Comprendere la Direttiva NIS 2

CONTENUTI DEL MANUALE

1. Cos'è la Direttiva NIS 2? 5

2. Cosa è cambiato? 9

3. Che impatto avrà la NIS 2? 13

4. Quali caratteristiche del prodotto possono contribuire a mitigare le minacce e a proteggere dagli attacchi? 17

5. Conclusione 19

1

Cosa è la Direttiva NIS 2?

La Direttiva NIS, nota anche come Direttiva (UE) 2016/1148, è una direttiva dell'UE che stabilisce i requisiti di sicurezza informatica per gli operatori di servizi essenziali e i fornitori di servizi digitali nell'Unione europea. La Direttiva NIS mira a garantire un livello elevato di sicurezza delle reti e delle informazioni in tutta l'UE e ad assicurare che gli operatori di servizi essenziali e i fornitori di servizi digitali adottino misure adeguate a gestire il rischio posto alle loro reti e ai loro sistemi informativi.

Il 10 novembre 2022, il Parlamento Europeo ha adottato la Direttiva NIS 2. Essa sostituisce e abroga la Direttiva NIS precedente. NIS 2 migliorerà la gestione del rischio nella sicurezza informatica e introdurrà obblighi di notifica degli eventi in vari settori come l'energia, i trasporti, l'assistenza sanitaria e l'infrastruttura digitale. Gli Stati membri avranno 21 mesi a partire dall'entrata in vigore della Direttiva per incorporare le disposizioni nella loro legislazione nazionale.

NIS 2 ha tre obiettivi generali:

Resilienza informatica

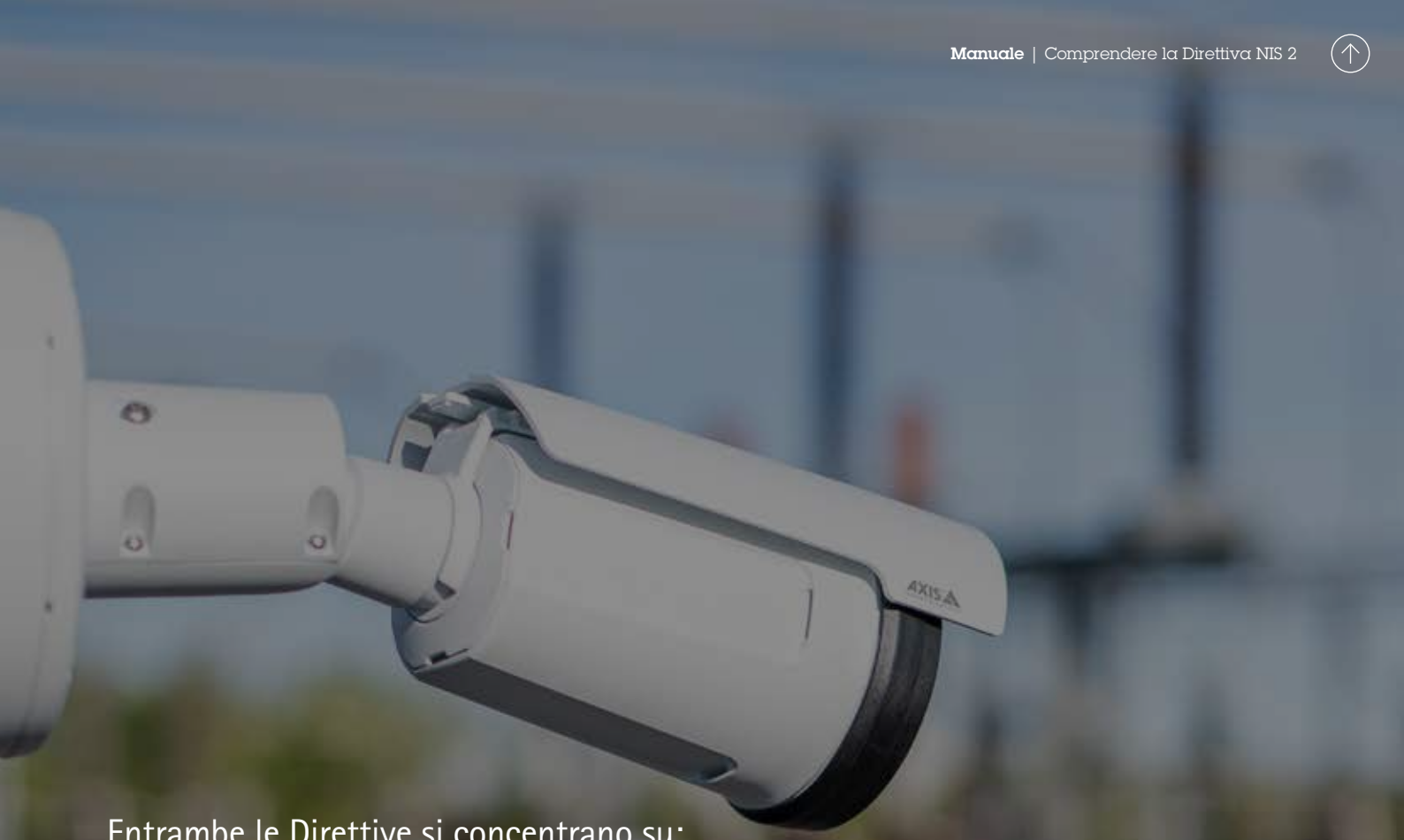
Aumentare la resilienza informatica di una un'ampia gamma di imprese con sede nell'Unione Europea che operano in tutti i settori rilevanti e che svolgono attività essenziali.

