Bundesamt
für Sicherheit in der
Informationstechnik

APP.5.4 Unified Communications und Collaboration (UCC)

1. Beschreibung

1.1. Einleitung

Unified Communications bezeichnet einen Dienst, der verschiedene Kommunikationsdienste in einer Anwendung und in der Regel auch einem Softclient vereint. Damit wird der Anteil der traditionellen Telefonie in der persönlichen digitalen Kommunikation reduziert. Die möglichen Kommunikationswege werden um zusätzliche Dienste wie Video, diverse Formen von Chats und Erreichbarkeitsanzeigen erweitert.

Eine Kommunikationsbeziehung zwischen zwei oder mehr Teilnehmenden wird unabhängig vom benutzten Dienst als Konversation bezeichnet.

Die häufig bei Unified Communications und Collaboration (UCC) genannte Zusammenarbeit (Collaboration) geht noch einen Schritt weiter. Während damit in der Vergangenheit häufig nur Dienste wie Screen Sharing und (digitales) Whiteboarding bezeichnet wurden, stellen UCC-Dienste viele weitere Funktionen zur Verfügung. Insbesondere beim Zusammenarbeiten von Teams hat sich eine Anzahl von Anwendungen etabliert, die häufig als Cloud-Dienst benutzt werden und neben Telefonie, Erreichbarkeitsanzeige, klassischen Chats, Video-Anrufen und Konferenzen auch Team-Chatbereiche sowie gemeinsame Dateiablagen beinhalten. Hinzukommen (offene) Schnittstellen, wodurch zusätzliche Anwendungen integriert werden können, so dass der Gesamtdienst funktional gegebenenfalls sehr umfangreich wird.

1.2. Zielsetzung

Ziel dieses Bausteins ist es, die Informationssicherheit als integralen Bestandteil beim erweiterten Kommunikationsspektrum von UCC-Diensten zu etablieren, ein Bewusstsein für die potenzielle Gefährdungslage dieser Anwendungen zu schaffen und Ansätze zur Vermeidung von Gefährdungen anzubieten.

1.3. Abgrenzung und Modellierung

Der Baustein APP.5.4 *Unified Communications und Collaboration (UCC)* ist auf alle IT-Systeme und Kommunikationsnetze sowie Anwendungen anzuwenden, mit denen UCC-Dienste betrieben werden.

Da UCC über Datennetze betrieben wird, sind zusätzlich zu diesem Baustein die Anforderungen der Bausteine NET.1.1 *Netzarchitektur- und Design* und NET.3.2 *Firewall* zu berücksichtigen.

Da sich der Geltungsbereich von Kommunikationsdiensten durch UCC zunehmend erweitert, gibt es eine besonders große Zahl von Überschneidungen mit anderen Bausteinen.

Dieser Baustein behandelt die folgenden Inhalte:

- die UCC-Dienste sowie Interaktion und Wechselwirkungen unterschiedlicher Dienste
- die (Soft-) Clients, die bereitgestellt werden, um diese Dienste zu benutzen und deren Funktionsumfang
- die zugehörigen Infrastrukturkomponenten, sofern diese nicht bereits durch andere Bausteine abgedeckt sind
- Themen, die sich aus dem (aus Sicht der Benutzenden) fließenden Übergang zwischen der UCC-Umgebung und weiteren Anwendungen ergeben

Folgende Inhalte sind ebenfalls von Bedeutung und werden an anderer Stelle behandelt:

- Falls über eine dedizierte TK-Anlage telefoniert wird, muss der Baustein NET.4.1 *TK-Anlagen* angewendet werden.
- Für Voice over IP (VoIP) als ein elementarer Dienst bei UCC-Diensten muss der Baustein NET.4.2 *VoIP* angewendet werden.
- Für die zentralen Server sowie diverse Endgeräte und Clients müssen die Bausteine SYS.1.1 *Allgemeiner Server* und SYS.2.1 *Allgemeiner Client* sowie gegebenenfalls spezifische Bausteine angewendet werden.
- Für die zugrundeliegenden Netze muss der Baustein NET.1.1 *Netzarchitektur und -design* angewendet werden.
- Falls UCC-Dienste aus der Cloud bereitgestellt werden, ist der Baustein OPS.2.2 *Cloud-Nutzung* anzuwenden.
- Um Dateiablagen abzusichern, die im Rahmen der UCC-Dienste bereitgestellt werden, sind insbesondere die Bausteine APP.3.3 *Fileserver* und SYS.1.8 *Speicherlösungen* anzuwenden.

