

BIAŁA KSIĘGA

Wrzesień 2025

Streszczenie

We współczesnym świecie, w którym przeplatają się różne dziedziny życia, zabezpieczenie systemów audio ma kluczowe znaczenie dla ochrony poufnych informacji i utrzymania produktywności. Sieciowe systemy audio są narażone na liczne zagrożenia, w tym nieautoryzowany dostęp, podsłuchy, ataki typu denial-of-service, złośliwe oprogramowanie czy luki w zabezpieczeniach własnego oprogramowania. Firma Axis zagrożeniom tym przeciwdziała, oferując najnowocześniejsze rozwiązania w zakresie bezpieczeństwa, harmonijnie integrujące się z istniejącą infrastrukturą, aby zapewnić niezawodność, skalowalność i szeroką ochronę.

Axis stosuje podejście „bezpieczeństwa w fazie projektowania” obejmujące szyfrowanie, uwierzytelnianie, bezpieczne aktualizacje oprogramowania, kontrolę dostępu, podniesione bezpieczeństwo systemu i rejestrowanie zdarzeń. Bezpieczne protokoły w rodzaju SIPS, SRTP, HTTPS i IEEE 802.1AE zabezpieczają komunikację i transmisję danych.

Oprogramowanie do zarządzania dźwiękiem Axis zapewnia kontrolę dostępu opartą na rolach, bezpieczne włączanie urządzeń do sieci oraz kompleksowe rejestrowanie zdarzeń, dostosowane zarówno do zastosowań lokalnych, jak i chmurowych.

Dzięki wykorzystaniu tych warstw zabezpieczeń sieciowe systemy audio Axis dają kompleksową ochronę przed cyberzagrożeniami.

Spis treści

1	Wprowadzenie	4
2	Ryzyko	4
3	Zalety sieciowych urządzeń audio Axis	4
4	Najważniejsze cechy bezpieczeństwa głośników i systemu	5
5	Bezpieczeństwo w całym systemie	5
5.1	Zabezpieczenia urządzenia	5
5.2	Protokoły bezpieczeństwa	6
5.3	Bezpieczeństwo w oprogramowaniu do zarządzania dźwiękiem	7
5.3.1	Rozwiązania lokalne	7
5.3.2	Rozwiązanie oparte na chmurze	8

1 Wprowadzenie

Systemy audio odgrywają kluczową rolę w komunikacji, bezpieczeństwie i produktywności w wielu branżach jak choćby handel detaliczny, transport, bezpieczeństwo publiczne czy szkolnictwo. Są jednocześnie atrakcyjnym celem cyberataków, dlatego konieczne jest stosowanie mocnych środków bezpieczeństwa. Korzystanie z podatnego na zagrożenia systemu audio może nieść poważne i daleko idące konsekwencje.

W niniejszej białej księdze omówiono główne warstwy zabezpieczeń w głośnikach i systemach audio Axis, mające na celu sprostanie tym wyzwaniom.

2 Ryzyko

Wraz z rosnącą popularnością sieciowych rozwiązań fonicznych w różnych branżach znacząco wzrosło potencjalne ryzyko związane z brakiem należytego zabezpieczenia systemów.

Sieciowe systemy audio mogą być narażone na kilka rodzajów zagrożeń.

- **Nieautoryzowany dostęp.** Niechronione urządzenia foniczne mogą być narażone na złośliwe działania dokonywane zdalnie, mogące doprowadzić do przejęcia kontroli nad głośnikami, nadawania nieautoryzowanych komunikatów lub zakłócania pracy w obiekcie.
- **Podsłuchiwanie i przechwytywanie danych.** Sieciowe systemy audio czasami przesyłają poufne dane głosowe przez sieci przewodowe lub bezprzewodowe. Bez szyfrowania, atakujący mogliby przechwytywać i zapisywać rozmowy, co prowadziłoby do naruszenia prywatności, szpiegostwa przemysłowego lub niewłaściwego wykorzystania poufnych informacji.
- **Ataki typu DoS.** Atakujący mogą narażać głośniki sieciowe lub serwery audio na nadmierny ruch sieciowy, powodując przeciążenie systemu i przerwy w działaniu usług. Ataki mogą spowodować ustanie działania systemów łączności awaryjnej w krytycznie ważnych momentach.
- **Ataki złośliwego oprogramowania i oprogramowania ransomware.** Podobnie jak zwykła infrastruktura IT, sieciowe urządzenia foniczne mogą zostać zainfekowane złośliwym oprogramowaniem lub oprogramowaniem ransomware. Atakujący mogą zablokować urządzenia, zażądać okupu lub wykorzystać zainfekowany system jako punkt wyjścia do ataku na rozleglejszą sieć.
- **Luki w zabezpieczeniach oprogramowania i łańcuchu dostaw.** Nieaktualne systemy operacyjne z niezaktualizowanymi lukami bezpieczeństwa łatwo wykorzystać do przejęcia kontroli nad urządzeniami fonicznymi. Nieprzezorne praktyki w łańcuchu dostaw sprzyjają powstawaniu luk w zabezpieczeniach jeszcze przed wdrożeniem, czyniąc systemy podatnymi na ataki od samego początku.

