Informationssicherheit

Netzwerk

Regelung Nr. 03.02.03

Internet-Telefonie / Video-Telefonie

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.0

Inhalt

I. Zweck

Das Ziel dieser Regelung ist die Festlegung von Sicherheitsanforderungen für IP-basierte Sprachkommunikation (VoIP), IP-basierte Videokommunikation und IP-basierte Sprach- und Videokonferenzen.

1. Allgemeines

1.1. Allgemeine Schutzziele

Je nach Land und Gesellschaft, in der VoIP angewendet wird, müssen unterschiedliche rechtliche und gesellschaftsspezifische Anforderungen beachtet werden. Für jedes VoIP-Implementierungsprojekt muss zunächst eine vollständige Liste mit Anforderungen ausgearbeitet werden.

1.1.1 Rechtliche Anforderungen

In jedem Land gelten unterschiedliche rechtliche Anforderungen, die erfüllt werden müssen. Jede Gesellschaft sollte die jeweiligen rechtlichen Bestimmungen[1] erkennen, dokumentieren und einhalten. Die Hauptthemen für die Rechtsvorschriften sind wie folgt[2]:

- Datenschutz
- Notrufe
- Gesetzeskonforme Überwachung, Vorratsdatenspeicherung:
  Je nach Ort des Hauptsitzes oder der jeweiligen Nutzung der Infrastruktur kann eine Schnittstelle zur gesetzeskonformen Überwachung oder Vorratsdatenspeicherung verpflichtend sein.
- Private Nutzung von VoIP-Infrastruktur

1.1.2 Anforderungen für Gesellschaften:

Dieses Dokument legt die konzernweiten Mindestanforderungen fest. Jede Gesellschaft sollte prüfen, ob weitere Anforderungen[3] erforderlich sind und diese dokumentieren. Erkannte gesellschaftsspezifische Anforderungen müssen beachtet werden.

1.2. Analyse der allgemeinen Sicherheitsanforderungen

Die allgemeinen Schutzziele sind in den Informationssicherheit Handlungsleitlinien[4] festgelegt. Die grundlegenden Sicherheitsanforderungen für die Schutzziele für die VoIP-Infrastruktur sowie Beispiele für Maßnahmen zum Schutz dieser Ziele werden in der folgenden Tabelle dargestellt.

[1] Siehe Anhang B.1.2

[2] Siehe Anhang B.1.3

[3] Siehe Anhang B.1.1

[4] Siehe Anhang A.1.2

Schutzziele	**Grundlegende Sicherheitsanforderungen für die VoIP-Infrastruktur (bindend)**	**Sicherheitsmaßnahmen in der VoIP-Infrastruktur (Umsetzungsleitlinien, nicht bindend)**
Vertraulichkeit	• Sprach-/Videodaten, Signaldaten und Call Data Records sind als sensible Daten einzustufen. • Konzernklassifizierung „Vertraulich“ • Absicherung von Sprach-/Videokommunikationsdaten, Verhindern des Abgreifens von Kommunikationsdaten • Absicherung von Call Data Records aller Kommunikationsarten	• Verwendung von sicheren Kommunikations- und Signalisierungsprotokollen wie SRTP, SIPS
Integrität	• Absicherung von Call Data Records für korrekte Abrechnung und Anrufrückverfolgbarkeit (falls erforderlich) • Absicherung von Adressbuchdaten gegen unerlaubter Manipulation • Absicherung von Systemverwaltungsprotokollen (Audit-Trail-Protokolle)	• Verwendung von sicheren Kommunikationstransport- und Signalisierungsprotokollen wie SRTP, SIPS • Sichere Speicherung von Call Data Records und Audit-Trails. Implementierung einer sicheren Authentifizierung für den Administrationszugriff.
Verfügbarkeit	• Es ist eine Verfügbarkeit von 99,9 % (Referenzzeitraum: 1 Monat) im Konzern für die VoIP-Infrastruktur festgelegt. Die genaue Verfügbarkeit muss vom Management genehmigt werden. • Reduzieren von Jitter und Latenzzeiten für eine gute Lesbarkeit • Sicherstellung der Möglichkeit, Notrufe durchzuführen	• Implementieren einer separaten Netzwerk-Infrastruktur für VoIP (VLAN) und Implementieren einer Bandbreitenbegrenzung, um ausreichend Bandbreite für das VOIP-VLAN zur Verfügung zu stellen oder Implementieren von QoS.
Nachverfolgbarkeit	• Gewährleistung der Integrität von Systemverwaltungsprotokollen (Audit-Trail-Protokolle)	• Gleiche Maßnahmen wie für das Schutzziel „Integrität“

