AXIS COMMUNICATIONS CYBERSECURITY MAGAZINE

Partner per la protezione

APPROFONDIMENTI e ISPIRAZIONI
DAL MONDO DELLA CYBERSECURITY

Entra >

AXIS COMMUNICATIONS

INTRODUZIONE

Un framework solido per la protezione

Come forse sapete, non esiste un'unica soluzione ai problemi di cybersecurity, né una sorta di "corazza incorporata" in ogni prodotto. Piuttosto, la cybersecurity è una questione di partnership di fiducia in cui tutti – subfornitori, produttori, installatori, integratori e utenti finali – hanno un ruolo importante. È anche questione di processi continui, più che di risultati una tantum.

Essendo partner responsabili per la cybersecurity, abbiamo raccolto una serie di articoli, consigli e ispirazioni. Riteniamo e ci auguriamo che possano esservi utili per rimanere aggiornati e proteggervi.

Prima di girare pagina, però, vorremmo parlarvi brevemente del framework di gestione dei rischi del National Institute of Standards and Technology (NIST). Poiché la cybersecurity consiste essenzialmente nel gestire i rischi, un buon punto di partenza è valutare quelli per la vostra azienda in termini di probabilità e potenziali danni utilizzando uno dei tanti framework di gestione.

Axis ha scelto di allineare il suo approccio alla cybersecurity con il framework NIST. Le linee guida del NIST sono utilizzate a livello internazionale e sono adatte non solo a grandi aziende e organizzazioni, ma anche a piccole e medie imprese. Anche se la vostra utilizza un framework diverso, è probabile che sia compatibile con il framework NIST.

Il framework NIST si basa su cinque pilastri: Identificare, Proteggere, Rilevare, Rispondere e Recuperare. Per maggiori informazioni su ognuno di questi pilastri, sul nostro ruolo di partner per la cybersecurity e sui vostri ruoli, visitate il sito www.axis.com/cybersecurity.

Nel frattempo, ci auguriamo che la rivista sia di vostro gradimento!

SOMMARIO

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 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, dovete chiedervi cosa siete disposti a fare per prevenire gli effetti negativi.

Conoscere i beni e le risorse

Per quanto riguarda i sistemi video, la prima risorsa da proteggere è il flusso video acquisito dalle telecamere. I beni sono le registrazioni contenute nel software di gestione video (VMS). Normalmente, l'accesso viene controllato assegnando privilegi diversi agli utenti. Altre risorse da considerare sono gli account utente e le password, le configurazioni, il sistema operativo, il firmware, il software e i dispositivi con connettività di rete.

Dettagli >

Da quali minacce proteggersi?

Il primo passo per proteggervi dalle minacce informatiche è conoscerle. In un sistema IT, si ritiene che i principali elementi da proteggere siano la riservatezza, l'integrità e la disponibilità. 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 tre minacce informatiche più comuni per la video-sorveglianza

1. Ingenuità ed errori non intenzionali degli utenti
2. Uso scorretto intenzionale del sistema
3. Manomissioni e sabotaggi

Dettagli >

1

Ingenuità ed errori non intenzionali degli utenti

Indipendentemente da quanto siano sofisticate le tecnologie che utilizzate per proteggere la rete, se un malintenzionato riesce a indurre anche una sola persona a cliccare su un link contenuto in un'e-mail, può già entrare. Per i cybercriminali, questo è il modo di attaccare più semplice, dunque il preferito. 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 scorretto delle password:** le password non sono sicure o non vengono protette/aggiornate adeguatamente.
- **Errata gestione dei componenti critici:** gli oggetti/elementi che consentono di accedere al sistema vengono smarriti o lasciati alla portata di tutti. Esempi: badge di accesso, telefoni, laptop e documenti.
- **Gestione inadeguata del sistema:** mancata installazione degli aggiornamenti di sistema e delle patch di sicurezza.
- **Miglioramenti infruttuosi:** 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 al video e i permessi operativi, concedendoli solo a un ristretto gruppo di persone fidate attraverso il VMS.