Dieser Baustein behandelt **nicht** die folgenden Inhalte:

- Der E-Mail-Dienst ist in der Regel nicht Teil der UCC-Dienste. Hier ist der Baustein APP.5.3 *Allgemeiner E-Mail-Client und -Server* anzuwenden.

2. Gefährdungslage

Da IT-Grundschutz-Bausteine nicht auf individuelle Informationsverbünde eingehen können, werden zur Darstellung der Gefährdungslage typische Szenarien zugrunde gelegt. Die folgenden spezifischen Bedrohungen und Schwachstellen sind für den Baustein APP.5.4 *Unified Communications und Collaboration (UCC)* von besonderer Bedeutung.

2.1. Eingeschränkte Verfügbarkeit von UCC-Diensten

UCC-Dienste unterliegen häufig erhöhten Anforderungen an die Verfügbarkeit und gleichzeitig hängt die Funktionstüchtigkeit von UCC-Diensten von weiteren IT-Systemen und Anwendungen ab.

Falls die Datennetze, die von UCC-Diensten verwendet werden, nicht voll funktionsfähig sind, kann das die Verfügbarkeit der UCC-Dienste beeinträchtigen. So können beispielsweise Störungen im Datennetz oder bei der Internetverbindung die Qualität der Kommunikation einschränken, was eine verzögerte Sprachverständigung, Artefakte im Videobild oder den Abbruch der Verbindung verursachen kann.

Abhängigkeiten zwischen kritischen IT-Systemen können auch die Funktionsfähigkeit von weiteren Diensten oder Organisationseinheiten behindern. Wenn beispielsweise UCC als Kommunikationsplattform zwingend erforderlich ist, um das Netz wiederaufzubauen, das Netz aber benötigt wird, damit die UCC-Dienste funktionieren, dann blockieren sich beide und können nicht wiederhergestellt werden.

Häufig werden UCC-Dienste als Cloud-Dienst benutzt oder bei einem Dienstleistungsunternehmen betrieben, wodurch Störungen bei externen Netzen oder beim Dienstleistungsunternehmen zu eingeschränkter Verfügbarkeit der UCC-Dienste führen können. Gleiches gilt für den Authentisierungsdienst, über den sich die Benutzenden an den UCC-Diensten anmelden. Fällt der Authentisierungsdienst aus, können die UCC-Dienste oft nicht mehr verwendet werden.

2.2. Unzureichende Planung von UCC

Wenn UCC nicht so geplant wird, wie es auch tatsächlich benutzt werden soll, kann dies Auswirkungen auf die Funktionalität aller UCC-Dienste haben. Werden UCC-Komponenten verändert oder vermehrt benutzt, z. B. durch eine erhöhte Anzahl von Benutzenden, kann eine ursprünglich geeignete Planung unzureichend werden.

Je nach Bereitstellungsart und benutzten Diensten können sich die Anforderungen der UCC-Komponenten an die Netze stark unterscheiden. Eine auf Sprachkommunikation fokussierte UCC-Komponente im eigenen Netz kann beispielsweise andere Anforderungen an Internet- und WAN-Verbindungen stellen als ein Cloud-Dienst, der auch mobil benutzt werden soll. Werden die Netze nicht so geplant, dass sie UCC-Dienste berücksichtigen, sind die UCC-Dienste nicht ausreichend benutzbar.

Entsprechende Gefährdungen gibt es auch für die zu berücksichtigenden Endgeräte. Besonders die Videokommunikation und die zugehörigen Funktionen stellen zum Teil sehr hohe Anforderungen an die Clients. Insbesondere bei Thin Clients kann dies zu Problemen führen, da UCC-Dienste häufig ganz oder teilweise auf dem Endgerät ausgeführt werden, um Kommunikationsdatenströme zu optimieren. Clients mit unzureichender Rechenleistung können beispielsweise Aussetzer oder Artefakte bei der Videokommunikation bedingen.

2.3. Fehlerhafte Konfiguration von UCC

Eine große Zahl von Funktionen und Diensten bedeutet oft auch eine Vielzahl von Konfigurationsmöglichkeiten. Dabei können Fehlkonfigurationen auftreten.

Benutzende können oder müssen ihre UCC-Clients teilweise selbst konfigurieren. Dies kann Benutzende aufgrund der Vielzahl von Konfigurationsmöglichkeiten überfordern und fehlerhafte Konfigurationen verursachen. Wenn beispielsweise im Büro und im Homeoffice verschiedene Headsets verwendet werden, muss die Konfiguration gegebenenfalls angepasst werden. Fehlkonfigurationen können dazu führen, dass Benutzende in Besprechungen nicht hör- oder sichtbar sind oder selbst keinen Ton hören. Darüber hinaus können ungewollt Informationen preisgegeben werden, wenn Raumsysteme so konfiguriert sind, dass eingehende Kommunikationsanfragen automatisch angenommen werden.