	• Gewährleisten der Integrität von Call Data Records[5].	

1.3. Allgemeine Sicherheitsanforderungen

Die folgenden grundlegenden Anforderungen müssen eingehalten werden.

1.3.1 Zugriffskontrolle

IP-basierte Kommunikationssysteme verwenden unterschiedliche Authentifizierungs- und Autorisierungsverfahren. Im Wesentlichen müssen folgende Fälle unterschieden werden:

- Authentifizierung eines VoIP/Video-Geräts auf einem zentralen System
- Eine Authentifizierung/Autorisierung muss implementiert werden, kann aber schwach sein (z. B. ein 6-stelliger numerischer Code).
- Authentifizierung eines VoIP/Video-Benutzers auf einer persönlich konfigurierten GUI oder Ähnlichem.
- Die Authentifizierung[6] sollte gemäß den allgemeinen Anforderungen für Anwendungen (z. B. Authentifizierung über ein zentrales Verzeichnis) erfolgen.
- Die Autorisierung[7] für die Nutzung von VoIP/Video erfolgt gemäß den allgemeinen Anforderungen für Anwendungen (z. B. Authentifizierung über ein zentrales Verzeichnis)

Für die Systemverwaltung gelten die Standardregelungen zur Zugriffskontrolle[8]. Eine Systemverwaltung über den analogen Telefondienst (POTS) ist verboten.

1.3.2 Netzwerktrennung

Datennetzwerke für Sprach- und Videokommunikation sollten von anderen Netzwerken aus betrieblichen (Verfügbarkeits-) Gründen getrennt werden (z. B. zur Reduzierung von Jitter, garantierte Bandbreite).

1.3.3 Verschlüsselung

- Alle Nutzdaten (z. B. Zugangsdaten, persönliche Daten, Sprach-/Videodaten, Signaldaten und Call Data Records) müssen entsprechend der Anforderungen aus den Informationssicherheit Handlungsleitlinien[9] verschlüsselt[10] werden. Wenn die Kommunikation vollständig innerhalb einer vertrauenswürdigen sicheren Netzwerkzone stattfindet (z. B. Büronetzwerk), muss keine Verschlüsselung der Nutzdaten erfolgen.

---

[5] Die Integrität von Call Data Records muss gemäß den rechtlichen Vorschriften des jeweiligen Landes geschützt werden.

[6] Siehe Anhang A.1.4

[7] Siehe Anhang A.1.4

[8] Siehe Anhang A.1.4

[9] Siehe Anhang A.1.2

[10] Siehe Anhang A.1.3

- Kommunikation über nicht vertrauenswürdige „externe“ Netzwerke (z. B. Internet, Mietleitungen) muss verschlüsselt werden.

1.3.4 Geräteverwaltung

Jedes Gerät, das mit einer zentralen Telefoneinheit verbunden wird, muss authentifiziert werden. Das 802.1x-Authentifizierungsprotokoll muss bevorzugt werden, mindestens muss jedoch eine MAC-Adressen-basierte Authentifizierung erfolgen.

Jedes Gerät muss mindestens folgende Sicherheitsfunktionen bieten:

- Authentifizierung
- Alle Benutzer und Administrationsschnittstellen eines Geräts müssen über eine eigene Authentifizierung und Autorisierung verfügen, um unautorisierte Zugriffe oder Änderungen in den Konfigurationseinstellungen zu verhindern.
- Zentrale Konfigurationseinstellungen und Administration von VoIP/Video-Geräten.
- Aufgrund der großen Anzahl an Geräten muss eine zentrale Administration eingerichtet werden. Die zentrale Administration muss die Benutzerverwaltung auf dem Gerät, und das Konfigurations- und Patchmanagement abdecken.

