AXIS COMMUNICATIONS

Cybersecurity

PER UNA MAGGIORE
CYBERSECURITY, INSIEME.

AXIS COMMUNICATIONS

INDICE

INTRODUZIONE

Ridurre il rischio di incidenti informatici

Proteggere i dispositivi di rete e i servizi software dalle minacce informatiche è fondamentale per mettere al sicuro dati e sistemi. Un sistema compromesso può pregiudicare la riservatezza e l'integrità dei dati, che possono anche rivelarsi inaccessibili quando ne abbiamo necessità.

Essendo partner responsabili per la cybersecurity abbiamo raccolto alcune considerazioni e linee guida che aiutano ad acquistare e proteggere i dispositivi per la sicurezza fisica basati su IP. Il nostro desiderio è che diventi più facile per voi applicare le necessarie misure di sicurezza le misure di sicurezza, affinché possiate utilizzare le offerte Axis nel modo più sicuro possibile.

Oltre a leggere le seguenti pagine, potete ottenere ulteriori informazioni sulla cybersecurity e su come incrementare la protezione insieme a noi alla pagina www.axis.com/cybersecurity.

Una responsabilità comune

La cybersecurity riguarda i dispositivi, le persone, le tecnologie e i processi continui. Chiaramente è necessario unire le forze per fare in modo che ogni anello della catena sia il più forte possibile. La cybersecurity è una responsabilità comune che richiede la collaborazione tra i seguenti stakeholder, compresi i clienti finali.

Produttori di dispositivi

La cybersecurity inizia da qui. I produttori devono applicare best practice di progettazione, sviluppo, produzione e manutenzione del software, per ridurre al minimo il rischio di problemi durante l'intero ciclo di vita del prodotto. È importante un attento controllo della catena di fornitura. I dispositivi devono avere funzionalità integrate che consentano di attuare vari controlli di sicurezza. Devono essere disponibili strumenti per una configurazione e una gestione efficienti che supportino i processi o le policy di sicurezza del cliente. Inoltre, devono esistere canali per informare i partner e i clienti sulle vulnerabilità individuate di recente.

Distributori

Per i distributori che non toccano direttamente i prodotti, la cybersecurity è relativamente semplice. I distributori a valore aggiunto devono invece considerare gli stessi aspetti degli integratori e degli installatori, soprattutto se acquistano dispositivi da un produttore e li rietichettano con un altro (o il proprio) marchio. La trasparenza è fondamentale. L'origine del dispositivo deve essere chiara.

Consulenti, integratori e installatori

Possono aiutare i clienti a identificare, progettare e attuare controlli di sicurezza e fare in modo che i dispositivi per la sicurezza fisica non rappresentino un ostacolo in rete. A questo scopo è utile sviluppare una strategia per le password, la gestione degli accessi da remoto e la manutenzione del software e dei dispositivi connessi. Altrettanto importante è la garanzia che i dispositivi installati siano dotati degli ultimi aggiornamenti e che il sistema venga esaminato con un antivirus. Parlando di cybersecurity in generale, occorre anche considerare i problemi legati all'utilizzo di dispositivi OEM/ODM, perché le responsabilità non sono sempre chiare in questo senso.

Clienti finali

Così come ogni azienda ha esigenze specifiche di cybersecurity, non esistono configurazioni universali. È invece importante applicare una serie di regole di sicurezza delle informazioni per definire il campo d'azione. Rimuovere gli account predefiniti, impostare password univoche e da archiviare in sicurezza e cambiare regolarmente, assegnare permessi differenziati e installare sempre le patch e gli aggiornamenti più recenti sono solo alcuni esempi di misure preventive.

Ricercatori

Spesso individuano le vulnerabilità dei dispositivi. Se la vulnerabilità non è intenzionale, in genere il ricercatore informa il produttore e gli offre la possibilità di correggere il problema prima di renderlo noto. Tuttavia, se una vulnerabilità critica ha carattere intenzionale, spesso si rivolgono al pubblico per sensibilizzarlo.

Dalla sicurezza fisica alla cybersecurity

Quando si parla di sicurezza fisica, è facile comprendere i rischi. Se una porta non è chiusa a chiave, il rischio che entrino persone non autorizzate è maggiore. Gli oggetti di valore lasciati in vista potrebbero essere rubati facilmente. Gli errori e gli incidenti possono causare danni a persone, proprietà e oggetti. In genere, la sicurezza fisica e la cybersecurity vengono trattate allo stesso modo.

Che siate responsabili della sicurezza fisica della vostra azienda o della cybersecurity, i principi da applicare sono gli stessi:

> Identificare e classificare i beni e le risorse (cosa proteggere)

> Identificare le minacce plausibili (da chi e da cosa proteggersi)

> Identificare le vulnerabilità sfruttabili (probabilità)

> Identificare i costi previsti in caso di violazioni (conseguenze). Spesso, il rischio viene calcolato moltiplicando la probabilità di una minaccia per le sue conseguenze. Dopo averlo calcolato, occorre chiedersi cosa si è disposti a fare per prevenire gli effetti negativi.

Che cos'è la cybersecurity?
La cybersecurity è la protezione di sistemi e servizi dalle minacce informatiche. Tra le pratiche di cybersecurity figurano processi di prevenzione dei danni e del ripristino di computer, sistemi e servizi di comunicazione elettronici, comunicazioni cablate ed elettroniche e informazioni memorizzate per assicurare riservatezza, integrità, disponibilità, sicurezza, autenticità e il nonripudio.

Da quali minacce proteggersi?

Gli elementi fondamentali da proteggere in un sistema IT (tecnologia dell'informazione) o OT (tecnologia delle operazioni) sono riservatezza, integrità, disponibilità e sicurezza. Tutto ciò che ha effetti negativi su questi elementi è un incidente di cybersecurity.

Esaminiamo dunque le minacce più comuni per la cybersecurity e le vulnerabilità che sfruttano. Le quattro minacce informatiche più comuni per i sistemi di sicurezza fisica basati su IP sono:

1. **Ingenuità ed errori non intenzionali degli utenti**
2. **Uso scorretto intenzionale del sistema**
3. **Manomissioni e sabotaggi**
4. **Sfruttamento delle vulnerabilità del software**

1 Ingenuità ed errori non intenzionali degli utenti

Non importa quanto siano efficaci le tecnologie utilizzate per proteggere la rete: l'elemento umano rimane un fattore determinante nelle violazioni di sicurezza.

Tra gli errori umani che spalancano la porta a un attacco figurano:

> **Ingegneria sociale**

Un utente viene manipolato psicologicamente fino a commettere errori o divulgare informazioni sensibili. Sono esempi di ingegneria sociale il phishing e lo scareware.

> **Uso improprio delle password**

Ad esempio, uso di password non complesse o password non protette e/o aggiornate in modo adeguato.

> **Errata gestione dei componenti critici**

Smarrimento o errata collocazione di elementi che consentono di accedere al sistema. Esempi: badge di accesso, telefoni, laptop e documenti.

> **Cattiva gestione del sistema**

Gli aggiornamenti di sistema e le patch di sicurezza non sono installati.

> **Miglioramenti non riusciti**

Alcune persone cercano di correggere qualcosa ma finiscono per ridurre le prestazioni del sistema.

Vulnerabilità ed errori umani

Le vulnerabilità più comuni imputabili ad errori umani sono causate dalla non consapevolezza dei rischi informatici e dalla mancanza di regole e processi a lungo termine per la gestione dei rischi. Per ridurre il rischio di errori umani, tutto il personale di un'azienda deve imparare le prassi ottimali di cybersecurity. Occorre anche limitare l'accesso ai dispositivi di rete a poche persone fidate tramite il sistema di gestione video (VMS) o gestione dei dispositivi.

2 Uso scorretto intenzionale del sistema

Un'altra minaccia fin troppo comune è l'uso scorretto di un sistema da parte di persone che ne hanno accesso legittimo.

Tra gli esempi di uso scorretto intenzionale:

Manipolazione dei servizi e delle risorse di sistema

Furto di dati

Danni intenzionali al sistema

Vulnerabilità e uso scorretto intenzionale

È importante adottare policy e processi duraturi per gestire le vulnerabilità e ridurre le minacce derivanti da un uso improprio intenzionale del sistema. È fondamentale controllare le persone che hanno il permesso di accedere ai dati sensibili, nonché limitarne il numero.

Il software utilizzato per la gestione dei dispositivi di rete per la sicurezza fisica, come le telecamere, deve utilizzare un account da amministratore con credenziali proprie. L'account deve essere univoco e non condiviso. Gli operatori del sito devono avere account personali nel software di gestione e nessuno di loro deve avere accesso diretto ai dispositivi di sicurezza fisica. Se vi sono motivi per consentire l'accesso diretto, questo deve essere temporaneo.

