WHITE PAPER

Segurança cibernética com o áudio em rede Axis

Setembro 2025

Resumo

No mundo interconectado de hoje, proteger os sistemas de comunicação de áudio é vital para proteger informações confidenciais e manter a eficiência operacional. Os sistemas de áudio em rede enfrentam inúmeras ameaças, incluindo acesso não autorizado, espionagem, ataques de negação de serviço, malware e explorações de software. A Axis aborda esses riscos com soluções de segurança de última geração que se integram perfeitamente às infraestruturas existentes, oferecendo confiabilidade, capacidade de dimensionamento e proteção robusta.

A Axis emprega uma abordagem de segurança desde a concepção, incorporando criptografia, autenticação, atualizações seguras de software, controle de acesso, aumento do nível de proteção do sistema e registro de eventos. Protocolos seguros, como SIPS, SRTP, HTTPS e IEEE 802.1AE, permitem uma comunicação e transmissão de dados seguras.

O software de gerenciamento de áudio da Axis oferece controle de acesso baseado em funções, integração segura e registro abrangente de eventos, atendendo a implantações locais e baseadas em nuvem.

Ao aproveitar essas camadas de segurança, os sistemas de áudio em rede Axis oferecem proteção completa contra ameaças cibernéticas.

Índice

1 Introdução

Os sistemas de áudio desempenham um papel crucial na comunicação, segurança e eficiência operacional em vários setores, como varejo, transporte, segurança pública e educação. Esses sistemas também são alvos atraentes para ataques cibernéticos e, portanto, implementar medidas de segurança robustas é essencial. Um sistema de áudio comprometido pode ter consequências graves e abrangentes.

Este white paper explora as principais camadas de segurança que os alto-falantes e sistemas de áudio Axis empregam para enfrentar esses desafios.

2 Compreendendo os riscos

Com a crescente implantação de sistemas de áudio em rede em todos os setores, os riscos potenciais associados a sistemas não seguros aumentaram significativamente.

Os sistemas de áudio em rede podem estar expostos a vários tipos de ameaças.

- **Acesso não autorizado.** Dispositivos de áudio desprotegidos podem ser acessados remotamente por agentes mal-intencionados, que podem assumir o controle dos alto-falantes, fazer comunicados não autorizados ou interromper as operações.
- **Espionagem e interceptação de dados.** Os sistemas de áudio em rede às vezes transmitem dados de voz confidenciais por redes com ou sem fio. Sem criptografia, os invasores poderiam interceptar e gravar conversas, levando a violações de privacidade, espionagem industrial ou uso indevido de informações confidenciais.
- **Ataques de negação de serviço (DoS).** Os invasores podem atacar os alto-falantes do sistema em rede ou os servidores de áudio com tráfego excessivo, causando sobrecarga do sistema e interrupção dos serviços. Esses ataques podem tornar os sistemas de comunicação de emergência inoperantes em momentos críticos.
- **Ataques de malware e ransomware.** Assim como a infraestrutura de TI tradicional, os dispositivos de áudio em rede podem ser comprometidos por malware ou ransomware. Os invasores podem bloquear dispositivos, exigir o pagamento de resgate ou usar o sistema comprometido como ponto de entrada para atacar a rede como um todo.
- **Explorações de software e vulnerabilidades ao longo da cadeia de suprimentos.** Sistemas operacionais desatualizados e com falhas de segurança não corrigidas podem ser explorados para que os invasores obtenham controle sobre dispositivos de áudio. Além disso, práticas inseguras ao longo da cadeia de suprimentos podem introduzir vulnerabilidades antes da implantação, tornando os sistemas suscetíveis desde o início.

3 Benefícios do áudio em rede Axis

A Axis fornece soluções de alto-falantes e sistemas de segurança de última geração, que se integram perfeitamente às infraestruturas existentes. A arquitetura aberta oferece compatibilidade com diversos sistemas e protocolos. Um sistema Axis é flexível e desenhado para crescer de acordo com as necessidades da sua organização, desde pequenas implantações até redes em escala empresarial. A Axis oferece sistemas de gerenciamento de áudio locais e baseados em nuvem.

A Axis utiliza uma abordagem de segurança desde a concepção para o desenvolvimento de software. Nosso modelo Axis Security Development Model (ASDM) define processos e ferramentas que garantem a integração da segurança ao longo de todo o ciclo de vida de desenvolvimento do software e que reduzem o risco de vulnerabilidades. O ASDM é aprimorado continuamente.

