DOCUMENTO TECNICO

Settembre 2025

Sommario

Nel mondo interconnesso di oggi, garantire la sicurezza dei sistemi di comunicazione audio è fondamentale per proteggere le informazioni sensibili e mantenere l'efficienza operativa. I sistemi audio basati sulla rete sono esposti a numerose minacce, tra cui accessi non autorizzati, intercettazioni, attacchi denial-of-service, malware e sfruttamento del software. Axis affronta questi rischi con soluzioni di sicurezza all'avanguardia che si integrano perfettamente con le infrastrutture esistenti, offrendo affidabilità, scalabilità e protezione robusta.

Axis adotta un approccio basato sulla sicurezza fin dalla progettazione, che integra crittografia, autenticazione, aggiornamenti software sicuri, controllo degli accessi, rafforzamento del sistema e registrazione degli eventi. Protocolli sicuri come SIPS, SRTP, HTTPS e IEEE 802.1AE consentono comunicazioni e trasmissioni dati sicure.

Il software di gestione audio Axis offre un sistema di controllo degli accessi basato sui ruoli, integrazione sicura e registrazione completa degli eventi, adattandosi sia alle implementazioni sul posto che a quelle basate su cloud.

Sfruttando questi livelli di sicurezza, i sistemi audio di rete Axis offrono una protezione end-to-end contro le minacce informatiche.

Indice

1 Introduzione

I sistemi audio svolgono un ruolo fondamentale per la comunicazione, la sicurezza e l'efficienza operativa in vari settori quali la vendita al dettaglio, i trasporti, la sicurezza pubblica e l'istruzione. Questi sistemi sono anche obiettivi appetibili per gli attacchi informatici, pertanto è fondamentale adottare misure di sicurezza efficaci. Un sistema audio compromesso può avere conseguenze gravi e di vasta portata.

Questo documento tecnico esplora i principali livelli di sicurezza che gli altoparlanti e i sistemi audio Axis utilizzano per affrontare queste sfide.

2 Comprensione dei rischi

Con la crescente diffusione delle soluzioni audio basate sulla rete in tutti i settori dei processi industriali, i rischi potenziali associati ai sistemi non protetti sono aumentati in modo significativo.

I sistemi audio basati sulla rete possono essere esposti a diversi tipi di minacce.

- **Accesso non autorizzato.** I dispositivi audio non protetti possono essere accessibili da remoto da parte di malintenzionati che potrebbero quindi assumere il controllo degli altoparlanti, diffondere annunci non autorizzati o interrompere le operazioni.
- **Intercettazioni audio e di dati.** I sistemi audio basati sulla rete talvolta trasmettono dati vocali sensibili su reti cablate o wireless. Senza crittografia, gli hacker potrebbero intercettare e registrare le conversazioni, violando la privacy, effettuando spionaggio industriale o uso improprio di informazioni riservate.
- **Attacchi denial-of-service (DoS).** Gli hacker possono inondare gli altoparlanti collegati in rete o i server audio con un traffico eccessivo, causando il sovraccarico del sistema e l'interruzione dei servizi. Tali attacchi potrebbero rendere inutilizzabili i sistemi di comunicazione di emergenza nei momenti critici.
- **Attacchi malware e ransomware.** Proprio come le infrastrutture IT tradizionali, anche i dispositivi audio basati sulla rete possono essere compromessi da malware o ransomware. Gli hacker potrebbero bloccare i dispositivi, richiedere il pagamento di un riscatto o utilizzare il sistema compromesso come punto di accesso per attaccare la rete più ampia.
- **Sfruttamento del software e vulnerabilità catena di fornitura.** I sistemi operativi obsoleti con falle di sicurezza non corrette possono essere sfruttati per ottenere il controllo dei dispositivi audio. Inoltre, pratiche di catena di fornitura non sicure possono introdurre vulnerabilità prima dell'implementazione, rendendo i sistemi vulnerabili sin dall'inizio.

3 Vantaggi dell'audio di rete Axis

Axis offre soluzioni all'avanguardia per la sicurezza degli altoparlanti e dei sistemi, facilmente integrabili con le infrastrutture esistenti. L'architettura aperta garantisce la compatibilità con diversi sistemi e protocolli. Il sistema Axis è flessibile e progettato per crescere insieme alle esigenze della società/organizzazione, dalle piccole implementazioni alle reti su scala aziendale. Axis offre sistemi di gestione Audio sia sul posto che basati su cloud.

Axis utilizza un approccio di sicurezza integrato nella progettazione per lo sviluppo di software. Il nostro modello di sviluppo Axis Security Development Model (ASDM) definisce i processi e gli strumenti che garantiscono l'integrazione della sicurezza nell'intero ciclo di vita dello sviluppo del software e riducono il rischio di vulnerabilità. L'ASDM è sottoposto a miglioramento continuo.