3 Manomissioni o sabotaggi

La protezione fisica è molto importante ai fini della cybersecurity:

> I dispositivi esposti possono essere manomessi.

> I dispositivi esposti possono essere rubati.

> I cavi esposti possono essere scollegati, deviati o tagliati.

Vulnerabilità e minacce fisiche

Le vulnerabilità più comuni si hanno quando i dispositivi non sono custoditi in aree chiuse (ad esempio server e switch), le telecamere sono facilmente raggiungibili o non protette da custodie e i cavi non sono inseriti in tracce a muro o canaline. I dispositivi possono anche esporre altre risorse sulla stessa rete.

Attenti alle conseguenze

I sistemi video, audio e di controllo accessi non elaborano transazioni finanziarie e non conservano i dati dei clienti. Dunque, un attacco a questi sistemi può essere difficile da monetizzare e ha valore limitato per la criminalità organizzata. Ma un sistema compromesso può diventare pericoloso per altri sistemi. In situazioni del genere, calcolare i costi è difficile. In molti casi, purtroppo, le aziende imparano a caro prezzo. La protezione è come la qualità: si ha quel che si paga. Acquistare a buon mercato potrebbe costare molto di più nel lungo periodo se il produttore non considera la cybersecurity nell'intero ciclo di vita del prodotto.

4 Sfruttamento delle vulnerabilità del software

Nello sviluppo del software esistono rischi, in genere bug o errori di programmazione, che possono causare vulnerabilità di sicurezza sfruttabili in un attacco. Maggiore è il numero di vulnerabilità software di un dispositivo, maggiore è il rischio di esposizione agli attacchi. Prima di immettere un dispositivo sul mercato, il produttore deve idealmente adottare un modello di sviluppo software che includa processi e strumenti per ridurre al minimo il rischio di vulnerabilità in tutte le fasi di sviluppo.

Anche se nel settore è raro che esistano versioni software completamente prive di errori, i bug e altre imprecisioni che mettono a rischio la sicurezza devono sempre essere identificati, corretti e comunicati ai clienti dal produttore. Pertanto, il produttore deve essere trasparente nel comunicare le vulnerabilità del software appena individuate e offrire una soluzione tempestiva ai clienti. È inoltre importante che il cliente installi gli aggiornamenti software contenenti patch di sicurezza e correzioni di bug appena il produttore le rende disponibili.

Considerazioni dei clienti finali per ridurre i rischi

Per iniziare, quando si acquistano dispositivi per la sicurezza fisica pensando alla cybersecurity, vanno considerati diversi elementi.

Innanzitutto occorre esaminare l'approccio alla cybersecurity dei produttori: hanno una policy aziendale per identificare e valutare costantemente le loro risorse in termini di sicurezza informatica? Valutano anche i rischi relativi? È altrettanto importante comprendere le interazioni tra i produttori e la catena di fornitura. Inoltre, i dispositivi sono progettati e realizzati con funzionalità di cybersecurity integrate? Sono supportati da questo punto di vista?

Quali misure offrono per garantire la cybersecurity durante tutto il ciclo di vita di un dispositivo di rete? Cosa succede se il sistema dell'utente subisce un attacco? I produttori hanno linee guida che aiutano a reagire a un problema di cybersecurity che riguarda i loro dispositivi?

Queste sono solo alcune domande che verranno approfondite nelle seguenti pagine.

Informarsi sul fornitore del sistema di sorveglianza e sui suoi fornitori

I pericoli per la sicurezza sono sempre presenti. Sorgono nuove minacce e la loro natura può cambiare nel tempo. Spesso, le aziende pensano solo al modo in cui i fornitori valutano e contrastano questi rischi. E i fornitori dei fornitori? Come fanno i fornitori a controllare la loro catena e garantire che tutti i prodotti seguano un percorso sicuro, dai componenti al prodotto finito?

Il vostro fornitore si impegna a ridurre al minimo i rischi per la sicurezza?

> Controlla l'intera catena di fornitura, dai componenti al prodotto finito?

> Ha un modello di sviluppo software in cui la sicurezza è parte integrante?

> Progetta e produce dispositivi con protezione integrata?

> Condivide informazioni e strumenti per adottare tutte le cautele necessarie?

> Risponde velocemente e con aggiornamenti gratuiti se riscontra nuove vulnerabilità nel software?

Partner della catena di fornitura

La sicurezza della catena di fornitura inizia con lo scegliere i partner giusti tramite una rigorosa valutazione. Questa deve includere un'analisi dei processi di gestione della qualità e della sostenibilità di ogni azienda, che deve almeno essere certificata da un'agenzia esterna secondo le normative ISO 9001 o IATF 16949.

Valutazione dei subfornitori

Il vostro fornitore deve valutare i processi di gestione dei rischi dei subfornitori, oltre alle loro infrastrutture e ai processi produttivi. Occorre programmare visite in loco e audit di follow-up per verificare che le strutture soddisfino i requisiti e gli standard per la qualifica dei fornitori approvati. Nel valutare un potenziale nuovo partner della catena di fornitura, deve essere condotta un'analisi approfondita della posizione finanziaria e del modello di proprietà dei subfornitori.

Subfornitori strategici

Per quanto riguarda i fornitori di componenti critici e i partner di produzione, i rapporti con loro tendono ad essere particolarmente stretti e duraturi. Sono subfornitori strategici, con cui il vostro fornitore realizza progetti, definisce obiettivi e si impegna reciprocamente e a lungo termine. Tutti i componenti critici dei dispositivi del vostro fornitore devono essere acquistati direttamente da subfornitori strategici e stoccati in sede. I componenti non critici possono essere acquistati da partner di produzione, ma solo se si trovano in una lista di vendor approvati.

Quanto è sicura la produzione del vostro fornitore?

- Il vostro fornitore definisce e monitora i processi di produzione?
- Sviluppa e produce strumentazioni critiche per la produzione?
- Fornisce un sistema per testare componenti, moduli e prodotti durante la produzione, oltre al software, ai computer per i collaudi e alle altre infrastrutture hardware IT?
- Il vostro fornitore raccoglie i dati sulla produzione 24 ore su 24 e 7 giorni su 7 per consentire un'analisi dei dati in tempo reale, valutare eventuali rischi e implementare piani di mitigazione?

Per il vostro fornitore, il modo migliore di garantire che i subfornitori siano conformi ai requisiti specifici è condurre regolari audit in sede, a cadenza annuale o biennale. Gli audit devono riguardare una serie di aspetti importanti come la conformità dei processi, il controllo qualità e i documenti di tracciabilità. Devono anche comprendere revisioni della movimentazione fisica in stabilimento, della gestione dell'inventario e dei macchinari di produzione.

Le revisioni aziendali trimestrali sono un ottimo modo per monitorare le performance rispetto alle aspettative. Per i subfornitori strategici, si consiglia di condurre queste revisioni al massimo livello dirigenziale.

Sicurezza fisica

Tutti i siti della catena logistica, dal fornitore dei componenti al centro di distribuzione, devono rispettare criteri rigorosi di sicurezza delle infrastrutture. Ad esempio, devono sorvegliare costantemente gli ingressi e le uscite, mentre gli accessi dei visitatori devono essere registrati e archiviati. Un altro requisito è l'uso di scanner per rilevare oggetti o materiali indesiderati. I trasporti devono essere affidati solo a vettori esperti che adottano regole e controlli di sicurezza rigorosi. Si consiglia inoltre di sorvegliare e documentare frequentemente le merci in entrata e in uscita tramite le telecamere.

Reti zero trust

Le reti sono sempre più vulnerabili. La crescita esponenziale dei dispositivi connessi crea endpoint di rete esposti agli attacchi, che sono diventati non solo più numerosi, ma anche più sofisticati. Per questo, è emerso il concetto di "zero trust".

Non fidarsi di niente e nessuno

Come suggerisce il nome, in una rete zero trust il presupposto è non fidarsi di nessuna entità connessa alla/in rete – che si tratti di una persona o una macchina – indipendentemente da dove si trovi e da come si connetta. Piuttosto, l'idea di fondo delle reti zero trust è "Non fidarsi mai, verificare sempre".

Concedere solo l'accesso minimo

Questo richiede che l'identità di un'entità che accede o è connessa in rete sia verificata più volte e in modi diversi, a seconda del suo comportamento e della sensibilità dei dati specifici ai quali accede. In sostanza, alle entità viene concesso il livello di accesso minimo necessario per svolgere il loro compito.

