LIVRE BLANC

Cybersécurité avec l'audio en réseau Axis

Septembre 2025

Avant-propos

Dans le monde interconnecté d'aujourd'hui, la sécurisation des systèmes de communication audio est essentielle pour protéger les informations sensibles et maintenir l'efficacité du fonctionnement. Les systèmes audio en réseau sont exposés à de nombreuses menaces, notamment les accès non autorisés, les écoutes clandestines, les attaques par déni de service, les logiciels malveillants et les exploits logiciels. Axis répond à ces risques avec des solutions de sécurité de pointe qui s'intègrent parfaitement aux infrastructures existantes, offrant fiabilité, évolutivité et protection robuste.

Axis adopte une approche de sécurité dès la conception, intégrant le chiffrement, l'authentification, les mises à jour logicielles sécurisées, le contrôle d'accès, le renforcement du système et la journalisation des événements. Des protocoles sécurisés tels que SIPS, SRTP, HTTPS et IEEE 802.1AE activent une communication et une transmission de données sécurisées.

Le logiciel de gestion audio Axis offre un contrôle d'accès basé sur les rôles, une intégration sécurisée et un enregistrement complet des événements, pour les déploiements sur site et dans le cloud.

En tirant parti de ces couches de sécurité, les systèmes audio en réseau Axis offrent une protection complète contre les cybermenaces.

Table des matières

1 Introduction

Les systèmes audio jouent un rôle crucial dans la communication, la sécurité et l'efficacité opérationnelle dans divers secteurs tels que le commerce de détail, les transports, la sécurité publique et l'enseignement. Ces systèmes constituent également des cibles attrayantes pour les cyberattaques, et par conséquent, il est essentiel de mettre en place des mesures de sécurité robustes. Un système audio compromis peut avoir des conséquences graves et de grande ampleur.

Ce livre blanc explore les principaux niveaux de sécurité utilisés par les haut-parleurs et les systèmes audio Axis pour relever ces défis.

2 Comprendre les risques

Avec le déploiement croissant de solutions audio en réseau dans toutes les industries, les risques potentiels associés aux systèmes non sécurisés ont considérablement augmenté.

Les systèmes audio en réseau peuvent être exposés à plusieurs types de menaces.

- **Accès non autorisé.** Les dispositifs audio non protégés peuvent bénéficier d'un accès distant par des personnes malveillantes qui pourraient alors prendre le contrôle des haut-parleurs, diffuser des annonces non autorisées ou perturber le fonctionnement.
- **Écoute clandestine et interception de données.** Les systèmes audio en réseau transmettent parfois des données vocales sensibles via des réseaux câblés ou sans fil. Sans cryptage, les pirates pourraient intercepter et procéder à l'enregistrement des conversations, ce qui entraînerait des atteintes à la confidentialité, de l'espionnage industriel ou l'utilisation abusive d'informations confidentielles.
- **Attaques par déni de service (DoS).** Les pirates peuvent inonder les haut-parleurs en réseau ou les serveurs audio d'un trafic excessif, provoquant une surcharge du système et une interruption des services. De telles attaques pourraient rendre les systèmes de communication d'urgence inopérants à des moments critiques.
- **Attaques par logiciels malveillants et ransomwares.** Tout comme les infrastructures informatiques traditionnelles, les dispositifs audio en réseau peuvent être compromis par des logiciels malveillants ou des ransomwares. Les pirates pourraient verrouiller les dispositifs, exiger le paiement d'une rançon ou utiliser le système compromis comme point d'entrée pour attaquer l'ensemble du réseau.
- **Exploits logiciels et vulnérabilités de la chaîne logistique.** Les systèmes d'exploitation obsolètes présentant des failles de sécurité non corrigées peuvent être exploités pour gain de contrôle des dispositifs audio. De plus, des pratiques peu sûres dans la chaîne d'approvisionnement peuvent introduire des vulnérabilités avant le déploiement, rendant les systèmes vulnérables dès le départ.

3 Avantages de l'audio en réseau Axis

Axis fournit des solutions de sécurité de pointe pour les haut-parleurs et les systèmes, qui assurent une intégration transparente aux infrastructures existantes. L'architecture ouverte assure la compatibilité avec divers systèmes et protocoles. Le système Axis est flexible et conçu pour évoluer en fonction des besoins de votre organisation, des petits déploiements aux réseaux à l'échelle de l'entreprise. Axis propose des systèmes de gestion audio sur site et basés sur le cloud.

Axis utilise une approche de sécurité intégrée pour le développement de logiciels. Notre cadre Axis Security Development Model (ASDM) définit les processus et les outils qui garantissent l'intégration de la sécurité tout au long du cycle de vie du développement logiciel et réduisent le risque de vulnérabilités. L'ASDM fait l'objet d'améliorations continues.