Uno dei tanti contributi al miglioramento è che valutiamo con regolarità i vari standard relativi alla sicurezza e li mappiamo su ASDM. Il nostro software soddisfa i rigorosi standard industriali in materia di privacy e sicurezza dei dati, compreso il GDPR (Regolamento generale sulla protezione dei dati) dell'UE.

4 Caratteristiche principali della sicurezza degli altoparlanti e del sistema

Con l'audio di rete Axis, la sicurezza è integrata nei dispositivi come anche nei sistemi di gestione.

Crittografia e autenticazione

- La crittografia garantisce la trasmissione sicura dei dati audio tramite TLS 1.2 e 1.3, impedendo a soggetti non autorizzati di intercettare e accedere alle informazioni.
- L'autenticazione garantisce che solo i dispositivi e gli utenti autorizzati possano accedere ai dispositivi, ma anche alla soluzione complessiva.

Aggiornamenti software sicuri per i dispositivi

- L'avvio sicuro (nella maggior parte dei prodotti) e le patch con firma digitale assicurano l'installazione esclusiva del software del dispositivo verificato . Questo protegge i sistemi da codici dannosi.

Controllo accessi

- AXIS Audio Manager Pro e AXIS Audio Manager Center utilizzano il controllo degli accessi basato sui ruoli (RBAC), che limita l'accesso al sistema solo al personale autorizzato.
- La gestione centralizzata consente agli amministratori IT di monitorare e controllare efficacemente le autorizzazioni.

Rafforzamento del sistema

- Le impostazioni predefinite sono ottimizzate per garantire la sicurezza fin dal primo utilizzo, riducendo le vulnerabilità.
- Ulteriori opzioni di configurazione consentono la personalizzazione in base a casi d'uso specifici. La guida al rafforzamento di AXIS OS riportata all'indirizzo *help.axis.com/axis-os-hardening-guide* fornisce consigli tecnici.

Registrazione e monitoraggio degli eventi

- La registrazione completa offre visibilità sulle attività del sistema. Ciò può fornire un aiuto nel rilevamento delle minacce in tempo reale e nell'analisi forense.

5 Sicurezza in tutto il sistema

Con l'audio di rete Axis, la sicurezza è integrata nei dispositivi e nei sistemi di gestione. I protocolli sicuri garantiscono un elevato livello di sicurezza nella comunicazione tra dispositivi e software di gestione.

5.1 Sicurezza del dispositivo

Tutti gli altoparlanti Axis funzionano con AXIS OS, il nostro software appositamente progettato per i dispositivi Axis. Garantisce valore a lungo termine, sicurezza informatica e integrazione di livello mondiale. Con AXIS OS, tutti i nostri altoparlanti ereditano le solide funzionalità di sicurezza dell'ecosistema Axis. Ciò garantisce coerenza e affidabilità su tutti i dispositivi e offre una protezione end-to-end per ogni implementazione. Le funzionalità di sicurezza includono file system crittografati e la piattaforma di sicurezza informatica basata su hardware Axis Edge Vault (*axis.com/soluzioni/edge-vault*).

Axis Edge Vault salvaguarda l'integrità dei dispositivi Axis e consente l'esecuzione di operazioni sicure basate su chiavi crittografiche. Consente di verificare e sfruttare l' ID dispositivo Axis conforme allo standard IEEE 802.1AR per l'integrazione sicura del dispositivo in reti zero trust tramite IEEE 802.1X e HTTPS. Con Axis Edge Vault, è possibile avviare il dispositivo in modo sicuro, integrarlo e avere la certezza che le informazioni sensibili, come le chiavi crittografiche, siano protette.

