**n/a**	**+**	**+**
Endgeräte und Clients				
A-6	Absicherung von frei zugänglichen Video-Endpunkten	**n/a**	**+**	**+**
A-7	Beenden von Sitzungen und Anmeldungen an Video-Endpunkten	**+**	**+**	**+**
A-8	Absicherung der internen Dateiablage des Video-Endpunkts	**+**	**n/a**	**+**
Netzwerk				
A-9	Dediziertes Sicherheitssegment für frei zugängliche Video-Endpunkte	**+**	**+**	**+**

	Legende: + = relevant; - = nicht relevant; n/a = nicht genutzte Funktion	**Forsch.-zentrum** (On-Prem)	**Start-up-Untern.** (Cloud)	**Groß-Untern.** (Hybrid)
A-10	Positionierung von Cloud Connector und Video Edge Server in einer DMZ	**n/a**	**+**	**+**
Planung und Betrieb				
A-11	Planung und Beschaffung der Videokonferenzlösung	**+**	**+**	**+**
A-12	Erstellung eines Rollen- und Berechtigungskonzepts	**+**	**+**	**+**
A-13	Bereitstellung von Informationen zur sicheren Nutzung von Videokonferenzen	**+**	**+**	**+**
A-14	Integration in das Schwachstellen- und Patch-Management	**+**	**+**	**+**
Standard-Anforderungen				
Anwendungen und zentrale Komponenten				
A-15	Verschlüsselung der mit IP übertragenen Daten der Video-Konferenz auf nicht vertrauenswürdigen Übertragungsstrecken	**+**	**+**	**+**
A-16	Deaktivierung nicht benötigter Dienste und Leistungsmerkmale	**+**	**+**	**+**
A-17	Sichere Nutzerverwaltung	**+**	**+**	**+**
A-18	Sichere Konfiguration von geplanten Videokonferenzen	**+**	**+**	**+**
A-19	Sichere Anbindung der Videokonferenzlösung an Systeme des Gebäudemanagements	**n/a**	**n/a**	**+**
A-20	Absicherung von Konferenzräumen	**+**	**+**	**+**
A-21	Absicherung und Einschränkung von Auswertungen von Videokonferenzinhalten	**n/a**	**n/a**	**+**
A-22	Festlegung des Speicherortes der Daten bei Outsourcing und Cloud-Nutzung	**n/a**	**+**	**+**
A-23	Cloud-Verfügbarkeit	**n/a**	**+**	**+**
Endgeräte und Clients				
A-24	Deaktivierung oder zumindest Absicherung eines Web-Servers auf einem Video-Endpunkt	**+**	**+**	**+**
A-25	Deaktivierung oder zumindest Einschränkung der Sprachsteuerung einer Videokonferenz	**n/a**	**+**	**+**
A-26	Einschränkung des lokalen Zugriffs auf die Konfiguration des Video-Endpunkts	**+**	**+**	**+**
A-27	Deaktivierung der automatischen Annahme eines Video-Anrufs	**+**	**-**	**+**
A-28	Signalisierung der Kameraaktivität	**+**	**+**	**+**
A-29	Geeignete Standortwahl	**+**	**+**	**+**
A-30	Ausblenden des Hintergrunds bei Videokonferenzen	**+**	**-**	**+**

	Legende: + = relevant; - = nicht relevant; n/a = nicht genutzte Funktion	**Forsch.-zentrum** (On-Prem)	**Start-up-Untern.** (Cloud)	**Groß-Untern.** (Hybrid)
A-31	Absicherung der direkten Kommunikation zwischen Standard-Client und Raumsystem	**n/a**	**+**	**+**
Netzwerk				
A-32	Dediziertes Sicherheitssegment für zentrale Komponenten des Videokonferenzsystems	**+**	**n/a**	**+**
A-33	Absicherung des lokalen Netzzugangs	**+**	**+**	**+**
A-34	Einsatz eines SBC am Internet-Übergang	**+**	**+**	**+**
Planung und Betrieb				
A-35	Erstellung von Fein- und Betriebskonzept für die Videokonferenzlösung	**+**	**+**	**+**
A-36	Einbindung der Videokonferenzlösung in Datensicherungs- und Archivierungskonzept	**+**	**n/a**	**+**
A-37	Penetrationstest der Videokonferenzlösung	**+**	**n/a**	**+**
A-38	Schulungen zur sicheren Nutzung von Videokonferenzen	**+**	**+**	**+**
A-39	Aufnahme der Videokonferenzlösung in die Prozesse zur Behandlung von Schwachstellen und Sicherheitsvorfällen	**+**	**+**	**+**
A-40	Überwachung durch IT-Monitoring	**+**	**n/a**	**+**
A-41	Integration in zentrales Log-Management	**+**	**n/a**	**+**
Anforderungen bei erhöhtem Schutzbedarf				
Anwendungen und zentrale Komponenten				
A-42	Durchgängige Verschlüsselung der mit IP übertragenen Daten einer Videokonferenz	**+**	**-**	**+**
A-43	Ende-zu-Ende-Verschlüsselung der mit IP übertragenen Daten einer Videokonferenz	**+**	**-**	**+**
A-44	Authentisierung zwischen Video-Endpunkten und zentralen Komponenten	**+**	**-**	**+**
A-45	Zusätzliche Absicherung der Konfiguration von geplanten Videokonferenzen	**+**	**-**	**+**
A-46	Protokollierung der Tätigkeit von Systembedienern	**+**	**-**	**+**
A-47	Zusätzliche Datensicherung	**+**	**-**	**+**
A-48	Zertifizierung nach Common Criteria für zentrale Komponenten des Videokonferenzsystems	**+**	**-**	**+**
A-49	Vermeidung von Verschlüsselungsendpunkten in einer Cloud	**n/a**	**-**	**+**
A-50	Keine Aufzeichnung von Videokonferenzinhalten	**+**	**-**	**-**

	Legende: + = relevant; - = nicht relevant; n/a = nicht genutzte Funktion	**Forsch.-zentrum** (On-Prem)	**Start-up-Untern.** (Cloud)	**Groß-Untern.** (Hybrid)
A-51	Einsatz von Host-basierten DLP-Systemen	**+**	**-**	**+**
A-52	Einschränkung von KI-Funktionen	**n/a**	**n/a**	**+**
Endgeräte und Clients				
A-53	Ausschließliche Nutzung von verschlüsselter Kommunikation	**+**	**-**	**+**
A-54	Verzicht auf Videokonferenzen in Großraumbüros	**+**	**-**	**+**
A-55	Verzicht auf Sprachsteuerung	**n/a**	**-**	**+**
Netzwerk				
A-56	Einsatz eines SBC am WAN-Übergang	**n/a**	**n/a**	**+**
A-57	Einsatz von Netz-basierten DLP-Systemen	**+**	**-**	**+**
Planung und Betrieb				
A-58	Sichere Administration	**+**	**-**	**+**
A-59	Ausschließliche Datenablage innerhalb der Europäischen Union (EU)	**+**	**-**	**+**
A-60	Überwachung durch ein Security Information and Event Management	**+**	**-**	**+**
A-61	Aufnahme der Videokonferenzlösung in die Notfallvorsorge	**+**	**-**	**+**
A-62	Lesender Zugriff auf von einem Dienstleister betriebene Komponenten	**n/a**	**-**	**+**

Tabelle 3: Auswahl von Sicherheitsanforderungen für Beispielszenarien

9 Hilfsmittel zur Beschaffung

Dieses Kapitel erläutert Hilfsmittel für eine Beschaffung, die eine sichere Videokonferenzlösung gewährleisten soll. Hierfür werden in Kapitel 9.1 beispielhaft drei unterschiedlich große Besprechungsräume mit einem adäquaten Raumsystem dargestellt. In Kapitel 9.2 werden sicherheitsrelevante Auswahlkriterien für eine Videokonferenzlösung spezifiziert. In Kapitel 9.3 wird für eine konkrete Anwendung der Kapitel 9.1 und 9.2 beispielhaft ein Leistungsverzeichnis für die in Kapitel 8.2 spezifizierte On-Premises-Lösung erarbeitet. Das Leistungsverzeichnis erhebt bewusst keinen Anspruch auf Vollständigkeit und berücksichtigt ausschließlich solche Auswahlkriterien, die für eine On-Premises-Lösung mit nur geringem Funktionsumfang relevant sind. Das Leistungsverzeichnis muss in jedem Fall an die individuellen Bedürfnisse einer Institution angepasst werden.

9.1 Beispielausstattung für verschiedene Raumgrößen

Raumsysteme ermöglichen es mittleren bis großen Personengruppen, an Videokonferenzen gemeinsam in einem Raum mit höchster Qualität teilzunehmen. Im Folgenden wird beispielhaft die dafür benötigte Ausstattung für kleine, mittelgroße und große Besprechungsräume dargestellt (siehe Abbildung 19).

Generell sollten die Teilnehmer einen Bildschirmabstand einhalten, der mindestens einmal bis maximal viermal der Bildschirmdiagonale entspricht, um die dargestellten Video-Inhalte adäquat erfassen zu können. Das LED-Display sollte eine Video-Auflösung von mindestens 1080p30 (FullHD mit 30 Bildern pro Sekunde) bieten. Optimal sollten die Video-Codecs H.265 und zukünftig AV1 unterstützt werden, mindestens jedoch H.264 SVC.

Die Kamera des Raumsystems sollte den gesamten Raum erfassen können, um den Eindruck nicht einzusehender Stellen zu vermeiden, der die anderen Teilnehmer verunsichern könnte.

Die Lautsprecher sollten für alle Teilnehmer eine angemessene Lautstärke bieten, d. h. mindestens 80 dB, und eine Lautstärke- und Klangregelung bieten.

Ein omnidirektionales Mikrofon für HD-Voice (AMR-WB, Advanced Multi-Rate Wide Band) sollte eine entsprechende Audioreichweite, Lautstärke- und Klangregler, Stummschaltung und Echounterdrückung bieten, um eine optimale Sprachübertragung zu gewährleisten.

Grundsätzlich sollten Besprechungsräume für Videokonferenzen optimal gestaltet werden. Hierfür sollten die folgenden Punkte geeignet umgesetzt werden:

- Die Farbgebung und Wandgestaltung im Raum sollte eine Interferenzbildung und zu hohe Kontraste vermeiden.
- Die Beleuchtung sollte verteiltes und weiches Licht erzeugen, um Reflexionen und Schatten zu vermeiden.
- Der Raum sollte angemessen abgedunkelt werden können, insbesondere sollte eine direkte Sonneneinstrahlung vermieden werden.
- Äußere Geräusche sollten vermieden bzw. abgeschirmt werden.
- Der Raumhall sollte minimiert werden, z. B. durch Akustikdecken oder -bilder.
- Das Mikrofon sollte für alle Teilnehmer möglichst im gleichen Abstand installiert werden.
- Kamera und Monitor sollten möglichst eng zusammen positioniert werden, damit der natürliche Gesprächseindruck erhalten bleibt.

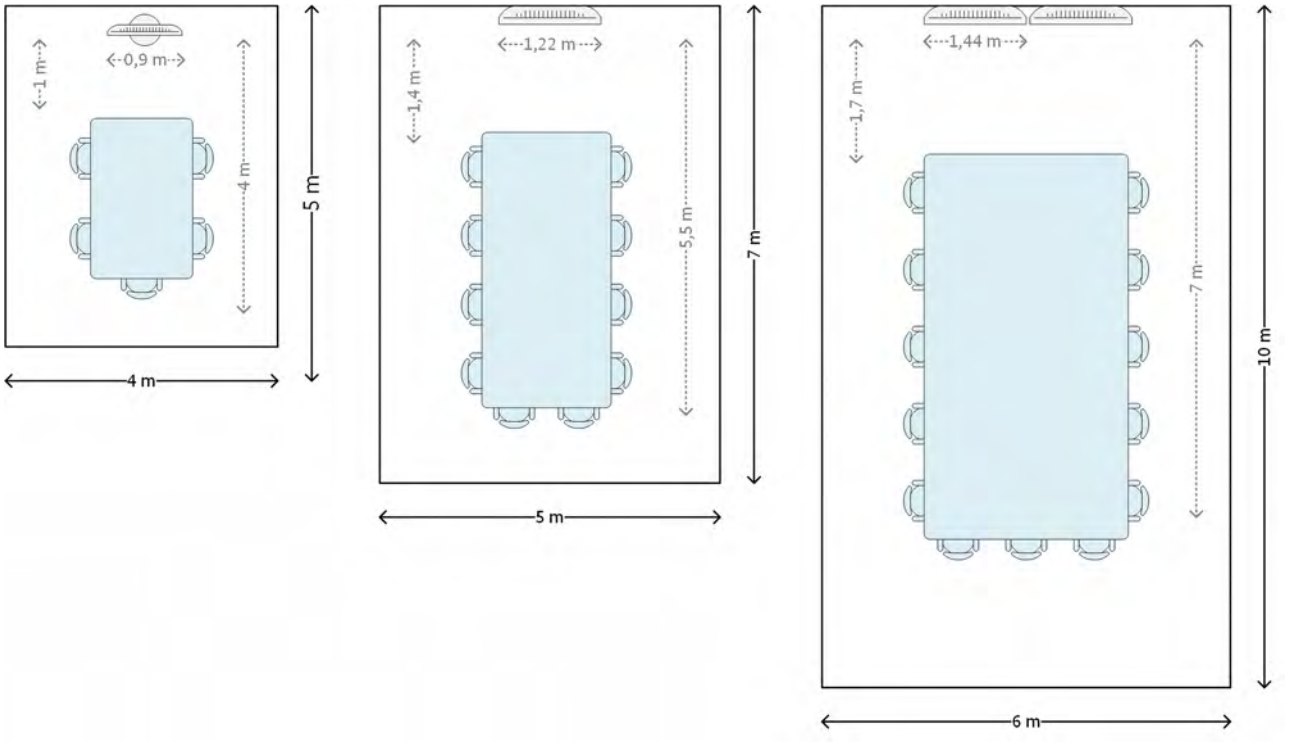

Abbildung 19: Darstellung der Abmessungen für kleinen, mittelgroßen und großen Besprechungsraum

9.1.1 Kleiner Besprechungsraum

Für kleine Besprechungsräume sind transportable Video-Endpunkte, z. B. in Form von Raumsystemen, in Erwägung zu ziehen, die flexibel in Büros oder kleinen Konferenzräumen von ca. 20 qm (ca. 4 x 5 m) aufgestellt werden können. In kleinen Besprechungsräumen nehmen typischerweise maximal 5 Personen an einer Videokonferenz teil. Ein geeigneter Endpunkt sollte die folgenden Anforderungen erfüllen:

- Es handelt sich um ein transportables LED-Display mit 40“ Bildschirmdiagonale (ca. 101 cm, ca. 90 x 60 cm).
- Kamera und Mikrofon/Lautsprecher sind integriert realisiert oder werden extern angeschlossen, z. B. per Aufsatz.
- Als Kamera wird entweder eine unbewegliche Kamera mit einer digitalen Bildausschnittwahl inklusive Zoom und einer entsprechenden Auflösung (größer FullHD) oder
  eine bewegliche Kamera mit FullHD, mindestens 40° vertikalem und 70° horizontalem Blickwinkel sowie mindestens vierfach verlustfreiem Zoom genutzt.
- Der Endpunkt verfügt über ein omnidirektionales Mikrofon mit mindestens 4 m Audioreichweite.

9.1.2 Mittelgroßer Besprechungsraum

Für mittelgroße Besprechungsräume sollte ein fest installierter Video-Endpunkt eingerichtet werden. Ein solcher Besprechungsraum ist ca. 35 qm (ca. 5 x 7 m) groß und kann von maximal 10 Personen genutzt werden, die gemeinsam an einer Videokonferenz teilnehmen. Ein solches Raumsystem sollte den folgenden Leistungsmerkmalen genügen:

- Es verfügt über ein wandmontiertes LED-Display mit 55“ Bildschirmdiagonale (ca. 139 cm, ca. 122 x 69 cm) mit optionalem Touch-Display.

- Optional kann ein weiteres identisches Display genutzt werden.
- Die beiden Displays können horizontal nebeneinander montiert werden und zur erweiterten Anzeige sowie zur getrennten Darstellung von beispielsweise verschiedenen Teilnehmern oder unterschiedlichem Inhalt genutzt werden.
- Kamera und Lautsprecher sind integriert realisiert oder werden extern angeschlossen, z. B. per Aufsatz.
- Als Kamera wird entweder eine unbewegliche Kamera mit einer digitalen Bildausschnittwahl inklusive Zoom und einer entsprechenden Auflösung (größer FullHD) oder
  eine bewegliche Kamera mit FullHD, mindestens 40° vertikalem und 70° horizontalem Blickwinkel sowie mindestens vierfach verlustfreiem Zoom genutzt.
- Das Raumsystem verfügt über mindestens ein, bevorzugt zwei angeschlossene 360°-Tisch-Mikrofone mit mindestens 3 m Audioreichweite.

9.1.3 Großer Besprechungsraum

Auch für einen großen Besprechungsraum sollte ein fest installierter Video-Endpunkt eingerichtet werden. Der Besprechungsraum ist ca. 60 qm (ca. 6 x 10 m) groß und kann von bis zu 15 Personen genutzt werden, die gemeinsam an einer Videokonferenz teilnehmen. Das Raumsystem sollte den folgenden Leistungsmerkmalen genügen:

- Es handelt sich um einen modularen Video-Endpunkt mit zwei wandmontierten 65“-LED-Bildschirmen (ca. 165 cm, ca. 144 x 81cm).
- Die beiden Displays können horizontal nebeneinander montiert werden und zur erweiterten Anzeige sowie zur getrennten Darstellung von beispielsweise verschiedenen Teilnehmern oder unterschiedlichem Inhalt genutzt werden.
- Als Kamera wird entweder eine unbewegliche Kamera mit digitaler Bildausschnittwahl inklusive Zoom und entsprechender Auflösung (größer FullHD) oder
  eine bewegliche Kamera mit FullHD, mindestens 40° vertikalem und 70° horizontalem Blickwinkel sowie mindestens vierfach verlustfreiem Zoom genutzt.
- Das Raumsystem verfügt über mindestens zwei, bevorzugt drei angeschlossene 360° Tisch- oder Decken-Mikrofone mit mindestens 3 m Audioreichweite.
- Optional können Richtmikrofone oder Headsets pro Teilnehmer angeschlossen werden.

9.2 Auswahlkriterien

Im Folgenden werden sicherheitsrelevante Auswahlkriterien spezifiziert, die sich aus den Anforderungen (siehe Kapitel 6) und den Umsetzungshinweisen (siehe Kapitel 7) ergeben. Hierfür wird zunächst in Kapitel 9.2.1 die Methodik zur Entwicklung von UfAB-konformen Kriterienkatalogen und in Kapitel 9.2.2 ein generischer Kriterienkatalog dargelegt.

9.2.1 Methodik

Bei der Identifizierung von Auswahlkriterien richtet sich dieses Kompendium nach der Methodik der Unterlage für die Ausschreibung und Bewertung von IT-Leistungen (UfAB, siehe [BMI-UfAB-2018]). Die UfAB nennt zwei Klassen von Kriterien:

- **Ausschlusskriterium:** Die Nichterfüllung einer als Ausschlusskriterium gekennzeichneten Anforderung führt zum Ausschluss eines Angebots. Ein Ausschlusskriterium muss vollständig erfüllt werden; auch eine Einschränkung des Kriteriums führt zu einem Ausschluss des Angebots. Ausschlusskriterien sind grundsätzlich als digitale Kriterien definiert, d. h. es gibt für sie nur zwei Zustände: vollständig erfüllt oder nicht erfüllt.
- **Bewertungskriterium:** Bewertungskriterien erhalten eine Gewichtung und stellen die Kriterien dar, die innerhalb einer Skala mit Punkten bewertet werden und so eine Leistungsbewertung der Lösung ermöglichen. Bewertungskriterien erfordern entweder eine differenzierte Antwort und eine entsprechend differenzierte Bewertung, um zu ermitteln, wie eine Leistung konkret ausgestaltet ist, oder eine digitale Antwort, deren Nichterfüllung jedoch nicht direkt zum Ausschluss des Angebots führt.