L'une des nombreuses entrées à cette amélioration consiste à évaluer régulièrement diverses normes liées à la sécurité et à les mettre en correspondance avec l'ASDM. Notre logiciel répond aux normes strictes de l'industrie en matière de confidentialité et de sécurité des données, notamment le RGPD (Règlement général sur la protection des données) de l'Union européenne.

4 Principales caractéristiques de la sécurité des haut-parleurs et du système

Avec l'audio en réseau Axis, la sécurité est intégrée aux dispositifs et aux systèmes de gestion.

Chiffrement et authentification

- Le cryptage assure la transmission sécurisée des données audio via TLS 1.2 et 1.3, empêchant ainsi toute personne non autorisée d'intercepter et d'obtenir un accès aux informations.
- L'authentification garantit que seuls les dispositifs et les utilisateurs autorisés peuvent disposer d'un accès aux dispositifs, mais aussi à l'ensemble de la solution.

Mises à jour sécurisées des logiciels des dispositifs

- La fonctionnalité Secure Boot (présente dans la plupart des produits) et les correctifs signés numériquement garantissent que seul le logiciel vérifié du dispositif est installé. Les systèmes sont ainsi protégés contre les codes malveillants.

Contrôle d'accès

- AXIS Audio Manager Pro et AXIS Audio Manager Center utilisent un contrôle d'accès basé sur les rôles (RBAC), qui limite l'accès au système au personnel autorisé uniquement.
- La gestion centralisée active les administrateurs informatiques pour surveiller et contrôler efficacement les autorisations.

Renforcement du système

- Les paramètres par défaut sont optimisés pour la sécurité dès l'installation, ce qui réduit les vulnérabilités.
- Des options de configuration supplémentaires permettent une personnalisation en fonction de cas d'utilisation spécifiques. Le guide de renforcement d'AXIS OS, disponible à l'adresse *help.axis.com/axis-os-hardening-guide*, fournit des conseils techniques.

Enregistrement et surveillance des événements

- L'enregistrement complet offre une visibilité sur les activités du système. Cela peut aider à la détection des menaces en temps réel et à la réalisation d'analyses médico-légales.

5 Sécurité dans l'ensemble du système

Avec l'audio réseau Axis, la sécurité est intégrée aux dispositifs et aux systèmes de gestion. Des protocoles sécurisés activent un haut niveau de sécurité dans la communication entre les dispositifs et le logiciel de gestion.

5.1 Sécurité du périphérique

Toutes les enceintes Axis fonctionnent sous AXIS OS, notre logiciel spécialement conçu pour les dispositifs Axis. Il permet une valeur à long terme, une cybersécurité et une intégration de classe mondiale. Avec AXIS OS, tous nos haut-parleurs bénéficient des fonctionnalités de sécurité robustes de l'écosystème Axis. Cela garantit la cohérence et la fiabilité sur tous les dispositifs et offre une protection complète pour chaque déploiement. Les fonctionnalités de sécurité comprennent des systèmes de fichiers chiffrés et la plate-forme de cybersécurité matérielle Axis Edge Vault (*axis.com/solutions/edge-vault*).

Axis Edge Vault protège l'intégrité des dispositifs Axis et permet l'exécution d'opérations sécurisées basées sur des clés cryptographiques. Il active la vérification et l'exploitation de l' identifiant de périphérique Axis conforme à la norme IEEE 802.1AR , pour une intégration sécurisée du dispositif dans des réseaux zéro confiance via l' IEEE 802.1X et le protocole HTTPS. Avec l' Axis Edge Vault, vous pouvez démarrer le dispositif en toute sécurité, l'intégrer et être sûr(e) que les informations sensibles telles que les clés cryptographiques sont protégées.

Avec Axis Edge Vault, vous pouvez être sûr que le dispositif Axis que vous avez reçu n'a pas été victime de sabotage ou compromis dans la chaîne logistique physique. Axis Edge Vault établit une chaîne de confiance et