Reti e architetture zero trust

Essendo sempre più attenti alla necessità di incrementare la cybersecurity, i clienti implementano reti e architetture zero trust; tra queste HTTPS e il più sofisticato standard IEEE 802.1X, che può consentire automaticamente l'accesso alla rete ai dispositivi autenticati o bloccare quelli non autenticati. Per i produttori è essenziale soddisfare questi requisiti includendo tecnologie o interfacce che supportino tali reti.

In una rete zero trust, il presupposto è non fidarsi di nessuna entità connessa alla/in rete.

La funzione del policy engine

Al centro di tutte le reti zero trust c'è il policy engine: si tratta di un software che consente a un'azienda di creare, monitorare e applicare regole di accesso ai dati e alle risorse di rete. I policy engine utilizzano una combinazione di analitiche di rete e regole programmate per concedere i permessi in base ai ruoli e a vari fattori.

Accettazione o rifiuto di ogni richiesta

In parole semplici, il policy engine confronta ogni richiesta di accesso alla rete con le regole e dice a chi deve farle rispettare se la richiesta sarà autorizzata o meno. In una rete zero trust, il policy engine definisce e applica la sicurezza dei dati e dei criteri di accesso tra modelli di hosting, posizioni, utenti e dispositivi.

Definizione e applicazione delle regole

Affinché un policy engine funzioni, le aziende devono definire attentamente regole e criteri all'interno dei principali controlli di sicurezza, come firewall di nuova generazione (NGFW), gateway di sicurezza per e-mail e cloud e software di prevenzione delle perdite di dati (DLP). Questi controlli si combinano per applicare microsegmentazioni della rete al di là dei modelli di hosting e delle posizioni geografiche.

Come è possibile accedere ai dati e alle risorse di rete?

I policy engine consentono di:

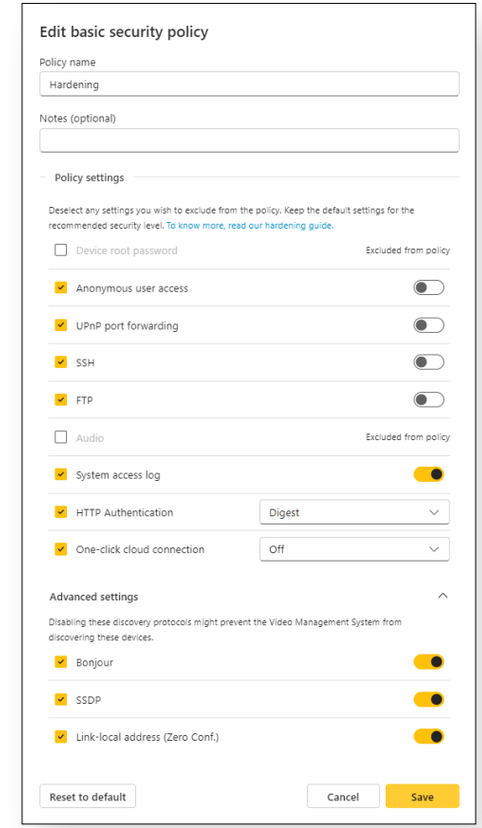
> Creare le regole

> Monitorare le regole

> Applicare le regole

Policy engine: presente e futuro

Oggi potrebbe essere necessario definire criteri nella console di gestione di ogni soluzione, ma le console sempre più integrate riescono a definire e aggiornare le policy fra i vari prodotti. La gestione delle identità e degli accessi (IAM), l'autenticazione multifattore, le notifiche push, le autorizzazioni per i file, la crittografia e l'orchestrazione della sicurezza hanno un ruolo fondamentale nella progettazione di architetture di rete zero trust.



Configurazione di un policy engine.

Gestione del ciclo di vita: perché è importante

Restare un passo avanti alle minacce

Una gestione efficace del ciclo di vita può aiutare le aziende a proteggere le proprie attività e a prepararsi meglio per il futuro. Occorre sapere dove risiedono i rischi e rimanere al corrente delle aree che potrebbero essere sfruttate. Questo è particolarmente importante per i sistemi di sicurezza, perché se una telecamera di sorveglianza smette di funzionare, le conseguenze possono essere molto gravi.

I dispositivi di rete devono essere aggiornati

Tutti i dispositivi di rete – dalle telecamere ai VMS – devono essere aggiornati e protetti con patch, per evitare che gli hacker sfruttino le vulnerabilità note e compromettano le protezioni esistenti.

I produttori rilasciano regolarmente aggiornamenti e patch di protezione del software dei dispositivi che rimediano a vulnerabilità/bug e risolvono altri problemi di prestazioni, in modo che il sistema sia stabile e sicuro.

Spesso, però, le aziende non riescono ad aggiornare il firmware o il sistema operativo su cui si basa l'hardware perché non hanno una visione d'insieme dei dispositivi in rete. Ma anche con una visione d'insieme, aggiornare tutti i dispositivi può essere complicato e far perdere molto tempo.

Se il software non viene aggiornato, i dispositivi possono essere vulnerabili agli attacchi informatici e causare ogni tipo di problema, dal mancato funzionamento a ingenti sanzioni da parte delle autorità di regolamentazione per non conformità.

Come si suol dire, la sicurezza di una rete non supera mai quella dei dispositivi connessi, quindi è importante gestire in modo efficace il ciclo di vita delle risorse fisiche collegate.

La doppia vita di un dispositivo

I cicli di vita dei dispositivi basati su software sono due:

1) Ciclo di vita funzionale del dispositivo, ovvero quanto a lungo può funzionare realisticamente. In genere, ad esempio, una telecamera di rete ha un ciclo di vita funzionale di 10-15 anni.

2) Ciclo di vita economico del dispositivo: quanto tempo passerà prima che il dispositivo inizi a costare di più per la manutenzione rispetto a una nuova tecnologia? Anche se una telecamera IP può funzionare per 15 anni, la sua durata effettiva è inferiore perché il panorama della cybersecurity cambia velocemente.

Gestione proattiva delle risorse

La gestione del ciclo di vita tiene conto del ciclo di vita funzionale ed economico delle risorse fisiche. Le aziende devono poter vedere chiaramente tutti i dispositivi distribuiti in rete per garantire che siano al sicuro dalle minacce.

L'approccio Axis alla cybersecurity

Axis si impegna a perseguire livelli elevati di cybersecurity. Lavoriamo costantemente per migliorare le nostre offerte e i processi di sicurezza informatica. Crediamo nell'importanza della trasparenza riguardo alla protezione delle nostre operazioni e della nostra catena di fornitura. Ci impegniamo a gestire lo sviluppo del software in modo da ridurre i rischi di vulnerabilità, ad affrontare subito le criticità rilevate e a garantire la sicurezza dei prodotti durante tutto il ciclo di vita, sostenendo attivamente la cybersecurity.

Le prossime pagine descrivono in dettaglio le misure che adottiamo come fondamenta della sicurezza e ciò che facciamo durante le varie fasi del ciclo di vita di un prodotto – produzione, installazione, funzionamento e smaltimento – per ridurre i rischi e proteggere i dispositivi Axis.

Le fondamenta della sicurezza

Approccio strutturato e sistematico alla sicurezza interna

Axis promuove un approccio collaborativo invitando tutti i dipendenti a contribuire per migliorare costantemente la sicurezza interna. Il nostro sistema di gestione della sicurezza delle informazioni (ISMS) certificato ISO 27001 è alla base del nostro framework di cybersecurity. Nell'ambito dell'ISMS, sono stati implementati controlli di sicurezza informatica per avere la certezza di seguire le best practice di gestione della nostra infrastruttura IT e della piattaforma di sviluppo software, nonché dei servizi connessi.

Seguendo un approccio strutturato e sistematico, proteggiamo la riservatezza, l'integrità e la disponibilità delle nostre risorse. Inoltre, Axis è conforme a una serie di requisiti normativi, framework e standard strategicamente selezionati, tra cui lo standard di cybersecurity ETSI EN 303 645 per il portafoglio di dispositivi con AXIS OS. Tuttavia, non contiamo esclusivamente sulle normative e sulle certificazioni; rispettarne di più non significa necessariamente essere più sicuri dal punto di vista informatico.