3 Zalety sieciowych urządzeń audio Axis

Axis dostarcza najnowocześniejsze rozwiązania w zakresie zabezpieczeń głośników i systemów oferujące płynną integrację z istniejącą infrastrukturą. Otwarta architektura zapewnia kompatybilność z różnymi systemami i protokołami. System Axis odznacza się swobodą zastosowań i pomyślany jest tak, aby rozwijać się wraz z potrzebami firmy, od skromnych instalacji po sieci skali enterprise. Axis oferuje zarówno lokalne, jak i chmurowe systemy zarządzania dźwiękiem.

Tworząc oprogramowanie, kieruje się podejściem bezpieczeństwa w fazie projektowania. Nasza struktura Axis Security Development Model (ASDM) określa procesy i narzędzia zapewniające integrację zabezpieczeń w całym cyklu życia oprogramowania i zmniejszające ryzyko wystąpienia luk w zabezpieczeniach. Model ASDM jest stale rozwijany.

Jednym z wielu czynników wpływających na rozwój jest regularna ocena różnych standardów związanych z bezpieczeństwem i odwzorowanie ich na model ASDM. Nasze oprogramowanie spełnia rygorystyczne normy przemysłowe w zakresie zachowania prywatności i bezpieczeństwa danych, w tym unijne rozporządzenie RODO (Rozporządzenie o Ochronie Danych Osobowych).

4 Najważniejsze cechy bezpieczeństwa głośników i systemu

W sieciowym systemie audio Axis zabezpieczenia wbudowane są w urządzenia, jak również systemy zarządzania.

Szyfrowanie i uwierzytelnianie

- Szyfrowanie zapewnia bezpieczną transmisję danych fonicznych za pośrednictwem protokołów TLS 1.2 i 1.3, uniemożliwiając nieuprawnionym osobom przechwycenie i wgląd w informacje.
- Uwierzytelnianie gwarantuje, że dostęp do urządzeń i całego rozwiązania mają wyłącznie urządzenia i użytkownicy autoryzowani.

Bezpieczne aktualizacje oprogramowania urządzeń

- Bezpieczne uruchomienie (w większości urządzeń) i cyfrowo podpisane poprawki zapewniają, że zainstalowane jest wyłącznie zweryfikowane oprogramowanie urządzenia. Stanowi to ochronę systemów przed działaniem złośliwego kodu.

Kontrola dostępu

- Aplikacje AXIS Audio Manager Pro i AXIS Audio Manager Center wykorzystują kontrolę dostępu opartą na rolach (RBAC – Role-Based Access Control), która ogranicza dostęp do systemu wyłącznie do uprawnionego personelu.
- Scentralizowane zarządzanie umożliwia administratorom systemu IT skuteczne monitorowanie i kontrolę uprawnień.

Podnoszenie bezpieczeństwa systemu

- Domyślne ustawienia zoptymalizowane są pod kątem bezpieczeństwa od razu po dostarczeniu urządzenia, co zmniejsza podatność na zagrożenia.
- Dodatkowe opcje konfiguracyjne umożliwiają dostosowanie do konkretnych zastosowań. Dokument „Zalecenia dotyczące zwiększenia funkcjonalności i bezpieczeństwa systemu AXIS OS” dostępny pod adresem help.axis.com/axis-os-hardening-guide zawiera porady techniczne w tym zakresie.

Rejestrowanie i monitorowanie zdarzeń

- Kompleksowe rejestrowanie zapewnia wgląd w czynności systemu. Wgląd taki może być pomocny w wykrywaniu zagrożeń w czasie rzeczywistym i analizie na potrzeby dowodowe.

5 Bezpieczeństwo w całym systemie

W sieciowym systemie audio Axis zabezpieczenia wbudowane są w urządzenia i systemy zarządzania. Bezpieczne protokoły umożliwiają uzyskanie wysokiego poziomu bezpieczeństwa w komunikacji pomiędzy urządzeniami a oprogramowaniem do zarządzania.