Un approccio unificato

Ridurre le incoerenze della resilienza nel mercato interno dei settori attualmente coperti dalla Direttiva NIS, unificando le capacità di sicurezza informatica.

Stabilire procedure

Migliorare la consapevolezza situazionale congiunta e la capacità collettiva di pianificare e rispondere agli attacchi informatici, potenziando la condivisione delle informazioni e stabilendo norme e procedure nel caso di incidente o crisi su larga scala.



Entrambe le Direttive si concentrano su:

> L'adozione di misure tecniche e organizzative al fine di aumentare la sicurezza delle loro reti e sistemi informatici.

> L'adozione di misure adeguate per prevenire incidenti di sicurezza e/o minimizzare il loro impatto al fine di garantire la continuità del servizio.

> La velocità delle comunicazioni verso le autorità competenti, senza indebito ritardo, di qualsiasi incidente di servizio che abbia un impatto significativo sulla continuità del servizio.

2

Cosa è cambiato?

La nuova proposta elimina la distinzione tra OES (Operatori di Servizi Essenziali) e DSP (Fornitori di Servizi Digitali), classificando invece le entità come essenziali o importanti. Non bisogna dimenticare che, secondo la vecchia Direttiva NIS, gli Stati membri erano responsabili di determinare quali entità avrebbero soddisfatto i criteri per qualificarsi come operatori di servizi essenziali. Al contrario, la nuova Direttiva NIS 2, introduce una regola basata sulle dimensioni delle aziende come principio generale per identificare le entità che ricadono sotto la direttiva. Ciò significa che tutte quelle entità di medie e grandi dimensioni che operano nei settori o forniscono servizi coperti dalla direttiva, rientreranno nel suo ambito di applicazione.

Ulteriori modifiche

1. La copertura della Direttiva NIS 2 è stata ampliata per incorporare nuovi settori (ad esempio, la gestione delle acque reflue, il settore alimentare, lo spazio e così via) in base alla loro criticità per l'economia e la società, includendo, a tal fine, tutte le medie e grandi imprese di questi settori. Allo stesso tempo, agli Stati membri viene garantita una certa flessibilità nell'identificare le entità più piccole con un profilo ad alto rischio.

2. La creazione, attraverso l'Agenzia dell'Unione Europea per la sicurezza informatica (ENISA), di una rete europea di collegamento per le organizzazioni che gestiscono le crisi informatiche nei vari paesi (EU-CyCLONe), al fine di sostenere la gestione coordinata della sicurezza informatica relativa a incidenti e crisi su larga scala a livello comunitario.

3. Viene stabilito un maggiore coordinamento nella divulgazione delle nuove vulnerabilità scoperte in tutta l'Unione.

4. Viene istituita una lista di sanzioni amministrative (simili a quelle del GDPR), incluse multe per la violazione degli obblighi di segnalazione e gestione dei rischi di sicurezza informatica.

