CYBERSECURITY

Gestione del ciclo di vita del dispositivo

I rischi per la cybersecurity esistono in ogni fase del ciclo di vita di un dispositivo di rete, dalla produzione allo smaltimento. Se i rischi vengono trascurati, possono causare interruzioni di servizio e perdite di riservatezza, integrità e disponibilità dei dati. Dunque, è fondamentale che tutte le parti in causa, dal fornitore al cliente finale, si assumano la responsabilità di gestire i rischi.

Le considerazioni sul ciclo di vita della sicurezza del dispositivo sono importanti già in fase di approvvigionamento. Un produttore deve adottare misure per ridurre i rischi per la cybersecurity prima che il prodotto raggiunga il cliente, mentre è in servizio e quando viene smaltito.

Le seguenti pagine illustrano le tecnologie, gli strumenti, le linee guida, gli approcci e i processi supportati da Axis per ridurre i rischi durante l'intero ciclo di vita di un dispositivo Axis.

Le basi della sicurezza: Axis Edge Vault, AXIS OS, Axis Security Development Model

Le basi della sicurezza: hardware, software e approccio

Proteggere l'integrità del prodotto e ridurre il rischio di vulnerabilità fin dall'inizio

Piattaforma di cybersecurity Axis Edge Vault
Questa piattaforma basata su hardware supporta funzionalità che proteggono l'identità e l'integrità del dispositivo dagli accessi non autorizzati, in modo da poter avviare in sicurezza il dispositivo, integrarlo e garantire che i dati sensibili come le chiavi siano protetti.

Sistema operativo AXIS OS
AXIS OS gestisce una serie di dispositivi Axis. Incorporando le best practice del settore nella gestione delle vulnerabilità, AXIS OS rappresenta la piattaforma ideale per rilasciare in modo rapido ed efficiente le funzionalità e le patch di sicurezza del software su numerosi prodotti.

Axis Security Development Model (ASDM)
È una metodologia applicata da Axis per ridurre il rischio che vengano rilasciati prodotti con vulnerabilità software. ASDM garantisce che le considerazioni sulla sicurezza siano parte integrante dello sviluppo del software. Tra le varie attività, prevede valutazioni dei rischi, modellazione delle minacce, analisi del codice, penetration test, programma bug bounty, scansione e gestione delle vulnerabilità.

Trasparenza
È un elemento importante del modo di lavorare di Axis per instaurare fiducia. Axis è una Common Vulnerability and Exposures (CVE) Numbering Authority, ovvero pubblica e informa gli interessati sulle vulnerabilità affinché i clienti possano intraprendere le azioni appropriate. Inoltre, pubblica una distinta base software (SBOM) per AXIS OS.

PRODUZIONE E DISTRIBUZIONE

Ridurre il rischio di compromissione dei componenti

- **Catena di fornitura:** i componenti critici vengono acquistati direttamente da fornitori strategici. Axis lavora a stretto contatto con i partner di produzione. I processi di produzione sono monitorati e i dati vengono condivisi 24 ore su 24 e 7 giorni su 7 con Axis, per un'analisi in tempo reale e la massima trasparenza.
- **Axis Edge Vault:** installato sui dispositivi Axis durante la produzione, Axis Edge Vault include le seguenti funzionalità:
  - **Keystore sicuro,** che comprende moduli di calcolo crittografico (come Secure Element, Trusted Platform Module, Trusted Execution Environment) per l'archiviazione a prova di manomissione delle chiavi.
  - **Firmware con firma digitale,** per garantire che la versione installata di AXIS OS provenga effettivamente da Axis. Inoltre, garantisce che il nuovo firmware da scaricare e installare sul dispositivo sia firmato da Axis.
  - **Secure Boot,** che consente al dispositivo di verificare che il firmware disponga di una firma Axis. Se il firmware non è autorizzato o è stato alterato, il processo di avvio viene interrotto e il dispositivo smette di funzionare. La combinazione di firmware con firma digitale, Secure Boot e impostazioni predefinite di fabbrica protegge dalle modifiche dannose durante la spedizione di un dispositivo.
  - **Axis Device ID,** un certificato univoco con le chiavi corrispondenti che può provare l'autenticità di un dispositivo Axis. Basato su IEEE 802.1AR, Axis Device ID consente l'identificazione sicura del dispositivo e l'onboarding su una rete.
  - **File system crittografato**, che protegge la configurazione specifica del cliente e le informazioni memorizzate nel file system dall'estrazione o dalla manomissione mentre il dispositivo non è in uso, ad esempio quando è in transito da un system integrator al cliente finale.