Dettagli >

Uso scorretto intenzionale del sistema

2

Un'altra minaccia fin troppo comune è l'uso scorretto del sistema video da parte di persone che ne hanno accesso legittimo. Tra gli esempi di uso scorretto intenzionale:

- Accesso non autorizzato e manipolazione di servizi e risorse del sistema
- Furto di dati
- Danni intenzionali al sistema

Vulnerabilità e uso scorretto intenzionale

È importante implementare regole e processi a lungo termine per gestire le vulnerabilità e ridurre il rischio di uso scorretto intenzionale del sistema. È importante controllare le persone che hanno il permesso di accedere ai dati sensibili, nonché limitarne il numero. Sui dispositivi devono essere utilizzati account separati per l'amministrazione e i client di uso quotidiano (VMS), ma anche un account temporaneo per la manutenzione e la risoluzione dei problemi. Se questi tre account coincidono, la password potrebbe essere nota in tutta l'azienda, favorendo usi scorretti intenzionali o accidentali.

Dettagli >

3

Manomissioni o sabotaggi

La protezione fisica dei sistemi IT è molto importante ai fini della cybersecurity:

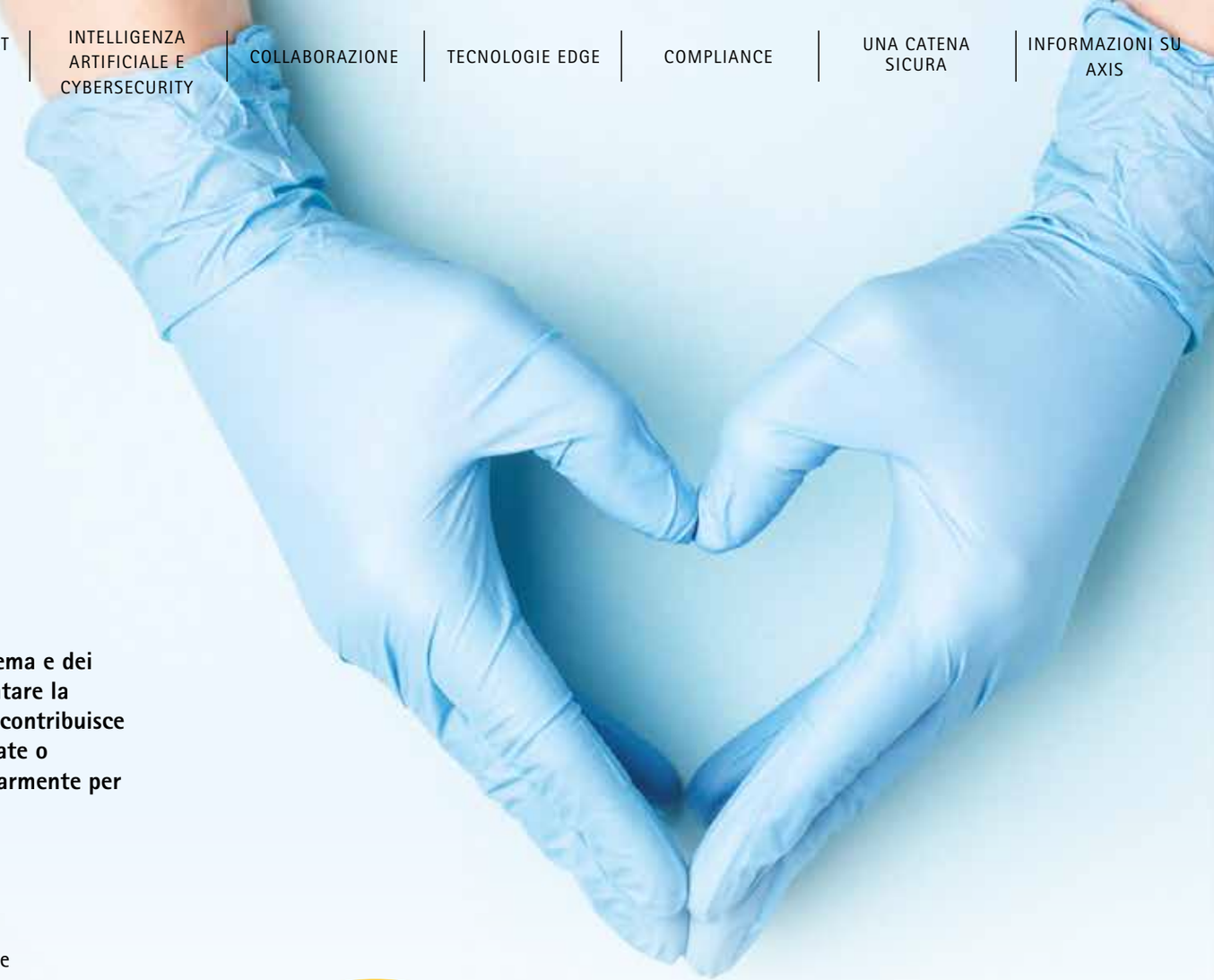
- I dispositivi esposti possono essere manomessi.
- I dispositivi esposti possono essere rubati.
- I cavi esposti possono essere scollegati, deviati o tagliati.