1.3.5 Outsourcing von VoIP/Video

Folgende Sicherheitsmaßnahmen müssen implementiert werden:

- Alle allgemeinen Sicherheitsmaßnahmen der vorhergehenden Kapitel müssen vom Outsourcingnehmer/Dienstleistungsanbieter implementiert werden. Diese Sicherheitsmaßnahmen müssen einem regelmäßigen Auditverfahren unterzogen werden.
- Im Outsourcingvertrag müssen Datenschutzaspekte in Bezug auf Sprach-/Videodaten, Call Data Records und Telefonbuchdaten enthalten sein. Die Anforderungen im Outsourcingvertrag müssen den gesellschaftsspezifischen Regelungen entsprechen[11].

1.3.6 Gateways zu anderen VoIP-/Videosystemen

Gateways zu anderen Sprach-/Videoinfrastrukturen müssen so konfiguriert werden, dass nur der notwendige Datenverkehr möglich ist. Auf den Gateways dürfen nur die erforderlichen Netzwerk-Ports geöffnet werden.

Zwischen den Gateways muss eine gegenseitige Authentifizierung eingerichtet werden.

[11] Siehe Kapitel 1.1.1 und 1.1.2

2. Technische Sicherheitsmaßnahmen

2.1. Ziel

Dieses Kapitel gibt einen Überblick über die wesentlichen technischen Sicherheitsmaßnahmen.

2.2. Anwendungsfälle und entsprechende Anforderungen

Es gibt zahlreiche Möglichkeiten zur Einrichtung einer VoIP-Infrastruktur. Dieses Kapitel legt die sicherheitsrelevanten Anforderungen für die drei wichtigsten Arten von VoIP-Infrastruktur fest.

- VoIP-Telefonie in einem geschlossenen Netzwerk mit einer zentralen Einheit und mehreren Endpunkten innerhalb des geschlossenen Netzwerks.
- VoIP-Telefonie als Verbindung zwischen zwei zentralen Einheiten (Trunking).
- VoIP-Telefonie als Gateway zu PSTN (öffentliches Telefonnetz).

2.2.1 VoIP-Telefonie in geschlossenen Netzwerken mit einer zentralen Einheit und mehreren Endpunkten

In geschlossenen VoIP-Netzwerken dürfen Verbindungen (Anrufe, Videotelefonie und Voice-Box) nur hergestellt werden, wenn sie durch eine zentrale Einheit (einzeln oder redundant) mithilfe von autorisierten Endpunkten oder durch andere zentrale Einheiten signalisiert werden. Wenn die Verbindung von einer zentralen Einheit gesteuert wird, sind Verbindungen zwischen den autorisierten Endpunkten erlaubt.

Die zentrale Einheit sorgt für das Signalisieren und Kontrollieren der Verbindungen innerhalb des Netzwerks. Das Signalisierung und die Verbindung müssen immer durch die zentrale Einheit hergestellt werden. Eine zentrale Einheit kann aus mehreren physischen und/oder logischen Einheiten bestehen[12].

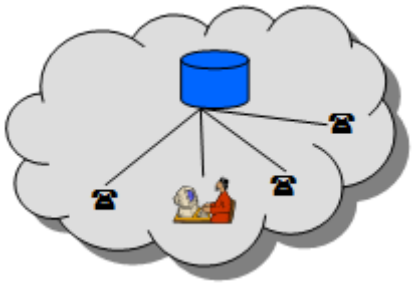

Abbildung 1: Eine zentrale Einheit und mehrere Endpunkte

Alle wesentlichen Funktionen/Dienste können folgenden Anwendungsfällen zugeordnet werden:

- Benutzeranmeldung/-abmeldung
- Geräteanmeldung/-abmeldung

[12] Siehe Kapitel 2.3

- Herstellen/Beenden eines Anrufs vom Endgerät zur zentralen Einheit
- Herstellen/Beenden eines Anrufs von der zentralen Einheit zum Endgerät
- Herstellen/Beenden eines Anrufs von Endpunkt zu Endpunkt (Verbindung wird durch zentrale Einheit gesteuert)