Maggiori informazioni sulla conformità Axis

RI. SE

CERTIFIKAT

ISO/IEC 27001

Härmed intygas att/This is to certify that

Axis Communications AB

Gränden 1, 223 69 LUND, SWEDEN

har ett ledningssystem för informationssäkerhet som uppfyller kraven enligt ISO/IEC 27001:2022 vad gäller
has an information security management system that fulfils the requirements of ISO/IEC 27001:2022 with respect to

Product management, utveckling och drift inom IT-infrastrukturtjänster och Axis Connected Services
Allt i enlighet med uttalande om tillämplighet fastställt 2023-11-14

Product management, development and operations within IT infrastructure services and Axis Connected Services
All in accordance with Statement of Applicability established 2023-11-14

Ursprungligen utfärdat/Originally issued	2019-02-27
Giltigt till och med/Expiry date	2025-02-26
Beslutsdatum/Decision date	2023-12-07

Jonas Madsen

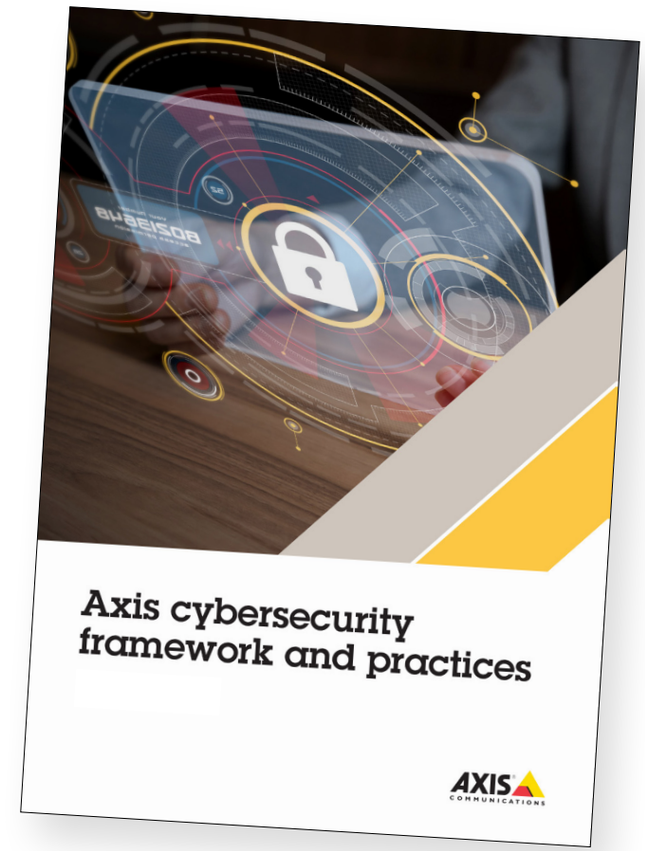
RISE Research Institutes of Sweden AB | Certification
Box 857, SE-501 15 Borås, Sweden
+46 10-516 50 00
certifiering@ri.se | www.ri.se

SP

Certifikat/Certificate 6134 I | version/issue 5 | 2023-12-07

This document is the property of RISE and may not be reproduced other than in full, except with the prior written approval by RISE.

Sida/Page 1(1)



Proteggere l'integrità dei prodotti e ridurre il rischio di vulnerabilità nel software

Passando dalla sicurezza interna alla sicurezza dei prodotti, le seguenti misure costituiscono le fondamenta della sicurezza dell'hardware e del software Axis e rispecchiano il nostro principio di trasparenza.

Piattaforma di cybersecurity Axis Edge Vault

Integrata sui dispositivi Axis, questa piattaforma basata su hardware include funzionalità che proteggono l'integrità dei dispositivi Axis, in modo da poterli avviare in modo sicuro, integrarli e garantire che i dati sensibili come le chiavi crittografiche siano protetti dagli accessi non autorizzati.

Maggiori informazioni su Axis Edge Vault

Axis Security Development Model (ASDM)

L'ASDM è la metodologia di sviluppo applicata da Axis per ridurre il rischio che vengano commercializzati prodotti con vulnerabilità software. Garantisce che le considerazioni sulla sicurezza siano parte integrante dello sviluppo del software e prevede attività come valutazioni dei rischi, modellazione delle minacce, analisi del codice, penetration test, programma bug bounty, scansione e gestione delle vulnerabilità. Rilevando e risolvendo tempestivamente i problemi in ogni fase di sviluppo, l'ASDM aiuta a ridurre i rischi legati alla sicurezza per i nostri clienti.

Maggiori informazioni sull'ASDM

AXIS OS

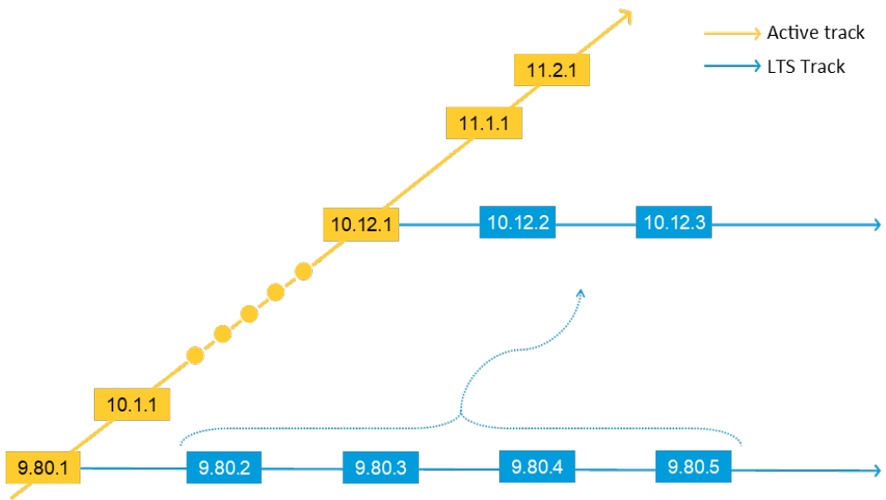
AXIS OS è il nostro sistema operativo basato su Linux per i dispositivi edge. Basato su principi come apertura, trasparenza e cybersecurity, questo potente sistema operativo prevede percorsi di aggiornamento diversi per i vari dispositivi Axis, consentendo di distribuire rapidamente funzionalità e patch di sicurezza su molti prodotti. È concepito per ridurre i rischi e mantenere i dispositivi e i servizi Axis aggiornati e protetti. La data di fine supporto di molti prodotti è indicata sul sito Axis, in modo da poter programmare per tempo lo smaltimento e la sostituzione dei dispositivi.

Maggiori informazioni su AXIS OS

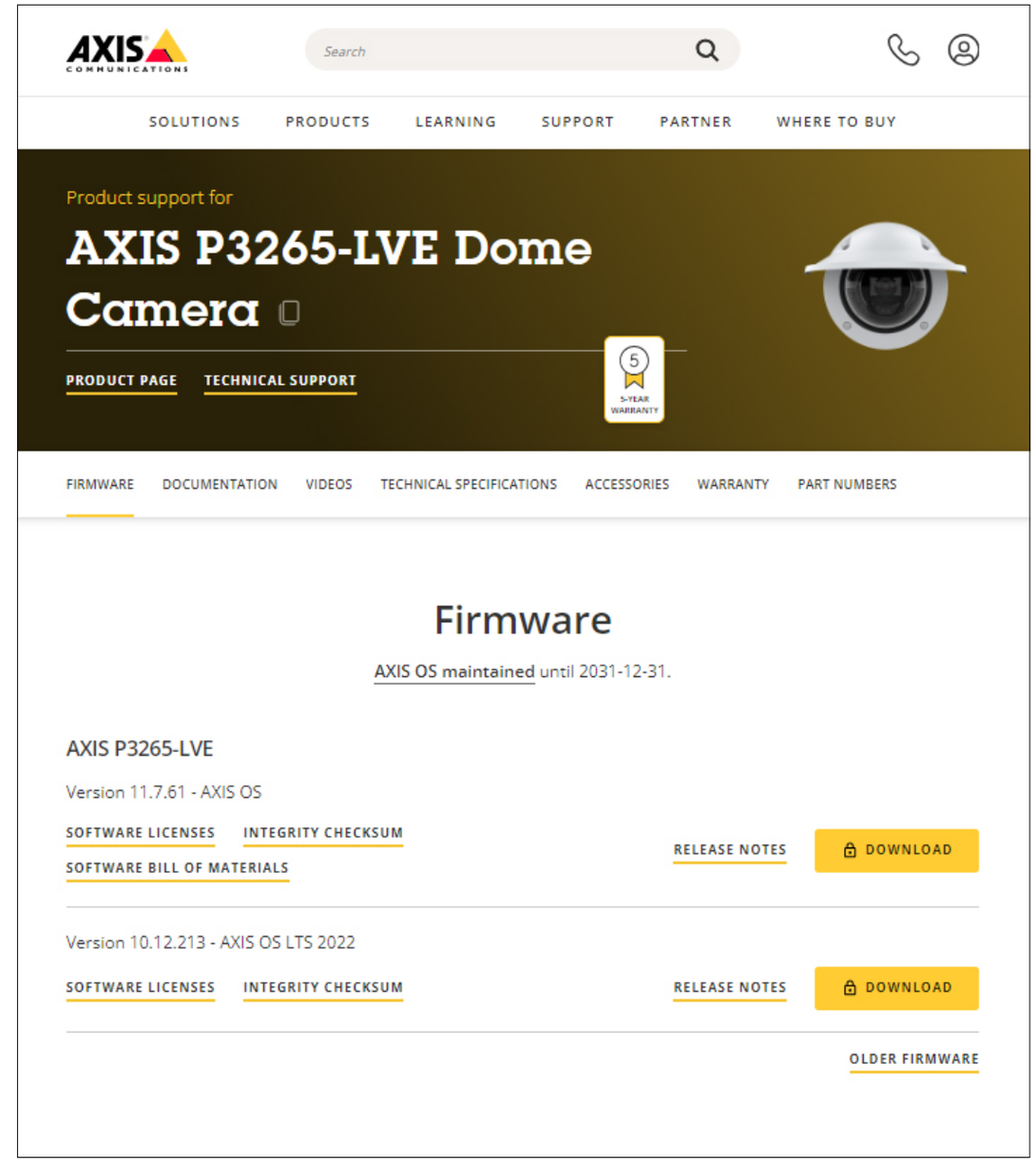
Distinta base del software (SBOM)