Ebenso können durch ein unzureichendes Identitäts- und Berechtigungskonzept Fehler auftreten, wenn UCC-Dienste konfiguriert werden. Administrierende, die im Rahmen der Einrichtung von neuen Konten ebenfalls zentrale Routing-Einstellungen ändern, können hierdurch eine gravierende Fehlkonfiguration verursachen. Diese kann dazu führen, dass Daten verloren gehen, oder der UCC-Dienst ausfällt.

Zu den Fehlkonfigurationen durch ein unzureichendes Identitäts- und Berechtigungskonzept gehören auch unzureichend eingeschränkte Berechtigungen von externen Teilnehmenden. Können diese beispielsweise unberechtigt auf Inhalte von Konversationen zugreifen, so können Informationen abfließen oder manipuliert werden.

2.4. Unbefugte oder missbräuchliche Benutzung der Administrationsrechte eines UCC-Dienstes

Durch die zugewiesenen Administrationsrechte können Administrierende die UCC-Dienste gegebenenfalls tiefgreifend ändern. Werden Administrationsrechte unbefugt oder missbräuchlich benutzt, kann dies weitreichende Folgen haben. Beispielsweise können Administrationsrechte dazu benutzt werden, um einen privaten Bereich, wie einen Chat oder eine Dateiablage, der ursprünglich nur für einen begrenzten Personenkreis zugänglich war, für alle Benutzenden des UCC-Dienstes freizugeben. Hierdurch können schützenswerte Informationen durch unbefugte Personen eingesehen und gegebenenfalls verändert werden.

Weiterhin können durch vorsätzlich veränderte Routing-Konfigurationen die UCC-Dienste nicht oder nur eingeschränkt zur Verfügung stehen. Falls beispielsweise sämtliche ausgehende Anrufe durch zentrale IT-Systeme blockiert werden, kann der Dienst Telefonie nicht mehr benutzt werden.

2.5. Preisgabe von schützenswerten Informationen

Moderne UCC-Clients verfügen über eine Vielfalt an Funktionen und sind daher für viele Benutzende unübersichtlich. Dies begünstigt Fehlbedienungen, die dazu führen können, dass Informationen nicht regelkonform weitergegeben werden. Wird versehentlich ein falscher Kontakt ausgewählt, erhält dieser gegebenenfalls per Chat ungewollt schützenswerte Informationen. Ein weiteres Szenario ist, ungewollt Informationen bei einer Bildschirmfreigabe preiszugeben, wenn beispielsweise versehentlich der E-Mail-Client statt der vorgesehenen Präsentation freigegeben wird.

Vielen Benutzenden ist nicht bewusst, dass die UCC-Dienste Daten, die beispielsweise innerhalb von privaten Chats gesendet werden, in einer Cloud abspeichern. So können unbewusst Ablagerichtlinien der Institution verletzt werden. Gleiches gilt für Dateien, in denen Konversationen aufgezeichnet wurden.

Teambereiche verfügen zwar in der Regel über einen definierten Kreis von Benutzenden und entsprechende Zugriffsbeschränkungen, jedoch ist vielen Benutzenden nicht bewusst, dass die Zugriffsrechte und Mitgliedschaften nachträglich modifiziert werden können. Dadurch können weitere Personen auf alle zuvor dort abgelegten Dateien zugreifen. Darüber hinaus werden häufig öffentliche Teambereiche erstellt, denen weitere Personen ohne explizite Erlaubnis beitreten können. Dadurch können gegebenenfalls Daten von unberechtigten Personen eingesehen werden. Beispielsweise kann ein Teambereich eines Projekts ausschließlich aus internen Benutzenden bestehen. Teilnehmende laden nun interne Dokumente hoch, da alle Teammitglieder intern sind. Wenn im weiteren Projektverlauf externe Personen in den Bereich eingeladen werden, können sie auf alle bisherigen Dokumente zugreifen.

2.6. Preisgabe von personenbezogenen Informationen

UCC-Dienste erheben an vielen Stellen Daten, die auch anderen Benutzenden angezeigt werden. Dies kann dazu führen, dass personenbezogene Informationen ungewollt preisgegeben werden.