5.1 Zabezpieczenia urządzenia

Wszystkie głośniki Axis działają w oparciu o system operacyjny AXIS OS, czyli nasze oprogramowanie układowe przeznaczone do urządzeń Axis. Zapewnia ono długoterminowe działanie urządzeń, cyberbezpieczeństwo oraz integrację na światowym poziomie. Dzięki oprogramowaniu AXIS OS wszystkie nasze głośniki zyskują niezawodne funkcje bezpieczeństwa z ekosystemu Axis. Zapewnia to spójność i niezawodność we wszystkich urządzeniach oraz kompleksową ochronę każdej naszej instalacji. Funkcje bezpieczeństwa obejmują szyfrowane systemy plików oraz sprzętową platformę cyberbezpieczeństwa Axis Edge Vault (axis.com/solutions/edge-vault).

Platforma Axis Edge Vault chroni integralność urządzeń Axis i umożliwia wykonywanie bezpiecznych operacji w oparciu o klucze kryptograficzne. Umożliwia weryfikację i wykorzystanie identyfikatora urządzenia Axis zgodnego z normą IEEE 802.1AR w celu bezpiecznego włączenia urządzenia do sieci IP typu zero trust network poprzez protokoły IEEE 802.1X i HTTPS. Dzięki platformie Axis Edge Vault można bezpiecznie uruchomić urządzenie, zintegrować je i być pewnym, że poufne informacje, jak choćby klucze kryptograficzne, są chronione.

Dzięki platformie Axis Edge Vault użytkownik zyskuje pewność, że dostarczone urządzenie Axis nie zostało zmodyfikowane ani naruszone w fizycznym łańcuchu dostaw. Axis Edge Vault ustanawia łańcuch zaufania i zapewnia nieprzerwany łańcuch oprogramowania zweryfikowanego kryptograficznie. Na przykład funkcja *podpisanego oprogramowania AXIS OS* urządzenia gwarantuje, że oprogramowanie pochodzi od firmy Axis, a zainstalować można wyłącznie aktualizacje oprogramowania podpisane przez Axis.

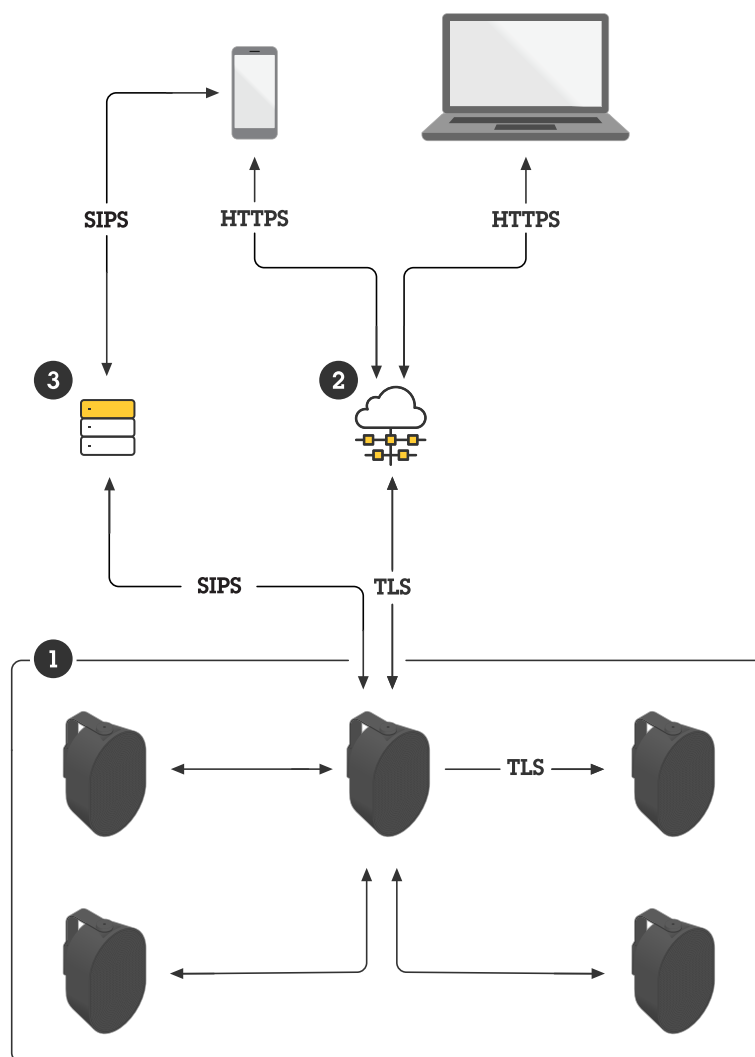
5.2 Protokoły bezpieczeństwa

Urządzenia i systemy firmy Axis wykorzystują protokoły oparte na otwartych platformach do bezpiecznej komunikacji, transmisji i strumieniowania.