Anhand solcher Kriterien nimmt der Beschaffer eine Bewertung sowohl der Eignung (Ausschlusskriterien) als auch der Leistung der ihm angebotenen Lösungen (Bewertungskriterien) vor. Die Kriterien dienen somit insbesondere der produktneutralen Ausschreibung von IT-Lösungen. Dem Beschaffer wird es auf Basis der Kriterien möglich, eine technische Bewertung der angebotenen Systeme vorzunehmen und diese in Relation zum Preis zu stellen.

UfAB sieht eine Einteilung der Kriterien in typischerweise drei Hierarchiestufen vor:

- Kriterienhauptgruppen (KHG)
- Kriteriengruppen (KG)
- Einzelkriterien (Kr)

Die in diesem Dokument genannten Auswahlkriterien für Komponenten einer Videokonferenzlösung werden dementsprechend unterteilt und in einem Kriterienkatalog verdichtet dargestellt.

Einstufung und Gewichtung der Kriterien, Kriteriengruppen und -hauptgruppen müssen individuell für jedes Einsatzszenario einer Institution vorgenommen werden. Um die Methodik zu verdeutlichen, werden im Musterleistungsverzeichnis Auswahlkriterien mit Einstufung und Gewichten für das betrachtete Szenario beispielhaft festgelegt (siehe Kapitel 9.3). Es werden ganzzahlige Gewichtungspunkte zwischen 1 und 3 vergeben. Hierbei stellt 3 die höchste Wichtigkeit für die Institution dar. Die Gewichtungspunkte einer Kriteriengruppe müssen in einer konkreten Ausschreibung gemäß UfAB-Methodik auf eine feste Summe, meist 10, relativiert werden. Bestimmte Kriterien werden beispielhaft als Ausschlusskriterien klassifiziert und statt mit einer numerischen Gewichtung mit dem Buchstaben „A“ versehen.

Es reicht jedoch nicht aus, sich bei der Beschaffung einer Videokonferenzlösung auf die vorliegenden Auswahlkriterien, die ausschließlich die Sicherheit der Lösung adressieren, zu beschränken. Zusätzlich sind die folgenden Punkte zu beachten:

1. Viele Kriterien, insbesondere Kriterien zur Absicherung der Kommunikation, müssen von allen beteiligten Instanzen, z. B. zentrale Komponenten und Video-Endpunkte oder verschiedene Typen von Video-Endpunkten, erfüllt werden. Im folgenden Kriterienkatalog sind diese jeweils nur einmal aufgeführt.
2. Die für die jeweils zugrunde liegende Technologie spezifizierten Anforderungen und Kriterien sind ebenfalls auf Gültigkeit zu prüfen und dem Kriterienkatalog zuzufügen.

   Beispiel: Eine VoIP-basierte Videokonferenzlösung wird eingeführt. In diesem Fall sind neben den in diesem Kompendium definierten Anforderungen auch die für VoIP-Systeme spezifischen Anforderungen zu berücksichtigen.
3. Für die geplante Architektur sind die Anforderungen für die vorgesehenen Basissysteme zu prüfen und dem Kriterienkatalog zuzufügen.

   Beispiel: Eine zentrale Komponente einer Videokonferenzlösung soll Windows-basiert und virtualisiert bereitgestellt werden. In diesem Fall sind auch die allgemein für Server-Systeme und Virtualisierungshosts spezifizierten Anforderungen zu berücksichtigen.
4. Im Rahmen der Konzepterstellung sind die Anforderungen gegebenenfalls entsprechend der individuellen Gegebenheiten und Sicherheitsrichtlinien der Institution zu ergänzen bzw. zu detaillieren, z. B. Spezifikation des erforderlichen Berechtigungskonzepts oder Festlegung der PIN-Mindestlänge bzw. der Komplexität des Passworts.

   Hierbei ist insbesondere zu beachten, dass etliche Anforderungen, die sich auf zentrale Komponenten beziehen, eine Entsprechung für die Endgeräte haben. Diese Dopplung ist im vorliegenden Kompendium nicht aufgeführt, für eine konkrete Ausschreibung jedoch erforderlich. Hier müssen die konkreten Anforderungen an die Gesamtlösung für alle Elemente harmonisiert und gegebenenfalls ergänzt werden.
5. Abhängig von der individuellen Architektur sind Anforderungen hinsichtlich der Anbindung an Umsysteme wie z. B. Datenbankserver, Präsenzserver oder Terminplaner sowie gegebenenfalls ergänzende Anforderungen an Netzwerkkomponenten zu ergänzen bzw. zu detaillieren.
6. Ebenfalls sind die zutreffenden Anforderungen auf die konkrete Planung anzupassen bzw. einzuschränken, z. B. Auswahl des konkreten Signalisierungs-Protokolls SIP auf TCP-Basis mit entsprechendem Sicherheitsmechanismus TLS anstelle von DTLS auf UDP-Basis.
7. Für die geforderten kryptografischen Verfahren sollten die vom BSI zum Zeitpunkt der Beschaffung empfohlenen Versionen und Schlüssellängen (siehe [BSI TR02102-2019]) dem Kriterienkatalog zugefügt werden bzw. die Kriterien entsprechend angepasst werden.
8. Die Anforderungen bzgl. der Unterstützung standardisierter Verfahren müssen bei einer konkreten Beschaffung den aktuellen Standardisierungen angepasst werden, z. B. Unterstützung von SDES gemäß dem dann aktuellen RFC statt dem aktuell gültigen RFC 6347.
9. Häufig werden an Videokonferenzsysteme geringere Anforderungen hinsichtlich Verfügbarkeit gestellt, als dies bei sonstigen zentralen Diensten erforderlich ist. Die Auswahlkriterien in Bezug auf die Sicherstellung und Überwachung der Verfügbarkeit der Videokonferenzlösung müssen den individuellen Anforderungen der Institution angepasst werden.

Vor der Beschaffung ist die Erstellung eines Architekturkonzepts für die zu beschaffende Lösung und für die Einbettung in die bestehende Infrastruktur vorzunehmen. Wesentlicher Teil dieser Konzeption ist die Anpassung bzw. Erstellung eines Sicherheitskonzepts für die zu beschaffende Videokonferenzlösung.

Aus dieser Gesamt-Konzeption werden sich im Allgemeinen angepasste und gegebenenfalls weitere Auswahlkriterien ergeben, die bei der Beschaffung zu berücksichtigen sind. Der resultierende Kriterienkatalog mit den Angaben der Anbieter bzw. der Leistungsbewertung muss zwingend

Vertragsbestandteil werden, um sicherzustellen, dass auch Auswahlkriterien, die nicht wirtschaftlich prüfbar sind, vom System entsprechend unterstützt werden.

Im Rahmen der Beschaffung werden häufig Produkt- und Abnahmetests durchgeführt. Typische Prüfroutinen können [BSI TLSTK-2014] entnommen werden.

9.2.2 Kriterienkatalog

KHG 1 Anwendungen und zentrale Komponenten

KG 1.1 Absicherung der Komponenten

K 1.1.1 Hochverfügbare Komponenten

Die zentralen Komponenten erfüllen die Anforderungen an Hochverfügbarkeit.

K 1.1.2 Redundante Komponenten im Aktiv-Passiv-Modus

Die zentralen Komponenten erfüllen die Anforderungen an Hochverfügbarkeit durch redundante Komponenten, die im Aktiv-Passiv-Modus agieren.

K 1.1.3 Redundante Komponenten im Aktiv-Aktiv-Modus

Die zentralen Komponenten erfüllen die Anforderungen an Hochverfügbarkeit durch redundante Komponenten, die im Aktiv-Aktiv-Modus mit Lastverteilung agieren.

K 1.1.4 Redundante Komponententeile

Die zentralen Komponenten verfügen über redundante Instanzen mindestens hinsichtlich Netzanschluss, Stromanschluss und Lüfter.

K 1.1.5 Deaktivierung und Sperrung von Diensten und Leistungsmerkmalen

Nicht benötigte oder als sicherheitskritisch eingestufte Dienste und Leistungsmerkmale auf zentralen Komponenten der Videokonferenzlösung können anlagenweit, gruppenweit und portweise deaktiviert und gesperrt werden.

K 1.1.6 Deaktivierung von Netzdiensten und Administrationsschnittstellen

Sämtliche Komponenten der Videokonferenzlösung, die über das IP-Netz der Institution oder über externe IP-Netze erreichbar sind, können durch anlagenweite, gruppenweite oder portweise Deaktivierung nicht benötigter Netzdienste, Protokolle und Administrationsschnittstellen gehärtet werden.

K 1.1.7 Deaktivierung von Komfortfunktionen

Sämtliche Komfortfunktionen der Videokonferenzlösung, z. B. automatische Zuordnung von Namen und Fotos, können je Funktion deaktiviert werden.

K 1.1.8 Zertifizierung nach Common Criteria

Die zentralen Komponenten der Videokonferenzlösung bzw. die Plattform sind nach Common Criteria zertifiziert.

K 1.1.9 Zertifizierung nach Common Criteria EAL

Die Zertifizierung nach Common Criteria weist die Stufe EAL2, EAL4 oder EAL4+ nach.

KG 1.2 Zugriffsschutz

K 1.2.1 Rollenbasiertes Berechtigungs- und Administrationskonzept

Die zentralen Komponenten der Videokonferenzlösung unterstützen ein rollenbasiertes Berechtigungs- und Administrationskonzept mit mindestens den Rollen Administrator, Nutzer, privilegierter Nutzer.

K 1.2.2 Zugriff auf externen Verzeichnisdienst

Die Nutzerverwaltung der Videokonferenzlösung kann über eine Anbindung an einen externen Verzeichnisdienst erfolgen.

K 1.2.3 Absicherung des Zugriffs

Für jeglichen Zugriff auf die Komponenten der Videokonferenzlösung ist eine Authentisierung mindestens mittels Benutzername und Passwort erforderlich.

K 1.2.4 Passwortrichtlinien

Die zentralen Komponenten der Videokonferenzlösung unterstützen die Durchsetzung von Passwortrichtlinien.

K 1.2.5 Sicherheits-Updates

Der AG wird über Sicherheits-Updates für die Komponenten umgehend informiert und diese werden vom Hersteller umgehend bereitgestellt.

K 1.2.6 Schutz vor Schadsoftware

Zentrale Komponenten der Videokonferenzlösung, insbesondere solche, die auf Standard-Betriebssystemen laufen, z. B. Linux oder Microsoft Windows, unterstützen einen Schutz vor Schadsoftware, beispielsweise durch Installation von entsprechenden Programmen.

KG 1.3 Session Border Controller (SBC)

K 1.3.1 Verschlüsselungsendpunkt

Der SBC terminiert Signalisierung und Medienströme und dient als Verschlüsselungsendpunkt innerhalb einer Institution.

K 1.3.2 Abweisung von unverschlüsselten Verbindungen

Der SBC kann so konfiguriert werden, dass er nur verschlüsselte Verbindungen zulässt und unverschlüsselte Verbindungen ablehnt bzw. die Weiterleitung unterbindet.

K 1.3.3 Durchleitung von Ende-zu-Ende-verschlüsselten Medienströmen

Der SBC unterstützt eine Ende-zu-Ende-Verschlüsselung der Mediendaten derart, dass er solche Verbindungen erkennt und ungeprüft weiterleitet.

K 1.3.4 Dedizierte Schnittstellen

Der SBC bietet mehrere Schnittstellen zur Anbindung verschiedener externer Netze, z. B. Internet und WAN.

K 1.3.5 Applikationsintelligenz

Der SBC verfügt über eine Applikationsintelligenz für die Absicherung der Signalisierung und der Nutzdaten und bietet zu Firewalls vergleichbare Filtermöglichkeiten.

K 1.3.6 Paketfilter

Der SBC beinhaltet einen Paketfilter.

K 1.3.7 Schutzmaßnahmen des SBC

Der SBC unterstützt Maßnahmen zur Entschärfung von DoS-Angriffen und verfügt über Optionen zur Kontrolle der Ressourcennutzung (Call Admission Control, CAC). Hierzu zählen beispielsweise Erkennung von fehlerhaften bzw. manipulierten Paketen (Protokollvalidierung), Limitierung der Anzahl an Verbindungen, Limitierung der Bandbreite für alle Verbindungen bzw. je Verbindung sowie Unterstützung von Whitelists und Blacklists

K 1.3.8 Anzahl unterstützter Verbindungen

Der SBC unterstützt die im Leistungsverzeichnis geforderte Anzahl Verbindungen.

KG 1.4 Multipoint Control Unit (MCU)

K 1.4.1 Deaktivierung der automatischen Annahme von Video-Anrufen

Die automatische Annahme eingehender Video-Anrufe kann deaktiviert werden bzw. auf eine vordefinierte Teilnehmer-Liste eingegrenzt werden.

K 1.4.2 Abweisung von unverschlüsselten Verbindungen

Die MCU kann so konfiguriert werden, dass sie nur verschlüsselte Verbindungen zulässt und unverschlüsselte Verbindungen ablehnt bzw. die Weiterleitung unterbindet.

K 1.4.3 Verschlüsselungsendpunkt

Die MCU terminiert Signalisierung und Medienströme und dient als Verschlüsselungsendpunkt innerhalb einer Institution.

K 1.4.4 Durchleitung von Ende-zu-Ende-verschlüsselten Medienströmen

Die MCU unterstützt eine Ende-zu-Ende-Verschlüsselung der Mediendaten derart, dass sie solche Verbindungen erkennt und weiterleitet.

K 1.4.5 Anzahl unterstützter Konferenzen

Die MCU unterstützt die im Leistungsverzeichnis geforderte Anzahl paralleler Konferenzen.

K 1.4.6 Anzahl unterstützter Teilnehmer

Die MCU unterstützt die im Leistungsverzeichnis geforderte maximale Anzahl Teilnehmer und die Anzahl gleichzeitiger Teilnehmer einer Videokonferenz.

KHG 2 Absicherung der Kommunikation

KG 2.1 Signalisierung

K 2.1.1 Gegenseitige Authentisierung mittels MTLS

Die Komponenten unterstützen eine gegenseitige Authentisierung mittels MTLS (Mutual TLS) zur gegenseitigen zertifikatsbasierten Authentisierung mit einem Kommunikationspartner (z. B. Video-Endpunkt, MCU, SBC).

K 2.1.2 Verschlüsselung der Signalisierung

Eine Verschlüsselung der Signalisierung wird von den Komponenten der Videokonferenzlösung unterstützt. Die Verschlüsselung kann separat für die verschiedenen Schnittstellen konfiguriert werden.

K 2.1.3 Verschlüsselung per TLS oder DTLS

TLS bzw. DTLS, jeweils in einer aktuell vom BSI als sicher eingestuften Version, werden zur Verschlüsselung der auf TCP bzw. UDP basierenden Signalisierung von den Komponenten der Videokonferenzlösung unterstützt.

K 2.1.4 Verschlüsselung per S/MIME

S/MIME wird zur Verschlüsselung der Signalisierung von den Komponenten der Videokonferenzlösung unterstützt.

KG 2.2 Mediendaten

K 2.2.1 Verschlüsselung der Medienströme

Eine Verschlüsselung der Medienströme wird von den Komponenten der Videokonferenzlösung unterstützt. Diese Anforderung gilt für alle Komponenten, die einen Medienstrom terminieren, z. B. MCU. Die Verschlüsselung kann separat für die verschiedenen Schnittstellen konfiguriert werden.

K 2.2.2 Ende-zu-Ende-Verschlüsselung der Mediendaten

Eine Ende-zu-Ende-Verschlüsselung der Medienströme wird vom Video-Endpunkt unterstützt.

K 2.2.3 Verschlüsselung per TLS/SSL-VPN

Die Videokonferenzlösung kann über TLS/SSL-basierte VPN-Techniken zum Schutz der Mediendaten abgesichert werden.

K 2.2.4 Verschlüsselung per SRTP

SRTP wird zur Verschlüsselung des Mediendaten unterstützt.

K 2.2.5 Schlüsselmanagement für SRTP

Ein dynamisches Schlüsselmanagement für SRTP ist im Rahmen der Videokonferenzlösung vorhanden.

K 2.2.6 Unterstützung von SDES

Die Videokonferenzlösung unterstützt SDES für ein SIP-basiertes dynamisches Schlüsselmanagement für SRTP. Die SDP-Informationen werden im Rahmen der Absicherung der SIP-Signalisierung über TLS oder S/MIME verschlüsselt übertragen.

K 2.2.7 Unterstützung von DTLS-SRTP

Die Videokonferenzlösung unterstützt DTLS-SRTP für ein dynamisches Schlüsselmanagement für SRTP.

KG 2.3 Konferenzbezogene Daten

K 2.3.1 Verschlüsselung von konferenzbezogenen Daten

Die Übertragung von konferenzbezogenen Daten kann im Rahmen der Videokonferenzlösung über verschlüsselte Protokolle erfolgen. Das System kann so konfiguriert werden, dass solche Daten ausschließlich über verschlüsselte Protokolle übertragen werden. Bevorzugt wird AES mit mindestens 128 Bit Schlüssellänge genutzt.

K 2.3.2 Verschlüsselte Kommunikation mit Umsystemen

Die Kommunikation mit anderen Diensten auf AG-Systemen, z. B. Präsenzdienst oder Gebäudetechnik, kann verschlüsselt erfolgen. Das System kann so konfiguriert werden, dass solche Daten ausschließlich über verschlüsselte Protokolle übertragen werden. Bevorzugt wird AES mit mindestens 128 Bit Schlüssellänge genutzt.

K 2.3.3 Sichere Anbindung an Umsysteme

Der Zugriff auf Umsysteme, z. B. auf Systeme der Gebäudetechnik, darf durch Nutzer nur nach angemessener Authentisierung erfolgen.

K 2.3.4 Einschränkung des Zugriffs auf Systeme der Gebäudetechnik

Der Zugriff bzw. Durchgriff auf Systeme der Gebäudetechnik kann von der Videokonferenzlösung auf bestimmte Rollen, z. B. nur Administratoren oder Moderatoren, eingeschränkt werden.

K 2.3.5 Sichere Einbindung in Datensicherungslösung

Die Videokonferenzlösung kann in die beim AG genutzte Datensicherungslösung eingebunden werden und alle konferenzbezogenen Daten sichern. Zugriff und Kommunikation sind hierbei gemäß den Vorgaben des AG authentisiert und verschlüsselt.

K 2.3.6 Anonymisierung von personenbezogenen Daten

Eine Anonymisierung von Kontaktdaten in Berichten und Protokollen wird durch die Videokonferenzlösung unterstützt. Anwendungen, die Datenträger mit personenbezogenen Daten verarbeiten, können die resultierenden Berichte und Protokolle in anonymisierter Form speichern.

K 2.3.7 Unterstützung von DLP

Die Videokonferenzlösung unterstützt die Einbindung des in der Institution eingesetzten Produktes für Host-basierte DLP.

KHG 3 Absicherung der Konferenzräume

KG 3.1 Kontrolle der Teilnehmer

K 3.1.1 Absicherung des Beitritts durch Berechtigungsstufe

Der Beitritt zu einem Konferenzraum kann durch Autorisierung mittels institutionsinterner Berechtigungsstufe (z. B. Berechtigung gemäß Nutzeraccount) und zugehöriger Authentisierung geschützt werden.