Unter anderem kann die Verfügbarkeit von Benutzenden sichtbar sein. Auch Zeitstempel an Beiträgen in Chats bis hin zu umfangreichen Auswertungen über Gespräche, Aktivitäten oder Inhalte für einzelne Benutzende können Teil einer UCC-Komponente sein. Dabei können sogar Personenprofile durch die UCC-Dienste gebildet werden. Auch Personen ohne erweiterte Berechtigungen erhalten häufig Zugriff auf diese Auswertungen. Dadurch können sie Rückschlüsse auf Arbeitszeiten und -inhalte sowie persönliche Beziehungen anderer Personen ziehen und diese beispielsweise zur Leistungsüberwachung verwenden.

Werden bei mobilem Arbeiten virtuelle Konferenzen benutzt, können ungewollt private Informationen an die Teilnehmenden der Konferenz übermittelt werden. Dazu zählen beispielsweise

Personen, die durch das Videobild laufen, persönliche Gegenstände im Hintergrund einer Videoübertragung oder Geräusche und Stimmen aus dem privaten Umfeld.

2.7. Wechselwirkungen bei UCC-Diensten

UCC-Dienste können untereinander Wechselwirkungen verursachen, welche die Funktionalität einschränken.

Um das Benutzungserlebnis zu verbessern, werden verschiedene Dienste häufig in einer Benutzungsoberfläche verknüpft. Dies kann jedoch zu Abhängigkeiten zwischen den Diensten führen. Wird beispielsweise der Videokonferenzdienst in eine Oberfläche zur Teamkollaboration integriert, kann der Videodienstes nicht mehr verwendet werden, falls die Oberfläche ausfällt.

UCC-Dienste benutzen häufig gemeinsame Ressourcen. Dies kann zu Konflikten führen, welche die Funktionalität beeinträchtigen. Werden Headsets beispielsweise von einer Telefonie- und einer Videokonferenzanwendung gleichzeitig verwendet, können die Headsets durch eine Anwendung blockiert werden und dann nicht mehr für die andere Anwendung zur Verfügung stehen.

Manche Anwendungen haben sehr hohe Ressourcenanforderungen. Wenn mehrere UCC-Dienste gleichzeitig auf einem IT-System ausgeführt werden, kann dies dazu führen, dass der Client überfordert ist und das IT-System ausfällt oder abstürzt. Wenn beispielsweise mehrere Videokonferenzanwendungen parallel im Hintergrund ausgeführt werden, kann die resultierende Auslastung des Arbeitsspeichers den Client stark beeinträchtigen.

2.8. Zugriff auf Applikationen oder Ressourcen durch Freigabe der Steuerung

Werden den Teilnehmenden innerhalb einer Konversation Desktop- oder Bildschirminhalte angezeigt, kann die Steuerung durch den Freigebenden an andere Benutzende übertragen werden. Dies kann jedoch dazu führen, dass der Freigebende die Kontrolle über weitere Handlungen verliert.

Da die Funktion zwar häufig vorhanden ist, in der Regel aber nur selten benutzt wird, sind viele Benutzende mit der Bedienung nicht vertraut, akzeptieren die Freigabe und verlieren dann die Kontrolle über ihren Client. Beispielsweise können Benutzende die Steuerung ihrer Maus freigeben, ohne zu wissen, wie die Freigabe beendet werden kann. Dadurch können Teilnehmende der Konversation möglicherweise auf weitere Anwendungen des Clients zugreifen.

2.9. Vorspiegelung falscher Identitäten

Dadurch, dass neue UCC-Dienste eingeführt werden und Externe neue Möglichkeiten erhalten, Kontakt aufzunehmen, ergeben sich neue Wege für Angreifende, die sich als vertrauenswürdige Kommunikationspartner und -partnerin ausgeben wollen, um so an vertrauliche Informationen zu gelangen.

Die Komplexität von UCC-Diensten erhöht die Wahrscheinlichkeit für Fehlbedienungen oder unbewusste Verletzungen von Sicherheitsrichtlinien durch die Benutzenden. Hyperlinks zu schädlichen Inhalten können beispielsweise geöffnet werden, weil die UCC-Dienste als interne Plattform mit erhöhter Vertrauenswürdigkeit wahrgenommen werden.

Häufig sind sich die Benutzenden nicht darüber bewusst, dass sie auch von unbekannten Externen kontaktiert werden können. Dadurch sind sie anfälliger für Social Engineering, beispielsweise über einen Chat oder eine Einladung zu einer Konversation.

Weiterhin können Angreifende ihre angezeigten Namen, ihre Stimme oder ihr Aussehen manipulieren. Dadurch kann sich zum Beispiel eine externe Person über die vermeintlich interne Kommunikationsplattform als vorgesetzte Person ausgeben, um so vertrauliche Informationen oder Dokumente direkt über den Chat zu erhalten.

3. Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.5.4 *Unified Communications und Collaboration (UCC)* aufgeführt. Der oder die Informationssicherheitsbeauftragte (ISB) ist dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Bei strategischen Entscheidungen ist der oder die ISB stets einzubeziehen.

Im IT-Grundschutz-Kompendium sind darüber hinaus weitere Rollen definiert. Sie sollten besetzt werden, insofern dies sinnvoll und angemessen ist.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Keine

Genau eine Rolle sollte *Grundsätzlich zuständig* sein. Darüber hinaus kann es noch *Weitere Zuständigkeiten* geben. Falls eine dieser weiteren Rollen für die Erfüllung einer Anforderung vorrangig zuständig ist, dann wird diese Rolle hinter der Überschrift der Anforderung in eckigen Klammern aufgeführt. Die Verwendung des Singulars oder Plurals sagt nichts darüber aus, wie viele Personen diese Rollen ausfüllen sollen.

3.1. Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für diesen Baustein vorrangig erfüllt werden.

APP.5.4.A1 Planung von UCC (B)

Es MUSS umfassend und detailliert geplant werden, wie und für welchen Zweck UCC eingesetzt werden soll. Die Planung MUSS insbesondere die Wechselwirkungen der UCC-Dienste berücksichtigen und mindestens folgende Aspekte beinhalten:

- Einsatzzwecke der vorgesehenen UCC-Dienste
- Funktionale Anforderungen an UCC als Gesamtheit und an die einzelnen UCC-Dienste
- Anforderungen zur Absicherung von UCC
- Festlegung zu Informationen und Daten, die über UCC übertragen werden dürfen
- Analyse der Kommunikation und der Abhängigkeiten von UCC-Diensten untereinander
- Produkt- und Dienstauswahl ausgehend von den definierten Anforderungen
- Aufstellen von organisatorischen Regelungen, um die UCC-Dienste zu benutzen

Bei der Planung MUSS berücksichtigt werden, wie UCC in die IT-Infrastruktur der Institution integriert wird. Hierbei MUSS insbesondere betrachtet werden, ob und wie die Systeme der UCC-Dienste innerhalb des Netzes separiert werden sollen und welche Schnittstellen zu weiteren benutzten Anwendungen notwendig sind.

APP.5.4.A2 Berücksichtigung von UCC in der Netzplanung (B)

Bevor UCC-Dienste eingeführt werden, MUSS geprüft werden, ob das Netz die UCC-spezifischen Leistungsparameter erfüllt. Falls die Leistungsparameter nicht erfüllt werden, MUSS festgelegt werden, wie hiermit umgegangen wird.

Sollen UCC-Dienste benutzt werden, SOLLTEN im Rahmen der allgemeinen Netzplanung insbesondere folgende Aspekte berücksichtigt werden:

- Erfüllung der UCC-spezifischen Leistungsparameter wie Paketverlust, Jitter und Latenz
- Netzkapazitäten (Bandbreite) für die festgelegte Benutzung der UCC-Dienste wie Videokonferenzen

- Berücksichtigung von Power over Ethernet (PoE) für stationäre Endgeräte
- Verfügbarkeit von WLAN für mobile Endgeräte

Falls die UCC-Dienste erweitert werden, SOLLTEN diese Aspekte erneut geprüft werden.

APP.5.4.A3 Initiales und regelmäßiges Testen der UCC-Dienste (B)

Für die UCC-Dienste MÜSSEN initial Tests durchgeführt werden, die verifizieren, dass die UCC-Komponenten untereinander und mit anderen UCC-Diensten interferenzfrei funktionieren. Ebenfalls MÜSSEN Tests mit ausgewählten Benutzenden durchgeführt werden, um insbesondere Wechselwirkungen mit anderen Anwendungen zu überprüfen.

Diese Tests SOLLTEN wiederholt werden, wenn die UCC-Dienste erweitert oder verändert werden.

Zusätzlich SOLLTE die Konfiguration der UCC-Dienste in regelmäßigen Abständen auf Plausibilität und Konformität für die festgelegten Einsatzzwecke überprüft werden.

