



NET.4: Telekommunikation

NET.4.2: VoIP

1 Beschreibung

1.1 Einleitung

Voice over IP (VoIP) bezeichnet das Telefonieren über Datennetze, insbesondere über das Internet. Um Signalisierungsinformationen zu übertragen, beispielsweise bei einem Anruf, werden spezielle Signalisierungsprotokolle eingesetzt. Die eigentlichen Nutzdaten wie Sprache oder Video werden mit Hilfe eines Medientransportprotokolls übermittelt. Beide Protokolle werden jeweils benötigt, um eine Multimediaverbindung aufzubauen und aufrechtzuerhalten. Bei einigen Verfahren wird nur ein Protokoll sowohl für die Signalisierung als auch für den Medientransport benötigt.

1.2 Zielsetzung

Dieser Baustein betrachtet die Sicherheitsaspekte der Endgeräte und Vermittlungseinheiten (Middleware) von VoIP. Die hier beschriebenen Komponenten gleichen hinsichtlich ihrer Funktionalität den im Baustein NET 4.1 *TK-Anlagen* beschriebenen Telekommunikationsanlagen.

1.3 Abgrenzung und Modellierung

Der Baustein NET.4.2 *VoIP* ist auf alle Kommunikationsnetze anzuwenden, in denen VoIP eingesetzt wird. Da VoIP über Datennetze betrieben wird, sind zusätzlich zu diesem Baustein die Anforderungen der Bausteine NET.1.1 *Netzarchitektur- und Design* oder NET.3.2 *Firewall* geeignet mit zu berücksichtigen.

In diesem Baustein werden die Sicherheitsaspekte von VoIP-Komponenten und der Sprachübertragung über VoIP betrachtet. Tauschen leitungsvermittelnde TK-Anlagen Informationen untereinander über ein Datennetz aus, ist dieser Baustein ebenfalls anzuwenden.

Die spezifischen Gefährdungen und Anforderungen von klassischen TK-Anlagen sowie Hybrid-Anlagen werden in dem Baustein NET 4.1 *TK-Anlagen* betrachtet.

Oft wird VoIP-Software nicht auf eigens dafür vorgesehene Hardware betrieben, sondern auf Standard-IT. Werden Softphones auf Clients installiert, sollten die Anforderungen des Bausteins SYS.2.1 *Allgemeiner Client* sowie der betriebssystemspezifischen Bausteine berücksichtigt werden. Wird Software für VoIP auf Servern betrieben, sollten neben den Anforderungen der betriebssystemspezifischen Bausteine die Anforderungen des Bausteins SYS.1.1 *Allgemeiner Server* erfüllt werden.

VoIP sollte grundsätzlich im Rahmen der Bausteine ORP.4 *Identitäts- und Berechtigungsmanagement*, OPS.1.1.3 *Patch- und Änderungsmanagement*, OPS.1.1.5 *Protokollierung*, sowie OPS.1.1.2 *ordnungsgemäße IT-Administration* mit berücksichtigt werden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein NET.4.2 *VoIP* von besonderer Bedeutung.

2.1 Fehlerhafte Konfiguration der VoIP-Middleware

Eine VoIP-basierte Telefonanlage kann in ähnlicher Weise von Fehlkonfigurationen betroffen sein wie eine leitungsvermittelnde Telefonlösung. So könnten beispielsweise Telefonbenutzern falsche Telefonnummern zugeordnet werden oder die gesamte Telefoninfrastruktur könnte ausfallen. Auch tendenziell unkritische Fehler, wie ein falsch geschriebener Name im Telefonbuch, können nicht ausgeschlossen werden.

Wird mittels VoIP kommuniziert, sind in der Regel mehrere IT-Systeme beteiligt. Wird SIP als Initialisierungsprotokoll eingesetzt, werden meist Systeme wie *Registriere*, *SIP-Proxy-Server* und *Location-Server* für die Kommunikation benötigt. Ändert sich die VoIP-Infrastruktur, müssen alle IT-Systeme angepasst werden. Dadurch können leicht Konfigurationsfehler entstehen. Auch wenn sich alle Dienste auf einem Server befinden, müssen diese häufig einzeln konfiguriert werden. Wird nur ein System fehlerhaft geändert, kann die gesamte Telefoninfrastruktur möglicherweise nicht mehr genutzt werden.