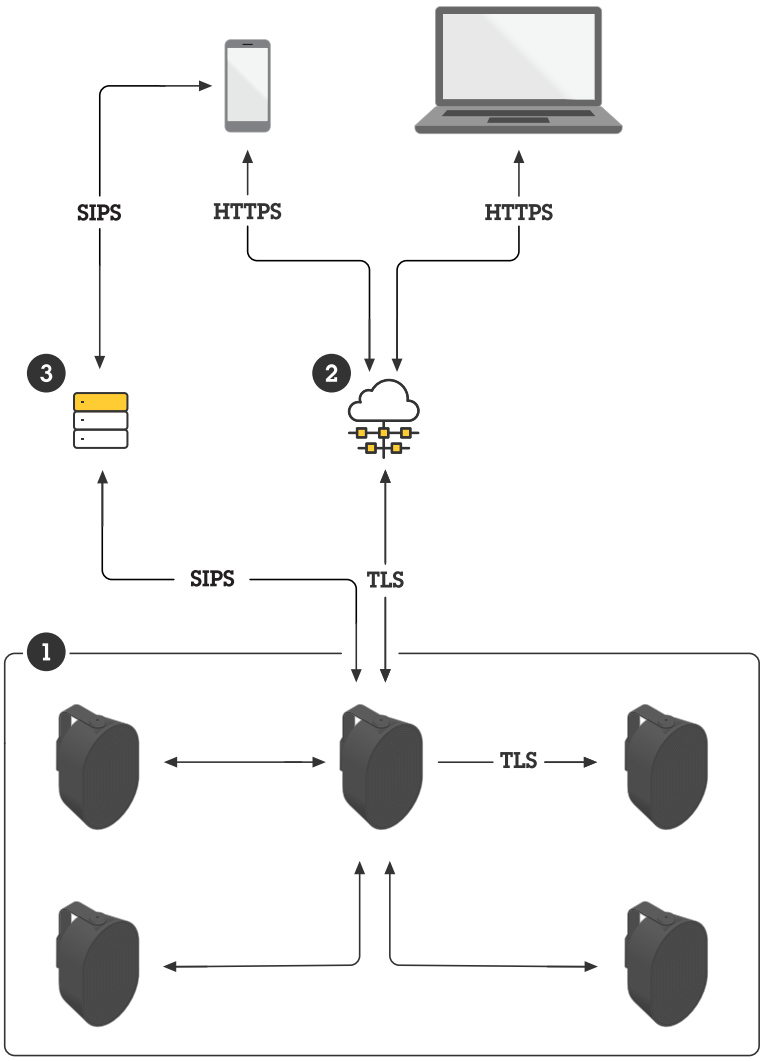
garantit une chaîne ininterrompue de logiciels validés cryptographiquement. Par exemple, la fonctionnalité *système d'exploitation signé* garantit que le logiciel du dispositif appartient à Axis et seules les mises à jour signées par Axis peuvent être installées.

5.2 Protocoles de sécurité

Les dispositifs et systèmes Axis utilisent des protocoles ouverts pour sécuriser les communications, les transmissions et les flux de données.

- **SIPS** (SIP Secure) : améliore le protocole SIP (Session Initiation Protocol) standard en intégrant le protocole TLS (Transport Layer Security). Une connexion sécurisée est ainsi établie entre un PBX IP et un téléphone VoIP. Une fois les paramètres de connexion sécurisée établis, le protocole SRTP (Secure Real-Time Transport Protocol) crypte les données vocales en paquets IP sécurisés pour leur transmission sur Internet. Cela permet un chiffrement complet entre l'émetteur (système téléphonique IP) et le récepteur (haut-parleur).

  En exploitant les protocoles SIPS et SRTP, les systèmes Axis sécurisent à la fois les données audio et la configuration de la connexion elle-même. Cela signifie que le flux audio et les détails de la connexion (tels que l'identité de l'appelant et le destinataire) sont entièrement cryptés et que le canal de communication sécurisé peer-to-peer est robuste.
- **Contrôleur multicast** : une fonctionnalité du contrôleur multicast des enceintes Axis permet la réception sécurisée des flux audio multicast envoyés via SRTP. Cela garantit le chiffrement des communications de groupe.
- **Transmit.cgi** et **receive.cgi**: Ces API VAPIX fournissent une méthode sécurisée pour envoyer et recevoir des flux audio dans le cadre d'une communication point à point chiffrée via HTTPS. CGI (Common Gateway Interface) est un protocole standard qui spécifie la communication entre un serveur Web et des programmes externes.
- **RTSPS** (Protocole de diffusion en continu sécurisé en temps réel) : protocole de contrôle réseau utilisé pour établir et gérer des flux multimédias en temps réel entre un serveur et un client. Cette fonctionnalité est prise en charge pour la diffusion sécurisée d'audio, grâce à un cryptage qui empêche tout accès non autorisé.
- **HTTPS** : toutes les API sont sécurisées par HTTPS afin de garantir la confidentialité et l'intégrité de toutes les communications.
- **IEEE 802.1AE** : également connu sous le nom de MACsec (Media Access Control Security), un protocole réseau qui crypte les communications réseau à l'aide de l'algorithme AES-128 sur les notions de base de la couche réseau 2. Associé aux protocoles HTTPS, RTSPS et SIPS, il permet un double chiffrement du trafic réseau et renforce considérablement la sécurité réseau.



Un système audio en réseau avec une communication sécurisée grâce à plusieurs protocoles ouverts.