APP.5.4.A4 Deaktivierung nicht benötigter Funktionen und Dienste (B)

UCC-Dienste DÜRFEN NUR mit dem geringsten notwendigen Funktionsumfang betrieben werden. Die verfügbaren Funktionen und Dienste MÜSSEN entsprechend der definierten Einsatzzwecke ausgewählt werden. Dabei MÜSSEN gegebenenfalls auftretende Wechselwirkungen zwischen den verschiedenen Komponenten eines UCC-Dienstes berücksichtigt werden. Außerdem MÜSSEN insbesondere die folgenden Dienste und Funktionen auf Notwendigkeit geprüft und gegebenenfalls deaktiviert oder eingeschränkt werden:

- Speicherung von personenbezogenen Daten durch die UCC-Komponenten
- Zugriff und Verarbeitung von personenbezogenen Daten durch Benutzende und den UCC-Dienst
- Benutzbarkeit von Funktionen wie Chat, Erreichbarkeitsstatus, Dateiablagen oder Team-Bereiche durch externe Teilnehmende
- Senden von Daten und Dateien an externe UCC-Dienste

Konversationsbezogene Log-Daten DÜRFEN NUR in minimal notwendigem Umfang gespeichert werden. Funktionen und Dienste, die auf (dauerhaft) gespeicherte Log-Daten zugreifen, MÜSSEN auf ihre Notwendigkeit geprüft und gegebenenfalls deaktiviert werden.

APP.5.4.A5 Rollen- und Berechtigungskonzept für UCC (B)

Das Rollen- und Berechtigungskonzept MUSS um UCC-spezifische Definitionen von Rollen und Berechtigungen ergänzt werden. Solche Definitionen MÜSSEN sowohl für alle internen Benutzenden als auch für die externen Benutzenden getroffen werden. Es MÜSSEN folgende Aspekte berücksichtigt werden:

- Berechtigungen zur zielgerichteten Benutzung von UCC-Diensten gemäß festgelegter Einsatzzwecke
- Berechtigungen zur Anpassung der Konfiguration von Konversationen
- Berechtigungen für spezielle Funktionen von UCC-Diensten wie Aufzeichnung von Konversationen und Zugriff auf Dateiablagen eines UCC-Dienstes

Darüber hinaus MÜSSEN die Berechtigungen der Konten ebenfalls auf das notwendige Minimum reduziert werden. Dienste, die nur für einen Teil der Benutzenden zur Verfügung stehen, DÜRFEN NICHT für die restlichen Benutzenden zugänglich sein.

Zudem SOLLTEN nur Benutzende mit einer entsprechenden Berechtigung auf Daten wie Aufzeichnungen oder Dateiablagen zugreifen können.

Die Festlegungen MÜSSEN festgehalten, regelmäßig und anlassbezogen geprüft und aktualisiert werden.

APP.5.4.A6 Verschlüsselung von UCC-Daten (B)

Sämtliche Kommunikation über unzureichend vertrauenswürdige Netze MUSS mit sicheren Verfahren verschlüsselt werden, sofern dies durch die jeweilige UCC-Komponente unterstützt wird. Falls eine Verschlüsselung für einzelne UCC-Komponenten oder einzelne Konversationen nicht möglich ist, MUSS die Festlegung, welche Informationen über diese UCC-Komponenten übertragen werden dürfen, geprüft und gegebenenfalls angepasst werden.

Insbesondere MUSS bei anwendungsübergreifender Kommunikation festgelegt werden, für welche Konversationen die Medienströme und die Signalisierung und welche weiteren Daten wie Chat oder Dateitransfer verschlüsselt übertragen werden müssen.

Dateiablagen, die persistente personenbezogene oder vertrauliche Daten enthalten, MÜSSEN mit Hilfe von sicheren Verschlüsselungsmechanismen abgesichert werden. Hierbei MÜSSEN sowohl interne Dateiablagen der UCC-Dienste als auch über Schnittstellen angebundene externe Dateiablagen berücksichtigt werden.

Die Benutzenden MÜSSEN zudem über den Status der Verschlüsselung innerhalb von Konversationen informiert werden.

APP.5.4.A7 Regelungen für eine sichere Benutzung der UCC-Dienste (B)

Konversationen, die mit Hilfe von UCC durchgeführt werden, MÜSSEN abgesichert werden. Hierbei MÜSSEN folgende Aspekte berücksichtigt werden:

- Auswahl der Teilnehmenden entsprechend dem Inhalt der Konversation
- zusätzliche Absicherung von geplanten Konversationen über Mechanismen wie PIN oder ein Passwort
- Zuweisung von Moderationsrechten an ausgewählte Benutzende der einladenden Institution
- Regelungen zum Umgang mit Aufzeichnungen von Konversationen
- Regelungen für Endgeräte, die von mehreren Benutzenden verwendet werden

Die Benutzenden MÜSSEN über Funktionen informiert werden, über die Konversationen abgesichert werden können. Ebenso MÜSSEN die Benutzenden dafür sensibilisiert werden, wie die UCC-Dienste sicher benutzt werden, insbesondere für externe Chats oder Videokonferenzen.

