WHITEPAPER

September 2025

Zusammenfassung

In der heutigen vernetzten Welt ist die Sicherung von Audiokommunikationssystemen für den Schutz sensibler Informationen und die Aufrechterhaltung der betrieblichen Effizienz von entscheidender Bedeutung. Vernetzte Audio-Systeme sind zahlreichen Bedrohungen ausgesetzt, darunter unbefugter Zugriff, Abhören, Denial-of-Service-Angriffe, Malware und Software-Exploits. Axis begegnet diesen Risiken mit modernsten Sicherheitslösungen, die sich nahtlos in bestehende Infrastrukturen integrieren lassen und Zuverlässigkeit, Skalierbarkeit und robusten Schutz bieten.

Axis verfolgt einen Security-by-Design-Ansatz, der Verschlüsselung, Authentifizierung, sichere Software-Updates, Zutrittskontrolle, Systemhärten und Ereignisprotokollierung umfasst. Sichere Protokolle wie SIPS, SRTP, HTTPS und IEEE 802.1AE ermöglichen eine sichere Kommunikation und Datenübertragung.

Die Audio-Management-Software von Axis bietet rollenbasierte Zutrittskontrolle, sicheres Onboarding und umfassende Protokollierung von Ereignissen und eignet sich sowohl für lokale als auch für cloudbasierte Bereitstellungen.

Durch die Nutzung dieser Sicherheitsebenen bieten die Netzwerk-Audio-Systeme von Axis einen umfassenden Schutz vor Cyber-Bedrohungen.

Inhalt

1 Einführung

Audio spielt eine entscheidende Rolle für die Kommunikation, Sicherheit und betriebliche Effizienz in verschiedenen Branchen wie Einzelhandel, Verkehr, öffentliche Sicherheit und Bildungswesen. Diese Systeme sind auch attraktive Ziele für Cyberangriffe, daher sind robuste Sicherheitsmaßnahmen unerlässlich. Ein beeinträchtigtes Audio-System kann schwerwiegende und weitreichende Folgen haben.

Dieses Whitepaper befasst sich mit den Haupt-Sicherheitsebenen, die Axis-Lautsprecher und Audio-Systeme einsetzen, um diesen Herausforderungen zu begegnen.

2 Die Risiken verstehen

Mit dem zunehmenden Einsatz vernetzter Audio-Lösungen in verschiedenen Industrien sind auch die potenziellen Risiken, die mit ungesicherten Systemen verbunden sind, erheblich gestiegen.

Vernetzte Audio-Systeme können verschiedenen Arten von Bedrohungen ausgesetzt sein.

- **Unberechtigter Zugriff.** Ungeschützte Audio-Geräte können von böswilligen Akteuren aus der Ferne aufgerufen werden, die dann die Kontrolle über Lautsprecher übernehmen, unbefugte Durchsagen machen oder den Betrieb stören könnten.
- **Abhören und Datenüberwachung.** Vernetzte Audio-Systeme übertragen manchmal sensible Sprachdaten über kabelgebundene oder kabellose Netzwerke. Ohne Verschlüsselung könnten Angreifer Gespräche abfangen und eine Aufzeichnung anfertigen, was zu Datenschutzverletzungen, Industriespionage oder Missbrauch vertraulicher Informationen führen könnte.
- **Denial-of-Service-Angriffe (DoS).** Angreifer können vernetzte Lautsprecher oder Audio-Server mit übermäßigem Datenaustausch überfluten, was zu einer Überlastung des Systems und einer Unterbrechung der Dienste führt. Solche Angriffe könnten Notfallkommunikationssysteme in kritischen Momenten außer Betrieb setzen.
- **Malware- und Ransomware-Angriffe.** Genau wie herkömmliche IT-Infrastrukturen können auch vernetzte Audio-Geräte durch Malware oder Ransomware gefährdet werden. Angreifer könnten Geräte sperren, Lösegeldforderungen stellen oder das kompromittierte System als Einstiegspunkt nutzen, um das gesamte Netzwerk anzugreifen.
- **Software-Exploits und Schwachstellen in der Lieferkette.** Veraltete Betriebssysteme mit ungepatchten Sicherheitslücken können ausgenutzt werden, um die Kontrolle über Audio-Geräte zu erlangen. Darüber hinaus können unsichere Praktiken in der Lieferkette bereits vor der Bereitstellung Schwachstellen verursachen, wodurch Systeme von Anfang an anfällig sind.