K 3.1.2 Absicherung des Beitritts durch Authentisierungs-Code

Der Beitritt zu einem Konferenzraum kann per dynamisch erzeugtem Authentisierungs-Code, PIN oder Passwort, geschützt werden.

K 3.1.3 Absicherung des Beitritts durch Nutzername

Der Beitritt zu einem Konferenzraum lässt sich durch Nutzername und Passwort schützen.

K 3.1.4 Gewährleistung der voreingestellten Sicherheitsmaßnahme

Das Reduzieren voreingestellter Sicherheitsmaßnahmen durch Nutzer der Videokonferenzlösung kann unterbunden werden, während die Erweiterung der Sicherheitsmaßnahmen erlaubt ist.

K 3.1.5 Signalisierung des Bei- bzw. Austritts

Treten Teilnehmer einer Konferenz bei bzw. treten Teilnehmer aus, so wird diese Änderung allen anderen Teilnehmern mitgeteilt. Dies kann über ein audiovisuelles oder akustisches Signal geschehen.

K 3.1.6 Informationen über aktuelle Teilnehmer

Das Konferenzsystem signalisiert allen Teilnehmern Informationen über die aktuellen Teilnehmer der aktuellen Videokonferenz, mindestens die Nutzernamen.

K 3.1.7 Gesonderte Authentisierung für Moderatoren

Das Konferenzsystem sieht für einen oder mehrere Teilnehmer einer Konferenz die Rolle eines Moderators vor, der sich durch eine spezielle PIN bzw. ein spezielles Passwort ausweist.

K 3.1.8 Einschränkung der Anzahl Moderatoren

Das Konferenzsystem erlaubt die Konfiguration einer Obergrenze für die Anzahl Moderatoren einer Videokonferenz. Die Obergrenze wird für Einladungen zu Videokonferenzen geprüft.

K 3.1.9 Virtueller Warteraum

Das Konferenzsystem verfügt über einen virtuellen Warteraum für Konferenzteilnehmer. Erst der Moderator erlaubt den Teilnehmern, an der Konferenz teilzunehmen.

K 3.1.10 Einschränkung der erlaubten Kanäle

Das Konferenzsystem erlaubt eine Konfiguration der erlaubten Kanäle, über die der Videokonferenz beigetreten werden kann. Insbesondere kann unterbunden werden, dass Teilnehmer über reine Sprach-Endpunkte teilnehmen.

K 3.1.11 Aufnahme und Ausschluss von Teilnehmern

Der Moderator einer Audiokonferenz kann gezielt Teilnehmer in die Konferenz aufnehmen und von der Konferenz ausschließen. Nur der Moderator kann die Konferenz beenden.

K 3.1.12 Aktive Einwahl

Der Initiator einer Konferenz kann die gewünschten Teilnehmer angeben und das System kontaktiert selbstständig alle Teilnehmer. Diese müssen dann ihre Teilnahme an der Konferenz bestätigen. Weitere Teilnehmer können nur durch den Moderator hinzugefügt werden.

K 3.1.13 Verhinderung der Weiterleitung von Einladungen

Die Weiterleitung von Einladungen zur Teilnahme an Videokonferenzen durch Teilnehmer kann verhindert werden. Nur der Moderator oder seine Vertreter können die Einladung weiterleiten.

K 3.1.14 Vertraulichkeit von Videokonferenzeinladungen

Vertrauliche Videokonferenzen können als solche markiert werden und derartige Einladungen werden nicht in öffentliche Kalenderfunktionen übernommen.

KG 3.2 Aufzeichnung und Auswertung von Konferenzen

K 3.2.1 Signalisierung der Aufzeichnung von Konferenzen

Die Aufzeichnung von Konferenzen wird allen Teilnehmern zu Beginn der Aufzeichnung optisch oder akustisch und während der gesamten Aufzeichnung optisch signalisiert.

K 3.2.2 Funktion zur Zustimmung zur Aufzeichnung von Konferenzen

Auf technischer Ebene kann von Konferenz-Teilnehmern eine Zustimmung zur Aufzeichnung der laufenden Video-Konferenz eingeholt werden. Hierbei wird z. B. ein Dialogfenster mit einem entsprechenden Hinweis angezeigt, welches von jedem Teilnehmer beantwortet werden muss.

K 3.2.3 Abgestimmter Start der Aufzeichnung von Konferenzen

Die Aufzeichnung der aktuellen Konferenz beginnt erst, nachdem die Zustimmung aller Teilnehmer vorhanden ist.

K 3.2.4 Schutz der gespeicherten Konferenzinhalte

Die Speicherung von aufgezeichneten Konferenzinhalten erfolgt verschlüsselt bzw. unterliegt einem Zugriffsschutz gemäß den Sicherheitsrichtlinien der Institution.

K 3.2.5 Unterbindung von Aufzeichnungen

Die dezentrale Erzeugung und Speicherung von Konferenzmitschnitten kann zentral unterbunden werden.

K 3.2.6 Funktion zur Zustimmung zur Auswertung von Konferenzen

Auf technischer Ebene kann von Konferenz-Teilnehmern eine Zustimmung zur Auswertung von Videokonferenzinhalten eingeholt werden. Hierbei wird z. B. ein Dialogfenster mit einer entsprechenden Auswahl angezeigt, welches von jedem Teilnehmer beantwortet werden muss.

K 3.2.7 Abgestimmte Auswertung von Konferenzen

Die Auswertung der aktuellen Konferenz oder von Aufzeichnungen erfolgt nur in dem Rahmen, dem die Teilnehmer zugestimmt haben und innerhalb der Vorgaben der Institution.

K 3.2.8 Dokumentation der Zustimmung

Das System dokumentiert die Zustimmung bzw. Ablehnung der Teilnehmer zur Aufzeichnung und Auswertung. Diese Dokumentation wird auch für die spätere Auswertung oder Weiterleitung von Aufzeichnungen und Auswertungen hinzugezogen.

K 3.2.9 Transkription von Aufzeichnungen

Die Videokonferenzlösung unterstützt eine Transkription der aufgezeichneten Inhalte in allgemein nutzbare Textformate.

K 3.2.10 Unterbindung von Transkription

Die Videokonferenzlösung unterstützt eine fallweise Aktivierung und Deaktivierung von Transkriptionen pro Videokonferenz.

K 3.2.11 Weitere KI-basierte Auswertung von Videokonferenzen

Die Videokonferenzlösung unterstützt Funktionen der Künstlichen Intelligenz zur Auswertung von laufenden Videokonferenzen, z. B. Identifizierung bzw. Verifikation von Teilnehmern anhand von Gesichtserkennung.

K 3.2.12 Weitere KI-basierte Auswertung von Aufzeichnungen

Die Videokonferenzlösung unterstützt über Transkription hinaus Funktionen der Künstlichen Intelligenz zur nachträglichen Auswertung von aufgezeichneten Videokonferenzen, z. B. Analyse von Gesprächsstrukturen.

K 3.2.13 Abschaltung von KI-basierten Funktionen

Die Videokonferenzlösung kann so konfiguriert werden, dass KI-basierte Funktionen nicht zum Einsatz kommen. Es kann frei konfiguriert werden, welche KI-basierten Funktionen unterbunden werden.

KG 3.3 Schutz von gespeicherten Daten

K 3.3.1 Gesicherter Zugriff auf gespeicherte Daten

Zum Schutz der gespeicherten Daten (Metadaten, Kontakte etc.) wird eine Schutzfunktion, z. B. eine Zwei-Faktor-Authentisierung oder eine elektronische Sperre des Video-Endpunkts, unterstützt. Diese kann durch die Eingabe von Nutzername und Passwort oder einer PIN realisiert werden.

K 3.3.2 Verschlüsselung von gespeicherten Daten

Die auf zentralen Komponenten und auf Video-Endpunkten gespeicherten Daten sind verschlüsselt.

K 3.3.3 Verschlüsselte Übertragung von Daten

Die Kommunikation zwischen der Videokonferenzlösung und Dateiablagen erfolgt verschlüsselt.

K 3.3.4 Konfigurierbarer Speicherort

Der Speicherort für konferenzbezogene Daten kann von den Teilnehmern ausgewählt werden. Institutionsinterne Richtlinien, z. B. keine Speicherung auf Cloud-Diensten, können als Einschränkung vordefiniert werden.

K 3.3.5 Manuelles Löschen nutzerspezifischer Daten

Das manuelle Löschen nutzerspezifischer Daten wie z. B. Konferenz-Journal, persönliche Kontakte oder Belegung der Kurzwahltasten wird von allen Video-Endpunkten unterstützt.

KHG 4 Endgeräte und Clients

KG 4.1 Absicherung der Geräte

K 4.1.1 Deaktivierung der automatischen Annahme von Video-Anrufen

Die automatische Annahme eingehender Video-Anrufe kann deaktiviert werden.

K 4.1.2 Statusleuchte zur Signalisierung des Betriebszustands

Der Video-Endpunkt besitzt eine Statusleuchte, die den Betriebszustand (Aktiv, Standby) signalisiert.

K 4.1.3 Statusleuchte zur Signalisierung der Kamera- und Mikrofonaktivität

Kameras des Video-Endpunkts verfügen über eine Anzeige für Kamera- bzw. Mikrofonaktivität.

K 4.1.4 Ein-/Aus-Schalter

Der Video-Endpunkt verfügt über einen Ein-/Aus-Schalter, mit dem das Gerät vollständig ausgeschaltet werden kann.

K 4.1.5 Deaktivierung von Wake-on-LAN

Funktionen, die den Video-Endpunkt automatisch aktivieren, z. B. Wake-on-LAN oder Aktivierung bei Anwesenheit von Personen, können deaktiviert werden.

K 4.1.6 Automatischer Standy-Modus

Die Video-Kamera des Video-Endpunkts wird nach einer gewissen Zeit der Inaktivität automatisch aus dem Raumsichtfeld gedreht bzw. deaktiviert. Gleichzeitig werden Mikrofone deaktiviert und/oder die Audioübertragung unterbrochen. Der Zeitraum kann frei konfiguriert werden.

K 4.1.7 Automatische Abmeldung bei Inaktivität

Wird der Video-Endpunkt für eine bestimmte Zeit nicht verwendet, werden angemeldete Benutzer automatisch abgemeldet und ihre Sitzungen beendet. Um den Video-Endpunkt wieder verwenden zu können, wird eine erneute Authentisierung verlangt. Der Zeitraum kann frei konfiguriert werden.

K 4.1.8 Abmeldefunktion bei Raumsystemen

Nach Beendigung der Videokonferenz kann ein Nutzer sich aus dem System ausloggen.

K 4.1.9 Einbindung Host-basierter DLP-Produkte

Video-Endpunkte unterstützen die Einbindung des in der Institution eingesetzten (mindestens aber eines marktüblichen) Host-basierten DLP-Produktes.

K 4.1.10 Minimierung von Plug-ins und Add-ons

Die Videokonferenzlösung erfordert keine Installation von Plug-ins oder Add-ons, die Sicherheitsrisiken bedeuten.

K 4.1.11 Mechanischer Manipulations- und Diebstahlschutz

Um Manipulation und Diebstähle von in öffentlich zugänglichen bzw. unübersichtlichen Bereichen aufgestellten Video-Endpunkten zu vermeiden, wird ein mechanischer Manipulations- und Diebstahlschutz unterstützt.

KG 4.2 Absicherung von Optik, Akustik und Konfiguration

K 4.2.1 Objektivabdeckung für Kameras

Die Kameras der Video-Endpunkte verfügen über Objektivabdeckungen.

K 4.2.2 Blendeneinstellung für Kameraobjektive

Die Kameraobjektive der Video-Endpunkte verfügen über eine den Lichtverhältnissen angepasste, jedoch möglichst weit geöffnete Blendeneinstellung, um die Schärfentiefe so gering wie möglich zu halten.

K 4.2.3 Ausblenden des Hintergrunds

Der Video-Endpunkt kann den Hintergrund aktiv ausblenden oder unkenntlich machen, sodass lediglich Personen im Vordergrund erkennbar sind.

K 4.2.4 Fokussierung auf Sprecher

Die Kamera des Video-Endpunkts kann automatisch den Sprecher fokussieren und so den Bildausschnitt auf Personen im Vordergrund begrenzen.

Ebenso kann der Fokus des Mikrofons automatisch auf den Sprecher gesetzt werden und Hintergrundgeräusche und -gespräche ausgeblendet werden.

K 4.2.5 Umstellung auf Audiokonferenz

Eine aktive Videokonferenz kann unterbrechungsfrei auf eine reine Audiokonferenz umgeschaltet werden.

K 4.2.6 Signalisierung unsicherer Verbindungen

Unsichere Verbindungen werden am Video-Endpunkt, z. B. durch ein entsprechendes Symbol, eindeutig signalisiert.

K 4.2.7 Anzeige von Einstellungs-Änderungen

Der Video-Endpunkt kann bei bestimmten Einstellungsänderungen, mindestens Deaktivierung der Verschlüsselung und Authentisierung, ein Warnsignal an den Nutzer bzw. Administrator geben, dass das Sicherheitsniveau unzureichend ist.

K 4.2.8 Anzeige von sicherheitskritischen Einstellungen

Der aktuelle Zustand von sicherheitsrelevanten Einstellungen, mindestens der Status der Verschlüsselung, wird permanent optisch angezeigt.

KG 4.3 Absicherung der Zugriffe

K 4.3.1 Unterschiedliche Einstellungsbereiche für Benutzer und Administration

Der Video-Endpunkt unterstützt unterschiedliche Einstellungsbereiche bzw. Rollen für Nutzer und Administratoren.

K 4.3.2 Deaktivierung / Umbenennung von Standard-Nutzer und -Passwort

Auf dem Video-Endpunkt kann der Standard- bzw. Default-Nutzer deaktiviert oder umbenannt werden. Voreingestellte Passwörter von Standard-Nutzern müssen beim ersten Anmelden am Endpunkt geändert werden.

K 4.3.3 Deaktivierung von Sprachsteuerung

Auf dem Video-Endpunkt kann die Nutzung einer Sprachsteuerung deaktiviert oder zumindest eingeschränkt werden. Generelle Voreinstellungen werden vom Video-Endpunkt übernommen.

K 4.3.4 Gesicherter Zugriff auf frei zugänglichen Video-Endpunkten

Zum Schutz der gespeicherten Daten wird eine Schutzfunktion unterstützt. Diese kann durch die Eingabe von Nutzername und Passwort oder einer PIN realisiert werden.

K 4.3.5 Verschlüsselung des Zugriffs auf Verzeichnisdienste

Der Video-Endpunkt kann so konfiguriert werden, dass der Zugriff auf Verzeichnisdienste, z. B. für ein zentrales Kontaktverzeichnis, ausschließlich über verschlüsselte Protokolle erfolgt.

K 4.3.6 Unterstützung von LDAPv3

Der Video-Endpunkt unterstützt LDAPv3 einschließlich der Erweiterung StartTLS gemäß aktuellem RFC-Stand.

K 4.3.7 Deaktivierung eines Web-Servers

Falls die Konferenzlösung einen Web-Server auf dem Video-Endpunkt erfordert, wird dieser ausschließlich für eine Videokonferenz aktiviert und bei Beenden der Videokonferenz deaktiviert. Der Web-Server ist gemäß den relevanten Bausteinen des IT-Grundschutz-Kompendiums gehärtet.

K 4.3.8 Administration über sichere Protokolle

Die Administration des Video-Endpunkts erfolgt ausschließlich über sichere Protokolle. Falls ein aktiver Web-Server erforderlich ist, ist dieser gemäß den relevanten Bausteinen des IT-Grundschutz-Kompendiums gehärtet.

K 4.3.9 Einschränkung des lokalen Zugriffs auf Konfiguration

Der lokale Zugriff auf die Konfigurations-Parameter des Video-Endpunkts, z. B. die Netzwerk- oder Video-Konfiguration, kann eingeschränkt bzw. deaktiviert werden.

KG 4.4 Schnittstellen

K 4.4.1 Absicherung von Schnittstellen

Die Kommunikation zwischen Video-Endpunkt und verbundenen Endgeräten, z. B. Laptop, erfolgt ausschließlich über gesicherte Protokolle mit geeigneter Authentisierung und Verschlüsselung. Dies gilt für alle Kommunikationsschnittstellen wie beispielsweise LAN, WLAN und Bluetooth.

K 4.4.2 Deaktivierung von ungenutzten Schnittstellen

Nicht erforderliche Schnittstellen des Video-Endpunkts können entfernt, mindestens jedoch deaktiviert werden.

K 4.4.3 Deaktivierung von unsicheren Protokollen

Unsichere Protokolle zur Kommunikation zwischen Video-Endpunkt und verbundenen Endgeräten, z. B. Dateitransfer via FTP, können unterbunden werden.

K 4.4.4 Deaktivierung der SPAN-Funktion

Falls ein Video-Endpunkt mehrere Netzschnittstellen bietet, kann eine SPAN-Funktion, bei der alle Pakete auf einen anderen Port weitergeleitet werden, deaktiviert werden.

K 4.4.5 Unterstützung von IEEE 802.1X

Der Video-Endpunkt unterstützt IEEE 802.1X zur Authentisierung am Switch-Port. Hierbei wird bevorzugt die Version IEEE 802.1X-2010 unterstützt, mindestens ist die Version IEEE 802.1X-2004 zu unterstützen.

K 4.4.6 Unterstützung von IEEE 802.1AE

Der Video-Endpunkt unterstützt IEEE 802.1AE zur Absicherung der Kommunikation auf Layer 2.

K 4.4.7 Unterstützung von QoS-Parametern

QoS-Parameter nach IEEE 802.1Q-2011 werden vom Video-Endpunkt (bzw. der Client-Anwendung und dem zu Grunde liegenden Betriebssystem) unterstützt.

KG 4.5 Absicherung der kommunikationsbezogenen Daten

K 4.5.1 Ende-zu-Ende-Verschlüsselung

Video-Endpunkte unterstützen eine Ende-zu-Ende-Verschlüsselung und können so konfiguriert werden, dass ausschließlich Verbindungen mit Ende-zu-Ende-Verschlüsselung aufgebaut werden können.

K 4.5.2 Umschaltung der Verschlüsselung

Nutzer an Video-Endpunkten können die Mechanismen und Schärfe der Verschlüsselung für eine Videokonferenz konfigurieren.

K 4.5.3 Nutzung von Profilen

Video-Endpunkte ermöglichen die Nutzung von vordefinierten Profilen. Die Endpunkte können so konfiguriert werden, dass zum Aufbau einer Videokonferenz ausschließlich vordefinierte Profile mit vorgegebenen Sicherheitseinstellungen genutzt werden können.

K 4.5.4 Keine lokale Speicherung

Der Video-Endpunkt ist so konfigurierbar, dass ein Speichern von konferenzbezogenen Daten auf integrierten Dateiablagen oder per USB bzw. Bluetooth angebundenen Dateiablagen unterbunden wird.

K 4.5.5 Warnung bei unsicheren Einstellungen

Der Video-Endpunkt kann bei bestimmten Einstellungs-Änderungen, mindestens Deaktivierung der Verschlüsselung und Authentisierung, ein Warnsignal an den Nutzer bzw. Administrator geben, dass das Sicherheitsniveau gegebenenfalls gesenkt wird.

K 4.5.6 Anzeige sicherheitsrelevanter Einstellungen

Der aktuelle Zustand von sicherheitsrelevanten Einstellungen, mindestens der Status der Verschlüsselung, wird permanent optisch angezeigt. Insbesondere wird bei deaktivierter Verschlüsselung der Mediendaten ein eindeutiges Signal an den Nutzer gegeben.