Entre as diversas contribuições para melhorias, nós realizamos avaliações regulares de várias normas relacionadas à segurança e mapeamos essas normas para o ASDM. Nosso software atende às rigorosas normas do setor relacionadas à privacidade e segurança de dados, incluindo o GDPR (Regulamento Geral sobre a Proteção de Dados) da União Europeia.

4 Principais recursos de segurança de alto-falantes e sistemas

Com o áudio em rede Axis, a segurança está incorporada aos dispositivos e também aos sistemas de gerenciamento.

Criptografia e autenticação

- A criptografia garante a transmissão segura de dados de áudio por meio do TLS 1.2 e 1.3, impedindo que pessoas não autorizadas interceptem e tenham acesso às informações.
- A autenticação garante que apenas dispositivos e usuários autorizados possam ter acesso aos dispositivos, mas também à solução como um todo.

Atualizações seguras do software do dispositivo

- A inicialização segura (na maioria dos produtos) e os patches assinados digitalmente garantem que apenas software verificado seja instalado no dispositivo. Isso protege os sistemas contra códigos maliciosos.

Controle de acesso

- O AXIS Audio Manager Pro e o AXIS Audio Manager Center utilizam controle de acesso baseado em funções (RBAC), que limita o acesso ao sistema apenas ao pessoal autorizado.
- O gerenciamento centralizado permite que os administradores de TI monitorem e controlem as permissões de maneira eficaz.

Aumento do nível de proteção do sistema

- As configurações padrão estão prontas para usar e são otimizadas para proporcionar segurança, reduzindo vulnerabilidades.
- Opções de configuração adicionais permitem personalizar com base em casos de uso específicos. O Guia para Aumento do Nível de Proteção do AXIS OS, encontrado em *help.axis.com/axis-os-hardening-guide*, fornece orientações técnicas.

Registro e monitoramento de eventos

- Registros abrangentes fornecem uma melhor visibilidade das atividades do sistema. Isso pode ajudar na detecção de ameaças em tempo real e na análise forense.

5 Segurança por todo o sistema

Com o áudio em rede Axis, a segurança está incorporada aos dispositivos e aos sistemas de gerenciamento. Protocolos seguros proporcionam altos níveis de segurança na comunicação entre dispositivos e software de gerenciamento.

5.1 Segurança do dispositivo

Todos os alto-falantes Axis operam com o AXIS OS, nosso software exclusivo para dispositivos Axis. Ele agrega valor no longo prazo, proporciona segurança cibernética e permite integração de excelência. Com o AXIS OS, todos os nossos alto-falantes recebem os recursos de segurança robustos do ecossistema Axis. Isso proporciona consistência e confiabilidade em todos os dispositivos, oferecendo proteção de ponta a ponta para cada implantação. Os recursos de segurança incluem sistemas de arquivos criptografados e a plataforma de segurança cibernética baseada em hardware Axis Edge Vault (*axis.com/solutions/edge-vault*).

O Axis Edge Vault protege a integridade dos dispositivos Axis e permite executar operações seguras com base em chaves criptográficas. Ele permite que o ID do dispositivo Axis em conformidade com IEEE 802.1AR seja verificado e aproveitado para a integração segura do dispositivo em redes de confiança zero por meio de IEEE 802.1X e HTTPS. Com o Axis Edge Vault, você pode inicializar e integrar o dispositivo com segurança, tendo a certeza de que informações confidenciais, como chaves criptográficas, estarão protegidas.