3 Vorteile von Axis Netzwerk-Audio

Axis bietet hochmoderne Lautsprecher- und Systemsicherheitslösungen, die sich nahtlos in bestehende Infrastrukturen integrieren lassen. Die offene Architektur gewährleistet Kompatibilität mit verschiedenen Systemen und Protokollen. Ein Axis-System ist flexibel und verfügt über eine Projektierung, die darauf ausgelegt ist, mit den Anforderungen Ihrer Organisation mitzuwachsen, von kleinen Implementierungen bis hin zu Netzwerken im Unternehmensmaßstab. Axis bietet sowohl lokale als auch cloudbasierte Audio-Management-Systeme an.

Axis verfolgt bei der Softwareentwicklung einen Security-by-Design-Ansatz. Unser Rahmenwerk „Axis Security Development Model" (ASDM) definiert Prozesse und Tools, die sicherstellen, dass wir Sicherheit in den gesamten Softwareentwicklungszyklus integrieren und das Risiko von Schwachstellen reduzieren. Das ASDM wird kontinuierlich verbessert.

Einer von vielen Eingängen zur Verbesserung ist, dass wir regelmäßig verschiedene sicherheitsrelevante Standards bewerten und diese auf ASDM abbilden. Unsere Software erfüllt strenge Branchenstandards für Datenschutz und -sicherheit, darunter die DSGVO (Datenschutz-Grundverordnung) der EU.

4 Wichtige Merkmale der Lautsprecher- und Systemsicherheit

Bei Axis Netzwerk-Audio ist die Sicherheit in die Geräte sowie in die Management-Systeme integriert.

Verschlüsselung und Authentifizierung

- Die Verschlüsselung sorgt für eine sichere Übertragung von Audio über TLS 1.2 und 1.3 und verhindert, dass Unbefugte das Audio abfangen und darauf Zugriff erhalten.
- Die Authentifizierung stellt sicher, dass nur autorisierte Geräte und Benutzer einen Zugriff auf die Geräte, aber auch auf die Lösung haben.

Sichere Updates für die Software des Geräts

- Secure Boot (in den meisten Produkten) und digital signierte Patches stellen sicher, dass nur verifizierte Gerätesoftware installiert wird. Dies schützt Systeme vor bösartigem Code.

Zutrittskontrolle

- AXIS Audio Manager Pro und AXIS Audio Manager Center verwenden eine rollenbasierte Zutrittskontrolle (RBAC), die den Systemzugriff auf autorisiertes Personal beschränkt.
- Durch die zentrale Verwaltung können IT-Administratoren Berechtigungen effektiv überwachen und kontrollieren.

Systemhärtung

- Die Standard-Einstellungen sind hinsichtlich der Sicherheit optimiert und reduzieren Schwachstellen.
- Zusätzliche Optionen für die Konfiguration ermöglichen eine Anpassung an spezifische Schutzziele. AXIS OS Härtungsleitfaden unter *help.axis.com/axis-os-hardening-guide* bietet technische Beratung.

Überwachung von Ereignissen

- Umfassende Protokollierung sorgt für Transparenz bei den Systemaktivitäten. Dies kann bei der Echtzeit-Erfassung von Bedrohungen und der forensischen Analyse hilfreich sein.

5 Sicherheit im gesamten System

Bei Axis Netzwerk-Audio ist die Sicherheit in die Geräte und Management-Systeme integriert. Sichere Protokolle aktivieren ein hohes Maß an Sicherheit bei der Kommunikation zwischen Geräten und Verwaltungssoftware.

5.1 Gerätesicherheit

Alle Axis-Lautsprecher funktionieren mit AXIS OS, unserer speziell für Axis-Geräte entwickelten Gerätesoftware. Es ermöglicht langfristige Wertschöpfung, Cybersicherheit und erstklassige Integration. Mit AXIS OS verfügen alle unsere Lautsprecher über die robusten Sicherheitsfunktionen des Axis-Ökosystems. Dies sorgt für Konsistenz und Zuverlässigkeit auf allen Geräten und bietet durchgängigen Schutz für jede Bereitstellung. Zu den Sicherheitsfunktionen gehören verschlüsselte Dateisysteme und die hardwarebasierte Cybersicherheitsplattform Axis Edge Vault (*axis.com/solutions/edge-vault*).