5. La proposta include sette elementi che tutte le aziende devono affrontare o implementare per rafforzare i requisiti di sicurezza:

- Analisi del rischio e politiche di sicurezza dei sistemi informativi
- Gestione degli incidenti (prevenzione, individuazione e risposta agli incidenti)
- Continuità operativa e gestione delle crisi
- Sicurezza della catena di approvvigionamento
- Sicurezza nelle reti e nei sistemi informativi
- Politiche e procedure per le misure di gestione del rischio di sicurezza informatica
- L'uso della crittografia e della cifratura

6. La proposta introduce misure di vigilanza più severe per le autorità nazionali, rinforza i requisiti di sicurezza e mira ad armonizzare i regimi sanzionatori tra gli Stati membri.

7. A livello europeo, la proposta rafforza la sicurezza informatica delle tecnologie chiave relative a informazione e telecomunicazioni. Gli Stati membri, in cooperazione con la Commissione e l'ENISA, dovranno effettuare valutazioni coordinate del rischio sulle catene di approvvigionamento critiche, basandosi sull'approccio efficace adottato nel contesto delle Raccomandazioni della Commissione sulla sicurezza informatica delle reti 5G.

8. La nuova Direttiva è stata allineata con la legislazione specifica del settore, in particolare con il Digital Operational Resilience Act (DORA), applicabile al settore finanziario, e con la Critical Entities Resilience Directive (CER), che rafforza la resilienza delle entità critiche che forniscono servizi vitali di cui dipendono le condizioni di vita dei cittadini dell'UE, come l'energia, i trasporti, la salute e l'approvvigionamento di acqua potabile. Ciò garantirà chiarezza giuridica e coerenza tra NIS 2 e queste leggi.

3

Che impatto avrà la NIS 2?

La Direttiva NIS richiede agli OES e ai DSP di proteggere le loro risorse critiche al fine di ridurre al minimo i rischi che un incidente di sicurezza potrebbe presentare per la fornitura dei loro servizi. In teoria, ogni organizzazione conosce quali sono le cose importanti per fornire il proprio servizio e gestire la propria attività. Si potrebbe sostenere che alcune tecnologie, come una telecamera di sorveglianza di rete, non siano considerate risorse critiche. Tuttavia, è importante adottare un approccio olistico durante la definizione del perimetro di sicurezza. Alcuni sistemi potrebbero presentare un rischio anche se non rientrano nel perimetro definito. Ad esempio, sebbene una telecamera possa non essere essenziale per il servizio, potrebbe comunque contenere vulnerabilità attraverso le quali un malintenzionato potrebbe lanciare un attacco alle risorse critiche dell'azienda. È quindi fondamentale che gli OES e i DSP tengano conto di tali rischi durante la loro valutazione in conformità alla Direttiva NIS.

Sostenere la conformità

Dato il maggiore focus sulla sicurezza delle catene di approvvigionamento, ci si aspetta che le organizzazioni che devono conformarsi alla NIS 2 svolgano un livello maggiore di verifiche e controlli sui propri partner tecnologici. Come parte di questo processo di valutazione e di analisi dei rischi dei fornitori, si prevede che le regolamentazioni e le procedure giocheranno un ruolo molto importante.

Dimostrare la maturità informatica

Mettere in sicurezza una rete, i suoi dispositivi e i servizi che supporta richiede la partecipazione attiva di tutta la catena di approvvigionamento dei fornitori, così come dell'organizzazione dell'utente finale. Axis fornisce strumenti, documentazione e formazione per aiutare a mitigare i rischi e mantenere i propri prodotti e servizi sempre aggiornati e protetti. Axis, a questo proposito, attua una grande quantità di politiche e di processi standardizzati e certificati da terze parti.