Per AXIS SO viene anche pubblicata una distinta base del software (SBOM) con un'ulteriore attenzione alla cybersecurity e una maggiore trasparenza per clienti, ricercatori di sicurezza e autorità. La distinta base è un elenco ampio e dettagliato dei componenti utilizzati per realizzare il sistema operativo dei dispositivi Axis. Offre informazioni dettagliate sulle best practice di cybersecurity applicate dai fornitori e dati utili per operatori specializzati nella valutazione delle vulnerabilità, nell'analisi delle minacce e nei piani di risoluzione.

Maggiori informazioni sulla distinta base del software



I percorsi di AXIS OS.



Gestione delle vulnerabilità rilevate

Come membro della Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA), Axis pubblica e informa gli stakeholder sulle vulnerabilità, in modo che i clienti possano intraprendere azioni appropriate e tempestive. Collaborando con ricercatori esterni, Axis rivela vulnerabilità ed esposizioni con un procedimento trasparente, responsabile e coordinato. Axis fornisce le patch per i dispositivi, i software o i servizi interessati e pubblica tutte le informazioni necessarie sul **suo sito** e tramite il database delle vulnerabilità del programma CVE. Inoltre offre un servizio di notifica che consente di registrarsi e ricevere informazioni sulle vulnerabilità e altre questioni relative alla sicurezza. Axis sottolinea che è importante tenere aggiornato il sistema operativo dei prodotti installati, per garantire che siano dotati delle patch di sicurezza più recenti.

Ulteriori informazioni sulla policy di gestione delle vulnerabilità Axis

Programma bug bounty

Nell'ambito della nostra strategia trasparente di gestione delle vulnerabilità, organizziamo anche un programma bug bounty. Il programma è condotto in collaborazione con Bugcrowd, leader nella cybersecurity in crowdsourcing. Ci impegniamo a instaurare rapporti professionali con ricercatori di sicurezza esterni e hacker etici. Partecipando al programma, i ricercatori che scoprono vulnerabilità su prodotti basati su AXIS OS hanno diritto a un premio in denaro ("bounty", in inglese "taglia"). Axis divulga poi in modo trasparente le vulnerabilità e fornisce patch per i prodotti interessati.

PRODUZIONE

DISTRIBUZIONE

Ridurre il rischio di componenti hardware e software compromessi

Sicurezza della catena di fornitura

Come tutti i prodotti, anche quelli per la sicurezza fisica devono funzionare secondo il progetto e la destinazione d'uso, restando sempre integri. Questo è possibile solo se l'hardware e il sistema operativo dei dispositivi vengono protetti adeguatamente da modifiche non autorizzate o manipolazioni durante il loro percorso nella catena di fornitura.

Controlli di qualità

Insieme ai fornitori e ai partner di produzione, Axis applica numerosi controlli di qualità per mantenere inalterata e tutelare l'integrità dei prodotti. I componenti vengono sempre acquistati da un fornitore della lista dei vendor approvati in base alla distinta materiali specificata da Axis. Senza l'autorizzazione di Axis il fornitore non può modificare le specifiche, le istruzioni di lavoro o i documenti di controllo qualità. Tutte le modifiche approvate devono essere documentate e registrate.

Tracciabilità

Una procedura di trattamento dei materiali ne garantisce sempre l'idoneità, rivelando eventuali discrepanze che potrebbero compromettere la qualità. I fornitori e i partner di produzione devono adottare un sistema di tracciabilità per poter seguire sempre la produzione dei lotti, dal materiale di origine al componente finito. Durante la produzione, il componente fisico viene sottoposto a diversi test, per verificarne la conformità ed evidenziare qualsiasi discrepanza.

Rilevamento di componenti contraffatti

Un'ispezione ottica automatica (AOI) contribuisce a verificare che non vengano montati componenti contraffatti. Axis sviluppa e produce le proprie apparecchiature di produzione critica, nonché il sistema di collaudo di componenti, moduli e prodotti nelle varie fasi di produzione. Questa procedura limita il rischio di manomissioni. Un ulteriore controllo di sicurezza prevede che tutti i dati dei test siano condivisi con Axis 24 ore su 24 e 7 giorni su 7, in modo da identificare immediatamente modifiche non autorizzate.

Maggiori informazioni sulla sicurezza della catena di fornitura Axis

Contrastare le minacce durante la distribuzione

Le funzionalità di cybersecurity integrate sui dispositivi Axis, insieme al ripristino delle impostazioni di fabbrica, proteggono da modifiche non autorizzate al software durante la spedizione. Le funzionalità supportate da Axis Edge Vault (descritte alla pagina successiva) proteggono le informazioni sensibili e garantiscono che i dispositivi eseguano solo un sistema operativo Axis originale.

Comprendere la sicurezza della catena di fornitura è necessario quando si valuta se i fornitori adottino misure che riducono i rischi per l'azienda che acquista.

Funzionalità di cybersecurity integrate

I dispositivi Axis sono dotati di funzionalità di sicurezza integrate che consentono di avviarli e integrarli in modo sicuro e di garantire che i dati sensibili siano protetti.

Piattaforma di cybersecurity Axis Edge Vault

La nostra piattaforma di cybersecurity basata su hardware offre solide basi per garantire che il dispositivo Axis sia un elemento affidabile della rete.
Axis Edge Vault include funzionalità* come:

> **Archivio chiavi sicuro**: prevede moduli di elaborazione crittografica per l'archiviazione sicura delle chiavi crittografiche, salvaguardando l'identità del dispositivo e altre informazioni sensibili dagli accessi non autorizzati anche in caso di manomissioni.
I moduli di elaborazione crittografica possono essere ambienti di esecuzione attendibili (Trusted Execution Environment) integrati nel System-on-Chip (SoC) Axis. Possono anche essere Secure Element o Trusted Platform Module, ovvero chip separati sulla scheda madre. I dispositivi Axis vengono realizzati utilizzando uno di questi moduli o una combinazione dei tre.

> **Firmware con firma digitale** e **Secure Boot**: garantiscono che il dispositivo possa scaricare ed eseguire solo un sistema operativo Axis originale (AXIS OS).