KHG 5 Cloud-spezifische Kriterien

KG 5.1 Übergreifende Aspekte

K 5.1.1 Management der Informationssicherheit

Der Cloud-Anbieter weist ein systematisches und nachhaltiges Management der Informationssicherheit durch Zertifizierungen nach ISO 27001, BSI IT-Grundschutz oder vergleichbare Prüfungen nach.

K 5.1.2 Cloud-spezifische Sicherheitsmaßnahmen

Die Umsetzung von Cloud-spezifischen Sicherheitsmaßnahmen wird durch eine Zertifizierung nach ISO 27017 oder ein Testat gemäß BSI C5 und für die Verarbeitung von personenbezogenen Daten eine Zertifizierung nach ISO 27018 (oder vergleichbar) nachgewiesen.

K 5.1.3 Erfüllung der Anforderungen an hohe Vertraulichkeit

Die im Eckpunktepapier „*Sicherheitsempfehlungen für Cloud Computing Anbieter*“ des BSI genannten Anforderungen werden vom Anbieter erfüllt, insbesondere die Anforderungen an eine hohe Vertraulichkeit, Kategorie C+.

K 5.1.4 Keine Verschlüsselungsendpunkte in der Cloud

Der Cloud-Anbieter realisiert die Videokonferenzlösung derart, dass kein Verschlüsselungsendpunkt in der Cloud positioniert sein muss, d. h. die zentralen Cloud-Komponenten können eine Ende-zu-Ende-verschlüsselte Verbindung weiterleiten.

K 5.1.5 Nachweis über Vertrauenswürdigkeit

Der Anbieter kann seine Vertrauenswürdigkeit angemessen nachweisen, beispielsweise durch entsprechende Zertifikate.

K 5.1.6 Sicherheitsüberprüfung des Betriebspersonals

Das vom Anbieter eingesetzte Betriebspersonal ist sicherheitsüberprüft. Dies gilt sowohl für Personal, das zwar vom Anbieter gestellt wird, jedoch im eigenen Rechenzentrum arbeitet, als auch für Personal, das im Rechenzentrum des Anbieters tätig ist.

K 5.1.7 Auditierung der Infrastruktur

Die Institution hat vertraglich geregelte Möglichkeiten zur Auditierung der Infrastruktur des Anbieters, soweit diese Infrastruktur für die genutzten Dienste relevant ist.

KG 5.2 Server und Anwendungen

K 5.2.1 Verschlüsselung

Der Anbieter stellt eine konsequente Verschlüsselung der Daten bei Transport, Speicherung und Verarbeitung sicher.

K 5.2.2 Homomorphe Verschlüsselung

Der Anbieter stellt eine konsequente Verschlüsselung mittels homomorpher Verschlüsselungsverfahren der Daten bei Transport, Speicherung und Verarbeitung sicher, d. h. der Anbieter muss die Daten nicht entschlüsseln, um sie verarbeiten zu können.

K 5.2.3 Härtung der Virtualisierungsplattform

Die vom Anbieter eingesetzte Virtualisierungsplattform ist zur Verarbeitung von Daten mit erhöhtem Schutzbedarf angemessen gehärtet und abgesichert.

K 5.2.4 Trennung von Virtuellen Maschinen (VMs) mit unterschiedlichem Schutzbedarf

Der Anbieter stellt sicher, dass keine Vermischung von VMs mit unterschiedlichem Schutzbedarf entsteht.

K 5.2.5 Speicherung in festgelegten Rechenzentren

Alle Daten werden ausschließlich in bei Vertragsabschluss festgelegten Rechenzentren, z. B. ausschließlich in der EU, gespeichert. Dies ist insbesondere dann relevant, wenn Dienste nicht im eigenen Rechenzentrum betrieben werden oder externe Dienste in Anspruch genommen werden.

K 5.2.6 Zusätzliche Datensicherung

Über die Datensicherung des Cloud-Dienstleisters gemäß SLAs ist eine zusätzliche automatisierte und manuelle Datensicherung möglich. Die Zielsysteme der Datensicherung sind frei konfigurierbar, z. B. AG-eigene Systeme. Die Kommunikation zur Datensicherung wird authentisiert und erfolgt verschlüsselt.

K 5.2.7 Einhaltung der DSGVO

Der Cloud-Anbieter hält für die gespeicherten und verarbeiteten Daten die Vorgaben der DSGVO ein. Dies gilt auch, wenn Dienste nicht im eigenen Rechenzentrum betrieben oder weitere Dienstleister einbezogen werden.

K 5.2.8 Zugriff auf Datenablage

Der Anbieter stellt eine flüchtige verschlüsselte Datenablage pro Videokonferenz bereit, über die die Videokonferenzteilnehmer Daten austauschen können. Zugriff hierauf haben ausschließlich die Teilnehmer der Konferenz. Die Datenablage wird mit Beendigung der Videokonferenz gelöscht.

K 5.2.9 Interoperabilität von Host-basierten DLP-Systemen

Das auf den institutionsinternen Video-Endpunkten eingesetzte Host-basierte DLP-System ist mit der technischen Lösung des Anbieters interoperabel.

KG 5.3 Verfügbarkeit

K 5.3.1 Hochverfügbarkeit des Cloud-Dienstes

Der Cloud-Anbieter gewährleistet einen hochverfügbaren Cloud-Service entsprechend der vereinbarten SLAs, z. B. durch georedundante Systeme über voll vermaschte Netze.

K 5.3.2 Redundanter Cloud-Zugang

Der Cloud-Anbieter stellt einen hochverfügbaren Zugang zum Cloud-Service bereit, z. B. durch einen redundanten Netzzugang über mehrere Zugangspunkte im eigenen Netz oder über verschiedene Internet-Provider.

K 5.3.3 Nutzung weiterer Cloud-Dienste

Der Cloud-Anbieter stellt auch eine hochverfügbare Anbindung und Ausstattung von weiteren Cloud-Diensten sicher, die er für die Bereitstellung seines Dienstes einsetzt.

K 5.3.4 Eignung der Netzinfrastruktur für erhöhten Schutzbedarf

Netzinfrastruktur und Internetanbindung des Anbieters sind den Anforderungen an einen erhöhten Schutzbedarf entsprechend ausgelegt.

K 5.3.5 Interoperabilität von Netz-basierten DLP-Systemen

Das im institutionsinternen Netz eingesetzte Netz-basierte DLP-System ist mit der technischen Lösung des Anbieters interoperabel.

KG 5.4 Netzwerk- und Systemmanagement

K 5.4.1 Erhöhtem Schutzbedarf angemessene Überwachung

Der Anbieter stellt eine dem erhöhten Schutzbedarf angemessene Überwachung der Dienste hinsichtlich Verfügbarkeit, Vertraulichkeit und Integrität sicher.

K 5.4.2 Lesender Zugriff auf bereitgestellte Komponenten

Der Anbieter gewährleistet einen lesenden Zugriff auf die bereitgestellten Komponenten z. B. zur Überprüfung der Verfügbarkeit.

K 5.4.3 Regelmäßige Audits

Der Anbieter ist verpflichtet, regelmäßig Audits hinsichtlich der Sicherheit seiner Videokonferenzlösung durch externe Experten durchführen zu lassen und die Ergebnisse dem AG zur Verfügung zu stellen.

K 5.4.4 Regelmäßige Berichte

Der Anbieter ist verpflichtet, regelmäßig Berichte über die korrekt durchgeführte Überwachung der Dienste zu erstellen.

K 5.4.5 Information bei Sicherheitsvorfällen

Der Anbieter ist verpflichtet, bei etwaigen Sicherheitsvorfällen unverzüglich die Institution zu informieren.

KHG 6 Betrieb

KG 6.1 Administration / Nutzung der Videokonferenzlösung

K 6.1.1 Out-of-Band-Administration

Eine Administration Out-of-Band ist für die zentralen Komponenten der Videokonferenzlösung möglich. Neben der operativen IP-Schnittstelle steht ein weiterer Kanal für die Konfiguration zur Verfügung.

K 6.1.2 Separate Ethernet-Management-Schnittstelle

Die zentralen Komponenten der Videokonferenzlösung unterstützen eine dedizierte Ethernet-Management-Schnittstelle für Out-of-Band-Management.

K 6.1.3 Auswahl der Management-Schnittstelle

Für die zentralen Komponenten der Videokonferenzlösung kann festgelegt werden, welche Schnittstelle für die Administration genutzt wird. Insbesondere kann die Administration über die produktive Schnittstelle unterbunden werden.

K 6.1.4 Einheitliche Administration

Alle Komponenten der Videokonferenzlösung können über eine einheitliche Oberfläche administriert werden.

K 6.1.5 Entkoppelter Zugriff

Die Videokonferenzlösung erlaubt einen entkoppelten administrativen Zugriff, z. B. über Terminal Server. Eine direkte IP-Verbindung zur Administration der Komponenten ist nicht erforderlich.

K 6.1.6 Zentrale Administration der Video-Endpunkte

Die Administration und Konfiguration der Video-Endpunkte kann von einer zentralen Stelle aus erfolgen.

K 6.1.7 Verschiedene Profile

Die Videokonferenzlösung unterstützt die zentrale Einrichtung von mehreren, frei konfigurierbaren Profilen, die für bestimmte Konferenztypen wichtige Voreinstellungen gewährleisten. Mindestens sind Profile für ungesicherte und gesicherte Videokonferenzen voreingestellt. Die Profile können von den zentralen Komponenten auf die Video-Endpunkte automatisiert verteilt werden.

K 6.1.8 Umfassende Profil-Inhalte

Die Profile unterstützen mindestens die Einstellung von Verschlüsselungsparametern, genutzten Protokollen und Codecs sowie zulässige Endpunkte und Teilnehmer.

K 6.1.9 Verfügbarkeit von Informationsmaterial

Für die Videokonferenzlösung steht umfassendes Informationsmaterial für Nutzung und Administration in deutscher Sprache zur Verfügung. Das Material adressiert insbesondere auch die Sicherheitseinstellungen für die Komponenten.

K 6.1.10 Wiederherstellung von Konfigurationen

Ein Mechanismus für die Konfigurationssicherung, z. B. in Dateien, und das schnelle Wiedereinspielen von Konfigurationsdateien ist verfügbar. Die Videokonferenzlösung unterstützt die Vorhaltung von mehreren Konfigurationsversionen.

K 6.1.11 Austausch von Komponententeilen im laufenden Betrieb

Um Komponenten bei Ausfall von Teilen, insbesondere Lüfter, Netzteile und Netzmodule, nicht komplett abschalten zu müssen, sind solche Komponententeile im laufenden Betrieb austauschbar.

K 6.1.12 Konfigurationsänderungen ohne Komplettabschaltung

Konfigurationsänderungen können ohne eine Komplettabschaltung der Komponente durchgeführt werden.

KG 6.2 Sichere Administration

K 6.2.1 Administration über verschlüsselte Protokolle

Die Administration und Konfiguration kann vollständig über verschlüsselte Protokolle, z B. HTTPS und SSHv2, erfolgen.

K 6.2.2 Abschaltung unverschlüsselter Protokolle

Die Nutzung von unverschlüsselten Protokollen für Administration und Monitoring, insbesondere HTTP, Telnet und SNMPv1/v2 ist abschaltbar.

K 6.2.3 Gesicherte Übertragung von Konfigurationen und Firmware-Updates

Zur Übertragung von Konfigurationen und Firmware-Updates ist ein gesicherter Kanal verwendbar, beispielsweise HTTPS, SCP/SFTP oder FTPS.

K 6.2.4 Unterstützung von SSHv2

SSHv2 wird mit Schlüssellängen von mindestens 128 Bit unterstützt. Bevorzugt wird AES mit 256, 192 und 128 Bit Schlüssellänge unterstützt.

K 6.2.5 Unterstützung von HTTPS

HTTPS wird mit Schlüssellängen von 128, 192 und 256 Bit unterstützt.

K 6.2.6 Unterstützung von SNMPv3

SNMPv3 wird mindestens mit den Modulen Authentication und Privacy unterstützt. Bevorzugt wird die Authentizität und Integrität durch HMAC-SHA-96 und die Vertraulichkeit durch CFB-AES abgesichert.

K 6.2.7 Authentisierung von Administrations-Zugriffen über RADIUS

Ein Administrations-Zugriff kann über RADIUS authentisiert und autorisiert werden.

K 6.2.8 Verschlüsselung von Passwörtern und Konfigurationsdaten

Die verwendeten Komponenten verschlüsseln Passwörter in den Konfigurationsdateien mit nach Stand der Technik als sicher geltenden Verfahren, z. B. Hash des Passworts.

KG 6.3 Monitoring und Alarming

K 6.3.1 Zentrales Monitoring

Die zentralen Systeme der Videokonferenzlösung können in eine übergreifende Monitoring-Lösung eingebunden werden. Die überwachten Parameter können frei konfiguriert werden.

K 6.3.2 Überwachung der Videokonferenz-Qualität

Eine Überwachung der Videokonferenz-Qualität, insbesondere bei Einbeziehung von Außenstellen oder Telearbeitsplätzen, erfolgt durch die Videokonferenzlösung. Diese Überwachung umfasst Parameter wie Verzögerung, Jitter, Paketverlust und MOS-Wert der Medienströme.

K 6.3.3 SIEM-Einbindung

Die zentralen Systeme der Videokonferenzlösung können in eine übergreifende SIEM-Lösung eingebunden werden.

K 6.3.4 Festlegung spezifischer Schwellwerte

Eine Festlegung von spezifischen Schwellwerten und zugehöriger Alarmierung ist möglich.

Bei Über- bzw. Unterschreitung von derartig definierten Schwellwerten erfolgt eine Alarmierung durch die zentralen Systeme an die entsprechenden Verantwortlichen bzw. Systeme.

K 6.3.5 Meldungen via SNMP-Traps

Meldungen zu Fehlern und zu sicherheitsrelevanten Ereignissen können von den zentralen Systemen als SNMP-Traps an eine zentrale Fehlerkonsole geschickt werden.

K 6.3.6 Meldungen via Syslog

Meldungen zu Fehlern und zu sicherheitsrelevanten Ereignissen können von den zentralen Systemen als Syslog-Meldungen an eine zentrale Fehlerkonsole geschickt werden.

KG 6.4 Protokollierung

K 6.4.1 Einbindung in zentrale Protokollierungslösung

Die zentralen Systeme der Videokonferenzlösung können in eine übergreifende Protokollierungslösung, d. h. ein zentrales Log-Management, eingebunden werden.

K 6.4.2 Protokollierung der Zugriffe

Alle Zugriffe auf die zentralen Systeme der Videokonferenzlösung werden protokolliert, mindestens mit Nutzer, Zeitpunkt und beteiligten Daten. Die Tiefe der Protokollierung bzw. für welche Systeme protokolliert wird, ist frei konfigurierbar.

K 6.4.3 Protokollierung der Tätigkeiten

Für die Zugriffe auf die zentralen Systeme der Videokonferenzlösung werden alle Tätigkeiten vollständig protokolliert.

K 6.4.4 Protokollierung von Konfigurationsänderungen

Alle Konfigurationsänderungen an zentralen Komponenten und Raumsystemen werden protokolliert.

K 6.4.5 Statusanzeige für Verschlüsselung

Der Status der Verbindungen (verschlüsselt/unverschlüsselt) wird im System entsprechend protokolliert, z. B. als Call Detail Record oder in einem Log-File.

K 6.4.6 Protokollierung von unautorisierten Zugriffen

Fehlgeschlagene Zugriffe, auch von Nutzerkonten, auf die Videokonferenzlösung werden im System protokolliert.

K 6.4.7 Protokollierung des Austauschs

Der Austausch von Komponenten bzw. Komponententeilen wird im System protokolliert.

9.3 Beispiel für ein Leistungsverzeichnis

Im Folgenden wird für das Beispiel einer On-Premises-Lösung (siehe Kapitel 8.2) ein vereinfachtes Leistungsverzeichnis (LV) dargestellt. Das Leistungsverzeichnis soll lediglich als Beispiel dienen, erhebt bewusst keinen Anspruch auf Vollständigkeit und berücksichtigt ausschließlich die notwendigen fachlichen Inhalte einer Ausschreibung für eine Videokonferenzlösung, die On-Premises installiert wird und nur einen geringen Funktionsumfang hat.

9.3.1 Gegenstand und Ziel der Ausschreibung

Der Auftraggeber (AG) plant im Rahmen der Umgestaltung der Kommunikationsinfrastruktur die Ablösung der bisherigen Videokonferenzlösung durch eine aktuelle Lösung.

Die anstehende Erneuerung und Verbesserung der vorhandenen Videokonferenzlösung ist im Kontext weiterer Infrastrukturprojekte zu sehen. Diese Projekte zielen unter anderem auf eine Verbesserung der WAN- und LAN-Infrastruktur sowie die Einführung von Voice over IP ab. Detailinformationen können aus den zu den Infrastrukturprojekten gehörenden Leistungsbeschreibungen entnommen werden.

Mit der Ausschreibung soll eine Videokonferenzlösung beschafft werden, die den Anforderungen des AG optimal gerecht wird und die folgenden Komponenten umfasst:

- Zentrale Komponenten im Hauptstandort
- Zentrale Komponenten in Außenstellen
- Raumsysteme
- Ergänzende Ausstattung für PCs, Laptops und mobile Endgeräte
- Sämtliche Lizenzkosten der eingesetzten Produkte
- Regelmäßige Software-Updates und –Upgrades
- Wartungsleistungen auf Basis definierter Service-Level-Vereinbarungen

9.3.2 Architekturkonzept

Die Videokonferenzlösung soll als On-Premises-Lösung für eine Institution mit einem Hauptstandort und zwei größeren und vier kleineren Außenstellen realisiert werden. Alle beteiligten internen Komponenten der Videokonferenzlösung können über das bestehende IP-LAN und IP-WAN miteinander kommunizieren (siehe Abbildung 20). Ein separates Netzwerk für die Videokonferenzlösung ist nicht erforderlich.

Darüber hinaus sollen mobile Teilnehmer und externe Partner via Internet in die Videokonferenzlösung eingebunden werden.

Zur Nutzung der Videokonferenzlösung sollen beliebige Video-Endpunkte eingesetzt werden können. Im Rahmen der Ausschreibung sollen neben den zentralen Komponenten auch

- mehrere Raumsysteme und Touch-Videomonitore sowie
- Hard- und Softwareergänzungen für Desktop-PCs beschafft werden.

Alle Teilnehmer der Videokonferenzlösung sollen auf vorhandene Umsysteme, z. B. Dateiserver und Chat-Server, zugreifen können.