- **SIPS** (SIP Secure): rozbudowuje standardowy protokół SIP (Session Initiation Protocol) poprzez zastosowanie zabezpieczeń TLS (Transport Layer Security). Umożliwia to ustanowienie bezpiecznego połączenia pomiędzy centralą SIP a telefonem VoIP. Po nawiązaniu bezpiecznego połączenia protokół SRTP (Secure Real-Time Transport Protocol) szyfruje dane głosowe do postaci bezpiecznych pakietów IP celem przesłania przez internet. Zapewnia to całościowe szyfrowanie transmisji od nadawcy (system telefoniczny IP) do odbiorcy (głośnik).

Wykorzystując protokoły SIPS i SRTP, systemy Axis zabezpieczają zarówno dane audio, jak i samo nawiązywanie połączenia. Oznacza to, że strumień foniczny i szczegóły połączenia (takie jak tożsamość nadawcy i odbiorcy) są w pełni szyfrowane, a kanał komunikacji peer-to-peer jest bezpieczny.

- **Kontroler Multicast**: funkcja kontrolera Multicast w głośnikach Axis umożliwia bezpieczny odbiór strumieni fonicznych Multicast wysyłanych za pośrednictwem protokołu SRTP. Zapewnia to szyfrowanie komunikacji grupowej.
- **Transmit.cgi** i **receive.cgi**: interfejsy API VAPIX zapewniają bezpieczną metodę wysyłania i odbierania strumieni fonicznych w ramach szyfrowanej komunikacji punkt-punkt za pośrednictwem protokołu HTTPS. CGI (Common Gateway Interface) to standardowy protokół formułujący komunikację między serwerem WWW a programami zewnętrznymi.
- **RTSPS** (Real-Time Streaming Protocol Secure): protokół kontroli sieci służący do ustanawiania i zarządzania strumieniami multimedialnymi w czasie rzeczywistym w komunikacji pomiędzy serwerem a klientem. Obsługiwany jest dla zapewnienia bezpiecznego strumienia fonicznego wykorzystującego szyfrowanie na potrzeby zapobiegania nieautoryzowanemu dostępowi.
- **HTTPS**: wszystkie interfejsy API są zabezpieczone protokołem HTTPS do zachowania poufności i integralności wszystkich komunikatów.
- **IEEE 802.1AE**: znany również jako MACsec (Media Access Control Security), protokół sieciowy szyfrujący komunikację sieciową przy użyciu algorytmu AES-128 w warstwie sieciowej 2. W połączeniu z protokołami HTTPS, RTSPS i SIPS ruch sieciowy jest zasadniczo podwójnie szyfrowany, co znacznie zwiększa bezpieczeństwo sieci.



Sieciowy system audio z bezpieczną komunikacją dzięki kilku protokołom opartym na otwartych platformach.

- 1 *AXIS Audio Manager Edge: lokalne zarządzanie dźwiękiem zintegrowane z głośnikami Axis*
- 2 *AXIS Audio Manager Center: scentralizowane zarządzanie dźwiękiem w chmurze hybrydowej*
- 3 *Centrala firmy partnerskiej*

5.3 Bezpieczeństwo w oprogramowaniu do zarządzania dźwiękiem

5.3.1 Rozwiązania lokalne

Lokalne rozwiązania Axis zaprojektowano z myślą o zarządzaniu strefami, ustalaniu priorytetów i zapewnieniu bezpiecznej komunikacji pomiędzy wieloma głośnikami w danej lokalizacji.

AXIS Audio Manager Edge. Oprogramowanie to jest wbudowane we wszystkie sieciowe głośniki Axis. Dzięki niemu każdy głośnik staje się pełnym, wszechstronnym systemem dźwiękowym, który nie wymaga odrębnego serwera z oprogramowaniem zarządzającym. Oprogramowanie AXIS Audio Manager Edge jest przeznaczone do zarządzania prostszymi projektami do 200 urządzeń w maks. 20 strefach.

- Obsługuje szyfrowanie w połączeniach pomiędzy urządzeniami. Domyślną metodą szyfrowania jest protokół TLS z certyfikatami samopodpisanymi, niemniej zaleca się instalację zaufanych certyfikatów na własnych urządzeniach i włączenie uwierzytelniania TLS w ustawieniach systemowych obiektu. Zapewni to ochronę przed atakami typu „man-in-the-middle”.
- Umożliwia bezpieczne włączanie urządzeń do sieci IP w obiekcie lokalnym. Wstępna konfiguracja odbywa się za pośrednictwem protokołu HTTPS z wykorzystaniem danych uwierzytelniających urządzenia. Odtąd do

komunikacji pomiędzy urządzeniami wykorzystywany jest protokół MQTT (TLS-PSK), a do przesyłania zaszyfrowanych danych RTP, takich jak strumienie foniczne pomiędzy urządzeniami, protokół SRTP.