INSTALLAZIONE

Affrontare i rischi dovuti all'inserimento in rete di prodotti compromessi o non adeguatamente protetti, che possono favorire accessi non autorizzati, l'estrazione di dati sensibili e il trasferimento di dati alterati tra gli endpoint della rete

- **Impostazioni di fabbrica:** riportare il dispositivo alle impostazioni di fabbrica prima di configurarlo. Questa procedura garantisce che il dispositivo sia completamente privo di software o configurazioni indesiderate, perché l'unico software rimanente è AXIS OS con le sue impostazioni predefinite.
- **Verificare la disponibilità di firmware più recente per il dispositivo:** tra la produzione e l'installazione potrebbe essere trascorso del tempo. Dunque, è buona norma controllare sul sito Axis la disponibilità di firmware più recente, che può contenere le ultime correzioni di bug per il dispositivo specifico.
- **Axis Device ID:** per garantire che sulla rete siano utilizzati solo dispositivi Axis originali, l'Axis Device ID può essere verificato utilizzando l'autenticazione IEEE 802.1X o quando si stabilisce un connessione di rete sicura tramite il protocollo HTTPS. Su una rete IEEE 802.1X, l'Axis Device ID può essere utilizzato per incrementare la sicurezza e ridurre i tempi di implementazione.
- **Keystore sicuro:** utilizzando moduli di calcolo crittografico, il keystore sicuro contiene informazioni sensibili come l'Axis Device ID e le chiavi caricate dal cliente, impedendo l'accesso non autorizzato e l'estrazione dannosa di informazioni sensibili anche nel caso in cui il dispositivo sia compromesso.
- **File system crittografato:** garantisce che nessun dato archiviato nel file system possa essere estratto o manomesso quando il dispositivo non è in uso.
- **Hardening Guide:** la AXIS OS Hardening Guide, disponibile sul portale AXIS OS del sito Axis, definisce una configurazione di base per affrontare le minacce più comuni, illustrando le best practicee offrendo consulenza tecnica. È inoltre disponibile una Hardening Guide per il software di gestione video AXIS Camera Station e per gli switch di rete Axis.
- **AXIS OS Security Scanner Guide:** Axis consiglia di eseguire scansioni di sicurezza dei dispositivi Axis per individuare vulnerabilità o configurazioni troppo deboli. La AXIS OS Security Scanner Guide spiega come procedere in seguito alle segnalazioni degli scanner e descrive i "falsi positivi" più comuni.
- **AXIS Device Manager:** questo strumento permette di configurare e gestire in modo efficiente i dispositivi a livello locale. Consente l'elaborazione batch delle attività di installazione e sicurezza, come la gestione delle credenziali dei dispositivi, la distribuzione dei certificati, la disabilitazione dei servizi non utilizzati e l'aggiornamento di AXIS OS.

PRODUZIONE

DISTRIBUZIONE

INSTALLAZIONE

IN SERVIZIO

SMALTIMENTO

IN SERVIZIO

Affrontare i rischi dovuti all'esecuzione di firmware con vulnerabilità note, all'aggiornamento di dispositivi con firmware non autenticato o all'abbandono di configurazioni sicure

> **Aggiornamento del firmware:** è essenziale garantire costantemente la cybersecurity di un dispositivo Axis aggiornando il firmware tramite il percorso Active o LTS (Long-Term Support) di AXIS OS. Disponibili gratuitamente, gli aggiornamenti del firmware che seguono i due percorsi includono le patch di sicurezza. Il firmware con firma digitale garantisce che possa essere installato solo firmware Axis originale.

> **AXIS Device Manager Extend:** questo strumento, che si affianca ad AXIS Device Manager, consente la gestione remota dei dispositivi Axis e semplifica la scalabilità delle attività di manutenzione, come l'aggiornamento del firmware di un dispositivo.

> **Gestione delle vulnerabilità:** Axis offre un servizio di notifica di sicurezza a cui è possibile iscriversi per ottenere informazioni su vulnerabilità e altri temi legati alla sicurezza.

> **AXIS OS Forensic Guide:** la guida offre consigli tecnici per chi conduce analisi forensi sui dispositivi Axis in caso di attacco informatico alla rete e all'infrastruttura IT in cui è installato un dispositivo Axis.

> **Video con firma:** abilitando questa funzione su una telecamera supportata, vengono aggiunte firme crittografiche al flusso video prima che lasci il dispositivo, consentendo di verificare se il video sia stato manomesso o meno. Questo è particolarmente importante in un'indagine o in un'azione penale.

SMALTIMENTO

Affrontare il rischio di dispositivi non più supportati e che presentano vulnerabilità note senza patch applicate, oltre al rischio che i dati sensibili rimangano sui dispositivi dopo lo smaltimento

> **Data di fine supporto del firmware:** per molti prodotti, la pagina dell'assistenza su Axis.com indica la data di fine supporto per il firmware del prodotto specifico, consentendo ai clienti di programmare per tempo lo smaltimento e la sostituzione dei dispositivi.

> **AXIS Device Manager Extend:** consente di monitorare in modo semplice lo stato della garanzia di tutti i dispositivi nel sistema, comprese le date di fine produzione e fine supporto. Queste informazioni consentono di preparare un dispositivo per lo smaltimento ed eliminare i rischi dovuti a dispositivi non supportati.

> **Linee guida:** il portale AXIS OS sul sito Axis fornisce linee guida per lo smaltimento di un dispositivo Axis. Riportando un dispositivo alle impostazioni di fabbrica, tutte le configurazioni e i dati vengono cancellati.

Per ulteriori informazioni, visita: **www.axis.com/about-axis/cybersecurity**

AXIS COMMUNICATIONS