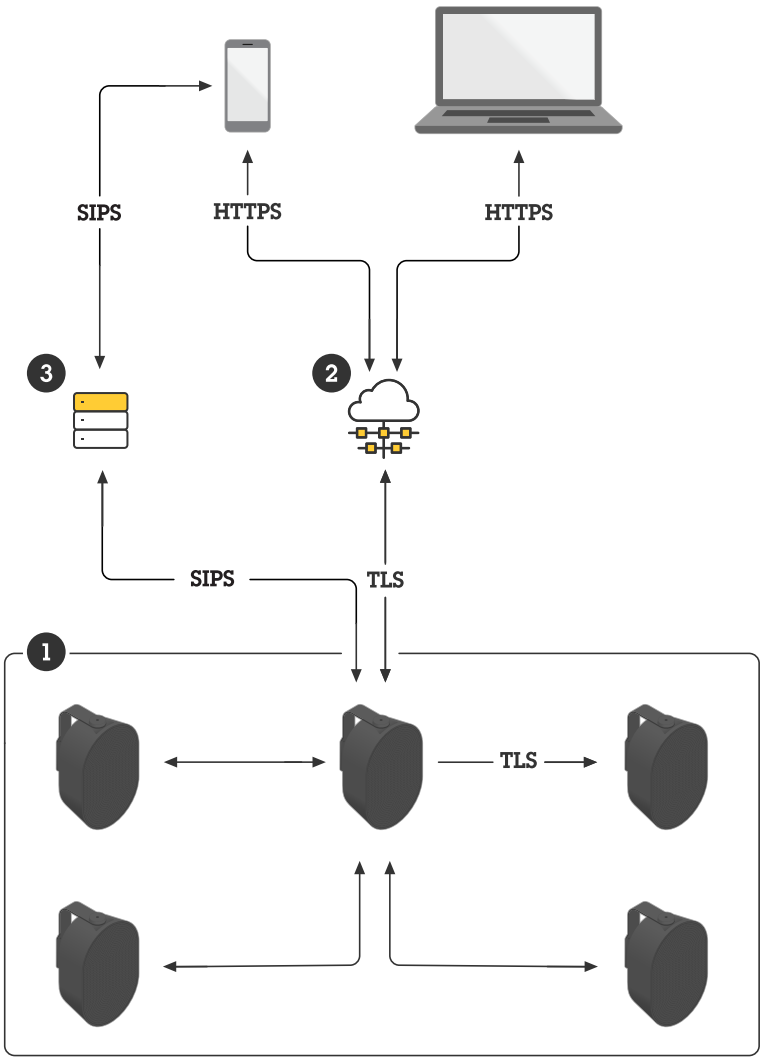
Grazie ad Axis Edge Vault si ha la certezza che il dispositivo Axis che si possiede non sia stato manomesso o compromesso nella catena di fornitura fisica. Axis Edge Vault stabilisce una catena di fiducia e garantisce una catena ininterrotta di software convalidato tramite crittografia. Ad esempio, la funzione *OS firmato* assicura che il software del dispositivo provenga da Axis e che sia possibile installare solo gli aggiornamenti firmati.

5.2 Protocolli di sicurezza

I dispositivi e i sistemi Axis utilizzano protocolli aperti per garantire comunicazioni, trasmissioni e streaming sicuri.

- **SIPS** (SIP Secure): migliora lo standard SIP (Session Initiation Protocol) incorporando TLS (Transport Layer Security). Questo stabilisce una connessione sicura tra un IP PBX e un telefono VoIP. Una volta stabilita la connessione sicura, il protocollo SRTP (Secure Real-Time Transport Protocol) crittografa i dati vocali in pacchetti IP sicuri per la trasmissione su Internet. Ciò garantisce una crittografia end-to-end dal trasmettitore (sistema telefonico IP) al ricevitore (altoparlante).

  Sfruttando SIPS e SRTP, i sistemi Axis proteggono sia i dati audio che la configurazione della connessione stessa. Ciò significa che l'audio e i dettagli della connessione (come l'identità del chiamante e del destinatario) sono completamente crittografati e che il canale di comunicazione peer-to-peer sicuro è solido.
- **Multicast controller**: una funzione multicast controller presente negli altoparlanti Axis consente la ricezione sicura di flussi Audio multicast inviati tramite SRTP. Ciò garantisce la crittografia delle comunicazioni di gruppo.
- **Transmit.cgi** e **receive.cgi**: Queste API VAPIX forniscono un metodo sicuro per inviare e ricevere flussi audio in comunicazioni punto-punto crittografate tramite HTTPS. CGI (Common Gateway Interface) è un protocollo standard che specifica la comunicazione tra un server Web e programmi esterni.
- **RTSPS** (Real-Time Streaming Protocol Secure): un protocollo di controllo di rete utilizzato per stabilire e gestire flussi multimediali in tempo reale tra un server e un client. Il protocollo è supportato per lo streaming audio sicuro, utilizzando la crittografia per impedire accessi non autorizzati.
- **HTTPS**: tutte le API sono protette con HTTPS per garantire la riservatezza e l'integrità di tutte le comunicazioni.
- **IEEE 802.1AE**: noto anche come MACsec (Media Access Control Security), un protocollo di rete che utilizza AES-128 per crittografare le comunicazioni di rete fondamentalmente sul livello 2 della rete. Se combinato con HTTPS, RTSPS e SIPS, il traffico di rete è essenzialmente crittografato due volte e la protezione della rete è notevolmente migliorata.



Un sistema audio di rete con comunicazione sicura grazie a diversi protocolli aperti.