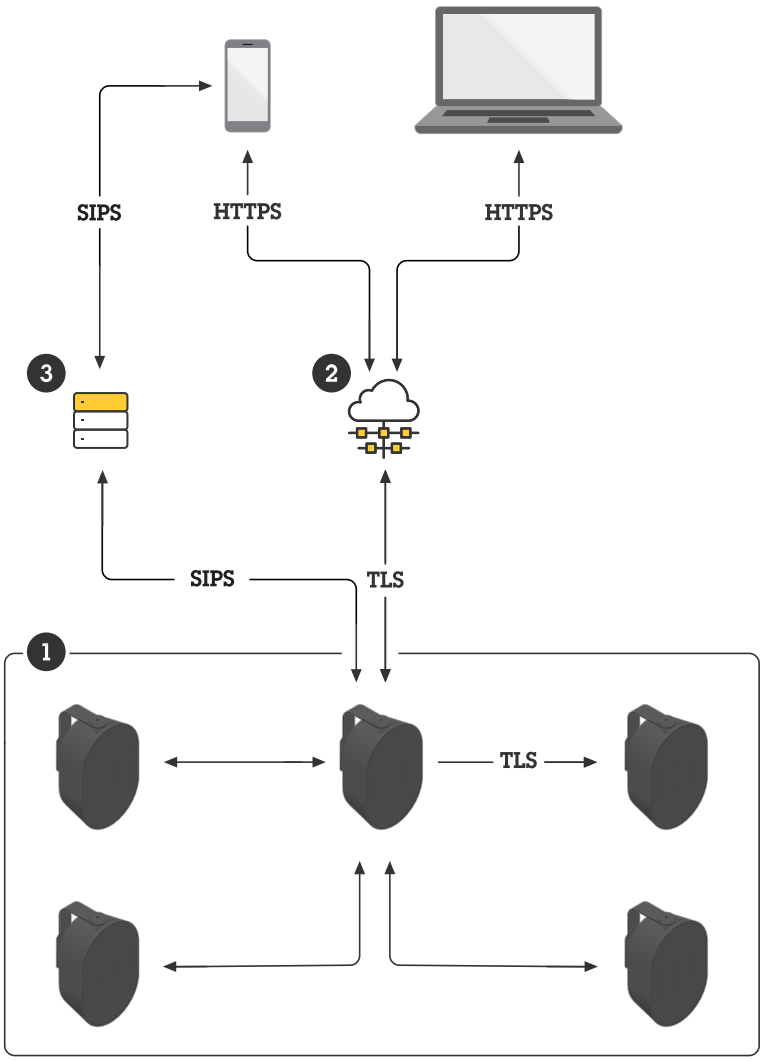
Com o Axis Edge Vault, você tem a garantia de que o dispositivo Axis que recebeu não sofreu manipulação ou foi comprometido ao longo da cadeia de suprimentos física. O Axis Edge Vault estabelece uma cadeia de confiança e assegura uma cadeia ininterrupta de software criptograficamente validado. Por exemplo, o recurso *signed OS* garante que o software do dispositivo pertence realmente à Axis e que somente atualizações assinadas pela Axis possam ser instaladas.

5.2 Protocolos de segurança

Os dispositivos e sistemas Axis utilizam protocolos abertos para comunicação, transmissão e stream seguros.

- **SIPS** (SIP Secure): aprimora o SIP (Session Initiation Protocol) padrão incorporando TLS (Transport Layer Security). Isso estabelece uma conexão segura entre um IP PBX e um telefone VoIP. Depois que a conexão segura é configurada, o SRTP (Secure Real-Time Transport Protocol) criptografa os dados de voz em pacotes IP seguros para transmissão pela Internet. Isso fornece criptografia de ponta a ponta, do transmissor (sistema de telefone IP) ao receptor (alto-falante).

  Ao utilizar o SIPS e o SRTP, os sistemas Axis protegem tanto os dados de áudio quanto a própria configuração da conexão. Isso significa que o stream de áudio e os detalhes da conexão (como identidade do chamador e destinatário) são totalmente criptografados e que o canal de comunicação seguro ponto a ponto é robusto.
- **Controlador multicast**: um recurso de controlador multicast nos alto-falantes Axis permite a recepção segura de streams de áudio multicast enviados via SRTP. Isso garante que a comunicação em grupo seja criptografada.
- **Transmit.cgi** e **receive.cgi**: essas APIs VAPIX fornecem um método seguro para enviar e receber streams de áudio em comunicação ponto a ponto criptografada via HTTPS. O CGI (Common Gateway Interface) é um protocolo padrão que especifica a comunicação entre um servidor web e programas externos.
- **RTSPS** (Real-Time Streaming Protocol Secure): um protocolo de controle de rede usado para estabelecer e gerenciar streams de mídia entre um servidor e um cliente em tempo real. Isso é compatível com streams de áudio seguros, utilizando criptografia para impedir acesso não autorizado.
- **HTTPS**: todas as APIs são protegidas com HTTPS para manter a confidencialidade e a integridade em todas as comunicações.
- **IEEE 802.1AE**: também conhecido como MACsec (Media Access Control Security), um protocolo de rede que criptografa a comunicação de rede de forma fundamental na camada 2 da rede usando AES-128. Se combinado com HTTPS, RTSPS e SIPS, o tráfego de rede é essencialmente criptografado duas vezes e a segurança em rede é significativamente aprimorada.



Um sistema de áudio em rede com comunicação segura graças a vários protocolos abertos.

1 *AXIS Audio Manager Edge: gerenciamento de áudio local integrado aos alto-falantes Axis*
2 *AXIS Audio Manager Center: gerenciamento de áudio centralizado em nuvem híbrida*
3 *PBX de parceiro*

5.3 Segurança no software de gerenciamento de áudio

5.3.1 Soluções locais

As soluções locais da Axis foram desenhadas para gerenciar o zoneamento, a priorização e a comunicação segura entre vários alto-falantes no local de instalação.