Vulnerabilità e minacce fisiche

Le manomissioni non riguardano solo le telecamere; anche i cavi di rete possono essere esposti e favorire violazioni. Altre vulnerabilità comuni e potenzialmente sfruttabili 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.

Attenti alle conseguenze

I sistemi video non elaborano transazioni finanziarie e non custodiscono i dati dei clienti. Questo significa che un attacco a un sistema video può essere difficile da monetizzare e che quindi ha un 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. Alla lunga, chi spende poco può ritrovarsi a spendere molto di più.



Il concetto di "cyber hygiene"

"Cyber hygiene" indica le procedure e gli accorgimenti che gli utenti di un sistema e dei dispositivi devono adottare per mantenere il sistema in buono stato e incrementare la sicurezza online. La cyber hygiene rientra spesso nei processi interni generali e contribuisce a mettere in sicurezza l'identità e altre informazioni che potrebbero essere rubate o danneggiate. Come l'igiene corporea, la cyber hygiene deve essere curata regolarmente per contrastare il deterioramento naturale del sistema e le minacce più comuni.

I vantaggi di una corretta "igiene"

Seguire procedure regolari di cyber hygiene per i dispositivi e i software ha vantaggi per la manutenzione e la sicurezza.

- La manutenzione fa sì che i dispositivi e i software siano sempre efficienti al massimo. File frammentati e programmi obsoleti aumentano il rischio di vulnerabilità. Le procedure di manutenzione aiutano a identificare tempestivamente i problemi e possono prevenire gravi danni. I sistemi in buono stato di manutenzione sono meno vulnerabili ai rischi per la cybersecurity.
- Dagli hacker ai ladri di identità, fino ai virus e ai malware intelligenti, le aziende sono sempre a rischio. Prevedendo le minacce e adottando corrette procedure di cyber hygiene, è possibile effettuare una diagnosi precoce e prepararsi ai rischi, oppure evitare che diventino realtà.

Come l'igiene corporea, la cyber hygiene deve essere curata regolarmente

Dettagli >

Uso di password univoche e sicure

Può sembrare ovvio, ma il modo più comune in cui i cyber criminali accedono ai sistemi è attraverso l'uso di password non sicure. La maggior parte dei sistemi IP viene consegnata con password e impostazioni predefinite. Dunque, è fondamentale cambiarle immediatamente seguendo le regole del reparto IT o dell'azienda. Le aziende devono provvedere a una gestione ottimale utilizzando password sicure e univoche (di almeno 8 caratteri), da cambiare regolarmente e da non condividere mai tra i vari siti. Far rispettare le regole sulle password non spetta ai sistemi informatici. Le aziende devono fare in modo che i dipendenti siano preparati e conoscano le prassi ottimali per la loro gestione. Si consiglia anche di utilizzare certificati per crittografare le password e i nomi utente.