- Zapewnia zewnętrzny dostęp do systemu na potrzeby zastosowań obsługowych za pośrednictwem interfejsu API przez HTTPS.

AXIS Audio Manager Pro. Oprogramowanie to przeznaczone jest dla większych i bardziej złożonych projektów. W jednym interfejsie umożliwia obsługę dużej liczby stref (ponad 500) i tysięcy urządzeń (ponad 5000). AXIS Audio Manager Pro ułatwia opracowywanie długoterminowych harmonogramów i dokonywanie zaawansowanych ustawień priorytetów.

- Zawiera kontrolę dostępu opartą na rolach, ograniczającą dostęp do systemu wyłącznie do upoważnionego personelu, obsługuje integrację z usługą Active Directory.
- Umożliwia bezpieczne włączanie urządzeń do sieci IP.
- Zawiera szczegółowy dziennik zdarzeń i kontroli. Dziennik ten może pomóc administratorom w śledzeniu zmian, monitorowaniu zachowań i rozwiązywaniu problemów.

5.3.2 Rozwiązanie oparte na chmurze

AXIS Audio Manager Center to usługa do zdalnego zarządzania i monitorowania systemów w lokalizacjach, w liczbie od kilku do kilku tysięcy. Usługa jest używana wraz z oprogramowaniem AXIS Audio Manager Edge w poszczególnych lokalizacjach. W systemach opartych na chmurach hybrydowych stosuje się zarówno elementy chmurowe, jak i lokalne, by zapewnić niezawodne i stabilne działanie.

AXIS Audio Manager Center upraszcza zarządzanie, zapewnia scentralizowane sterowanie i obsługuje bezpieczne włączanie urządzeń do sieci. Praca użytkowników systemu jest znacznie ułatwiona, ponieważ wystarczy jednokrotne logowanie, aby ustawić harmonogram komunikatów, tło muzyczne, reklamy i inne treści dla wybranych lokalizacji lub stref. Główne funkcje zabezpieczeń to:

- Kontrola dostępu oparta na rolach: ogranicza dostęp do systemu wyłącznie do upoważnionego personelu.
- Scentralizowane zarządzanie użytkownikami: obsługuje użytkowników / grupy *My Axis* lub Active Directory na potrzeby sprawnej administracji. Nie jest konieczne w przypadku użytkowników lokalnych.
- Bezpieczne włączanie urządzeń do sieci: upraszcza dołączanie urządzeń do sieci IP z zachowaniem należytego bezpieczeństwa dzięki zabezpieczeniom z chmury, wykorzystując niepowtarzalne certyfikaty zainstalowane w każdym urządzeniu.
- Uproszczenie bezpiecznych konfiguracji E2E: umożliwia bezpieczne konfigurowanie z protokołem SIPS wraz z obsługą certyfikatów.
- Monitorowanie stanu i powiadomienia: zapewnia scentralizowane monitorowanie stanu systemu i natychmiastowe powiadomienia o potencjalnych problemach.
- Bezpieczna komunikacja: cała komunikacja pomiędzy chmurą a urządzeniami jest szyfrowana za pośrednictwem protokołu TLS, a wzajemne uwierzytelnianie dwukierunkowe z TLS zapewnia wysokie bezpieczeństwo.
- Zdalny dostęp: umożliwia bezpieczny zdalny dostęp do lokalnego obiektu z dowolnego miejsca.

O firmie Axis Communications

Axis wspiera rozwój inteligentnego oraz bezpiecznego świata przez poprawę bezpieczeństwa, ochrony, efektywności działania i wiedzy biznesowej. Jako firma zajmująca się technologiami sieciowymi oraz lider branży, Axis oferuje rozwiązania z zakresu dozoru wizyjnego, kontroli dostępu, systemów domofonowych i systemów audio. Ich rozszerzeniem i uzupełnieniem są inteligentne aplikacje analityczne oraz wysokiej jakości szkolenia.

Axis zatrudnia około 5000 pracowników w ponad 50 krajach oraz współpracuje z partnerami z obszaru technologii i integracji systemów na całym świecie w celu dostarczania swoich rozwiązań klientom. Firma została założona w 1984 roku i ma swoją siedzibę w Lund w Szwecji.