Axis Edge Vault schützt die Integrität von Axis Geräten und ermöglicht die Ausführung sicherer Vorgänge auf der Grundlage kryptografischer Schlüssel. Es ermöglicht es, die IEEE 802.1AR-konforme Axis-Geräte-ID zu verifizieren und für eine sichere Einbindung des Geräts in Zero-Trust-Netzwerken über IEEE 802.1X und HTTPS zu nutzen. Mit Axis Edge Vault können Sie das Gerät sicher booten, es integrieren und sicherstellen, dass sensible Informationen wie kryptografische Schlüssel geschützt sind.

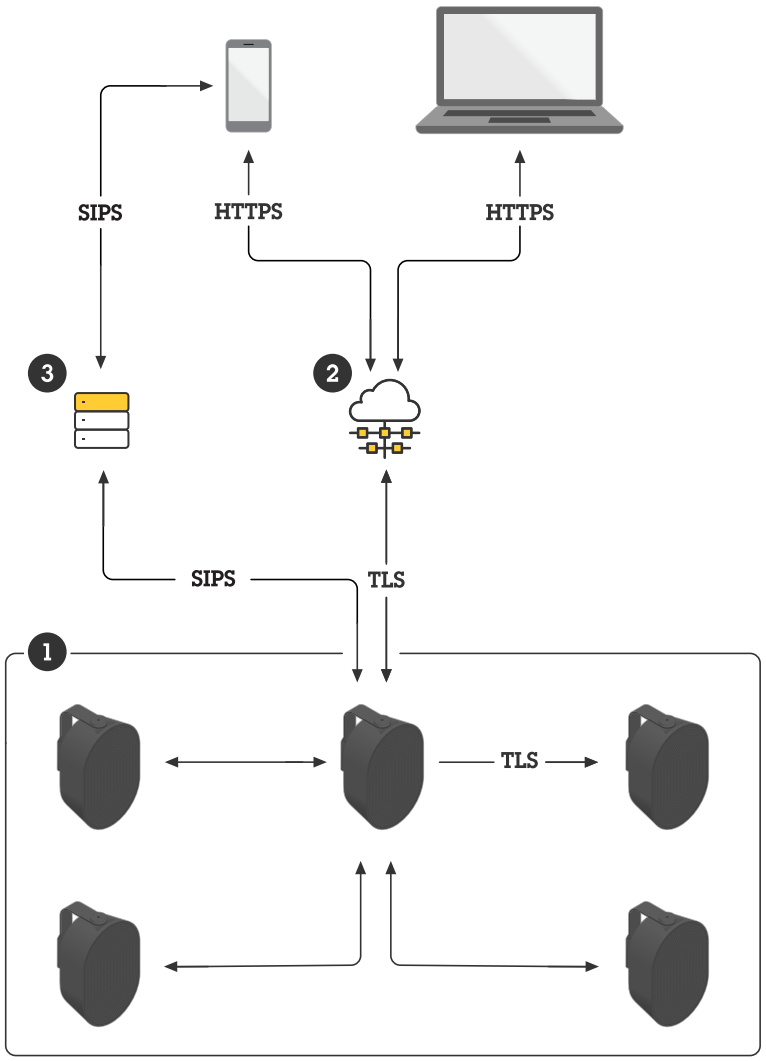
Mit Axis Edge Vault können Sie sicher sein, dass das Axis-Gerät, das Sie erhalten haben, in der physischen Lieferkette nicht manipuliert oder beeinträchtigt wurde. Axis Edge Vault etabliert eine Vertrauenskette und gewährleistet eine lückenlose Kette kryptografisch validierter Software. Beispielsweise stellt ein *signiertes Betriebssystem* sicher, dass die Software von Axis stammt und nur signierte Softwareupdates installiert werden können.

5.2 Sicherheitsprotokolle

Axis-Geräte und -Systeme verwenden offene Protokolle für sichere Kommunikation, Übertragung und Videostreams.