2.2.2 SIP-Trunking

SIP-Trunking ist eine Technik zur Verbindung von VoIP-Infrastrukturen verschiedener Einheiten zum Austausch von VoIP-Daten. Immer mehr Verbindungen zum Festnetz (PSTN) werden über SIP-Trunks hergestellt. SIP-Trunking darf nur zwischen zentralen Einheiten implementiert werden. Dabei spielt es keine Rolle, ob die zentrale Einheit für ein VoIP-Netzwerk oder für ein herkömmliches Telefonnetzwerk verwendet wird.

Alle wesentlichen Funktionen/Dienste können folgenden Anwendungsfällen zugeordnet werden:

- Herstellen/Beenden von Anrufen
- Anrufdienste
- Dienstleistungen

2.2.3 VoIP-Telefonie als Gateway zum öffentlichen Telefonnetz (PSTN)

Ein VoIP-Gateway zum Festnetz überträgt IP-Verbindungen zum Festnetz (z. B. ISDN) und umgekehrt. Das Gateway muss von der zentralen Einheit verwaltet werden.

2.3. Einheiten

Logische und physische Einheiten:

- Endpunkte: Telefone, Softphones (z. B. auf einem Laptop)
- Zentrale Einheiten: Je nach Implementierung besteht die zentrale Einheit ausfolgenden Komponenten:
  - Gatekeeper, Registrierung usw.
  - Gateways für Signalisierung, Medienkonverter usw.
  - Anwendungsserver für erweiterte Telekommunikationsdienste
  - Datenbanken zur Informationsspeicherung
- Netzwerk: bestehend aus Kabeln, Switches, Firewall, Routern usw.

2.4. Protokolle

Nur SIP/SIP TLS (Session Initiation Protocol), RTP/SRTP (Secure Realtime Transport Protocol) und H.323 dürfen als VoIP-Standard genutzt werden. Aus Sicherheitsgründen wird die Verwendung von SRTP (Secure Realtime Transport Protocol) und SIPS (Session Initiation Protocol Secure) empfohlen.

2.5. Allgemeine Anforderungen

- Eine Verbindung muss durch ein angemeldetes Telefon über eine zentrale Einheit hergestellt werden.
- Verbindungsdaten dürfen nur zu Abrechnungs- und Betriebszwecken (z. B. Problemanalyse) gespeichert werden.

2.5.1 Netzwerkzugriff für VoIP-Clients

Ein VoIP-Telefon muss sich als Client gemäß IEEE 802.1x authentifizieren können.

Die Endpunkt-Authentifizierung über Zertifikate muss bevorzugt werden. Wenn der Client keine Zertifikate unterstützt, muss die Authentifizierung über Benutzername und Kennwort erfolgen. Eine MAC-Adressen-basierte Authentifizierung ist nur erlaubt, wenn das Gerät keine der anderen Authentifizierungsmethoden unterstützt.

2.5.2 Anforderungen an die Dokumentation

Es muss eine Beschreibung des VoIP-Systems erstellt werden. Das Personal der Organisationseinheit für IT-Sicherheit muss bei Bedarf darauf zugreifen können.

Die Systembeschreibung muss mindestens folgende Punkte umfassen:

- Systemlayout
- Systemarchitektur/-struktur
- Datenpfade für individuelle Nutzung
- Datenbeschreibung für alle Datenpfade
- Art des Datenspeichers und Backup
- Schutz des Datenspeichers vor unerlaubtem Zugriff
- Implementierte Dienste
- Verwendete Protokolle
- Rollen- und Rechtekonzept
- Beschreibung von Laufzeitumgebungen insbesondere von Servern
- Anwendung von Schutzmaßnahmen für Funktionen und Daten

Für Benutzer muss ein Benutzerhandbuch zur Verfügung gestellt werden, in dem die Funktionen von VoIP sowie deren Bedienung beschrieben sind.