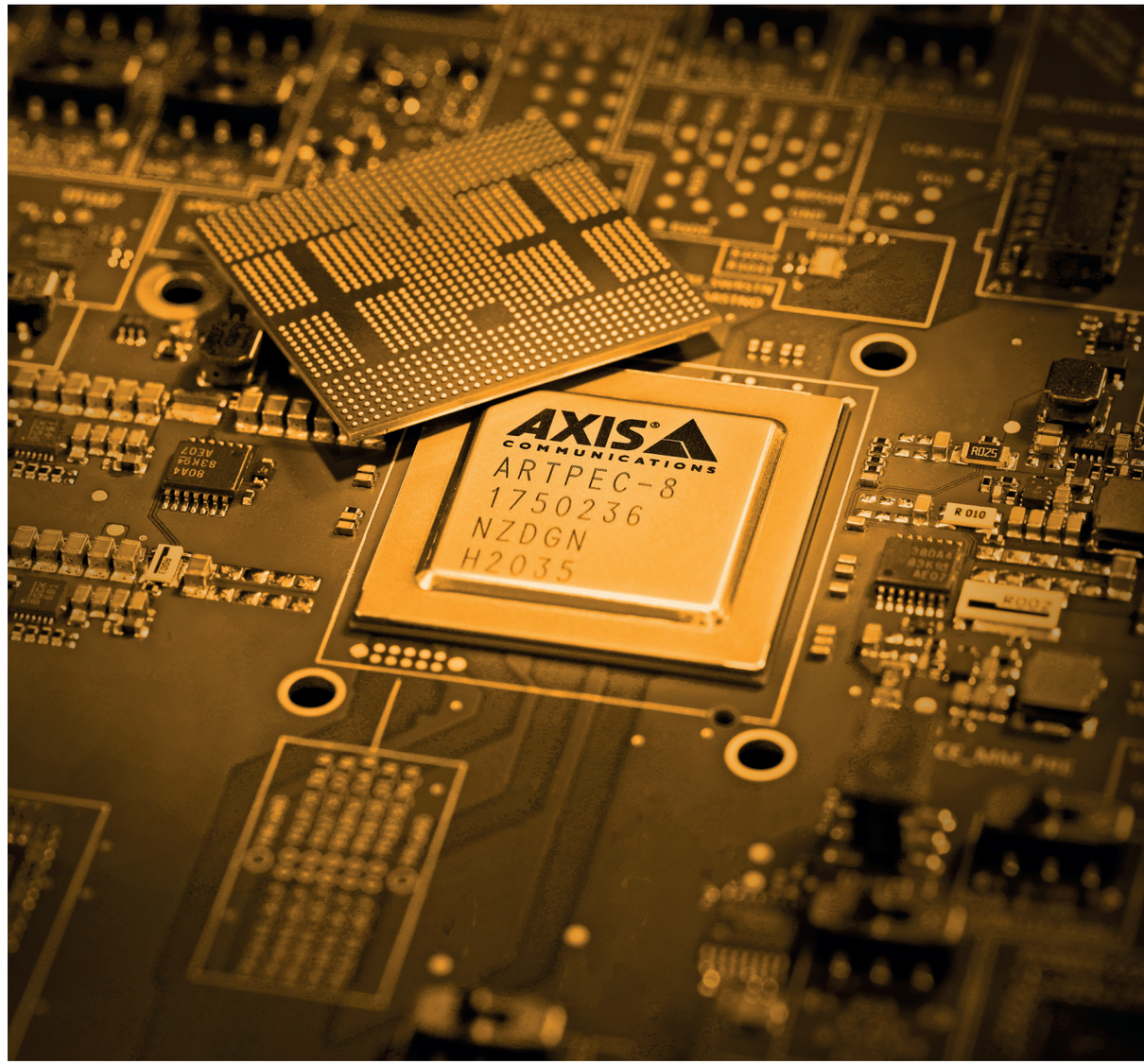
> **ID del dispositivo Axis ID**, conforme a IEEE 802.1AR, per l'identificazione e l'onboarding in sicurezza del dispositivo in rete.

> **File system crittografato**, che protegge i dati del file system dall'estrazione o dalla manomissione quando il dispositivo non è in uso, ad esempio durante il transito da un system integrator al cliente finale.

> **Video firmato**, che consente agli utenti di verificare l'autenticità del video acquisito e garantire che non sia stato manomesso.

**Nota: le funzionalità di Axis Edge Vault non sono supportate da tutti i dispositivi. Consultare la scheda tecnica o il Selettore prodotti Axis per verificare le funzionalità supportate dal prodotto.*

Maggiori informazioni su Axis Edge Vault



Impostazioni predefinite

Oltre alle funzionalità di sicurezza del prodotto, i dispositivi Axis vengono forniti con impostazioni di protezione predefinite.

Credenziali e protocolli di rete

Il dispositivo Axis non funziona finché non vengono impostati account che prevedono un nome utente e una password. Dopo averli impostati, l'accesso alle funzioni di amministrazione e/o ai flussi video viene concesso solo inserendo queste credenziali.

Sui dispositivi Axis, inoltre, solo un numero minimo di protocolli e servizi di rete è abilitato di default, come HTTP e HTTPS per l'accesso alle interfacce del dispositivo, RTSP e RTP per lo streaming video e audio e alcuni protocolli come UPnP e Bonjour per il rilevamento dei dispositivi Axis da parte di applicazioni di terze parti.

Soddisfare i requisiti delle reti zero trust dei clienti

Axis soddisfa i requisiti delle reti zero trust realizzando prodotti con ID dispositivo univoci e supportando il protocollo HTTPS e lo standard IEEE 802.1X, ma anche IEEE 802.1AR per l'autenticazione dei dispositivi e IEEE 802.1AE MACsec per la crittografia automatica dei dati.

HTTPS è abilitato di default, consentendo l'impostazione sicura delle password dei dispositivi. Inoltre, permette al software di gestione video che utilizza HTTPS di verificare il certificato SSL firmato da una CA attendibile; questa funzionalità è supportata dall'ID dispositivo Axis dei prodotti più recenti.

Il supporto per IEEE 802.1X, IEEE 802.1AR e IEEE 802.1AE, abilitato di default sui prodotti Axis, consente l'onboarding automatico dei dispositivi, l'autenticazione e la crittografia end-to-end. In questo modo, i professionisti IT hanno a disposizione meccanismi standard per integrare in modo efficiente e sicuro i dispositivi Axis in una rete aziendale che supporta IEEE 802.1X. I clienti che utilizzano dispositivi Axis in una rete Aruba possono scaricare la guida all'integrazione, con le configurazioni ottimali per l'onboarding e la gestione sicuri dei dispositivi Axis.

Maggiori informazioni sulle soluzioni Axis per l'IT aziendale

INSTALLAZIONE

Cybersecurity durante l'installazione

Un dispositivo Axis è un endpoint di rete come qualsiasi altro dispositivo, ad esempio un laptop, un computer desktop o un dispositivo mobile. A differenza di un laptop, però, i dispositivi Axis non consentono agli utenti di visitare siti potenzialmente dannosi, aprire allegati sospetti o installare applicazioni non attendibili. Un dispositivo video, audio o per il controllo accessi ha comunque un'interfaccia che può esporre a rischi il sistema a cui è connesso.

Le Hardening Guide, disponibili per i prodotti Axis, offrono consigli su come ridurre l'esposizione ai rischi informatici. Eccone alcuni: ad esempio, si consiglia di riportare un dispositivo alle impostazioni di fabbrica prima di configurarlo, per assicurarsi che sia privo di software o configurazioni indesiderate.

Inoltre, verificare che il dispositivo abbia la versione di AXIS OS più recente, che contiene le patch di sicurezza e le correzioni di bug più aggiornate e specifiche.

È necessario impostare password complesse, limitare l'accesso diretto all'interfaccia web del dispositivo, configurare il dispositivo in modo da utilizzare solo HTTPS (che cripta il traffico dati tra il client e il dispositivo) e disabilitare i servizi e funzioni per ridurre i rischi superflui. È anche importante impostare la data e l'ora corrette sul dispositivo per avere registri di sistema accurati e garantire che i certificati digitali, su cui si basano servizi come HTTPS e IEEE 802.1X, possano essere convalidati e utilizzati. Uno strumento che consente una configurazione e una gestione efficiente dei dispositivi Axis in locale è AXIS Device Manager.

Permette di eseguire in batch le attività di installazione e sicurezza, come la gestione delle credenziali dei dispositivi, la distribuzione dei certificati digitali, la disabilitazione dei servizi non utilizzati e l'aggiornamento di AXIS OS. Leggere la pagina successiva per ulteriori informazioni sul software di gestione dei dispositivi.

Per i consigli sulla protezione avanzata e totale dei dispositivi basati su AXIS OS, leggere la AXIS OS Hardening Guide. Per accedere alle Hardening Guide del software di gestione video e degli switch di rete Axis, visitare la pagina Risorse per la cybersecurity. Per informazioni su come integrare perfettamente i dispositivi Axis nelle infrastrutture e nelle reti IT aziendali vedere Soluzioni Axis per l'IT aziendale.