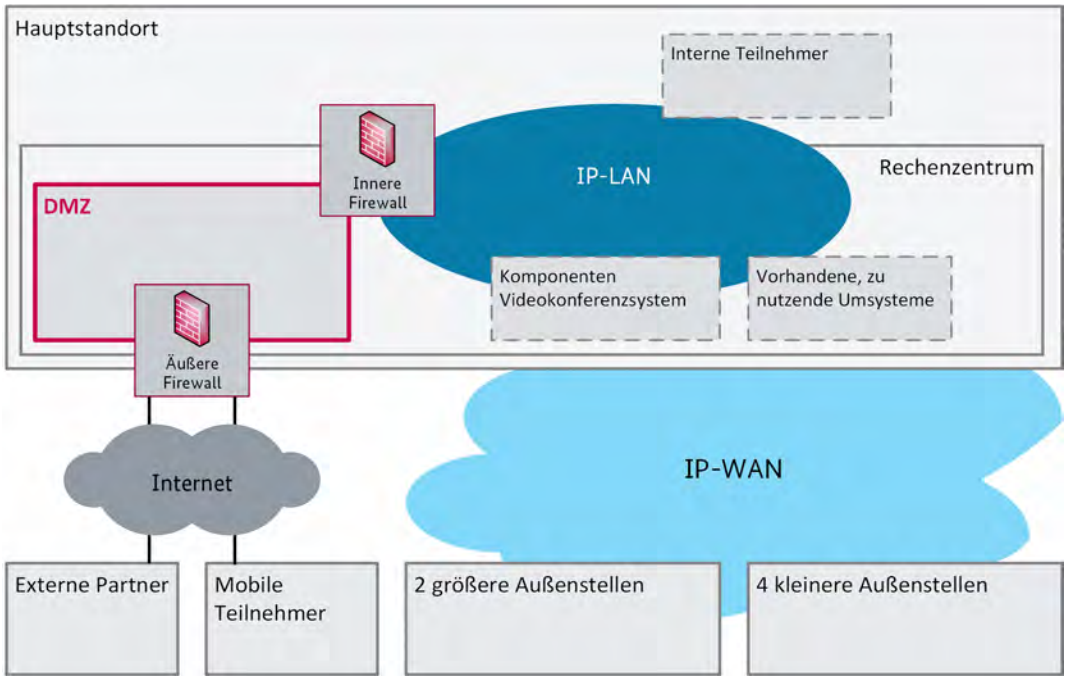

Abbildung 20: Institutionsstruktur

Die Videokonferenzlösung soll zwei Nutzungsmöglichkeiten bieten:

Video-Endpunkte sollen direkte Punkt-zu-Punkt-Verbindungen für Videokonferenzen zwischen zwei Teilnehmern über alle Netze herstellen können (siehe Abbildung 21).

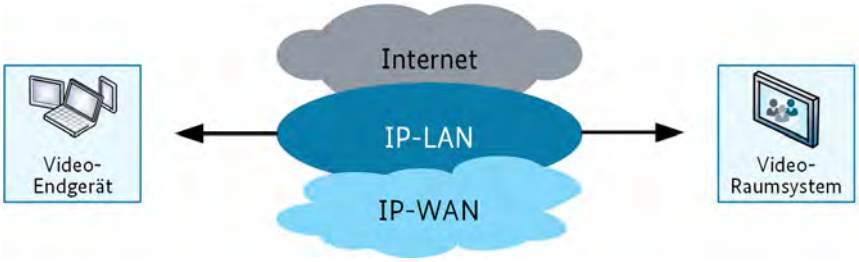

Abbildung 21: Punkt-zu-Punktverbindung

Multipoint Control Units (MCUs) ermöglichen Mehrpunkt-Videokonferenzen mit unterschiedlichsten Video-Endpunkten, Codecs, Protokollen und Auflösungen (siehe Abbildung 22). Es können Verbindungen zwischen internen und externen Teilnehmern über alle Netze hergestellt werden.

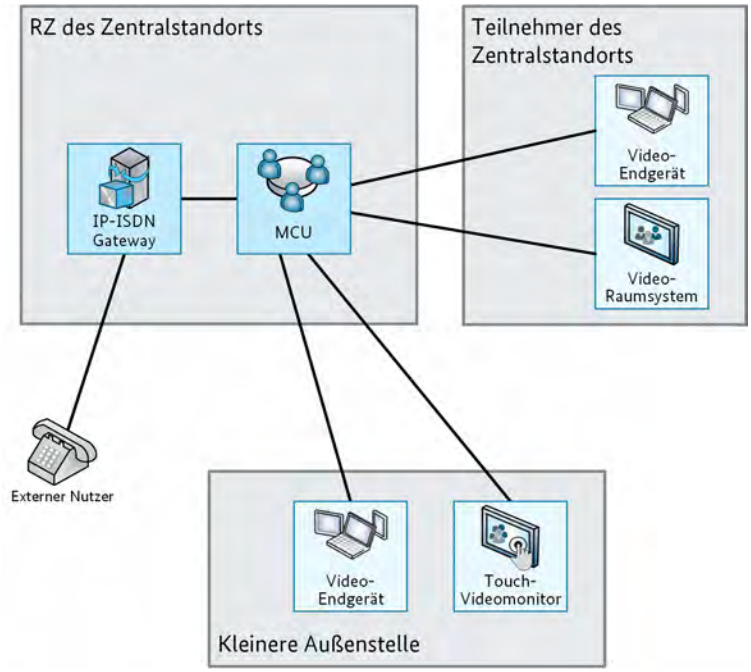

Abbildung 22: Nutzung der Videokonferenzlösung über eine MCU

Die Integration von Nutzern, die via Internet an einer Videokonferenz teilnehmen, wird über einen Session Border Controller abgesichert. Dieser wird als dedizierte Komponente in einer DMZ im AG-Rechenzentrum positioniert.

Für die Videokonferenzlösung werden weitere Einheiten benötigt, die als dedizierte Komponenten oder als integraler Bestandteil der MCU realisiert werden können. Mindestens sind die folgenden Einheiten vorzusehen:

- Registrierungseinheit
- Routing-Einheit
- Management-Einheit

Gegebenenfalls muss die Lösung um weitere Komponenten ergänzt werden. In diesem Fall muss der Bieter dies darlegen und im Angebot mit aufnehmen.

Die Videokonferenzlösung wird als autarkes System realisiert, um eindeutige Zuständigkeiten zu gewährleisten. Die zentrale MCU sowie die ergänzenden zentralen Komponenten im Hauptstandort sind in Form einer gemeinsamen oder mehrerer Hardware-Appliances anzubieten.

Die zentralen MCUs in größeren Außenstellen sollen als Soft-MCU, d. h. als Software basierend auf einem Standard-Betriebssystem realisiert werden.

Der AN verantwortet die abgestimmte Härtung der Videokonferenzlösung.

Die für die Videokonferenzlösung erforderlichen Systeme sind in Abbildung 23 als Übersichtsskizze dargestellt, die zu beschaffenden Komponenten sind mit grünem Rand markiert.

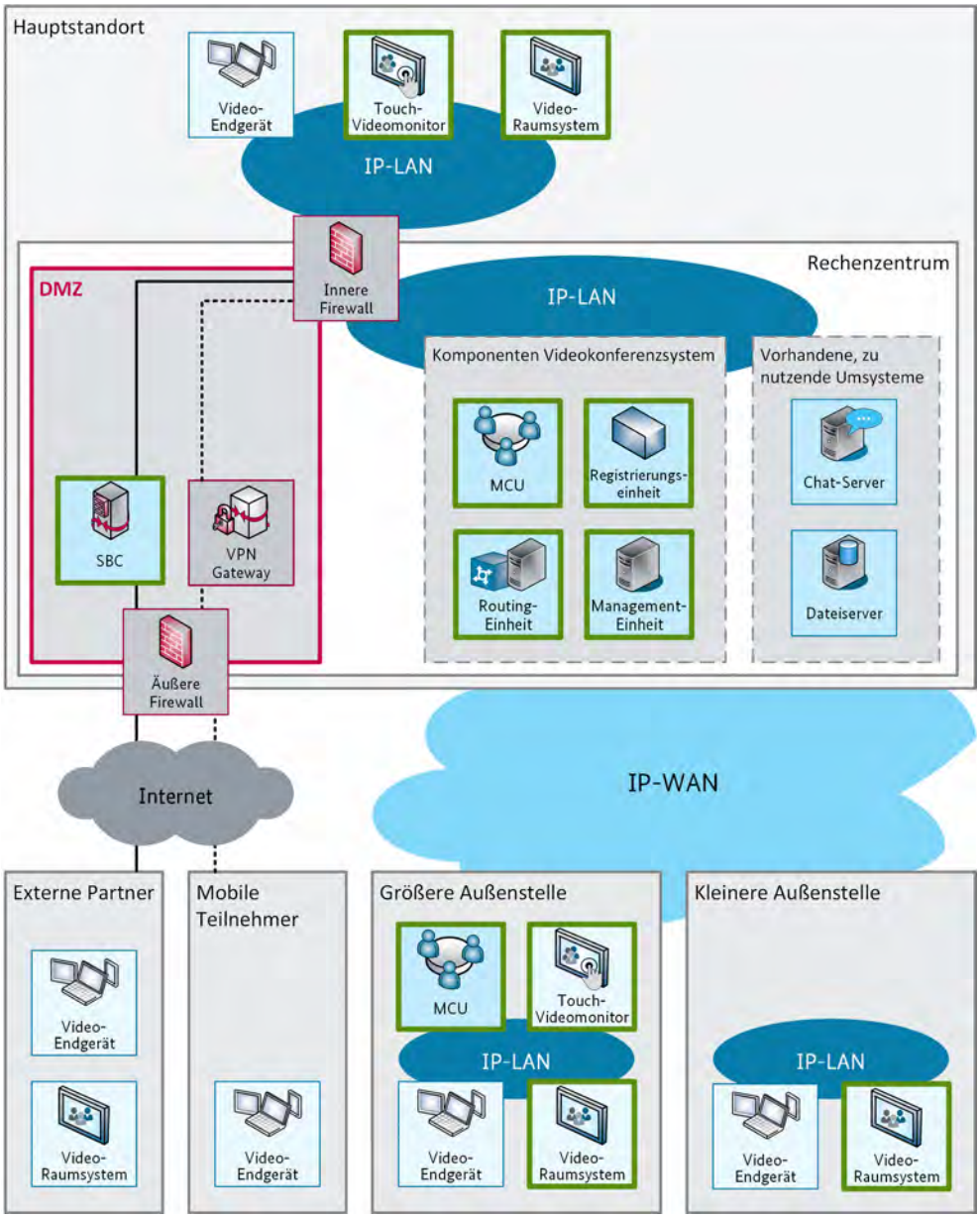

Abbildung 23: Erforderliche Komponenten für Videokonferenzlösung

9.3.3 Anzubietende Leistungen

Es soll eine Videokonferenzlösung mit den spezifizierten Anforderungen gemäß Kapitel 9.3.5 bis Kapitel 9.3.7 angeboten werden. Alle Komponenten sollen On-Premises beim AG aufgebaut werden.

Die Leistungen umfassen:

- Lieferung der in Kapitel 9.3.9 aufgeführten Komponenten
- Lieferung von zusätzlichen Komponenten, die vom Bieter für die beschriebene Videokonferenzlösung als notwendig erachtet werden
- Vor-Ort-Installation, Konfiguration, Härtung, Test, Inbetriebnahme der Videokonferenzlösung im Zentralstandort und den größeren Außenstellen

- Unterstützung bei der Implementierung (per Remote-Zugriff, Telefon, E-Mail etc.) für die transportablen Raumsysteme in kleineren Außenstellen
- Service, d. h. Software-Support und Hardware-Wartung für die angebotenen Komponenten
- Administrator- und Nutzer-Schulungen für die Videokonferenzlösung

9.3.4 Abgrenzung und Mitwirkungsleistungen des AG

Kein Bestandteil der Leistungen sind die folgenden Komponenten und Dienstleistungen:

- IP-LAN und -WAN sowie Internet-Zugang
- UC-nahe Dienste wie Chat- und Präsenzdienst
- Firewalls und VPN-Gateway zur Absicherung der Zugänge
- Desktop-PCs, Laptops und mobile Endgeräte

  Hier sind lediglich für Desktop-PCs erforderliche Hard- und Software-Ergänzungen Gegenstand der Ausschreibung.
- Dedizierter Speicher zur Aufzeichnung von Videokonferenzen und zur Datenablage
- Datensicherungs- und Archivierungslösung für die Videokonferenz-bezogenen Daten
- Betrieb der Videokonferenzlösung
- Installation und Implementierung der transportablen Raumsysteme

Der AG stellt für den Aufbau der Videokonferenzlösung die erforderliche Gebäudeinfrastruktur zur Verfügung:

- IP-Infrastruktur zum Anschluss der Komponenten
- Geeignete Umgebungsbedingungen für die Besprechungsräume, in denen die Video-Endpunkte genutzt werden
- Administrations-Arbeitsplätze mit Zugang zu den zentralen Komponenten der Videokonferenzlösung
- Stromversorgung, Klimatisierung, Installationsschränke

9.3.5 Funktionale Anforderungen

Die Videokonferenzlösung muss die folgenden funktionalen Anforderungen erfüllen:

9.3.5.1 Allgemein

- Anbindung externer Videokonferenzsysteme

  Der Nutzer ist in der Lage, auch andere Videokonferenzsysteme basierend auf H.323, SIP oder WebRTC zu erreichen. Dazu sind die angebotene Software und eine marktübliche USB-Kamera sowie Headset ausreichend.
- Einbindung externer Video-Endpunkte

  Externe Video-Endpunkte können die Videokonferenzlösung über frei verfügbare Browser nutzen, leichte Funktionseinschränkungen sind hierbei tolerierbar.

- Interne und externe Teilnehmer

  Videokonferenzen sind sowohl zwischen den Videokonferenzsystemen des Auftraggebers mit internen und externen Teilnehmern möglich als auch mit externen, nicht direkt gekoppelten Videokonferenzsystemen.
- Alle eingesetzten videokonferenzfähigen Endpunkte können eine Punkt-zu-Punkt-Videokonferenz aufbauen. Zusätzlich ist die Teilnahme an Mehrpunkt-Videokonferenzen möglich. Relevante Endpunkte sind:
  - Raumsysteme (Codec-Einheit, Bildschirm, Kamera und Zubehör)
  - Desktop- und Laptop-Systeme (Video-Soft-Client)
  - Smartphones (iOS, Android) und Tablet-PCs (iOS, Android)
- Alle Komponenten der Videokonferenzlösung unterstützen eine IP-Schnittstelle und das SIP-Protokoll.
- Die zentralen MCUs unterstützen unterschiedlichste Schnittstellen (IP, ISDN etc.) und Protokolle.
- Es besteht die Möglichkeit, sowohl unverschlüsselte als auch verschlüsselte Audio- und Videokonferenzen via SRTP oder TLS durchzuführen.
- Die Videokonferenzlösung ermöglicht die Nutzung von folgenden Audio- und Video-Codecs, Protokollen sowie Auflösungen:
  - Audio-Codecs: G.711 als Standard, G.722 für erhöhte Sprachqualität, G.729 für geringe Bandbreite, Opus für Browser-Zugriffe
  - Video-Codecs: ITU H.263, ITU H.264 alle Varianten, ITU H.265, VP8, VP9
  - Protokolle / Standards: H.323, SIP, WebRTC
  - Auflösung: High Definition (HD / Full-HD) mit 720p (1280 x 720) und 1080p (1920 x 1080)
  - Rückwärtskompatibilität zu niedrigeren Bildauflösungen: VGA (640 x 480)
  - Annahme von allen eingehenden Auflösungen der unterschiedlichen Systeme
- Die Videokonferenzlösung ermöglicht die Einrichtung von mindestens 5 Profilen für Voreinstellungen.
- Die Speicherung der Konfigurationsdaten, insbesondere Profile etc., erfolgt auf einem internen Speicher der Videokonferenzlösung. Eine Aufzeichnung von Videokonferenzinhalten ist nicht vorgesehen.
- Alle Teilnehmer können auf Daten auf AG-eigenen Dateiservern zugreifen und die Inhalte in der Videokonferenz präsentieren.
- Eine Anbindung an Systeme der Gebäudetechnik ist nicht vorgesehen.

9.3.5.2 Dedizierte MCU

Zur Verwaltung und Verarbeitung der Audio- und Video-Daten der verschiedenen Teilnehmersysteme bei Mehrpunkt-Videokonferenzen soll eine dedizierte, hochverfügbare Multipoint Control Unit (MCU) im Zentralstandort mit den folgenden Leistungsmerkmalen am Zentralstandort eingesetzt werden:

- Unterstützung von Konferenzen mit bis zu 30 Teilnehmern an bis zu 30 Standorten
- Das System ist für mehrere parallele Videokonferenzen ausgelegt:
  - 100 parallele 2er Audio- / Video-Konferenzen in Full HD oder
  - 50 parallele 3er Audio- / Video-Konferenzen in Full HD oder
  - 20 parallele 10er Audio- / Video-Konferenzen in Full HD

- Hohe Anforderungen an Stabilität, Qualität und Verfügbarkeit
- Einbindung unterschiedlichster Endpunkte mit unterschiedlichen Schnittstellen und unterschiedlichen Qualitäts- und Bandbreitenoptionen
- Unterstützung gängiger Verschlüsselungsverfahren

Alle für den Betrieb einer MCU erforderlichen Komponenten, beispielsweise zentrale MCU-Einheit oder Firewall-Traversal, sind darzustellen und anzubieten.

9.3.5.3 Soft-MCU-System

An den größeren Außenstellen sollen Punkt-zu-Punkt-Videokonferenzen und Mehrpunkt-Videokonferenzen ermöglicht werden. Hierzu soll eine auf Standard-Betriebssystem basierende Software-MCU beschafft werden.

- 10 parallele Audio- / Video-Konferenzen in Full HD
- 10 aktive Teilnehmer pro Videokonferenz

9.3.5.4 Session Border Controller

Für den Anschluss an das öffentliche Telekommunikationsnetz (PSTN/NGN) wird mittels hochverfügbarem Session Border Controller (SBC) eine definierte Abgrenzung vom internen IP-Netzwerk und dem externen IP-Netzwerk realisiert.

- Es sind mindestens 300 gleichzeitige SIP-Verbindungskanäle möglich.
- Der SBC arbeitet in Richtung des Netzes des AG mit verschlüsselten Signalisierungs- und Medienströmen.
- Der SBC terminiert die verschlüsselten Daten und arbeitet in Richtung externer Anschlüsse (SIP-Provider) bei Bedarf unverschlüsselt.
- Der SBC weist die folgenden Eigenschaften auf:
  - VoIP-/UC-Firewall-Funktion mit dynamischer Port-Öffnung für Medienströme
  -
  - Application-Layer-Gateway-Funktionalität
  - Unterstützung relevanter Schlüsselaustauschverfahren (z. B. DTLS-SRTP)
  - Transkodierung von Medienströmen mit relevanten Codecs gemäß Kapitel 9.3.5.1
  - Adaption von (hersteller-spezifischen) SIP-Dialekten
  - Zentrales Management
  - Normalisierung der SIP-Signalisierung (insbesondere Anpassung der Rufnummern entsprechend dem erforderlichen Format des Ziels)
- Bei einem Ausfall einer SIP-Strecke erfolgt unabhängig vom Ort des Fehlers, durch Re-Routing die Zuordnung aller danach folgender Verbindungsanfragen an den noch aktiven SBC der jeweils anderen Strecke.

9.3.5.5 Video-Raumsysteme

Raumsysteme ermöglichen es mittleren bis großen Personengruppen, an Videokonferenzen mit höchster Qualität teilzunehmen. Es sollen Raumsysteme für kleine, mittelgroße und große Besprechungsräume eingesetzt werden.

Gefordert wird die folgende Ausstattung:

- Codec-Einheit
- Bildschirm / Monitor
- Raummikrofon
- Kamera
- Mediamodul, Datenanwendung
- Anzeigen von Dokumenten (Application Sharing)

Raumsysteme für kleine Besprechungsräume

Für mehrere kleine Besprechungsräume sollen insgesamt vier transportable, dedizierte Videokonferenz-Endpunkte angeboten werden, die flexibel in Büros oder kleinen Konferenzräumen von ca. 20 qm (ca. 4 x 5 m) genutzt werden. Maximal 5 Personen sind in einem solchen Besprechungsraum parallel in eine Videokonferenz eingebunden.

Die Endpunkte müssen die Anforderungen gemäß Kapitel 9.1 und 9.1.1 erfüllen.

Mittelgroßer Besprechungsraum

Für zwei mittelgroße Besprechungsräume soll pro Besprechungsraum je ein fest installierter Video-Endpunkt eingerichtet werden. Die Besprechungsräume sind ca. 35 qm (ca. 5 x 7 m) groß. Maximal 10 Personen sind in einem solchen Besprechungsraum parallel in eine Videokonferenz eingebunden.