- **SIPS** (SIP Secure): erweitert das Standard-SIP (Session Initiation Protocol) durch die Integration von TLS (Transport Layer Security). Dadurch wird eine sichere Verbindung zwischen einer IP-Telefonanlage und einem VoIP-Telefon hergestellt. Sobald die sichere Verbindung eingestellt ist, verschlüsselt SRTP (Secure Real-Time Transport Protocol) Sprachdaten in sichere IP-Pakete für die Übertragung über das Internet. Dies ermöglicht eine End-to-End-Verschlüsselung vom Sender (IP-Telefonsystem) zum Empfänger (Lautsprecher).

  Durch die Nutzung von SIPS und SRTP sichern Axis-Systeme sowohl die Audio-Daten als auch den Setup selbst. Das bedeutet, dass der Audio-Stream und die Verbindungsdetails (wie Anruferidentität und Empfänger) vollständig verschlüsselt sind und der sichere Peer-to-Peer-Kommunikationskanal robust ist.
- **Multicast-Controller-**: Eine Multicast-Controller-Funktion in Axis-Lautsprechern ermöglicht den sicheren Empfang von Multicast-Audio-Streams, die über SRTP gesendet werden. Dadurch wird sichergestellt, dass die Gruppenkommunikation verschlüsselt ist.
- **Transmit.cgi** und **receive.cgi**: Diese VAPIX-APIs bieten eine sichere Methode zum Senden und Empfangen von Audio-Streams in verschlüsselter Punkt-zu-Punkt-Kommunikation über HTTPS. CGI (Common Gateway Interface) ist ein Standardprotokoll, das die Kommunikation zwischen einem Webserver und externen Programmen festlegt.
- **RTSPS** (Real-Time Streaming Protocol Secure): Ein Netzwerksteuerungsprotokoll, das zum Einrichten und zur Verwaltung von Echtzeit-Medienstreams zwischen einem Server und einem Client verwendet wird. Dies wird für sicheres Audio-Streaming unterstützt, wobei Verschlüsselung zum Einsatz kommt, um unbefugten Zugriff zu verhindern.
- **HTTPS-**: Alle APIs sind mit HTTPS gesichert, um die Vertraulichkeit und Integrität aller Kommunikationen zu gewährleisten.
- **IEEE 802.1AE**: Auch bekannt als MACsec (Media Access Control Security), ein Netzwerkprotokoll, das die Netzwerkkommunikation auf Netzwerkebene 2 in den Grundlagen mit AES-128 verschlüsselt. In Kombination mit HTTPS, RTSPS und SIPS wird der Datenaustausch im Wesentlichen doppelt verschlüsselt und die Netzwerksicherheit erheblich verbessert.



Ein Netzwerk-Audio-System mit sicherer Kommunikation dank mehrerer offener Protokolle.

1 *AXIS Audio Manager Edge: Lokale Audio-Verwaltung, integriert in Axis-Lautsprecher*
2 *AXIS Audio Manager Center: Audioverwaltung in der Hybrid-Cloud*
3 *Partner-Telefonanlage*

5.3 Sicherheit bei Audio-Management-Software

5.3.1 Lokale Lösungen

Die lokalen Lösungen von Axis sind projektiert zur Verwaltung von Zonen, Prioritäten und zur sicheren Kommunikation zwischen mehreren Sprechern vor Ort.

AXIS Audio Manager Edge. Diese Management-Software ist in jeden Netzwerk-Lautsprecher von Axis integriert. Dadurch wird jeder Lautsprecher zu einem kompletten All-in-One-Soundsystem, für das kein separater Software-Management-Server erforderlich ist. AXIS Audio Manager Edge ist für die Verwaltung von Projekten mit geringer Komplexität vorgesehen, die aus bis zu 200 Geräten in bis zu 20 Zonen bestehen.

- Unterstützt die Verschlüsselung zwischen Geräten. Die Standardverschlüsselungsmethode ist TLS mit selbstsignierten Zertifikaten. Wir empfehlen jedoch, vertrauenswürdige Zertifikate auf Ihren Geräten zu installieren und die TLS-Authentifizierung in den Systemeinstellungen der Website zu aktivieren. Dies bietet Schutz vor Man-in-the-Middle-Angriffen.
- Ermöglicht die sichere Einbindung von Geräten in die lokale Umgebung. Das Setup erfolgt über HTTPS mit den Anmeldedaten des Geräts. Danach wird MQTT (TLS-PSK) für die Kommunikation zwischen Geräten verwendet und SRTP wird zum Senden verschlüsselter RTP-Daten wie Audio-Streams zwischen den Geräten verwendet.