2.2 Fehlerhafte Konfiguration der VoIP-Komponenten

Unabhängig davon, ob es sich bei VoIP-Komponenten um dedizierte Hardware („Appliances“) oder softwarebasierte Systeme handelt, ist die Konfiguration entscheidend für die fehlerfreie Funktion des Systems. Neben den Einstellungen zur Signalisierung, die bei der Planung festgelegt wurden, spielt das Übertragungsverfahren für die Medienströme eine wichtige Rolle. Durch ein Kompressionsverfahren kann die Größe der Datenpakete mit den Sprachinformationen verkleinert werden.

Durch die fehlerhafte Konfiguration des Übertragungsverfahrens können Probleme bei der Übertragung auftreten. Wird ein ungeeignetes Verfahren eingesetzt und werden Sprachinformationen zu stark komprimiert, verschlechtert sich oft die Sprachqualität. Wird hingegen ein Verfahren gewählt, das eine zu geringe Kompression vornimmt, wird der Nachrichtenstrom nicht ausreichend vermindert und das Datennetz kann überlastet werden.

2.3 Abhören von Telefongesprächen

Wenn Telefongespräche oder Daten unverschlüsselt übertragen werden, könnten Angreifer grundsätzlich Informationen mithören oder mitlesen. So könnten sie beispielsweise die Telefonkabel direkt anzapfen oder an einer zwischen den Gesprächsteilnehmern vermittelnden TK-Anlage lauschen. Bei VoIP können Telefongespräche und Datenübertragungen sogar einfacher als bei klassischen TK-Anlagen abgehört werden. Alle Sprachinformationen werden innerhalb eines Medienstroms, beispielsweise mit dem Realtime Transport Protocol (RTP), übertragen. Durch Techniken wie Spoofing und Sniffing stehen bei VoIP den Angreifern auch alle Möglichkeiten von Angriffen in Datennetzen zur Verfügung.

Bei vielen TK-Anlagen können Anrufer den Empfängern Nachrichten hinterlassen, wenn diese zum Zeitpunkt des Anrufs telefonisch nicht erreichbar sind. Einige Anrufbeantworter, vor allem bei VoIP-Anlagen, verschicken diese Informationen als Audio-Datei in einer E-Mail. Der Inhalt dieser E-Mail könnte direkt von einem Angreifer abgefangen und angehört werden.

2.4 Missbrauch frei zugänglicher Telefonanschlüsse

Oft werden Telefone betrieben, die keinem Benutzer persönlich zugeordnet sind. Einige dieser Telefone, wie zum Beispiel solche in Druckerräumen, sind nur einem eingeschränkten Personenkreis zugänglich. Andererseits sind Telefone häufig in Bereichen zu finden, die für Besucher frei zugänglich sind. Dazu zählen beispielsweise Parkhäuser oder Bereiche vor Zugangskontrollsystemen. Besitzen diese Telefone

ein elektronisches Telefonbuch, in dem interne Telefonnummern gespeichert sind, könnten diese Nummern ungewollt nach außen gelangen.

Beim Einsatz von VoIP-Telefonen in frei zugänglichen Bereichen können weitere Aspekte relevant sein. Denn sie haben einen hohen Software-Anteil und werden häufig in Datennetzen betrieben, die auch für andere IT-Anwendungen genutzt werden. Ein Angreifer könnte deshalb durch den direkten Zugriff auf Geräteinformationen versuchen, Schwachstellen in der VoIP-Software auszunutzen oder selbst schädliche Software zu installieren.

VoIP-Telefone müssen an ein Datennetz angeschlossen sein. Ein Angreifer könnte an diesen Netzanschluss ein mobiles IT-System anschließen und so unter Umständen auf das von außen durch eine Firewall geschützte interne Netz zugreifen. Diesen Zugang kann er möglicherweise für Angriffe auf die Vertraulichkeit, Integrität und Verfügbarkeit ausnutzen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins *NET.4.2 VoIP* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Erfüllung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	Rollen
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Benutzer

3.1 Basis-Anforderungen

Die folgenden Anforderungen **MÜSSEN** für den Baustein *NET.4.2 VoIP* vorrangig erfüllt werden:

NET.4.2.A1 Planung des VoIP-Einsatzes (B)

Die Bedingungen, unter denen VoIP eingesetzt werden soll, **MÜSSEN** festgelegt werden. Es **MUSS** unter anderem entschieden werden, ob vollständig oder partiell auf VoIP umgestiegen werden soll. Besondere Anforderungen an die Verfügbarkeit von VoIP oder an die Vertraulichkeit und Integrität der Telefonate bzw. der Signalisierungsinformationen **SOLLTEN** vorab ermittelt werden. Geeignete Signalisierungs- und Medientransportprotokolle **MÜSSEN** vor dem Einsatz ausgewählt werden.