1 *AXIS Audio Manager Edge : gestion audio sur site intégrée aux haut-parleurs Axis*
2 *AXIS Audio Manager Center : gestion audio centralisée dans le cloud hybride*
3 *PBX partenaire*

5.3 Sécurité des logiciels de gestion audio

5.3.1 Solutions sur site

Les solutions sur site Axis sont conçues pour gérer la gestion du zonage, la hiérarchisation et la sécurité des communications entre plusieurs haut-parleurs sur site.

AXIS Audio Manager Edge. Ce logiciel de gestion est intégré à chaque haut-parleur audio réseau d'Axis. Chaque haut-parleur devient ainsi un système audio complet et autonome, sans nécessité d'un serveur de gestion logiciel séparé. AXIS Audio Manager Edge est destiné à la gestion de projets peu complexes comprenant jusqu'à 200 dispositifs répartis dans 20 zones maximum.

- Prend en charge le chiffrement entre les dispositifs. La méthode de chiffrement par défaut est TLS avec des certificats auto-signés, mais nous vous recommandons d'installer des certificats de confiance sur vos dispositifs et d'activer l'authentification TLS dans les paramètres système du site. Cela offre une protection contre les attaques de type « man-in-the-middle ».
- Active l'intégration sécurisée des dispositifs au site local. La configuration initiale s'effectue via HTTPS à l'aide des identifiants du dispositif. Le protocole MQTT (TLS-PSK) est ensuite utilisé pour la communication

entre les dispositifs et le protocole SRTP est utilisé pour envoyer des données RTP cryptées, telles que des flux audio, entre les dispositifs.

- Fournit un accès au système externe pour les cas d'utilisation du fonctionnement via l'API HTTPS.

AXIS Audio Manager Pro. Ce logiciel de gestion est destiné à des projets plus substantiels et plus complexes. Il peut gérer un grand nombre de zones (plus de 500) et des milliers de dispositifs (plus de 5 000) dans une seule interface. AXIS Audio Manager Pro facilite la planification à long terme et les paramètres de priorité avancés.

- Comprend un contrôle d'accès basé sur les rôles, qui limite l'accès au système au personnel autorisé uniquement, avec prise en charge de l'intégration Active Directory.
- Active une intégration sécurisée des dispositifs.
- Comprend un journal détaillé des événements et des audits. Cela fournit un enregistrement complet de l'activité du système, qui peut aider les administrateurs à suivre les modifications, à surveiller le comportement et à résoudre les problèmes.

5.3.2 Solution basée sur le cloud

AXIS Audio Manager Center est un service d'administration et de surveillance à distance de systèmes multisite, qui vont de quelques sites à plusieurs milliers. Il est utilisé conjointement avec AXIS Audio Manager Edge sur chaque site local. Avec des composants basés sur le cloud et des composants sur site, c'est une solution de cloud hybride pratique et stable.

AXIS Audio Manager Center simplifie la gestion, offre un contrôle centralisé et assure l'intégration sécurisée des dispositifs. La charge de travail des utilisateurs est nettement réduite, avec une connexion unique pour programmer des annonces, la musique de fond, des publicités et plus encore pour les sites ou les zones sélectionné(e)s. Les principales caractéristiques de sécurité comprennent :

- Contrôle d'accès basé sur les rôles (RBAC) : limite l'accès au système au personnel autorisé uniquement.
- Gestion centralisée des utilisateurs : prend en charge les utilisateurs/groupes *My Axis* ou Active Directory pour une administration simplifiée. Pas besoin d'utilisateurs locaux.
- Intégration sécurisée : simplifie l'intégration sécurisée des dispositifs grâce à la fiabilité du cloud et en utilisant des certificats uniques installés sur chaque dispositif.
- Simplifie les configurations E2E sécurisées : active une configuration sécurisée de SIPS, y compris la gestion des certificats.
- Surveillance de l'état de santé et notifications : assure une surveillance centralisée de l'état de santé du système et déclenche des alertes immédiates en cas de problèmes potentiels.
- Communication sécurisée : toutes les communications entre le cloud et les dispositifs sont cryptées via TLS, avec TLS mutuel (authentification bidirectionnelle) garantissant une sécurité robuste.
- Accès distant : active un accès distant sécurisé au site local à partir de n'importe quel emplacement.

À propos d'Axis Communications

En améliorant la sûreté, la sécurité, l'efficacité opérationnelle et l'intelligence économique, Axis contribue à un monde plus sûr et plus intelligent. Leader de son secteur dans les technologies sur IP, Axis propose des solutions en vidéosurveillance, contrôle d'accès, visiophonie et systèmes audio. Ces solutions sont enrichies par des applications d'analyse intelligente et soutenues par des formations de haute qualité.

L'entreprise emploie environ 5000 personnes dans plus de 50 pays et collabore avec des partenaires technologiques et intégrateurs de systèmes du monde entier pour fournir des solutions sur mesure à ses clients. Axis a été fondée en 1984, son siège est situé à Lund en Suède.aboutaxis_text2