Die Endpunkte müssen die Anforderungen gemäß Kapitel 9.1 und 9.1.2 erfüllen, ein Touch-Display bieten und sollten ein weiteres identisches Display ansteuern können (nicht Teil der Ausschreibung).

Großer Besprechungsraum

Für einen großen Besprechungsraum im zentralen Standort soll ein fest installierter Video-Endpunkt eingerichtet werden. Der Besprechungsraum ist ca. 60 qm (ca. 6 x 10 m) groß. Maximal 15 Personen sind in einem solchen Besprechungsraum parallel in eine Videokonferenz eingebunden.

Der Endpunkt muss die Anforderungen gemäß Kapitel 9.1 und 9.1.3 erfüllen. Zwei Monitore und zwei 360°-Tischmikrofone sind für den großen Besprechungsraum Teil der Ausschreibung.

9.3.5.6 Video-Soft-Client

Für Desktop-PCs, Laptops und mobile Endgeräte wie Smartphones und Tablets werden Soft-Clients für die Videokonferenzlösung und Zubehör für Videokonferenzen bereitgestellt.

- Laptop
  - Software-Client für PCs mit Microsoft Windows oder Apple macOS
  - Nutzung von integrierter Kamera und vorhandenem Headset
- Desktop-PC
  - Software-Client für PCs mit Microsoft Windows oder Apple macOS
  - Kamera mindestens FullHD, ohne Mikrofon

  - Nutzung von vorhandenem Headset
- Mobiles Endgerät (Smartphone, Tablet)
  - Software-Client für Smartphones und Tablets mit Apple iOS und Android-Betriebssystemen
  - Nutzung von integrierter Kamera und Mikrofon
  - Nutzung von vorhandenem Headset
- Anzeigen von Dokumenten (Application Sharing)

9.3.6 Anforderungen an die Plattform

Die Videokonferenzlösung muss die folgenden Anforderungen an die Plattform erfüllen:

- Die zentralen Komponenten im Zentralstandort, insbesondere SBC und MCU, sind als dedizierte Hardware-Appliances realisiert. Die zu beschaffenden Einheiten, exklusive SBC, können auf einer Hardware-Appliance zusammengefasst sein.
- SBC und MCU am Zentralstandort werden separat als Hardware-Appliances realisiert.
- Jede Appliance wird redundant an die Netz- und Strominfrastruktur angeschaltet.
- Der SBC erhält zwei redundante Internet-Anbindungen.
- Die angebotene Lösung nutzt zur Kommunikation Schnittstellen gemäß 10BASE-T.
- Die Videokonferenzlösung gewährleistet für die zentralen Appliances eine Hochverfügbarkeit über redundante Komponenten, die in zwei Teilen eines Rechenzentrums positioniert werden und im Active-Passive-Modus agieren.
- Die angebotene Lösung ist derart dimensioniert, dass sie die in der Leistungsbeschreibung definierten Anforderungen optimal unterstützt.
- Es ist geplant, die Lösung schrittweise einzuführen und bei Bedarf zu erweitern. Hierfür soll die Videokonferenzlösung entsprechend flexibel skalierbar sein. Ein Austausch von zentralen Komponenten sollte bei einer Erweiterung nicht erforderlich sein.

9.3.7 Operative Anforderungen

Die Videokonferenzlösung muss die folgenden operativen Anforderungen erfüllen:

9.3.7.1 Bedienbarkeit

- Grundfunktionen und Menüstrukturen sind für beide MCU-Typen identisch.
- Grundfunktionen und Menüstrukturen sind für alle Video-Endpunkte identisch.
- Die Teilnehmer arbeiten in erster Linie nicht mit IP-Adressen oder DNS-Namen, sondern mit Alias-Namen und Telefonnummern (E.164). Es werden alphanumerische und numerische Alias-Namen unterstützt.
- Ein zentrales Telefonverzeichnis unterstützt die Anwender bei der Namenssuche. Es steht ein zentrales Telefonverzeichnis zur Verfügung, das eine Kopplung mit bestehenden Directory Systemen sowie einen Datenaustausch zwischen den Systemen ermöglicht.
- Innerhalb einer bestehenden Punkt-zu-Punkt-Konferenz ohne MCU ist es möglich, die Konferenz zu einer Mehrpunkt-Konferenz zu erweitern, ohne dass ein Verbindungsabbruch erfolgt.

- Für die Videokonferenzlösung ist umfassendes Schulungs- und Anleitungsmaterial verfügbar, das die Nutzer bei der Bedienung der Lösung unterstützt.

9.3.7.2 Management

Die Management-Einheit muss die vollständige Steuerung, Überwachung, Administration und Wartung der Lösung zentral ermöglichen:

- Die Management-Einheit ermöglicht eine Nutzung durch beliebige Endpunkte via Web-Browser. Die Arbeitsplätze zur Nutzung der Management-Einheit sind nicht Teil der Ausschreibung; sie werden vom AG gestellt.
- Die zentralen Komponenten und die Raumsysteme können zentral verwaltet werden.
- Für die Komponenten stehen regelmäßige Updates bereits, die dem Stand der Technik entsprechen. Sicherheitsupdates werden vom Hersteller umgehend bereitgestellt.
- Sowohl der Totalausfall einer zentralen Komponente als auch Ausfälle einzelner Einheiten, beispielsweise der Ausfall eines Netzteils, oder andere Fehler werden als Alarm im Rahmen des Betriebsmanagements signalisiert.
- Die Videokonferenzlösung ist in eine automatisierte Datensicherungslösung einbindbar, die insbesondere die Konfigurationen speichert.
- Die Lösung ist ergänzend zur Management-Einheit in eine vorhandene zentrale Monitoring-Lösung einbindbar.
- Administrative Zugriffe auf die Komponenten der Videokonferenzlösung können über ein Privileged Access Management (PAM) kontrolliert werden.
- Die Administrationsaufgaben umfassen
  - Benutzerverwaltung,
  - Rechteverwaltung der Benutzer und der Systeme sowie
  - Einrichtung von Konferenzprofilen.
- Die Steuerungsaufgaben umfassen
  - Bandbreitenkonfiguration,
  - Qualitäts-Monitoring (Audio- und Videoqualität) sowie
  - Systemkopplung der redundanten Systeme
- Die Management-Einheit ermöglicht eine zentrale Softwarepflege für alle Komponenten und Video-Endpunkte.
- Um allgemeine Probleme und Sicherheitsvorfälle feststellen und analysieren zu können, kann die Videokonferenzlösung in ein Security Information and Event Management (SIEM) eingebunden werden.

9.3.8 Sicherheitsanforderungen

Die Videokonferenzlösung wird hinsichtlich der Sicherheitsanforderungen gemäß der UfAB-Methodik bewertet. Der Katalog der Sicherheitsanforderungen in Tabelle 4 spiegelt die Anforderungen in Kapitel 9.3.5 bis 9.3.7 wider und repräsentiert einen Auszug aus den in Kapitel 9.2.2 spezifizierten Auswahlkriterien mit exemplarischen Einstufungen und Gewichtungen. Der Katalog muss in jedem Fall an die individuellen Bedürfnisse einer Institution angepasst werden.

Nummer	Kriterium	Einstufung	Gewichtung
KHG 1	**Anwendungen und zentrale Komponenten**		
KG 1.1	**Absicherung der Komponenten**		
K 1.1.1	Redundante Komponententeile – Netzteil und Lüfter	B	2
K 1.1.2	Deaktivierung und Sperrung von Diensten und Leistungsmerkmalen	B	3
K 1.1.3	Deaktivierung von Netzdiensten und Administrationsschnittstellen	B	3
K 1.1.4	Deaktivierung von Komfortfunktionen	B	2
K 1.1.5	Zertifizierung nach Common Criteria	B	2
KG 1.2	**Zugriffsschutz**		
K 1.2.1	Rollenbasiertes Berechtigungs- und Administrationskonzept	**A**	-
K 1.2.2	Absicherung des Zugriffs	**A**	-
K 1.2.3	Passwortrichtlinien	B	3
K 1.2.4	Sicherheits-Updates	B	3
K 1.2.5	Schutz vor Schadsoftware	B	2
KG 1.3	**Session Border Controller (SBC)**		
K 1.3.1	Verschlüsselungsendpunkt	**A**	-
K 1.3.2	Abweisung von unverschlüsselten Verbindungen	B	2
K 1.3.3	Applikationsintelligenz	**A**	-
K 1.3.4	Paketfilter	B	3
K 1.3.5	Schutzmaßnahmen des SBC	B	2
K 1.3.6	Anzahl unterstützter Verbindungen	**A**	-
KG 1.4	**Multipoint Control Unit (MCU)**		
K 1.4.1	Deaktivierung der automatischen Annahme von Video-Anrufen	B	3
K 1.4.2	Abweisung von unverschlüsselten Verbindungen	B	2
K 1.4.3	Verschlüsselungsendpunkt	**A**	-
K 1.4.4	Anzahl unterstützter Konferenzen und Teilnehmer	**A**	-
KHG 2	**Absicherung der Kommunikation**		
KG 2.1	**Signalisierung**		
K 2.1.1	Gegenseitige Authentisierung mittels MTLS	**A**	-
K 2.1.2	Verschlüsselung der Signalisierung	**A**	-
K 2.1.3	Verschlüsselung per TLS oder DTLS	B	3
K 2.1.4	Verschlüsselung per S/MIME	B	1
KG 2.2	**Mediendaten**		
K 2.2.1	Verschlüsselung der Medienströme	**A**	
K 2.2.2	Verschlüsselung per TLS/SSL-VPN	B	2
K 2.2.3	Verschlüsselung per SRTP	B	3

Nummer	Kriterium	Einstufung	Gewichtung
K 2.2.4	Schlüsselmanagement für SRTP	B	3
K 2.2.5	Unterstützung von SDES	B	2
K 2.2.6	Unterstützung von DTLS-SRTP	B	2
KG 2.3	**Konferenzbezogene Daten**		
K 2.3.1	Verschlüsselung von konferenzbezogenen Daten	**A**	-
K 2.3.2	Verschlüsselte Kommunikation mit Umsystemen	**A**	-
K 2.3.3	Sichere Einbindung in Datensicherungslösung	B	3
K 2.3.4	Anonymisierung von personenbezogenen Daten	B	2
K 2.3.5	Unterstützung von DLP	B	1
KHG 3	**Absicherung der Konferenzräume**		
KG 3.1	**Kontrolle der Teilnehmer**		
K 3.1.1	Absicherung des Beitritts durch Berechtigungsstufe	B	3
K 3.1.2	Absicherung des Beitritts durch Authentisierungs-Code	B	2
K 3.1.3	Gewährleistung der voreingestellten Sicherheitsmaßnahme	B	3
K 3.1.4	Signalisierung des Beitritts bzw. Austritts	**A**	-
K 3.1.5	Informationen über aktuelle Teilnehmer	**A**	-
K 3.1.6	Verhinderung der Weiterleitung von Einladungen	B	2
KG 3.2	**Auswertung von Konferenzen**		
K 3.2.1	Funktion zur Zustimmung zur Auswertung von Konferenzen	**A**	-
K 3.2.2	Abgestimmte Auswertung von Konferenzen	**A**	-
K 3.2.3	Dokumentation der Zustimmung	A	-
K 3.2.4	KI-basierte Auswertung von Videokonferenzen	B	3
K 3.1.5	Abschaltung von KI-basierten Funktionen	B	3
KG 3.3	**Schutz von gespeicherten Daten**		
K 3.3.1	Gesicherter Zugriff auf gespeicherte Daten	**A**	-
K 3.3.2	Verschlüsselung von gespeicherten Daten	B	3
K 3.3.3	Verschlüsselte Übertragung von Daten	**A**	-
K 3.3.4	Manuelles Löschen nutzerspezifischer Daten	B	3
KHG 4	**Endgeräte und Clients**		
KG 4.1	**Absicherung der Geräte**		
K 4.1.1	Deaktivierung der automatischen Annahme von Video-Anrufen	B	3
K 4.1.2	Statusleuchte zur Signalisierung des Betriebszustands	B	3
K 4.1.3	Statusleuchte zur Signalisierung der Kamera- und Mikrofonaktivität	B	3
K 4.1.4	Ein-/Aus-Schalter	B	1
K 4.1.5	Automatischer Standby-Modus	B	3
K 4.1.6	Automatische Abmeldung bei Inaktivität	B	3
K 4.1.7	Abmeldefunktion bei Raumsystemen	**A**	-
K 4.1.8	Minimierung von Plug-ins und Add-ons	B	2
KG 4.2	**Absicherung von Optik und Konfiguration**		
K 4.2.1	Objektivabdeckung für Kameras	B	2
K 4.2.2	Blendeneinstellung für Kameraobjektive	B	3
K 4.2.3	Ausblenden des Hintergrunds	B	3
K 4.2.4	Fokussierung auf Sprecher	B	2

Nummer	Kriterium	Einstufung	Gewichtung
K 4.2.5	Signalisierung unsicherer Verbindungen	**A**	-
K 4.2.6	Anzeige von sicherheitskritischen Einstellungen	**A**	-
KG 4.3	**Absicherung der Zugriffe**		
K 4.3.1	Unterschiedliche Einstellungsbereiche für Benutzer und Administration	B	3
K 4.3.2	Deaktivierung / Umbenennung von Standard-Nutzer und -Passwort	**A**	-
K 4.3.3	Deaktivierung von Sprachsteuerung	B	1
K 4.3.4	Gesicherter Zugriff auf frei zugänglichen Video-Endpunkten	**A**	-
K 4.3.5	Verschlüsselung des Zugriffs auf Verzeichnisdienste	B	3
K 4.3.6	Deaktivierung eines Web-Servers	B	2
K 4.3.7	Administration über sichere Protokolle	**A**	-
KG 4.4	**Schnittstellen**		
K 4.4.1	Absicherung von Schnittstellen	B	3
K 4.4.2	Deaktivierung von ungenutzten Schnittstellen	B	2
K 4.4.3	Deaktivierung von unsicheren Protokollen	B	3
K 4.4.4	Unterstützung von QoS-Parametern	B	1
KG 4.5	**Absicherung der kommunikationsbezogenen Daten**		
K 4.5.3	Nutzung von Profilen	**A**	-
K 4.5.5	Warnung bei unsicheren Einstellungen	**A**	-
K 4.5.6	Anzeige sicherheitsrelevanter Einstellungen	**A**	-
KHG 5	**Betrieb**		
KG 5.1	**Administration / Nutzung der Videokonferenzlösung**		
K 5.1.1	Einheitliche Administration	B	3
K 5.1.2	Entkoppelter Zugriff	**A**	-
K 5.1.3	Verschiedene Profile mit umfassenden Profil-Inhalten	**A**	-
K 5.1.4	Verfügbarkeit von Informationsmaterial	B	2
K 5.1.5	Wiederherstellung von Konfigurationen	B	2
K 5.1.6	Austausch von Komponententeilen im laufenden Betrieb	B	1
KG 5.2	**Sichere Administration**		
K 5.2.1	Administration über verschlüsselte Protokolle	**A**	
K 5.2.2	Abschaltung unverschlüsselter Protokolle	B	3
K 5.2.3	Gesicherte Übertragung von Konfigurationen und Firmware-Updates	B	2
K 5.2.4	Unterstützung von SSHv2	B	3
K 5.2.5	Unterstützung von HTTPS	B	3
K 5.2.6	Verschlüsselung von Passwörtern und Konfigurationsdaten	**A**	-
KG 5.3	**Monitoring und Protokollierung**		
K 5.3.1	Zentrales Monitoring	B	2
K 5.3.2	Festlegung spezifischer Schwellwerte	B	3
K 5.3.3	Meldungen via Syslog	B	3
K 5.3.4	Einbindung in zentrale Protokollierungslösung	B	2
K 5.3.5	Protokollierung der Zugriffe, insbesondere unautorisierte Zugriffe	**A**	-
K 5.3.6	Protokollierung von Konfigurationsänderungen	B	3
K 5.3.7	Statusanzeige für Verschlüsselung	B	2

Tabelle 4: Sicherheitsanforderungen für Beispiel-Leistungsverzeichnis

9.3.9 LV-Positionen

Alle erforderlichen Komponenten sind im Angebot aufzuführen und in Tabelle 5 mit Einheitspreisen und Gesamtpreis auszuweisen. Sollten Komponenten aus mehreren Sub-Komponenten bestehen, z. B. im Fall von Appliances, sind alle Einzelpreise separat auszuweisen und der Einheitspreis bzw. Gesamtpreis hieraus zu berechnen.

Falls weitere Komponenten als die gelisteten erforderlich sind, um die Architektur und die Anforderungen in Kapitel 9.3.5 bis 9.3.8 zu gewährleisten, so sind diese zu ergänzen und ebenfalls mit Einheitspreis und Gesamtpreis auszuweisen.

Sollten Staffelpreise anhand der Anzahl der Lizenzen bestehen, so sind diese darzustellen.

Lieferort für die Komponenten ist der Zentralstandort der Institution bzw. die Außenstellen (in Deutschland).

Nr.	Leistungsbeschreibung	Menge/ Einh.	Einheitspeis (EP) Gesamtpreis (GP)
1.	**Zentrale Komponenten für Zentralstandort**		
1.01	Dedizierte MCU für Zentralstandort Hochverfügbare Hardware-Appliance für eine zentrale MCU, die das Architekturkonzept realisiert und den relevanten Anforderungen in Kapitel 9.3.5 bis 9.3.8 genügt Hardware- und Software-Kosten inklusive Lieferung und Service für 3 Jahre gemäß den vereinbarten SLAs Prozentsatz für Service in Prozent zum HW/SW-Preis: ……..	1 St	EP: …….. GP: ……..
1.02	Registrierungseinheit für Videokonferenzlösung Hochverfügbare Hardware-Appliance, die das Architekturkonzept realisiert und den relevanten Anforderungen in Kapitel 9.3.5 bis 9.3.8 genügt Die Registrierungseinheit kann ein integraler Teil der MCU oder gemeinsam mit den Positionen 1.03 und 1.04 auf einer Hardware-Appliance realisiert werden. Hardware- und Software-Kosten inklusive Lieferung und Service für 3 Jahre gemäß den vereinbarten SLAs Prozentsatz für Service in Prozent zum HW/SW-Preis: ……..	1 St	EP: …….. GP: ……..
1.03	Routing-Einheit analog zu Position 1.02/Registrierungseinheit	1 St	EP: …….. GP: ……..
1.04	Management-Einheit analog zu Position 1.02/Registrierungseinheit	1 St	EP: …….. GP: ……..
1.05	Session Border Controller für Zentralstandort Hochverfügbare Hardware-Appliance für einen zentralen SBC, der das Architekturkonzept realisiert und den relevanten Anforderungen in Kapitel 9.3.5 bis 9.3.8 genügt Hardware- und Software-Kosten inklusive Lieferung und Service für 3 Jahre gemäß den vereinbarten SLAs Prozentsatz für Service in Prozent zum HW/SW-Preis: ……..	1 St	EP: …….. GP: ……..