II. Verantwortlichkeiten

II.I Kapitel 1: Internet-Telefonie / Video-Telefonie

Diese Regelung ist von allen Betreibern von IT-Systemen anzuwenden und einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

Anhang

A. Allgemeines

A.1 Mitgeltende Dokumente

A.1.1 Informationssicherheit Regelung Nr. 03.01.09 Ausnahmeprozess

A.1.2 Informationssicherheitshandlungsleitlinien für Mitarbeiterinnen und Mitarbeiter

A.1.3 Informationssicherheit Regelung Nr. 03.01.02 Kryptographie

A.1.4 Informationssicherheit Regelung Nr. 03.01.05 Authentifizierung und IAM

A.2 Referenzen zu Standards

Die folgende Tabelle zeigt die Referenzen zu den Standards ISO/IEC 27001:2013, ISO/IEC 27001:2005 und VDA.

Thema	Kapitel	ISO 27001:2013	ISO 27001:2005	VDA
Documented operating procedures	2.5.2	A.12.1.1	-	-

A.3 Anlagen

A.3.1 Anlage 1 Feedbackformular

Das Feedbackformular für Änderungsvorschläge zu Regelungen kann von der MyNet-Webseite Gesellschaften → Audi Brussels → Organisation → Finanz (B/F) → IT (B/FP) → IT-Sicherheit → Regelwerk heruntergeladen werden.

Das Feedback-Formular ist folgendermaßen auszufüllen:

Die Spalten 2 bis 6 müssen für jede vorgeschlagene Änderung ausgefüllt werden. Änderungen, für die nicht alle Spalten 2 bis 6 ausgefüllt sind, werden automatisch ohne weitere Prüfung abgelehnt.

Spalte 3: Folgende Kommentararten sind möglich: a=allgemein, f=fachlich, r=redaktionell

Spalte 4: Bitte bisherigen Text, Tabelle oder Bild einfügen

Spalte 5: Bitte vollständig umformulierten Text, geänderte Tabelle oder geändertes Bild einfügen

Spalte 6: Bitte begründen Sie die gewünschte Änderung möglichst ausführlich.

Bitte senden Sie das ausgefüllte Formular an: it-security.audibx@audi.de

A.4 Gültigkeit

Diese Regelung ist mit der Veröffentlichung sofort gültig.

Bereits bestehende Ausnahmeregelungen sind spätestens bei der nächsten Änderung (z.B. Verlängerung, Änderung der Auflagen) an diese Regelung anzupassen.

Nächster Überprüfungstermin: 06.08.2021

Für die Meldung von Änderungswünschen verwenden Sie bitte das vorgegebene Formular[13].

A.5 Dokumentenhistorie

Version	Name	Org.-Einheit	Datum	Bemerkung
1.0	Andreas Walter	B/FP	07.08.2019	Veröffentlicht

[13] Siehe Anhang A.3.1 Anlage 1 Feedbackformular

B. Spezifische Ausprägungen

B.1 Kapitel 1: Allgemeines

B.1.1 Bei Outsourcing ist Informationssicherheit Regelung Nr. 03.01.16 Dienstleistungen durch Dritte zu beachten

B.1.2 Keine weiteren Details

B.1.3 Folgende Konkretisierung:

- Datenschutz: GDPR / DSGVO
- Notrufe:
  Europa: Die Regelungen und Maßnahmen hinsichtlich der Anforderungen für Notrufe werden festgelegt durch
  - ETSI EMTEL (Notruf-Telekommunikation)
  - ETSI TR 002 299: Collection of European Regulatory Principles (Europäische Regulierungsgrundsätze)
  - EGEA 2 07-02: Operational Needs for Access to Emergency Services (Betriebliche Anforderungen für Zugang zu Notfalldiensten)
  - ETSI TR 102 180: Emergency call handling (Umgang mit Notrufen)
- Private Nutzung von VoIP-Infrastruktur
  In einigen Ländern kann die private Nutzung einer gesellschaftseigenen Telekommunikationsinfrastruktur rechtliche, betriebliche oder technische Auswirkungen auf die Infrastruktur haben. Diese Tatsache muss in der Analysephase für Anforderungen beachtet werden.