Axis offre strumenti, documentazione e formazione per aiutare i clienti a ridurre i rischi e mantenere aggiornati e protetti i dispositivi e i servizi Axis. **Visitare la pagina Risorse per la cybersecurity.**

IN SERVIZIO

Cybersecurity dei dispositivi in servizio

Mentre un dispositivo è in funzione, uno dei modi più importanti per garantirne la cybersecurity è assicurarsi che il firmware o il sistema operativo (AXIS OS) sia aggiornato. In questo modo si ha la certezza che il dispositivo incorpori le patch di sicurezza e le correzioni di bug più recenti. Le funzionalità dei dispositivi Axis, come il firmware con firma digitale e Secure Boot, garantiscono che sia possibile installare e utilizzare solo una versione originale di AXIS OS. Le versioni di AXIS OS sono disponibili gratuitamente seguendo i percorsi di aggiornamento Active e LTS (Long-Term Support). Scegliendo il percorso Active, AXIS OS viene aggiornato con nuove funzionalità, mentre il percorso LTS non le supporta per ridurre al minimo il rischio di problemi di compatibilità. Entrambi i percorsi, tuttavia, includono patch di sicurezza e correzioni di bug. Un modo per tenere sotto controllo le vulnerabilità appena riscontrate è iscriversi al Servizio di notifiche di sicurezza Axis. Le vulnerabilità pubblicate contengono istruzioni su come correggere i dispositivi con il nuovo software.

Per rendere più semplice ed efficiente l'aggiornamento del sistema operativo di un numero elevato di dispositivi, Axis offre software come AXIS Device Manager e AXIS Device Manager Extend.

Come funziona il software di gestione dei dispositivi?

Il software di gestione dei dispositivi può acquisire in tempo reale un inventario completo di tutte le telecamere, gli encoder, i dispositivi di controllo accessi, audio e altri dispositivi connessi alla rete. Esegue una scansione dell'intera rete e acquisisce tutte le informazioni più importanti, come numero di modello, indirizzi IP e MAC, versione del software dei dispositivi e stato dei certificati.

Il quadro completo

Con un quadro dettagliato di tutto l'ecosistema di rete è più facile applicare regole e procedure coerenti di gestione del ciclo di vita su tutti i dispositivi e svolgere in sicurezza le operazioni di installazione, deployment, configurazione, sicurezza e manutenzione.

Le policy e le best practice di cybersecurity per la gestione dei dispositivi devono rispondere a domande su aspetti come la complessità e la frequenza di aggiornamento delle password, i servizi non utilizzati da disattivare per ridurre l'esposizione agli attacchi, la frequenza di scansione dei dispositivi per individuare vulnerabilità e le procedure attualmente previste per valutare i livelli di rischio quando un produttore pubblica violazioni note.

Risparmiare tempo e fatica

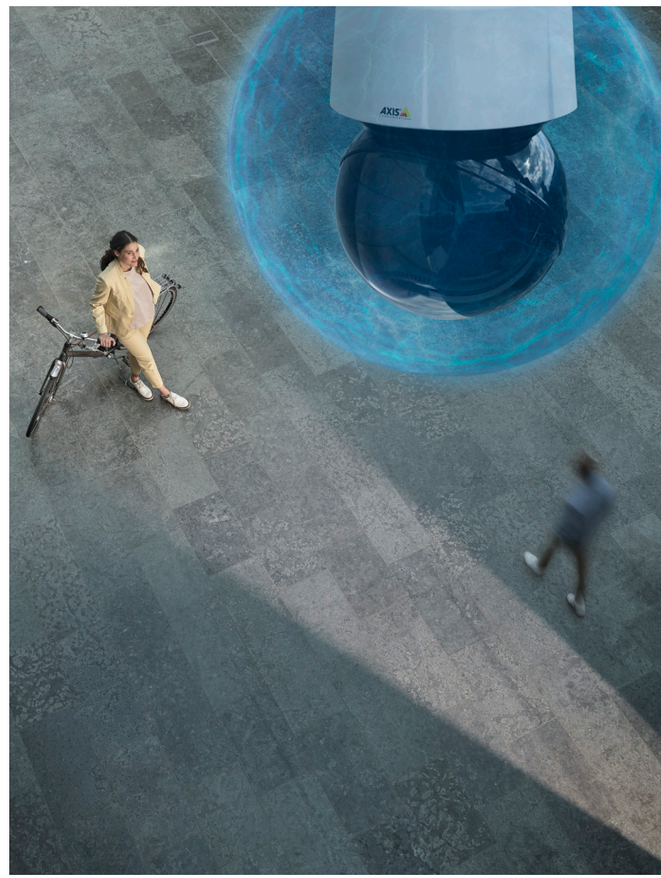
Il software di gestione dei dispositivi aiuta le aziende a risparmiare tempo e fatica quando devono gestire i rischi per la cybersecurity. Il software può essere utilizzato per:

> Inviare modifiche del sistema, aggiornamenti software e nuovi certificati digitali a tutti i dispositivi contemporaneamente.

> Creare o riconfigurare facilmente le impostazioni di sicurezza e applicarle all'intera rete per garantire che tutti i dispositivi rispettino le regole e le procedure di sicurezza più recenti.

> Verificare che tutti i dispositivi dispongano della versione software più recente e sicura.

> Gestire i privilegi degli utenti nell'intera rete e configurare le modifiche.



Approfondimenti dettagliati in tempo reale

Gli strumenti di gestione dei dispositivi consentono alle aziende di visualizzare lo stato del loro ecosistema, in tempo reale e in modo approfondito. Ad esempio, è possibile vedere quali dispositivi devono essere aggiornati con gli ultimi aggiornamenti software e certificati, nonché avere informazioni sulle date di fine produzione e supporto in modo da programmare la sostituzione dei dispositivi.

Strumenti di gestione dei dispositivi Axis

I software AXIS Device Manager e AXIS Device Manager Extend aiutano a gestire in modo efficiente i dispositivi Axis e si completano a vicenda.

AXIS Device Manager

AXIS Device Manager aiuta a garantire un'installazione e una configurazione rapida e semplice dei nuovi dispositivi. Questo strumento locale supporta tutte le principali attività operative, di installazione e di sicurezza, compresa l'installazione di aggiornamenti software e applicazioni. Consente di configurare i dispositivi Axis con impostazioni di backup e ripristino e di visualizzare lo stato della garanzia. È anche possibile applicare controlli di cybersecurity come i certificati HTTPS e IEEE 802.1X.

Maggiori informazioni su AXIS Device Manager

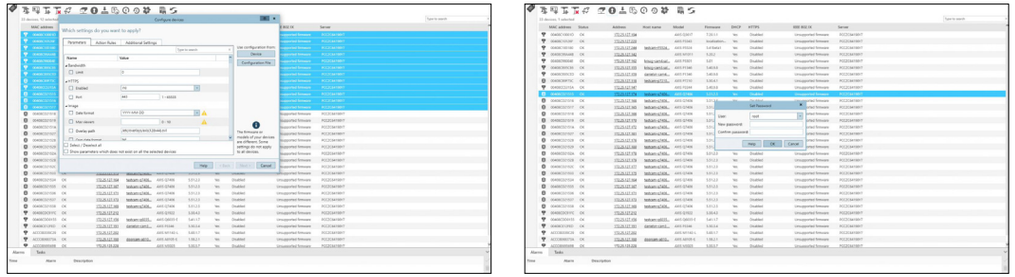
AXIS Device Manager Extend

Ideale per aziende distribuite in più sedi, AXIS Device Manager Extend aiuta a gestire da remoto le risorse di tutti i siti. Questa applicazione facile da usare semplifica la scalabilità di attività di manutenzione essenziali, come l'aggiornamento di AXIS OS, la definizione e applicazione delle policy di sicurezza e la gestione delle applicazioni. Dotata di una dashboard live, accelera la risoluzione dei problemi fornendo una visuale complessiva dei potenziali problemi del sistema, come dispositivi offline o fuori garanzia. Inoltre offre suggerimenti sulle impostazioni dei dispositivi per ridurre al minimo le minacce per la sicurezza e le vulnerabilità. Le policy di sicurezza possono essere definite, applicate e attuate su tutti i dispositivi Axis.

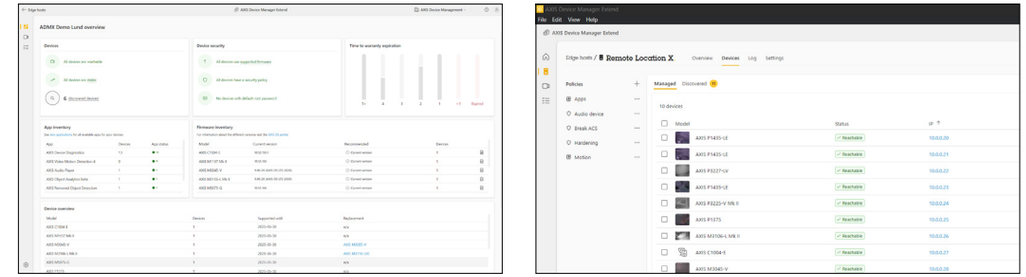
Maggiori informazioni su AXIS Device Manager Extend

In caso di violazione di sicurezza

Se la rete viene violata Axis mette a disposizione la AXIS OS Forensic Guide per condurre un'analisi forense dei dispositivi Axis connessi.