Nr.	Leistungsbeschreibung	Menge/ Einh.	Einheitspeis (EP) Gesamtpreis (GP)
1.06	Lizenzen für Videokonferenzlösung Lizenzen, die den relevanten Leistungsanforderungen in in Kapitel 9.3.5 bis 9.3.8 genügen Sollten Staffelpreise für die Anzahl der Lizenzen bestehen, so sind diese darzustellen. Sollten mehrere Lizenzen erforderlich sein, z. B. separate Lizenzkosten für MCU und SBC, so sind diese Kosten getrennt darzustellen.	1 St	EP: …….. GP: ……..
	Gesamtpreis Zentrale Komponenten für Zentralstandort		**……..**
2.	**Zentrale Komponenten in Außenstellen**		
2.01	Soft-MCU für abgesetzten Standort MCU als Software basierend auf Standard-Betriebssystem, die das Architekturkonzept realisiert und den relevanten Anforderungen in Kapitel 9.3.5 bis 9.3.8 genügt Software-Kosten inklusive Lieferung und Service für 3 Jahre gemäß den vereinbarten SLAs Prozentsatz für Service in Prozent zum SW-Preis: ……..	2 St	EP: …….. GP: ……..
	Gesamtpreis Zentrale Komponenten in Außenstellen		**……..**
3.	**Video-Endpunkte**		
3.01	Raumsystem für kleine Besprechungsräume Transportables Raumsystem, das den relevanten Anforderungen in Kapitel 9.3.5 bis 9.3.8 genügt. Das Raumsystem sollte bevorzugt als voll integriertes System angeboten werden. Alle für ein Raumsystem erforderlichen Komponenten sind im Angebot aufzuführen und mit Einzelpreisen auszuweisen. Hardware- und Software-Kosten inklusive Lieferung und Service für 3 Jahre gemäß den vereinbarten SLAs Prozentsatz für Service in Prozent zum HW/SW-Preis: ……..	4 St	EP: …….. GP: ……..
3.02	Raumsystem für mittelgroße Besprechungsräume Raumsystem, das den relevanten Anforderungen in Kapitel 9.3.5 bis 9.3.8 genügt Alle für ein Raumsystem erforderlichen Komponenten sind im Angebot aufzuführen und mit Einzelpreisen auszuweisen. Hardware- und Software-Kosten inklusive Lieferung und Service für 3 Jahre gemäß den vereinbarten SLAs Prozentsatz für Service in Prozent zum HW/SW-Preis: ……..	2 St	EP: …….. GP: ……..

Nr.	Leistungsbeschreibung	Menge/ Einh.	Einheitspeis (EP) Gesamtpreis (GP)
3.03	Raumsystem für große Besprechungsräume Modulares Raumsystem, das den relevanten Anforderungen in Kapitel 9.3.5 bis 9.3.8 genügt Alle für ein Raumsystem erforderlichen Komponenten sind im Angebot aufzuführen und mit Einzelpreisen auszuweisen. Hardware- und Software-Kosten inklusive Lieferung und Service für 3 Jahre gemäß den vereinbarten SLAs Prozentsatz für Service in Prozent zum HW/SW-Preis:	1 St	EP: ..... GP: .....
3.04	Video-Client für Windows-Laptops Software inkl. Lizenz, nutzbar für Betriebssystem Microsoft Windows, die den relevanten Anforderungen in Kapitel 9.3.5 bis 9.3.8 genügt Sollten Staffelpreise anhand der Anzahl der Lizenzen bestehen, so sind diese darzustellen. Software-Kosten inklusive Lieferung und Service für 3 Jahre gemäß den vereinbarten SLAs Prozentsatz für Service in Prozent zum SW-Preis:	20 St	EP: ..... GP: .....
3.05	Video-Client für Mac-Laptops Software inkl. Lizenz, nutzbar für Betriebssystem Apple macOS, die den relevanten Anforderungen in Kapitel 9.3.5 bis 9.3.8 genügt Sollten Staffelpreise anhand der Anzahl der Lizenzen bestehen, so sind diese darzustellen. Software-Kosten inklusive Lieferung und Service für 3 Jahre gemäß den vereinbarten SLAs Prozentsatz für Service in Prozent zum SW-Preis:	20 St	EP: ..... GP: .....
3.06	Video-Client für Desktop-PCs Software inkl. Lizenz für Betriebssystem Microsoft Windows, die den relevanten Anforderungen in Kapitel 9.3.5 bis 9.3.8 genügt Sollten Staffelpreise anhand der Anzahl der Lizenzen bestehen, so sind diese darzustellen. Software-Kosten inklusive Lieferung und Service für 3 Jahre gemäß den vereinbarten SLAs Prozentsatz für Service in Prozent zum SW-Preis:	10 St	EP: ..... GP: .....
3.07	Kamera für Desktop-PCs Desktop-Kamera zum Anschluss auf Desktop-Monitor, mindestens FullHD, ohne Mikro, nutzbar durch Software-Client Hardware- und Software-Kosten inklusive Lieferung und Service für 3 Jahre gemäß den vereinbarten SLAs Prozentsatz für Service in Prozent zum HW/SW-Preis:	10 St	EP: ..... GP: .....

Nr.	Leistungsbeschreibung	Menge/ Einh.	Einheitspeis (EP) Gesamtpreis (GP)
3.08	Video-Client für mobile Endgeräte Software/App inkl. Lizenz für Smartphones und Tablets basierend auf Apple iOS oder Android-Betriebssystem, die den relevanten Anforderungen in Kapitel 9.3.5 bis 9.3.8 genügt Sollten Staffelpreise anhand der Anzahl der Lizenzen oder unterschiedliche Kosten für iOS und Android bestehen, so sind diese separat darzustellen. Software-Kosten inklusive Lieferung und Service für 3 Jahre gemäß den vereinbarten SLAs Prozentsatz für Service in Prozent zum SW-Preis: ……..	50 St	EP: …….. GP: ……..
	Gesamtpreis Video-Endpunkte		**……..**
4.	**Dienstleistungen**		
4.01	Installation, Implementierung, Härtung, Konfiguration und Inbetriebnahme der gelieferten zentralen Komponenten gemäß Feinplanung Die Kalkulation der Kosten ist detailliert darzulegen.	1 St	EP: …….. GP: ……..
4.02	Installation, Implementierung, Härtung, Konfiguration und Inbetriebnahme der gelieferten Komponenten (MCU und Raumsysteme) an einer Außenstelle gemäß Feinplanung Die Kalkulation der Kosten ist detailliert darzulegen.	2 St	EP: …….. GP: ……..
4.03	Installation, Implementierung, Härtung, Konfiguration und Inbetriebnahme der gelieferten Raumsysteme am zentralen Standort gemäß Feinplanung Die Kalkulation der Kosten ist detailliert darzulegen.	1 St	EP: …….. GP: ……..
4.04	Implementierungsunterstützung remote für Raumsysteme in kleineren Außenstellen.	1 St	EP: …….. GP: ……..
4.05	Proof of Concept und Abnahme der gesamten Videokonferenzlösung	1 St	EP: …….. GP: ……..
4.06	Dokumentation der Videokonferenzlösung inkl. Konfigurationen gemäß Vorgaben des AG	1 St	EP: …….. GP: ……..
4.07	Administrator-Schulung für die angebotene Videokonferenzlösung für 5 Teilnehmer, 2 Schulungstage à 8 Unterrichtsstunden	1 St	EP: …….. GP: ……..
4.08	Nutzer-Schulung für die angebotene Videokonferenzlösung für 15 Teilnehmer, 1 Schulungstag à 4 Unterrichtsstunden	1 St	EP: …….. GP: ……..
	Gesamtpreis Dienstleistungen		**……..**
	Gesamtpreis Videokonferenzlösung		**……..**

Tabelle 5: Positionen für Beispiel-Leistungsverzeichnis

10 Zusammenfassung und Ausblick

Das vorliegende Kompendium hat deutlich gezeigt, dass moderne Videokonferenzlösungen inzwischen eine sehr komplexe Systemlandschaft mit unterschiedlichsten Komponenten, vielfältigen Kommunikationsschnittstellen und tiefgreifenden Zugriffs- und Interaktionsmöglichkeiten mit der sonstigen IT darstellen (siehe Kapitel 2 und 3). Eine Videokonferenzlösung ist hier quasi in der Rolle einer Spinne in der Mitte eines großen Netzes von Anwendungen und Systemen zu sehen.

Für die Informationssicherheit ist jedoch genau das ein Alarmsignal, denn ein Sicherheitsvorfall kann so über die reine Videokonferenzlösung hinaus eine erhebliche Wirkung entfalten. Beispielsweise kann ein Angreifer ausgehend von der Videokonferenzlösung über die verfügbaren Schnittstellen andere Anwendungen angreifen.

Auch die operativen Aspekte moderner Videokonferenzsysteme wurden im vorliegenden Kompendium genau betrachtet (siehe Kapitel 4). Die technische Komplexität moderner Videokonferenzsysteme machen auch Nutzung und Betrieb schwieriger und somit trägt dies ebenfalls zur Risikolage bei. Wenn beispielsweise eine moderne Videokonferenzlösung nicht in ein IT-Monitoring integriert ist, weil dies in der Vergangenheit nicht als erforderlich erachtet wurde, kann es sein, dass das eben beschriebene Angriffsszenario erst viel zu spät auffallen würde.

Diese im Vergleich zu klassischen Videokonferenzsystemen deutlich vergrößerte Gefährdungslage wurde in diesem Kompendium genau untersucht (siehe Kapitel 5) und es wurde ein umfassender Katalog an Sicherheitsanforderungen und Umsetzungshinweisen erarbeitet (siehe Kapitel 6 und 7), der sich am BSI IT-Grundschutz-Kompendium orientiert. Hier wurden insbesondere auch die Aspekte betrachtet, die sich durch den Einsatz aktueller Trends wie Cloud Computing und durch neuartige Techniken wie Künstliche Intelligenz (KI) und Internet of Things (IoT) ergeben. Wo sinnvoll möglich, wurde dabei auf bereits vorliegende Standards oder Bausteine des IT-Grundschutz-Kompendiums verwiesen.

Das Ergebnis ist ein Werkzeugkasten von 62 Anforderungen und entsprechenden Maßnahmen, mit dem die gesamte Palette von Videokonferenzsystemen über den gesamten Lebenszyklus abgesichert werden kann, insbesondere unter Berücksichtigung von Maßnahmen für den erhöhten Schutzbedarf. Die Anforderungen und Maßnahmen betrachten dabei strukturiert die Anwendungen und zentralen Komponenten, die Endgeräte und Clients, das Netzwerk und die operativen Aspekte von der Planung bis zum Betrieb inklusive Außerbetriebnahme.

Beispiele von grundlegenden Basisanforderungen sind die Absicherung von Metadaten (siehe A-3) und von Aufzeichnungen von Konferenzen (siehe A-4), da hier besonders vertrauliche Daten und speziell personenbezogene Daten vorliegen. Bereits bei normalem Schutzbedarf sollte gemäß Standardanforderung A-15 auf nicht oder eingeschränkt vertrauenswürdigen Übertragungsstrecken (Internet, aber auch WAN) stets eine Verschlüsselung der mit IP übertragenen Konferenzdaten erfolgen. Bei erhöhtem Schutzbedarf hinsichtlich Vertraulichkeit oder Integrität sollten die Daten durchgängig auf der gesamten Übertragungsstrecke verschlüsselt werden (siehe A-42).

Bei der Anwendung des vorliegenden Kompendiums muss beachtet werden, dass es entscheidend ist, die Anforderungen und Umsetzungsempfehlungen nicht blind umzusetzen. Statt dessen sollte eine Auswahl getroffen werden, die zu der eigenen eingesetzten Lösung sinnvoll passt. Außerdem sollten die Anforderungen und Umsetzungsempfehlungen kritisch an den eigenen Rahmenbedingungen und Möglichkeiten gemessen werden, z. B. der Enterprise Architecture der Institution, und gegebenenfalls sogar angepasst werden. Dies kann aber umgekehrt auch für eine Enterprise Architecture gelten, die aus Gründen der Informationssicherheit z. B. um Videokonferenzsysteme erweitert wird.

Um hierzu einen Eindruck zu vermitteln, wurden in Kapitel 8 verschiedene Szenarien entworfen und exemplarische Sicherheitskonzepte für diese Szenarien erstellt.

Hier ist besonders wichtig, dass Informationssicherheit ohne Risikomanagement undenkbar ist und für Anforderungen, die nicht angemessen umgesetzt werden können, das entstehende Risiko systematisch bewertet werden muss. Dies ist ein grundlegender Bestandteil eines Informationssicherheitsmanagementsystems (Information Security Management System, ISMS) z.B. auf Basis von ISO 27001 oder BSI IT-Grundschutz, das natürlich auch für die Absicherung von Videokonferenzsystemen das eigentliche Fundament bildet (siehe Abbildung 24).

Gerade eine unzureichende Planung kann zu unnötig erhöhten Sicherheitsrisiken führen, wenn beispielsweise vergessen wurde, gewisse Sicherheitsfunktionen zu fordern, die am Ende nicht von der beschafften Lösung unterstützt werden. Um den Anwender des vorliegenden Kompendiums bereits bei der Planung und Beschaffung einer Videokonferenzlösung zu unterstützen, wurden in Kapitel 9 entsprechende Hilfsmittel erarbeitet. Exemplarisch wurden zunächst für Raumsysteme Beispielausstattungen für verschiedene Raumgrößen beschrieben, was bewusst über den Bereich der Informationssicherheit hinaus geht. Anschließend wurden sicherheitsrelevante Auswahlkriterien für Videokonferenzsysteme erarbeitet, die sich nach der Methodik der Unterlage für die Ausschreibung und Bewertung von IT-Leistungen (siehe [BMI-UfAB-2018]) richten. Anschließend wurde ein exemplarisches Leistungsverzeichnis entwickelt und diskutiert, das sowohl funktionale, plattformspezifische, operative als auch sicherheitsbezogene Anforderungen abdeckt.

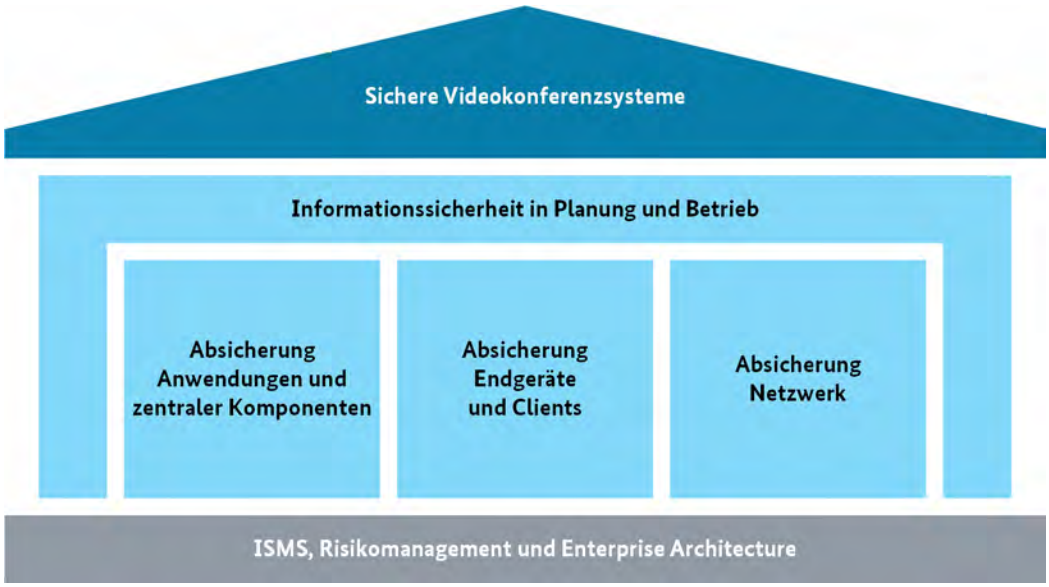

Abbildung 24: Basis und tragende Säulen für die Informationssicherheit von Videokonferenzsystemen

Es ist davon auszugehen, dass der Markt der Videokonferenzlösungen, Meeting Solutions und UCC-Lösungen immer stärker konvergiert und es dabei kaum noch Bereiche geben wird, die ohne Cloud-Dienste auskommen. Der Fokus muss sich an dieser Stelle daher immer stärker auf die sichere Cloud-Nutzung konzentrieren. Standards wie ISO 27017 und Anforderungskataloge wie BSI C5 und Baustein *OPS.2.2 Cloud-Nutzung* des IT-Grundschutz-Kompendiums werden dabei immer wichtiger.

Die Absicherung von KI-basierten Diensten und die Nutzung von IoT-Geräten in Videokonferenzen stellen alle Beteiligten jedoch noch vor einige Herausforderungen. Hier ist es insbesondere für den Anwender des vorliegenden Kompendiums wichtig, diese Aspekte im Sicherheitskonzept geeignet zu berücksichtigen, die Risiken zu bewerten und Schwachstellen genau nachzuverfolgen.

Literaturverzeichnis

[BMI-UfAB-2018] Beschaffungsamt des Bundesministeriums des Innern, Zentralstelle IT-Beschaffung (ZIB), „Unterlage für Ausschreibung und Bewertung von IT-Leistungen, April 2018, verfügbar unter https://www.cio.bund.de/SharedDocs/Publikationen/DE/IT-Beschaffung/ufab_2018_download.pdf?__blob=publicationFile

[BSI C5-2017] BSI, „Anforderungskatalog Cloud Computing (C5)“, September 2017, verfügbar unter https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Anforderungskatalog/Anforderungskatalog_node.html

[BSI SocEng] BSI für Bürger, „IT-Sicherheit am Arbeitsplatz: Social Engineering – der Mensch als Schwachstelle“, aktuelle Webseite, verfügbar unter https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/IT_Sicherheit_am_Arbeitsplatz/SoEng/Social_Engineering_node.html

[BSI Cloud] BSI, „Cloud Computing Grundlagen“, aktuelle Webseite, verfügbar unter https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/Grundlagen/Grundlagen_node.htm]

[BSI GSK-2019] BSI, „IT-Grundschutz-Kompendium - Edition 2019“, Februar 2009, verfügbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

[BSI S2002-2017] BSI, „BSI-Standard 200-2, IT-Grundschutz-Methodik“, November 2017, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.pdf?__blob=publicationFile&v=7

[BSI TLSTK-2014] BSI, „Technische Leitlinie Sichere TK-Anlagen BSI TL-02103“, September 2014, verfügbar unter https://www.bsi.bund.de/DE/Publikationen/TL-sichere-TK-Anlagen/TL02103_htm.html

[BSI TR02102-2019] BSI, „BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen“, Januar 2019, verfügbar unter https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

[BSI TR03125-2018] BSI, „BSI Technische Richtlinie 03125 Beweiswerterhaltung kryptographisch signierter Dokumente“, März 2018, verfügbar unter https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03125/BSI_TR_03125_V1_2_1.pdf?__blob=publicationFile&v=2

[DSGVO-2018] Bundesministerium für Wirtschaft und Energie, „Europäische Datenschutzgrundverordnung“, gültig seit 25.5.2018, verfügbar unter https://www.bmwi.de/Redaktion/DE/Artikel/Digitale-Welt/europaeische-datenschutzgrundverordnung.html

[IETF RFC3550-2003] IETF, RFC 3550, „RTP: A Transport Protocol for Real-Time Applications“, Juli 2003, verfügbar unter https://www.ietf.org/rfc/rfc3550.txt

[IETF RFC3261-2002] IETF, RFC 3261, „SIP: Session Initiation Protocol“, Juni 2002, verfügbar unter https://www.ietf.org/rfc/rfc3261.txt

[IETF RFC3711-2004] IETF, RFC 3711, „The Secure Real-time Transport Protocol (SRTP)“, März 2004, verfügbar unter https://www.ietf.org/rfc/rfc3711.txt

[IETF RFC4511-2006] ETF, RFC 4511, „Lightweight Directory Access Protocol (LDAP): The Protocol“, Juni 2006, verfügbar unter https://www.ietf.org/rfc/rfc4511.txt

[IETF RFC6188-2011] IETF, RFC 6188, „The Use of AES-192 and AES-256 in Secure RTP“, März 2011, verfügbar unter https://www.ietf.org/rfc/rfc6188.txt