1 *AXIS Audio Manager Edge: gestione audio locale integrata negli altoparlanti Axis*
2 *AXIS Audio Manager Center: gestione audio centralizzata su cloud ibrido*
3 *Partner PBX*

5.3 Sicurezza nel software di gestione audio

5.3.1 Soluzioni sul posto

Le soluzioni sul posto di Axis sono progettate per gestire la suddivisione in zone, la definizione delle priorità e la comunicazione sicura tra più altoparlanti in loco.

AXIS Audio Manager Edge. Questo software di gestione è integrato su ogni altoparlante audio di rete Axis Rende ogni altoparlante un sistema audio completo e tutto in uno, senza bisogno di un server di gestione software separato. AXIS Audio Manager Edge è progettato per gestire progetti a bassa complessità che comprendono fino a 200 dispositivi in un massimo di 20 zone.

- Supporta la crittografia tra dispositivi. Il metodo di crittografia predefinito è TLS con certificati autofirmati, ma si consiglia l'installazione di certificati attendibili sui dispositivi e di abilitare l'autenticazione TLS nelle impostazioni di sistema del sito. Questo garantisce protezione contro gli attacchi man-in-the-middle.
- Consente l'integrazione sicura dei dispositivi nel sito locale. La configurazione iniziale viene eseguita tramite HTTPS con le credenziali del dispositivo. Successivamente, MQTT (TLS-PSK) viene utilizzato per la comunicazione tra i dispositivi e SRTP viene utilizzato per inviare dati RTP crittografati, come flussi audio, tra i dispositivi.

- Fornisce accesso al sistema esterno per casi d'uso operativi tramite API HTTPS.

AXIS Audio Manager Pro. Questo software di gestione è concepito per sistemi più grandi e progetti più complessi. È in grado di gestire un numero elevato di zone (oltre 500) e migliaia di dispositivi (oltre 5000) in un'unica interfaccia. AXIS Audio Manager Pro facilita la programmazione a lungo termine e le impostazioni avanzate delle priorità.

- Include il controllo degli accessi basato sui ruoli, che limita l'accesso al sistema solo al personale autorizzato, con supporto per l'integrazione con Active Directory.
- Consente l'integrazione sicura dei dispositivi.
- Include un registro dettagliato di eventi e verifiche. Ciò fornisce una registrazione completa dell'attività del sistema, che può aiutare gli amministratori a tenere traccia delle modifiche, monitorare il comportamento e risolvere i problemi.

5.3.2 Soluzione basata su cloud

AXIS Audio Manager Center è un servizio per la gestione e il monitoraggio remoti di sistemi multisito, scalabilità da pochi siti a diverse migliaia. Viene utilizzato insieme ad AXIS Audio Manager Edge in ogni sito locale. Poiché impiega componenti locali e cloud, si tratta di una soluzione cloud ibrida conveniente e stabile.

AXIS Audio Manager Center semplifica la gestione, offre un controllo centralizzato e gestisce l'integrazione sicura dei dispositivi. Il carico di lavoro dell'utente si riduce significativamente con un Single Sign-On per pianificare avvisi, musica di sottofondo, annunci e altro ancora per siti o aree selezionate. Le principali caratteristiche di sicurezza includono:

- Controllo degli accessi basato sui ruoli (RBAC): limita l'accesso al sistema solo al personale autorizzato.
- Gestione centralizzata degli utenti: supporta *My Axis* o utenti/gruppi Active Directory per un'amministrazione semplificata. Non sono necessari utenti locali.
- Integrazione sicura: semplifica l'integrazione sicura dei dispositivi con la fiducia del cloud, utilizzando certificati univoci installati su ciascun dispositivo.
- Semplifica le configurazioni E2E protette: consente la configurazione sicura di SIPS, compresa la gestione dei certificati.
- Monitoraggio dello stato di salute e notifiche: offre un monitoraggio centralizzato dello stato di salute del sistema e avvisi immediati in caso di potenziali problemi.
- Comunicazione sicura: tutte le comunicazioni tra il cloud e i dispositivi sono crittografate tramite TLS, con TLS reciproco (autenticazione bidirezionale) che garantisce una solida sicurezza.
- Accesso remoto: consente un accesso remoto sicuro al sito locale da qualsiasi luogo.

Informazioni su Axis Communications

Axis permette di creare un mondo più intelligente e sicuro migliorando la sicurezza, la protezione, l'efficienza operativa e la business intelligence. In qualità di azienda leader nelle tecnologie di rete, Axis offre videosorveglianza, controllo accessi, intercom e soluzioni audio, che supporta con applicazioni analitiche intelligenti e una formazione di alta qualità.

Axis ha oltre 5000 dipendenti in più di 50 paesi e collabora con partner tecnologici e integratori di sistemi in tutto il mondo per fornire soluzioni ai clienti. Fondata nel 1984, Axis è una società con sede a Lund, in Svezia.