- Bietet externen Systemzugriff für operative Schutzziele über HTTPS-API.

AXIS Audio Manager Pro. Diese Management-Software ist für größere, komplexere Projekte bestimmt. Sie kann eine große Anzahl von Zonen (500+) und Tausende von Geräten (5000+) in einer einzigen Schnittstelle verwalten. AXIS Audio Manager Pro erleichtert den langfristigen Zeitplan und die erweiterten Prioritätseinstellungen.

- Beinhaltet rollenbasierte Zutrittskontrolle, die den Zugriff auf das System auf autorisiertes Personal beschränkt, mit Unterstützung für die Active Directory-Integration.
- Ermöglicht die sichere Einbindung von Geräten.
- Enthält ein detailliertes Ereignis- und Auditprotokoll. Dies liefert eine umfassende Aufzeichnung der Systemaktivitäten, die der Verwaltung dabei helfen kann, Änderungen zu verfolgen, das Verhalten zu überwachen und Probleme zu beheben.

5.3.2 Cloudbasierte Lösung

AXIS Audio Manager Center ist ein Dienst für die Fernverwaltung und Überwachung von Systemen mehrerer Standorte, von wenigen Standorten bis zu mehreren Tausend. Es wird zusammen mit dem AXIS Audio Manager Edge an allen lokalen Standorten verwendet. Die hybride Cloud-Lösung nutzt aus Gründen der Praktikabilität und Stabilität sowohl cloudbasierte als auch lokale Komponenten.

AXIS Audio Manager Center vereinfacht die Verwaltung, ermöglicht eine zentrale Steuerung und sorgt für eine sichere Einbindung von Geräten. Der Arbeitsaufwand für Benutzer verringert sich deutlich, da sie sich nur einmal anmelden müssen, um Durchsagen, Hintergrundmusik, Werbung und mehr für ausgewählte Standorte bzw. Zonen zu planen. Die Haupt-Sicherheitsmerkmale umfassen:

- Rollenbasierte Zutrittskontrolle (RBAC): beschränkt den Zugriff auf das System ausschließlich auf autorisiertes Personal.
- Zentrale Benutzerverwaltung: unterstützt *My Axis* oder Active Directory-Benutzer/Gruppen für eine optimierte Verwaltung. Keine lokalen Benutzer erforderlich.
- Sicheres Onboarding: vereinfacht das sichere Onboarding von Geräten mit Vertrauen aus der Cloud, indem es einzigartige Zertifikate verwendet, die auf jedem Gerät installiert werden.
- Vereinfacht gesicherte E2E-Konfigurationen: ermöglicht die sichere Konfiguration von SIPS, einschließlich der Zertifikatsverwaltung.
- Health-Monitoring und Benachrichtigungen: bietet eine zentralisierte Überwachung des Systemzustands und sofortige Warnmeldungen bei potenziellen Problemen.
- Sichere Kommunikation: die gesamte Kommunikation zwischen der Cloud und den Geräten wird über TLS verschlüsselt, wobei gegenseitiges TLS (Zwei-Wege-Authentifizierung) für robuste Sicherheit sorgt.
- Fernzugriff: ermöglicht einen sicheren Fernzugriff auf lokale Standorte von überall aus.

Über Axis Communications

Axis ermöglicht eine smartere und sichere Welt durch die Verbesserung von Sicherheit, Schutz, betrieblicher Effizienz und Geschäftsanalytik. Als Technologieführer im Bereich Netzwerk-Video bietet Axis Videosicherheits-, Zutrittskontroll-, Intercom- und Audiolösungen. Die branchenweit anerkannten Schulungen der Axis Communications Academy vermitteln fundiertes Expertenwissen zu den neuesten Technologien.

Das 1984 gegründete schwedische Unternehmen beschäftigt etwa 5.000 engagierte MitarbeiterInnen in über 50 Ländern und bietet mit Technologie- und Systemintegrationspartnern auf der ganzen Welt kundenspezifische Lösungen an. Der Hauptsitz ist in Lund, Schweden.