[ISO 27001-2017] DIN EN ISO/IEC 27001:2017, „Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme – Anforderungen“, ISO/IEC 27001:2013 einschließlich Cor 1:2014 und Cor 2:2015, Juni 2017, verfügbar unter https://www.beuth.de/de/norm/din-en-iso-iec-27001/269670716

[ISO 27017-2015] ISO/IEC 27017:2015, „Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services“, Dezember 2015, verfügbar unter https://www.iso.org/standard/43757.html

[ISO 27018-2019] ISO/IEC 27018:2019, „Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors“, Januar 2019, verfügbar unter https://www.iso.org/standard/76559.html

[ITU H225-2009] ITU-T, H.225.0, „Call signalling protocols and media stream packetization for packet-based multimedia communication systems“, Dezember 2009, verfügbar unter https://www.itu.int/rec/T-REC-H.225.0-200912-I/en

[ITU H235-2005] ITU-T, H.235.1-7, „H.323 security: Framework for security in H series (H.323 and other H.245-based) multimedia systems“, September 2005, verfügbar unter https://www.itu.int/rec/T-REC-H.235.0-200509-I/en

[ITU H245-2011] ITU-T, H.245, „Control protocol for multimedia communication“, Mai 2011, verfügbar unter http://www.itu.int/rec/T-REC-H.245-201105-I/en

[ITU H323-2009] ITU-T, H.323, „Packet-based multimedia communications systems“, Dezember 2009, verfügbar unter https://www.itu.int/rec/T-REC-H.323-200912-I/en

[ITU H320-2002] ITU-T, H.320, „Narrow-band visual telephone systems and terminal equipment“, März 2004, verfügbar unter https://www.itu.int/rec/T-REC-H.320/en

[NIST BTS-2017] National Institute of Standards and Technology, „Guide to Bluetooth Security“, Mai 2017, verfügbar unter https://www.nist.gov/publications/guide-bluetooth-security-1

[NIST SP-2018] NIST Special Publication 500-325, „Fog Computing Conceptual Model“, März 2018, verfügbar unter https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-325.pdf

[W3C RTC-2018] W3C, „WebRTC 1.0: Real-time Communication Between Browsers“, September 2018, verfügbar unter https://www.w3.org/TR/2018/CR-webrtc-20180927/

Abkürzungsverzeichnis

1-2-3

3GPP	3rd Generation Partnership Project

A

AAC-ELD	Advanced Audio Coding - Enhanced Low Delay
ACL	Access Control List
AES	Advanced Encryption Standard
AG	Auftraggeber
AI	Artificial Intelligence
AMR-WB	Adaptive Multi-Rate – Wide Band
AN	Auftragnehmer
API	Application Programming Interface
APP	Application
ARP	Address Resolution Protocol
AV	Audio und Video
AVC	Advanced Video Coding

B

BMI	Bundesministeriums des Innern
BSD	Berkley Software Distribution
BSI	Bundesamt für Sicherheit in der Informationstechnik

C

CAC	Call Admission Control
CERT	Computer Emergency Response Team
CFB	Cipher Feedback Mode
CIF	Common Intermediate Format
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
Codec	Coder/Decoder
CRM	Customer Relationship Management
CTI	Computer Telephony Integration

D

DB	Datenbank
DIN	Deutsches Institut für Normung
DLP	Data Loss Prevention
DMZ	De-Militarized Zone
DNS	Domain Name Service
DoS	Denial of Service
DSGVO	Datenschutz-Grundverordnung
DTLS	Datagram TLS

E

EAL	Evaluation Assurance Level

EAP	Extensible Authentication Protocol
EN	Europäische Norm
EP	Einheitspreis
ETSI	European Telecommunications Standards Institute
EU	Europäische Union

F

FTP	File Transfer Protocol
FTPS	FTP over SSL

G

GARP	Gratuitous ARP
GP	Gesamtpreis
GSK	(BSI IT-) Grundschutz-Kompendium
GUI	Graphical User Interface

H

HD	High Definition (Video/TV)
HDMI	High Definition Multimedia Interface
HMAC	(Keyed-)Hash Message Authentication Code
HSM	Hardware Security Module
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
HW	Hardware

I

IaaS	Infrastructure as a Service
IAM	Identity and Access Management
ICA	Independent Computing Architecture
IDPS	Intrusion Detection and Prevention System
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	International Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IMAP	Internet Message Access Protocol
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	IP security
iSAC	internet Speech Audio Codec
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
IT	Information Technology
ITU-T	International Telecommunication Union – Telecommunication (Internationale Fernmeldeunion)

K

kbps	Kilobit per Second
KG	(UfAB) Kritieriengruppe
KHG	(UfAB) Kritierienhauptgruppe
KI	Künstliche Intelligenz

L

LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LED	Light-Emitting Diode
LLDP-MED	Link Layer Discovery Protocol - Media Endpoint Discovery
LV	Leistungsverzeichnis

M

MAC	Media Access Control
MACsec	MAC security
mbps	Megabit per Second
MCU	Multipoint Control Unit
MDM	Mobile Device Management
MIB	Management Information Base
MOS	Mean Opinion Score
MTLS	Mutual TLS

N

NAC	Network Access Control
NAS	Network Attached Storage
NAT	Network Address Translation
NGN	Next Generation Network(s)
NIST	National Institute of Standards and Technology

O

ODBC	Open Database Connectivity
OS	Operating System

P

PaaS	Platform as a Service
PAM	Privileged Access Management
PC	Personal Computer
PIN	Persönliche Identifikationsnummer
PoC	Proof of Concept
POP	Point of Presence
PSTN	Public Switched Telephone Network

Q

QCIF	Quarter Common Intermediate Format
QoS	Quality of Service

R

RADIUS	Remote Authentication Dial In User Service
RDP	Remote Desktop Protocol
RFC	Request For Comment (IETF)
RPO	Recovery Point Objective
RTCP	RTP Control Protocol
RTO	Recovery Time Objective
RTP	Real-Time Transport Protocol

S

S/MIME	Secure Multipurpose Internet Message Extensions
SaaS	Software as a Service
SAN	Storage-Area-Network
SBC	Session Border Controller
SCP	Secure CoPy (Protocol)
SDES	Security Descriptions for Media Streams
SDP	Session Description Protocol
SFTP	Secure File Transfer Protocol / SSH File Transfer Protocol
SHA	Secure Hash Algorithm
SIEM	Security Incident and Event Management
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SMTPS	Simple Mail Transfer Protocol Secure
SNMP	Simple Network Management Protocol
SP	(NIST) Special Publication
SPAN	Switched Port Analyzer
SQL	Structured Query Language
SRTCP	Secure RTP Control Protocol
SRTP	Secure Real-time Transport Protocol
SSE	Server Sent Event
SSH	Secure Shell
SSL	Secure Sockets Layer
SVC	Scalable Video Coding
SW	Software

T

TCP	Transmission Control Protocol
TK	Telekommunikation
TL	(BSI) Technische Leitlinie
TLS	Transport Layer Security
TLSTK	(BSI) Technische Leitlinie Sichere TK-Anlagen
TR	(BSI) Technische Richtlinie
TV	Television

U

UC	Unified Communications
UCC	Unified Communications & Collaboration
UDP	User Datagram Protocol
UfAB	Unterlage für die Ausschreibung und Bewertung von IT-Leistungen
URL	Uniform Resource Locator
US	United States (of America)
USA	United States of America
USB	Universal Serial Bus

V

VDI	Virtual Desktop Infrastructure
VGA	Video Graphics Array
VK	Videokonferenz
VM	Virtual Machine
VoIP	Voice over IP
VPN	Virtual Private Network
VS	Verschlusssache

W

W3C	World Wide Web Consortium
WAN	Wide Area Network
WebRTC	Web Real-Time Communication
WLAN	Wireless Local Area Network
WoL	Wake on LAN

X

XHR	XMLhttpRequest
XML	Extensible Markup Language

Glossar

Begriff	Beschreibung
Application Sharing	Beim Application Sharing teilen sich mehrere Teilnehmer per Fernzugriff eine Applikation oder bearbeiten gemeinsam gleichzeitig ein Dokument, z. B. bei einer Videokonferenz.
ARP Spoofing	Das sogenannte Address Resolution Protocol Spoofing (ARP Spoofing, auch ARP Poisoning genannt), gestattet es, durch missbräuchliche, aber standardkonforme Verwendung eines Gratuitous ARP (GARP) innerhalb einer Broadcast-Domäne eines LAN jegliche Kommunikation eines Endgeräts über den Angreifer zu leiten. Der Angreifer muss sich hierzu lediglich an einen Netzport innerhalb der Broadcast-Domäne anschließen. Auch kann der Angriff über einen Computer, von dem aus das angegriffene Videokonferenzsystem direkt erreichbar ist, über ein Trojanisches Pferd erfolgen. Von diesem Computer werden die abgefangenen Daten über eine erlaubte Kommunikations-beziehung per Internet an den eigentlichen Angreifer übermittelt.
Augmented Reality	Augmented Reality (deutsch: erweiterte Realität) kombiniert die realen Wahrnehmungen eines Menschen mit von Computern erzeugten Ergänzungen, die in Echtzeit die realen Wahrnehmungen aufwerten. Bekannte Beispiele von Augmented Reality sind das Einblenden der Bestmarke beim Skispringen im Fernsehen sowie das Anzeigen von zusätzlichen Informationen zu Sehenswürdigkeiten im Smartphone.
Codec	Codec ist eine Wortkreuzung aus den englischen Begriffen „coder“ und „decoder“. Ein Codec bezeichnet ein Verfahren, mit dem analoge Informationen in digitale Informationen umgewandelt werden. Bekannte Varianten sind Audio-Codec (Sprach-Codec) und Video-Codec, der Sprach bzw. Videoinformationen nach einem bestimmten Verfahren kodiert, dekodiert und gegebenenfalls komprimiert, wobei sowohl das sendende als auch das empfangende Gerät den gleichen Kodierungsstandard unterstützen müssen.
Cloud Computing	Laut BSI bezeichnet Cloud Computing das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur wie z. B. Rechenleistung, Speicherplatz, Plattformen und Software (siehe [BSI Cloud]).
Computer Telephony Integration	Computer Telephony Integration (CTI) bezeichnet die koordinierte Steuerung von Interaktionen über ein Telefon und einen PC, z. B. den automatischen Aufbau, Annahme und Beendigung von Telefongesprächen sowie Weitervermittlung von Gesprächen.
Content Sharing	Im Zusammenhang mit Videokonferenzen wird unter Content Sharing das gemeinsame Bearbeiten von Inhalten, z. B. durch Application Sharing oder Whiteboarding verstanden.
Desktop Sharing	Beim Desktop Sharing, auch Screen Sharing genannt, wird der gesamte Bildschirminhalt eines Computers an mehrere andere Computer übertragen. Dies kann im Rahmen von Videokonferenzen, aber auch für Fernwartung oder Web-Seminare genutzt werden.
Fat Client	Als Fat Client wird ein Endgerät bezeichnet, welches autark als eigenständige, vollwertig ausgestattete Komponente genutzt werden kann.
Intrusion Detection and Prevention System	Ein Intrusion Detection and Prevention System (IDPS) ist eine Weiterentwicklung eines IDS und bietet die Möglichkeit unerwünschte Zugriffe, Inhalte und Angriffe zu erkennen und zu unterbinden. Sobald das IDPS einen Verstoß gegen die vereinbarten Regeln erkennt, erfolgen eine Protokollierung, eine Meldung an den Administrator und eine Unterbrechung der als Angriff erkannten Kommunikation. Im Gegensatz hierzu unterstützt ein Intrusion Detection System (IDS) lediglich Angriffserkennung, Protokollierung und Meldung.

Begriff	Beschreibung
IEEE	Das Institute of Electrical and Electronics Engineers (IEEE) ist eine Organisation von Personen aus Elektrotechnik und Ingenieurwesen und ist die weltweit führende Organisation für die Standardisierung im Bereich der Elektronik und der Informationstechnik. Bekannteste Standards sind die Standards IEEE 802.3 (Ethernet), IEEE 802.11 (WLAN) und IEEE 802.1X (Port-basierte Netzzugangskontrolle) für LANs.
IETF	Die Internet Engineering Task Force (IETF) ist ein internationales Gremium aus Fachleuten der Informationstechnik, welches die Internet-Spezifikationen erarbeitet. Die relevanten Dokumente heißen RFCs (Requests for Comment) und sind fortlaufend durchnummeriert. Jeder RFC erhält eine Kategorisierung: Historic, Experimental, Informational oder Standards Track von Proposed Standard über Draft Standard bis Standard. RFCs haben aus historischen Gründen zwar Empfehlungscharakter, faktisch jedoch haben RFCs mit der Kategorisierung Standards Track normativen Charakter.
Immersion (bei VKs)	Immersion bedeutet das „Eintauchen“ in eine Videoübertragung durch Auflösung der räumlichen Grenzen. Die betroffene Person fühlt sich nicht als Beobachter, sondern als Beteiligter.
ITU	Die International Telecommunication Union (ITU), d. h. die Internationale Fernmeldeunion, mit Sitz in Genf ist eine Unterorganisation der Vereinten Nationen und erstellt Richtlinien für die technischen Aspekte der Telekommunikation.
Infrastructure as a Service	Infrastructure as a Service (IaaS) ist ein Cloud-Service, bei dem Hardware-Ressourcen bis hin zu einem ganzen Rechenzentrum virtualisiert zur Verfügung gestellt werden.
Internet of Things	Das Internet of Things (IoT) besteht aus IoT-Geräten, die über das Internet gesteuert oder ausgelesen werden können, aber auch untereinander kommunizieren können.
Künstliche Intelligenz	Die Künstliche Intelligenz (KI, englisch Artificial Intelligence, AI) beschäftigt sich mit der maschinellen Nachbildung von menschlichen Entscheidungsstrukturen und dem maschinellen Lernen, um intelligentes Verhalten zu automatisieren.
Least-Privilege-Prinzip	Das Least-Privilege-Prinzip sieht vor, dass jeder Nutzer, jeder Dienst und jedes System nur die Rechte erhält, die er bzw. es zur Ausführung seiner Aufgaben auch wirklich benötigt.
Man-in-the-Middle	Ein Man-in-the-Middle (MitM) ist ein System, das in einen Kommunikationspfad eingeklinkt wird, ohne dass die Kommunikationspartner dies bemerken.
Next Generation Network	Ein Next Generation Network (NGN) unterscheidet zwischen Access Network (Zugangsnetz) und Core Network (Kernnetz) und nutzt generell das Internet Protocol (IP).
On-Premises	On-Premises bedeutet in den eigenen Räumlichkeiten der Institution.
Out-of-Band-Management	Als Out-of-Band-Management wird jegliche Management-Kommunikation verstanden, die über eine Infrastruktur erfolgt, die nicht für die produktive Kommunikation verwendet wird.
Präsenzdienst	Ein Präsenzdienst verarbeitet Informationen zur Gesprächsbereitschaft und zu den verfügbaren Kommunikationskanälen sowie zu deren grafischer Darstellung und signalisiert dies den anderen Nutzern des Dienstes.
Privileged Access Management	Privileged Access Management (PAM) beschreibt eine Technologie zur Kontrolle von externen oder internen Zugriffen mit privilegierten Rechten auf IT-Anwendungen und IT-Systeme über Netze.
Profiling	Profiling bezeichnet die Erstellung eines Gesamtbildes einer Persönlichkeit durch erfasste Informationen für bestimmte Zwecke, z. B. zur Tätersuche.
Public Switched Telephone Network	Das Public Switched Telephone Network (PSTN, auch Fernsprechnetz genannt) bezeichnet das öffentliche Telefonnetz, welches analoge und ISDN-Verbindungen vermittelt.

Begriff	Beschreibung
Repository	Unter einem Repository versteht man eine zentrale Ablage für Daten mit ihren Metadaten, bei Programmpaketen z. B. Beschreibungen der Pakete.
Recovery Point Objective	Recovery Point Objective (RPO) beschreibt den Zeitraum, in dem Daten verloren gehen dürfen, ohne die Geschäftsprozesse nachhaltig zu schädigen, d. h. RPO spezifiziert den zeitliche Abstand zwischen zwei Datensicherungen.
Recovery Time Objective	Recovery Time Objective (RTO) beschreibt die Zeit, die vom Schadenseintritt bis zur vollständigen Wiederherstellung der produktiven Umgebung toleriert werden kann.
Security Information and Event Management	Ein Security Information and Event Management (SIEM) kombiniert ein Security Information Management und ein Security Event Management. Es sammelt Log-Daten von verschiedensten Systemen, analysiert und korreliert sie in Echtzeit und generiert Sicherheitsalarme, wenn es Unregelmäßigkeiten oder Auffälligkeiten erkennt.
Social Engineering	Laut BSI werden beim Social Engineering menschliche Eigenschaften wie Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt, um Personen geschickt zu manipulieren. Der Angreifer verleitet das Opfer auf diese Weise beispielsweise dazu, vertrauliche Informationen preiszugeben, Sicherheitsfunktionen auszuhebeln, Überweisungen zu tätigen oder Schadsoftware auf dem privaten Gerät bzw. einem Computer im Firmennetz zu installieren (siehe [BSI SocEng])
Software as a Service	Software as a Service (SaaS) ist ein Cloud-Service, bei dem Software virtualisiert in der Cloud zur Verfügung gestellt wird. Die Benutzer greifen über das Internet meist über einen Browser auf die Software zu. Die gesamte darunter liegende Infrastruktur befindet sich ebenfalls in der Cloud bei dem entsprechenden Provider.
Thin Client	Ein Thin Client ist ein Endgerät mit eingeschränkter Ausstattung, welches nur unter Nutzung eines Servers (z. B. Terminal Server) die vollständige Funktionalität bietet.
Townhall Meeting	Unter Townhall Meeting wird die Übertragung eines einzelnen Datenstroms zu vielen Endpunkten verstanden. Es gibt also einen Redner und viele Zuhörer.
Transkription (einer VK)	Bei einer Transkription einer Videokonferenz wird die Sprache in einen Text überführt. Dies kann sowohl manuell (bei aufgezeichneten Videokonferenzen) als auch automatisch durch Einsatz von Künstlicher Intelligenz erfolgen.
Unified Communi-cations & Collaboration	Unified Communications and Collaboration (UCC) integriert Werkzeuge zur Zusammenarbeit in Kommunikationslösungen.
Video-Endpunkt	Als Video-Endpunkte, auch Video-Terminals genannt, werden die Endgeräte bezeichnet, mit denen Nutzer an einer Videokonferenz teilnehmen können. Sie stellen die Anfangs- und Endpunkte der Bild- und Tonübertragung dar. Die Spannweite reicht hier von klassischen Raumsystemen, über Standard-IT-Ausstattung wie PC und Laptop und Videotelefone bis hin zu mobilen Endgeräten wie Smartphones oder Tablets
Virtualisierung	Erzeugung von nicht physischen, jedoch separierten Netz-, Server- oder Software-Elementen und Zusammenfassung auf einer physischen Komponente, z. B. Unabhängige, virtuelle Routing-Instanzen auf einer Netzwerk-Komponente.
Virtual Private Cloud	Eine Virtual Private Cloud beschreibt eine Private Cloud, die sich innerhalb einer Public Cloud befindet.
Wake-on-LAN	Wake-on-LAN (WoL) ermöglicht den Start eines Gerätes beim Empfang eines speziellen Datenpakets. Dies ist nicht nur im lokalen Netz, sondern auch via Internet möglich.
Whiteboarding	Unter Whiteboarding wird die gemeinsame Nutzung eines virtuellen Whiteboards in einer Videokonferenz verstanden. Jeder Teilnehmer kann Ergänzungen oder Änderungen am dargestellten Inhalt vornehmen. Diese werden den anderen Teilnehmern sofort angezeigt.

Stichwortverzeichnis / Index