Schermate dell'interfaccia di AXIS Device Manager.



Schermate dell'interfaccia di AXIS Device Manager Extend.

SMALTIMENTO

Prepararsi allo smaltimento

Gli aggiornamenti e le patch sono il modo migliore per mantenere la cybersecurity, ma non sono sempre disponibili quando un dispositivo diventa troppo vecchio per essere supportato. Dal punto di vista della sicurezza informatica, i dispositivi obsoleti e privi di patch rappresentano un grande rischio. Un dispositivo trascurato potrebbe diventare un facile punto di accesso per gli hacker.

È importante programmare lo smaltimento per evitare il rischio di utilizzare dispositivi non più supportati e con vulnerabilità potenzialmente irrisolte. Axis indica la data di fine supporto del sistema operativo, in modo da poter preparare per tempo lo smaltimento e la sostituzione di un dispositivo. Inoltre AXIS Device Manager Extend consente di ottenere informazioni su garanzia, fine produzione e fine supporto per tutti i dispositivi del sistema.

Anche la rimozione dei dati su un dispositivo da smaltire è importante. Ripristinando le impostazioni di fabbrica, è possibile cancellare rapidamente tutte le configurazioni e i dati dal dispositivo. Visitare il portale AXIS OS per ulteriori dettagli sullo smaltimento dei dispositivi.

Compliance

I governi approvano sempre più leggi e regolamenti sulla cybersecurity e tutte le aziende operanti nei loro confini devono rispettarli. Allo stesso modo i settori e le aziende impongono sempre più la conformità a determinati standard, inclusa la certificazione di prodotti e servizi. È dovere di tutti gli stakeholder assicurare il rispetto delle leggi e dei regolamenti e implementare linee guida e specifiche nei loro processi aziendali.

Conformità alla cybersecurity come punto di partenza

In ambito di cybersecurity essere conformi significa seguire gli standard e i requisiti normativi delle autorità. Anche se gli standard e le certificazioni sono senza dubbio importanti, c'è dell'altro.

Esiste sempre il rischio che rispettare standard e certificazioni diventi una sorta di "compitino".

La conformità alla cybersecurity è in costante evoluzione e ciò che una volta era un "plus" diventa rapidamente obbligatorio.

Ecco perché le aziende devono considerarli un punto di partenza e non di arrivo, un requisito minimo anziché un traguardo. Il vero obiettivo dei fornitori è offrire prodotti e servizi che possano essere gestiti nel modo più sicuro possibile, ma anche offrire indicazioni e trasparenza ai clienti per avere una garanzia costante di cybersecurity.

Normative

Le normative sulla cybersecurity costringono le aziende a proteggere i propri sistemi e informazioni e a garantire che i prodotti e i servizi abbiano un livello minimo di sicurezza. Ecco alcune delle normative più importanti e come si applicano.

Nel 2023 è entrata in vigore la Direttiva NIS2. Gli stati membri dell'Unione Europea hanno tempo fino a ottobre 2024 per recepire le misure nelle leggi nazionali. Questa direttiva richiede a tutte le aziende dell'UE che operano in settori essenziali di adottare un elevato livello di cybersecurity. Le aziende possono essere sanzionate per negligenza, anche se i problemi di cybersecurity sono imputabili ai loro fornitori.

In futuro, dunque, le valutazioni dei fornitori e la sicurezza della catena di fornitura saranno ancora più importanti. La direttiva impone indirettamente obblighi a produttori, importatori e distributori, che dovranno rispettare un obbligo di diligenza durante tutto il ciclo di vita dei prodotti.

A dicembre 2023, l'UE ha raggiunto un accordo provvisorio su un nuovo regolamento chiamato Cyber Resilience Act, che definisce standard comuni di sicurezza informatica per prodotti hardware e software con elementi digitali. La normativa comprende prodotti collegati direttamente o indirettamente a un altro dispositivo o un'altra rete, come i dispositivi IoT. L'atto proposto intende ridurre il numero di incidenti, aumentando al tempo stesso la trasparenza e garantendo una migliore protezione dei dati. Il Regno Unito ha approvato una legge simile denominata UK Product Security and Telecommunications Infrastructure, che entrerà in vigore ad aprile 2024.

Le aziende che lavorano con il governo degli Stati Uniti possono anche dover rispettare standard come la Cybersecurity Maturity Model Certification, che richiede una certificazione sulla gestione interna delle procedure di cybersecurity.

Garantire la cybersecurity richiede vigilanza e manutenzione continue.

Standard e certificazioni

La maggior parte degli standard e delle certificazioni prevede funzionalità, contromisure e processi per garantire che la sicurezza sia un elemento integrante. A questi possono affiancarsi test esterni, come penetration test e programmi bug bounty, per individuare vulnerabilità del software.

Anche se affidarsi alle certificazioni dei prodotti può dare una certa tranquillità a clienti e istituzioni, è opportuno notare che generalmente le certificazioni durano un solo anno, dopodiché il prodotto deve essere ricertificato. Con nuove tecnologie e funzionalità che vengono costantemente sviluppate e immesse sul mercato, le certificazioni possono rimanere indietro.

Da notare anche che, sebbene gli standard possano contribuire a incrementare la cybersecurity, non costituiscono una garanzia contro gli incidenti. Le aziende devono esaminare continuamente le minacce e le policy di sicurezza.

Perché Axis?

Cybersecurity

La cybersecurity è parte integrante di Axis. Ispira il nostro sistema interno di sicurezza delle informazioni, la gestione della catena di fornitura, lo sviluppo di prodotti e servizi e la gestione delle vulnerabilità del software. Consideriamo la cybersecurity una responsabilità comune e continua in cui la trasparenza è fondamentale. Il nostro obiettivo è consentire ai clienti di utilizzare le nostre offerte nel modo più sicuro possibile. Ecco perché i nostri prodotti sono progettati e realizzati con funzionalità di cybersecurity integrate e impostazioni di protezione predefinite e perché mettiamo a disposizione le Hardening Guide. Monitoriamo costantemente i pericoli e cerchiamo nuovi modi per aumentare la sicurezza. In qualità di CVE Numbering Authority, rimediamo alle nuove vulnerabilità riscontrate applicando patch e divulgandole al pubblico, in modo che il cliente possa intraprendere azioni appropriate e tempestive. Offriamo aggiornamenti software per incrementare la sicurezza dei dispositivi Axis dopo l'installazione. Inoltre con strumenti come AXIS Device Manager e AXIS Device Manager Extend, semplifichiamo la gestione dei dispositivi Axis per ridurre i rischi per la cybersecurity durante tutto il loro ciclo di vita.

Altri motivi per scegliere Axis

> **Qualità in tutto ciò che facciamo:**
Tutti i prodotti vengono sottoposti a test approfonditi per regalare la massima tranquillità ai clienti.

> **Tecnologie innovative:**
Mettiamo insieme tecnologia e immaginazione per migliorare al tempo stesso performance e facilità di utilizzo. Basate su standard aperti, le nostre soluzioni sono flessibili, scalabili e facili da integrare.

> **Sostenibilità ad ogni livello:**
Axis manifesta l'impegno costante di uno sviluppo responsabile nei confronti dell'ambiente utilizzando materiali sostenibili. Circa il 90% delle telecamere e degli encoder Axis immessi sul mercato nel 2022 era privo di PVC.

> **Presenza globale, competenza locale:**
Axis vanta il maggior numero al mondo di prodotti video di rete installati con dipendenti in oltre 50 Paesi. Condividiamo idee ed esperienzee ci teniamo costantemente aggiornati sugli ultimi sviluppi.

> **Il potere delle partnership:**
Grazie all'impegno verso i suoi Partner, Axis è diventata l'azienda produttrice di telecamere più integrata sul mercato.

Informazioni su Axis Communications

Axis permette di creare un mondo più intelligente e sicuro grazie a soluzioni che migliorano la sicurezza e le prestazioni aziendali. In qualità di azienda leader nelle tecnologie di rete, Axis offre prodotti e servizi per la videosorveglianza, il controllo accessi, intercom e sistemi audio, che supporta con applicazioni analitiche intelligenti e una formazione di alta qualità.

Axis ha oltre 4000 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.

©2024 Axis Communications AB. AXIS COMMUNICATIONS, AXIS, ARTPEC e VAPIX sono marchi registrati di Axis AB in diverse giurisdizioni. Tutti gli altri marchi sono proprietà dei rispettivi proprietari.