3.2. Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für diesen Baustein. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.5.4.A8 Einsatz eines Session Border Controller am Provider-Übergang (S)

Für die UCC-Kommunikation über eingeschränkt vertrauenswürdige Netze SOLLTE mindestens für Sprachdienste ein Session Border Controller (SBC) am Netzübergang bzw. beim Übergang zum SIP-Provider eingesetzt werden. Der SBC SOLLTE als Verschlüsselungsendpunkt die Signalisierung und die Medienströme terminieren. Der SBC SOLLTE für die Signalisierung und die Medienströme Filterfunktionen unterstützen, die die jeweiligen Konversationen zusätzlich absichern.

APP.5.4.A9 Sichere Konfiguration von UCC (S)

Um UCC sicher zu konfigurieren, SOLLTEN mindestens die folgenden Aspekte berücksichtigt werden:

- Verschlüsselung von Signalisierungs- und Mediendaten auch auf vertrauenswürdigen Übertragungsstrecken
- Absicherung von gespeicherten Daten, insbesondere Festlegung für Zugriffsberechtigung auf Aufzeichnungen von Konversationen

- Einschränkung der zur Verfügung stehenden Dienste auf ausschließlich interne Benutzende
- Einschränkung der Übertragung von Erreichbarkeitsinformationen

Gespeicherte Daten SOLLTEN verschlüsselt werden. Auf gespeicherte Daten SOLLTEN Benutzende nur nach vorheriger Authentisierung zugreifen können.

Der IT-Betrieb SOLLTE sichere Einstellungen vorgeben, die verwendet werden, wenn Konversationen erstellt werden. Für textbasierte Konversationen SOLLTE ein Malware-Schutz aktiviert werden.

Die Umsetzung SOLLTE festgehalten, regelmäßig und anlassbezogen auf Einhaltung der Vorgaben geprüft und angepasst werden.

APP.5.4.A10 Absicherung und Einschränkung von Auswertungen von Inhalten (S)

Die Art einer (automatischen) Auswertung von Konversationsinhalten SOLLTE schon im Vorfeld sorgfältig geprüft werden und ihr Nutzen gegen den Schutzbedarf abgewogen werden. Es SOLLTE die Möglichkeit bestehen, entsprechende Funktionen entweder vollständig oder pro Konversation zu deaktivieren und eine inhaltliche Auswertung der Kommunikation zu verhindern. Besondere Beachtung SOLLTEN KI-Funktionen und die Übertragung von Daten an Onlinedienste erhalten.

Werden Inhalte über den Zweck der Konversation hinausgehend ausgewertet, MUSS dazu auch eine Zustimmung der an der Konversation teilnehmenden Personen eingeholt werden.

Werden während der Auswertung von Konversationen persistente Daten erzeugt, SOLLTEN für diese geeignete Schutzmaßnahmen umgesetzt werden.

3.3. Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für diesen Baustein exemplarische Vorschläge für Anforderungen aufgeführt, die über dasjenige Schutzniveau hinausgehen, das dem Stand der Technik entspricht. Die Vorschläge SOLLTEN bei erhöhtem Schutzbedarf in Betracht gezogen werden. Die konkrete Festlegung erfolgt im Rahmen einer individuellen Risikoanalyse.

APP.5.4.A11 Sicherstellung der Verfügbarkeit von Kommunikationsdiensten (H)

Die Verfügbarkeit von UCC-Diensten SOLLTE insbesondere durch folgende technische Maßnahmen sichergestellt werden:

- redundante Auslegung zentraler Server und Dienste
- Benutzung von Call Admission Control (CAC) zur Qualitätssicherung von Telefonie und Video-Diensten
- möglichst autark funktionierende UCC-Dienste

Darüber hinaus SOLLTE bei Cloud-basierten UCC-Diensten der Cloud-Provider sowie der Internet-Provider ausfallsicher an das eigene Netz angebunden werden.

Zudem SOLLTE ein SIP-Provider, der Rufnummern bereitstellt und den Übergang ins öffentliche Telefonnetz bildet, hochverfügbar an das eigene Netz angebunden werden.

Die Verfügbarkeit SOLLTE durch ein Monitoring der UCC-Dienste überwacht werden.

APP.5.4.A12 Einbindung von UCC in die Notfallplanung (H)

Ausgehend von einer Business Impact Analyse SOLLTE geprüft werden, welche UCC-Dienste in der Notfallplanung berücksichtigt werden sollen. Hierbei SOLLTEN in Notfallsituationen für einzelne UCC-Dienste alternative Anwendungen bereitgestellt werden. Insbesondere SOLLTE für die Benutzenden die Erreichbarkeit von wichtigen Diensten wie der Notruf gewährleistet werden.