Es **SOLLTE** entschieden werden, ob und wie die VoIP-Infrastruktur an öffentliche (Daten-)Netze angebunden werden soll. Die Kapazitäten und das Design von vorhandenen Datennetzen **SOLLTEN** bei der Planung berücksichtigt werden.

NET.4.2.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

NET.4.2.A3 Sichere Administration und Konfiguration von VoIP-Endgeräten (B)

Nicht benötigte Funktionen der Endgeräte **MÜSSEN** deaktiviert werden. Die Konfigurationseinstellungen **DÜRFEN NICHT** unberechtigt geändert werden. Alle Sicherheitsfunktionen der Endgeräte **SOLLTEN** vor dem produktiven Einsatz getestet werden. Die eingesetzten Sicherheitsmechanismen und die verwendeten Parameter **SOLLTEN** dokumentiert werden.

NET.4.2.A4 Einschränkung der Erreichbarkeit über VoIP (B)

Es MUSS entschieden werden, wie externe Gesprächspartner auf die VoIP-Architektur zugreifen können. Es MUSS verhindert werden, dass IT-Systeme aus unsicheren Netzen direkte Datenverbindungen auf die VoIP-Komponenten der Institution aufbauen können. Wenn alle ein- und ausgehenden Verbindungen über ein zentrales IT-System abgewickelt werden sollen, SOLLTE sichergestellt werden, dass alle Signalisierungs- und Sprachinformationen zwischen dem öffentlichen und dem privaten Datennetz nur über dieses autorisierte IT-System ausgetauscht werden.

NET.4.2.A5 Sichere Konfiguration der VoIP-Middleware (B)

Die VoIP-Komponenten MÜSSEN so konfiguriert sein, dass sie den Schutzbedarf angemessen erfüllen. Die Default-Konfigurationen der VoIP-Middleware MÜSSEN vor der produktiven Inbetriebnahme angepasst werden. Alle Installations- und Konfigurationsschritte SOLLTEN so dokumentiert werden, dass die Installation und Konfiguration durch einen sachkundigen Dritten anhand der Dokumentation nachvollzogen und wiederholt werden können. Alle nicht benötigten Dienste der VoIP-Middleware MÜSSEN deaktiviert werden.

NET.4.2.A6 ENTFALLEN (B)

Diese Anforderung ist entfallen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein NET.4.2 VoIP. Sie SOLLTEN grundsätzlich erfüllt werden.

NET.4.2.A7 Erstellung einer Sicherheitsrichtlinie für VoIP (S)

Die zentralen sicherheitstechnischen Anforderungen an VoIP sowie das zu erreichende Sicherheitsniveau SOLLTEN in der institutionsweiten Sicherheitsrichtlinie aufgenommen werden. In dieser Sicherheitsrichtlinie SOLLTEN alle allgemeinen sicherheitstechnischen Vorgaben konkretisiert werden. Außerdem SOLLTEN in der Richtlinie die Vorgaben für den Betrieb und die Nutzung der VoIP-Komponenten geregelt sein. Hierbei SOLLTEN auch die verschiedenen VoIP-Funktionen, wie zum Beispiel Voicemails, betrachtet werden. Die VoIP-Sicherheitsrichtlinie SOLLTE allen beteiligten Personen und Gruppen zugänglich und bekannt sein.

NET.4.2.A8 Verschlüsselung von VoIP (S)

Es SOLLTE entschieden werden, ob und welche Sprach- und Signalisierungsinformationen verschlüsselt werden sollen. Generell SOLLTEN alle VoIP-Datenpakete, die das gesicherte LAN verlassen, durch geeignete Sicherheitsmechanismen geschützt werden. Die Benutzer SOLLTEN über die Nutzung der VoIP-Verschlüsselung informiert werden.

NET.4.2.A9 Geeignete Auswahl von VoIP-Komponenten (S)

Bevor VoIP-Komponenten beschafft werden, SOLLTE eine Anforderungsliste erstellt werden. Anhand der Anforderungsliste SOLLTEN die am Markt erhältlichen Produkte bewertet werden. Diese Anforderungsliste SOLLTE alle Merkmale zur Erreichung des angestrebten Sicherheitsniveaus umfassen. Es SOLLTE geregelt werden, wie die am Markt erhältlichen Produkte gemäß der Anforderungsliste bewertet werden können.

NET.4.2.A10 ENTFALLEN (S)

Diese Anforderung ist entfallen.