AXIS Audio Manager Edge. Esse software de gerenciamento vem integrado em todos os alto-falantes de áudio em rede da Axis. Isso torna cada alto-falante um sistema de som completo e multifuncional, sem a necessidade de um servidor de gerenciamento de software separado. O AXIS Audio Manager Edge destina-se a gerenciar projetos de baixa complexidade, compostos de até 200 dispositivos em até 20 zonas.

- Oferece suporte para criptografia entre dispositivos. O método de criptografia padrão é TLS com certificados autoassinados, mas recomendamos que você instale certificados confiáveis em seus dispositivos e ative a autenticação TLS nas configurações do sistema do local. Isso oferece proteção contra ataques man-in-the-middle (intermediários).
- Permite a integração segura de dispositivos à instalação local. A configuração inicial é realizada por HTTPS com as credenciais do dispositivo. Depois disso, o MQTT (TLS-PSK) é usado para comunicação entre

dispositivos e o SRTP é usado para enviar dados RTP criptografados, como streams de áudio, entre os dispositivos.

- Fornece acesso externo ao sistema para casos de uso operacionais por meio da API HTTPS.

AXIS Audio Manager Pro. Esse software de gerenciamento foi concebido para projetos de maior porte e mais avançados. Ele pode lidar com um grande número de zonas (mais de 500) e milhares de dispositivos (mais de 5.000) em uma única interface. O AXIS Audio Manager Pro facilita a programação de longo prazo e as configurações avançadas de prioridade.

- Inclui controle de acesso baseado em funções, que limita o acesso ao sistema apenas ao pessoal autorizado, com suporte para integração com o Active Directory.
- Permite a integração segura de dispositivos.
- Inclui um registro detalhado de eventos e auditorias. Isso fornece um registro abrangente da atividade do sistema, o que pode ajudar os administradores a rastrear alterações, monitorar comportamentos e solucionar problemas.

5.3.2 Solução baseada em nuvem

O AXIS Audio Manager Center é um serviço de gerenciamento e monitoramento remotos de sistemas para vários locais de instalação, que pode ser dimensionado para alguns ou para milhares de locais. Ele é usado em conjunto com o AXIS Audio Manager Edge em cada site local. Utilizando componentes baseados na nuvem e locais, esta é uma solução conveniente e estável de nuvem híbrida.

O AXIS Audio Manager Center simplifica o gerenciamento, oferece controle centralizado e lida com a integração segura dos dispositivos. A carga de trabalho do usuário é significativamente reduzida com login único para agendar comunicados, música de fundo, anúncios e muito mais para sites ou zonas selecionados. Os recursos principais de segurança incluem:

- Controle de acesso baseado em função (RBAC): limita o acesso ao sistema apenas ao pessoal autorizado.
- Gerenciamento centralizado de usuários: oferece suporte a usuários/grupos do *My Axis* ou Active Directory para uma administração simplificada. Não há necessidade de usuários locais.
- Integração segura: simplifica a integração segura de dispositivos com confiança da nuvem, usando certificados exclusivos instalados em cada dispositivo.
- Simplifica as configurações E2E seguras: permite a configuração segura do SIPS, incluindo o gerenciamento de certificados.
- Monitoramento da integridade e notificações: oferece monitoramento centralizado da integridade do sistema e alertas imediatos sobre possíveis problemas.
- Comunicação segura: toda a comunicação entre a nuvem e os dispositivos é criptografada via TLS, com TLS mútuo (autenticação bidirecional), garantindo uma segurança robusta.
- Acesso remoto: permite acesso remoto seguro ao site local, de qualquer lugar.

Sobre a Axis Communications

A Axis possibilita um mundo mais inteligente e seguro, aprimorando a segurança, proteção, eficiência operacional e inteligência nos negócios. Como uma empresa de tecnologia em rede e líder do setor, a Axis oferece soluções de videomonitoramento, controle de acesso, interfones e áudio. Essas soluções são aprimoradas por meio de aplicativos de análise inteligentes e apoiadas por treinamentos de alta qualidade.aboutaxis_text

A Axis conta com cerca de 5.000 funcionários dedicados, em mais de 50 países, e colabora com parceiros de tecnologia e integração de sistemas em todo o mundo para oferecer soluções aos clientes. A Axis foi fundada em 1984 e está sediada em Lund, na Suécia.