Zudem SOLLTE ein Notfallplan für die UCC-Dienste erstellt werden, in dem notwendige Konfigurationen sowie Routing-Anpassungen, die über den Telefonie-Provider realisiert werden, behandelt werden.

Ebenso SOLLTE der Wiederanlauf der UCC-Komponenten und -Dienste unter Berücksichtigung der Wechselwirkungen innerhalb der UCC-Dienste festgelegt werden.

APP.5.4.A13 Sichere Administration von SIP-Trunks (H)

Wenn SIP-Trunks administriert werden, SOLLTE für folgende Tätigkeiten ein 4-Augen-Prinzip angewendet werden:

- Änderungen an Routing-Konfigurationen
- Änderungen an Parametern, die im Rahmen von Call Admission Control benutzt werden
- Änderungen hinsichtlich der Verschlüsselung sowohl in Richtung des eigenen Netzes als auch in Richtung des Provider-Netzes
- Änderungen an weiteren sicherheitsrelevanten Konfigurationen wie der lokalen Speicherung von Verbindungsdaten

APP.5.4.A14 Ende-zu-Ende-Verschlüsselung (H)

Für UCC-Kommunikation SOLLTE eine sichere Ende-zu-Ende-Verschlüsselung benutzt werden. Die Ende-zu-Ende-Verschlüsselung SOLLTE sich sowohl auf die Signalisierung als auch auf die Mediendaten von Audio- und Videokommunikation mit zwei oder mehr Teilnehmenden erstrecken.

Bei Konversationen zwischen UCC-Diensten von verschiedenen Herstellenden SOLLTEN die übertragenen Informationen eingeschränkt werden, sofern eine Ende-zu-Ende-Verschlüsselung nach Stand der Technik nicht möglich ist.

APP.5.4.A15 Einschränkung von KI-Funktionen (H)

Die Benutzung von KI-Funktionen SOLLTE deaktiviert oder auf ein Minimum reduziert werden. Ist eine permanente Deaktivierung nicht möglich oder erwünscht, SOLLTE festgelegt werden, dass Benutzende der UCC-Dienste zu Beginn einer Konversation zielgerichtet KI-Funktionen deaktivieren, falls dies möglich ist.

APP.5.4.A16 Einsatz eines SBC an weiteren Netzübergängen (H)

Ergänzend zu einem SBC am Netzübergang zum Provider, SOLLTEN weitere SBC an internen Netzübergängen eingesetzt werden. Hierbei SOLLTEN insbesondere Netzübergänge zwischen Netzsegmenten mit unterschiedlichem Schutzbedarf berücksichtigt werden.

Der SBC SOLLTE sicherstellen, dass die Verschlüsselungsmechanismen an den SBC-gesicherten Netzsegmentübergängen anforderungskonform realisiert werden.

APP.5.4.A17 Einschränkung der Benutzung von UCC-Diensten (H)

Folgende Aspekte SOLLTEN mindestens berücksichtigt werden, um die UCC-Dienste sowie die übertragenen Daten zusätzlich abzusichern:

- Einschränkung der Dienste entsprechend des Schutzbedarfs der übertragenen Informationen
- Benutzung einer Multi-Faktor-Authentisierung für Benutzende
- Deaktivierung von Funktionen für externe Benutzende
- Deaktivierung der Speicherung von Metadaten
- Einschränkung der Sichtbarkeit von kommunikationsbezogenen Daten für Administrierende

Darüber hinaus SOLLTEN zusätzliche technische und organisatorische Vorkehrungen getroffen werden, um Konversationen über die Vergabe von PINs bzw. Passwörtern hinaus abzusichern.

APP.5.4.A18 Einbindung von UCC in ein Sicherheitsmonitoring (H)

Die zentralen UCC-Komponenten SOLLTEN durch ein Sicherheitsmonitoring überwacht werden. Dies SOLLTE mindestens für Komponenten umgesetzt werden, die wie Multipoint Control Units Verschlüsselungsendpunkte realisieren oder die wie SBCs an Vertrauensgrenzen positioniert sind.

Wird für die IT der Institution ein System zur zentralen Detektion und automatisierten Echtzeitüberprüfung von Ereignismeldungen eingesetzt, SOLLTEN die zentralen UCC-Komponenten hierin eingebunden werden.

4. Weiterführende Informationen

4.1. Wissenswertes

Für die Auswahl von Verschlüsselungsverfahren und Schlüssellängen sollte die technische Richtlinie „BSI-TR-02102: Kryptographische Verfahren: Empfehlungen und Schlüssellängen“ des BSI beachtet werden.