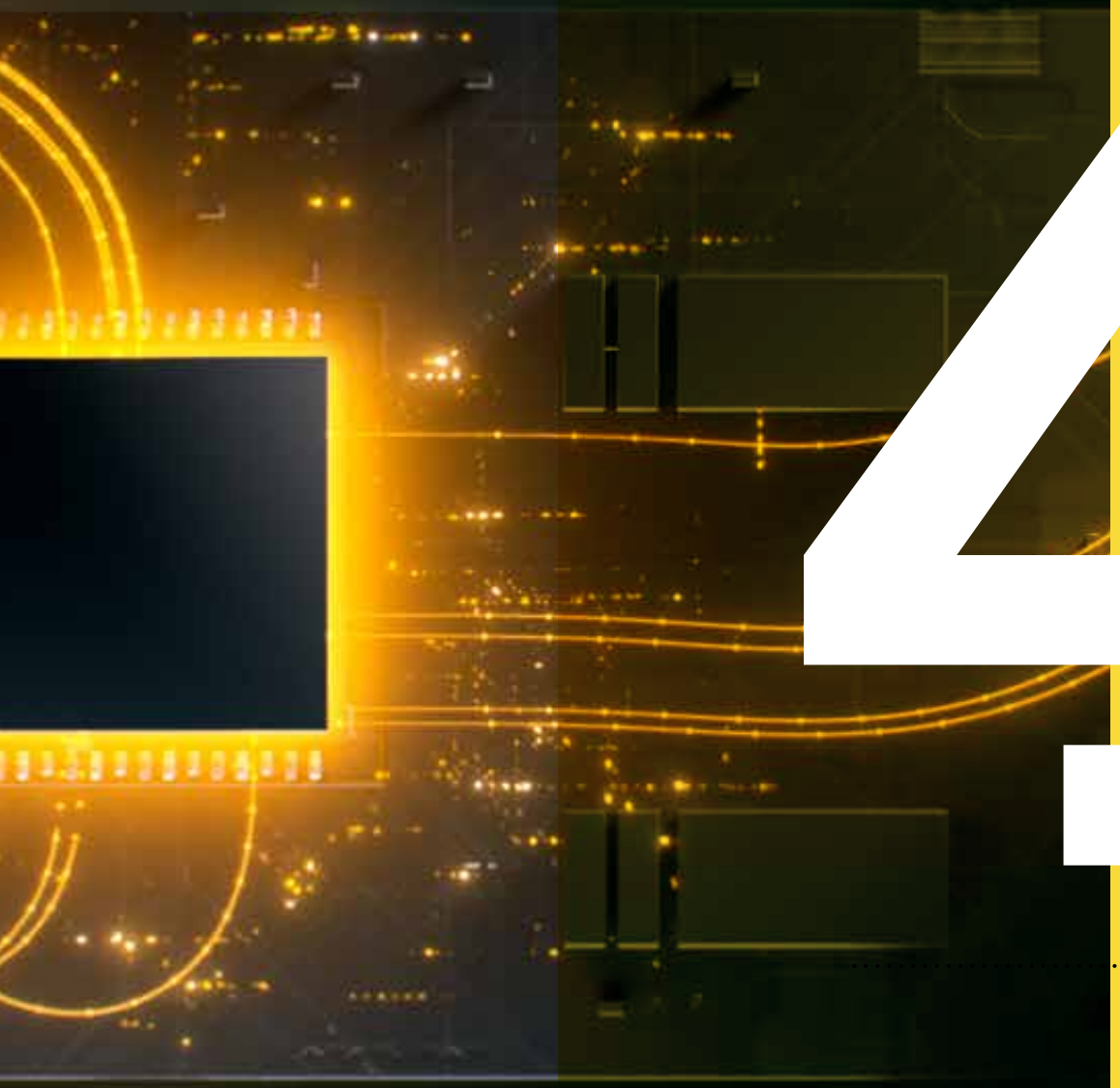
Sono le seguenti:

- Certificazione ISO/IEC 27001 per il nostro sistema di gestione della sicurezza delle informazioni (ISMS)
- Cyber Essentials Plus
- Building Security in Maturity Model (BSIMM)
- Axis Security Development Model (ASDM) – una linea guida che definisce il processo e gli strumenti utilizzati da Axis per sviluppare software con un elevato livello di sicurezza intrinseca lungo l'intero ciclo di vita dei propri prodotti, dall'installazione alla dismissione
- Axis è un'autorità certificata CVE (CVE Numbering Authority) nell'ambito del dominio MITRE
- Politica di Gestione delle Vulnerabilità
- Notifiche degli avvisi di sicurezza

Integrità dei prodotti nella supply chain

L'integrità del prodotto può essere garantita solo quando l'hardware e il firmware sono protetti con successo da modifiche o manipolazioni non autorizzate durante tutto il percorso del prodotto attraverso la catena di approvvigionamento. Insieme ai propri fornitori di materiali e ai partner che provvedono all'assemblaggio dei prodotti, Axis applica una moltitudine di controlli di qualità e sicurezza per mantenere e proteggere l'integrità dei suoi prodotti. Ad esempio:

- Il Sistema di Gestione della Sicurezza delle Informazioni (ISMS) di Axis è certificato ISO 27001, il che significa che segue processi e standards riconosciuti a livello internazionale per la gestione dell'infrastruttura informatica interna e dei sistemi che supportano il percorso del prodotto attraverso la catena di approvvigionamento.
- Axis applica il concetto di "Zero Trust" basato sul principio del "non fidarsi mai e verificare costantemente", sia per le persone che per le macchine, che si connettono alle reti e alle infrastrutture.
- I componenti sono sempre reperiti tramite fornitori presenti nella Lista di Fornitori Approvati, in conformità con gli elenchi di materiali e le specifiche di produzione emesse da Axis.
- Il fornitore non può apportare modifiche alle specifiche di produzione critiche senza il permesso di Axis. Qualsiasi modifica, dopo l'approvazione, deve essere documentata e tracciata.
- Il processo di gestione dei materiali assicura sempre il perfetto stato degli stessi, mettendo in evidenza eventuali deviazioni che potrebbero comprometterne la qualità.
- Ai fornitori e ai partner che si occupano degli assemblaggi, è richiesto di mantenere un sistema che assicuri la completa tracciabilità dei lotti prodotti, a partire dai componenti in ingresso fino alle parti finite. Durante la produzione, le varie parti saranno sottoposte a molteplici test, come il Controllo di Qualità in Arrivo (IQC) e l'Ispezione Ottica Automatica (AOI), per verificare che non siano montati componenti contraffatti o non autorizzati.
- L'equipaggiamento specifico per la produzione delle parti più critiche e il relativo sistema di test, sono sviluppati, prodotti e forniti da Axis, così come il sistema per testare i componenti, i moduli e i prodotti ai diversi livelli durante la produzione. Queste procedure limitano i rischi legati alle manipolazioni. Axis, per i suoi prodotti, mette a disposizione una notevole quantità di funzionalità di sicurezza integrate avanzate.
- ARTPEC® è la piattaforma di microprocessori (SoC) sviluppata internamente da Axis, conforme al National Defense Authorization Act (NDAA) promulgato negli Stati Uniti. ARTPEC ha funzionalità di sicurezza integrate esclusivamente progettate per i dispositivi Axis. Tra queste si evidenziano il Signed Firmware, il quale garantisce che solo firmware autorizzato e sicuro possa essere installato, e il Secure Boot, che impedisce l'avvio di firmware non digitalmente firmato da Axis.
- A ulteriore garanzia dei controlli di sicurezza, tutti i dati di test sono condivisi con Axis 24/7 dai nostri partner che provvedono all'assemblaggio, in modo che eventuali modifiche non autorizzate possano essere identificate immediatamente.



4

Quali caratteristiche del prodotto possono contribuire a mitigare le minacce e a proteggere dagli attacchi?

Questa sezione descrive alcune delle funzionalità di sicurezza avanzate disponibili nei prodotti Axis.

Signed firmware

Il signed firmware è implementato dal fornitore del software e prevede la firma digitale del firmware con una chiave privata. Quando il firmware ha questa firma associata ad esso, il dispositivo lo convalida prima di accettare l'installazione. Se il dispositivo rileva che l'integrità del firmware è compromessa, l'aggiornamento del firmware verrà respinto.

Secure boot

L'avvio sicuro (Secure Boot) è un processo di avvio che consiste in una catena ininterrotta di software criptograficamente convalidato, che inizia nella memoria non volatile di sola lettura (boot ROM). A completamento delle funzionalità del Signed Firmware, Secure Boot garantisce che un dispositivo possa avviarsi solo con un firmware digitalmente firmato tramite le chiavi crittografiche corrette.

Axis Edge Vault

Axis Edge Vault è un modulo computazionale di crittografia che può essere utilizzato per operazioni crittografiche su certificati memorizzati in modo sicuro. Edge Vault è un modulo di memoria sicuro, protetto da manomissioni, che consente a ciascun dispositivo di proteggere i propri segreti. Edge Vault costituisce una base per l'implementazione di funzionalità di sicurezza estremamente avanzate.

Axis device ID

L'Axis device ID funziona come un passaporto digitale ed è univoco per ciascun dispositivo. Esso viene memorizzato in modo sicuro e permanente in Edge Vault come certificato, firmato dal certificato originale di Axis. L'Axis device ID è è stato progettato per certificare l'origine del dispositivo, consentendo un nuovo nuovo livello di identificazione univoca del dispositivo per tutto il ciclo di vita del prodotto.