NET.4.2.A11 Sicherer Umgang mit VoIP-Endgeräten [Benutzer] (S)

Benutzer, die VoIP-Endgeräte einsetzen, SOLLTEN über die grundlegenden VoIP-Gefährdungen und Sicherheitsmaßnahmen informiert sein. Außerdem SOLLTEN sie geeignete Passwörter zur Absicherung von Voicemails auswählen.

NET.4.2.A12 Sichere Außerbetriebnahme von VoIP-Komponenten (S)

Wenn VoIP-Komponenten außer Betrieb genommen oder ersetzt werden, SOLLTEN alle

sicherheitsrelevanten Informationen von den Geräten gelöscht werden. Nach dem Löschvorgang SOLLTE überprüft werden, ob die Daten auch tatsächlich erfolgreich entfernt wurden. Vertrauliche Informationen SOLLTEN auch von Backup-Medien gelöscht werden. Alle Beschriftungen, insbesondere der Endgeräte, SOLLTEN vor der Entsorgung entfernt werden. Es SOLLTE frühzeitig mit Herstellern, Händlern beziehungsweise Service-Unternehmen geklärt werden, welche Maßnahmen zur Löschung sicherheitsrelevanter Informationen mit den Vertrags- und Garantiebedingungen vereinbar sind.

NET.4.2.A13 Anforderungen an eine Firewall für den Einsatz von VoIP (S)

Es SOLLTE überprüft werden, ob die bestehende Firewall für den Einsatz von VoIP angepasst werden kann. Ist dies nicht der Fall, SOLLTE eine zusätzliche Firewall hierfür beschafft und installiert werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein NET.4.2 VoIP exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

NET.4.2.A14 Verschlüsselung der Signalisierung (H)

Die Integrität und Vertraulichkeit der Signalisierungsinformationen SOLLTE durch geeignete kryptogarisches Verfahren gewährleistet werden. Nicht nur die Nutzdaten, sondern auch die Authentisierungsdaten SOLLTEN durchgängig verschlüsselt werden. Der Zugriff auf das VoIP-Gateway SOLLTE durch VoIP-Adressen und H.323-Identitäten so weit wie möglich eingeschränkt werden. Es SOLLTEN zusätzlich Ende-zu-Ende-Sicherheitsmechanismen für den Medientransport und die Signalisierung benutzt werden. Es SOLLTE dokumentiert werden, wie die Signalisierung geschützt wird.

NET.4.2.A15 Sicherer Medientransport mit SRTP (H)

Mediendaten und Informationen zur Steuerung dieser Daten, die über das Real-Time Transport Protocol (RTP) übertragen werden, SOLLTEN in geeigneter Weise geschützt werden. Die Nutzdaten SOLLTEN durch den Einsatz von Secure Real-Time Transport Protocol (SRTP) beziehungsweise Secure Real-Time Control Protocol (SRTCP) geschützt werden. Die sicherheitsrelevanten Optionen der Implementierung des Protokolls SOLLTEN dokumentiert werden.

NET.4.2.A16 Trennung des Daten- und VoIP-Netzes (H)

Das VoIP-Netz SOLLTE in geeigneter Weise vom Datennetz getrennt werden. Es SOLLTE geregelt werden, wie mit Geräten umzugehen ist, die auf das VoIP- und Datennetz zugreifen müssen. VoIP-Endgeräte in einem VoIP-Netz SOLLTEN NUR die vorgesehenen VoIP-Verbindungen zu anderen IT-Systemen aufbauen können.

4 Weiterführende Informationen

4.1 Wissenswertes

Das BSI hat im Rahmen der Technischen Leitlinien die „BSI-TL-02013 für organisationsinterne Telekommunikationssysteme mit erhöhtem Schutzbedarf“ veröffentlicht.

Das National Institute of Standards and Technology (NIST) hat im Rahmen seiner Special Publications die NIST Special Publication 800-5 zu „Security Considerations for Voice Over IP Systems“ veröffentlicht.

5 Anlage: Kreuzreferenztablelle zu elementaren Gefährdungen

Die Kreuzreferenztablelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tablelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten

Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein NET.4.2 VoIP von Bedeutung.

- G 0.9 Ausfall oder Störung von Kommunikationsnetzen
- 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 0.26 Fehlfunktion von Geräten oder Systemen
- G 0.27 Ressourcenmangel
- G 0.28 Software-Schwachstellen oder -Fehler
- 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 0.40 Verhinderung von Diensten (Denial of Service)
- G 0.45 Datenverlust
- G 0.46 Integritätsverlust schützenswerter Informationen