Memorizzazione sicura delle chiavi tramite "trusted platform module" (TPM)

Il Trusted Platform Module (TPM) è un componente che fornisce un certo insieme di funzionalità crittografiche adatte a proteggere le informazioni da accessi non autorizzati. La chiave privata è memorizzata nel TPM e non lascia mai il TPM. Tutte le operazioni crittografiche che richiedono l'uso della chiave privata vengono inviate al TPM per essere elaborate. Ciò garantisce che la parte segreta del certificato non lasci mai l'ambiente sicuro all'interno del TPM e che quindi rimanga al sicuro anche in caso di violazione della sicurezza.

Signed video

La funzionalità Signed Video garantisce che le immagini registrate possano essere verificate come non manomesse, senza dover ricostruire la catena di passaggi del file video. Ogni telecamera utilizza il proprio Axis device ID, conservato in modo sicuro nel modulo Axis Edge Vault, per aggiungere una firma digitale nel flusso video. Quando il video viene riprodotto, il lettore del file mostra se il video è intatto. La funzionalità Signed Video rende possibile rintracciare l'origine della registrazione video fino alla telecamera, e verificare che essa non sia stata manomessa e sia ancora nella sua forma originale.

HTTPS Enabled

L'HTTPS è abilitato di default con un certificato "self-signed" a partire da AXIS OS 7.20.
Ciò consente di impostare la password del dispositivo in modo sicuro. In AXIS OS 10.10 e versioni successive, il certificato "self-signed" è stato sostituito dall'Axis Device ID, secondo lo standard IEEE 802.1AR.

Di seguito sono elencati gli strumenti e le guide di Axis per supportare il processo di installazione, messa in servizio e manutenzione:

Hardening Guide

Come linee guida per strutturare le nostre raccomandazioni in un contesto di sicurezza informatica, Axis ha scelto di seguire i metodi delineati nel CIS Controls versione 8, pubblicati dal Center for Internet Security (CIS). Precedentemente noti come SANS Top 20 Critical Security Controls, i controlli CIS evidenziano 18 categorie di Controlli di Sicurezza Critici (CSC), focalizzati sulla gestione delle categorie di rischio relative alla sicurezza informatica più comuni, affrontate da un'organizzazione. Queste raccomandazioni possono essere trovate nel documento Axis. Hardening Guide, diponibile sul nostro sito web.

AXIS Device Manager

AXIS Device Manager è lo strumento di riferimento per l'installazione e la configurazione rapida e semplice di nuovi dispositivi. Offre agli installatori di sicurezza e agli amministratori di sistema uno strumento altamente efficace per gestire tutte le principali operazioni di installazione, messa in sicurezza e manutenzione, sia per singola telecamera, che per più dispositivi contemporaneamente. Utilizzare AXIS Device Manager è il modo più efficiente per rilevare i dispositivi Axis in una rete, implementare politiche di sicurezza sugli stessi e svolgere tutti gli aggiornamenti del firmware in modo rapido ed efficiente.

Conclusione

Sebbene sia molto improbabile che i sistemi di sicurezza vengano classificati come risorse critiche, è importante che gli OES (Operatori di Servizi Essenziali) e i DSP (Fornitori di Servizi Digitali) adottino un approccio olistico durante la fase di definizione del perimetro di sicurezza. Ciò significa che le tecnologie di sicurezza fisica devono essere valutate in modo approfondito secondo le valutazione della Direttiva NIS 2, per evidenziare eventuali rischi potenziali.

Axis adotta una visione a 360 gradi riguardo alla sua offerta di sicurezza informatica. I prodotti sono progettati con funzionalità integrate per affrontare le problematiche riguardanti la sicurezza informatica, in aggiunta ad un'ampio ventaglio di procedure, processi, strumenti, documentazioni e piani di formazione già esistenti, che aiuteranno a mitigare i rischi per mantenere protetti i clienti.

Informazioni su Axis Communications

Axis permette di creare un mondo più intelligente e sicuro attraverso la creazione di soluzioni per migliorare la sicurezza e le prestazioni aziendali. Come azienda di tecnologia di rete e leader del settore, Axis offre soluzioni nella videosorveglianza, il controllo degli accessi, gli intercomunicanti e i sistemi audio. Queste soluzioni sono potenziate da applicazioni di analisi intelligenti e supportate da formazione di alta qualità.

Axis conta circa 4.000 dipendenti dedicati in oltre 50 paesi e collabora con partner di tecnologia e integrazione di sistemi in tutto il mondo per fornire soluzioni ai clienti. L'azienda è stata fondata nel 1984 e ha sede a Lund, in Svezia.