Una password formata da una parola di uso comune o da un solo nome può essere craccata in pochi secondi, a prescindere dalla lunghezza.

Utilizzare e installare i dispositivi seguendo le regole del reparto IT o sicurezza

Quando si usa un dispositivo, i servizi non utilizzati non andrebbero mai lasciati attivi. Per i cybercriminali è un modo semplice di attaccare e installare applicazioni dannose. Disattivando i servizi non utilizzati e installando solo applicazioni attendibili, si hanno meno probabilità che un hacker riesca a sfruttare una vulnerabilità del sistema. È altrettanto fondamentale che i dispositivi siano installati correttamente e che le porte di rete e delle schede SD non siano mai accessibili al pubblico.

Dettagli >

Definire chiaramente ruoli e responsabilità

È necessario stabilire regole e procedure chiare per garantire che i dipendenti abbiano i privilegi di accesso corretti per la loro area di responsabilità. Le aziende devono configurare gli account seguendo la logica del "minimo privilegio": ovvero, gli utenti devono accedere solo alle risorse di cui hanno bisogno per svolgere il loro lavoro. Gli account predefiniti non dovrebbero mai essere utilizzati. Se si utilizzano account temporanei per la manutenzione, eliminarli sempre al termine delle operazioni.

Mai affidarsi alle impostazioni predefinite di un dispositivo, soprattutto la password. Gli ID account degli amministratori e le password predefinite dei dispositivi più comuni si possono trovare facilmente con una ricerca su Google, semplificando fin troppo l'accesso agli hacker. Attivare e configurare sempre i servizi di protezione dei dispositivi e utilizzare le impostazioni predefinite solo a scopo dimostrativo.

Il **61%** dei lavoratori usa i dispositivi sia per attività personali che per lavoro

L'**80%** dei dipendenti ammette di utilizzare applicazioni Software-as-a-Service (SaaS) non approvate per lavoro

Il **75%** delle intrusioni in rete sfrutta credenziali non sicure o rubate

Dettagli >

Utilizzare il firmware più recente

I vostri dispositivi sono aggiornati con il firmware più recente? Bug o falle presenti su sistemi e dispositivi lasciano le aziende esposte agli attacchi e possono consentire agli hacker di rubare chiavi private dei server o password degli utenti. È importante seguire un piano di gestione degli aggiornamenti software/firmware ben documentato e garantire che i dispositivi di rete siano sempre dotati del firmware e degli aggiornamenti di sicurezza più recenti.

Eseguire un'analisi dei rischi

Quanto dovrebbe spendere la vostra azienda per proteggere le sue risorse? Analizzando le potenziali minacce interne ed esterne, ma anche le conseguenze se le principali risorse dovessero essere danneggiate o perse, potete dare priorità ai vostri sforzi per proteggerle. Esistono anche framework di gestione dei rischi per la cybersecurity, come quello del NIST (National Institute of Standards and Technology), che propongono utili linee guida e procedure.

Il numero di violazioni è aumentato significativamente nel 2019, con oltre

8,5 miliardi di documenti/registri

esposti – più di tre volte rispetto al 2018.*

*IBM X-Force Threat Intelligence Index 2020 - Acquisire conoscenze sulla protezione dei sistemi e sulle eventuali minacce

Dettagli >

Quanto è sicura la vostra catena di fornitura?

Lavorando a stretto contatto con tutta la filiera produttiva, potete capire meglio i pericoli per la vostra rete e i dispositivi connessi. Oggi, molti produttori IT forniscono procedure ottimali o guide per consolidare la protezione dei dispositivi di rete, oltre a documentare la sicurezza della catena di fornitura. Se questi documenti non sono disponibili, è importante parlarne con il produttore o reperire altri contenuti generati dagli utenti. I dispositivi devono rispettare le vostre regole IT, sia individualmente che all'interno del sistema.

Utilizzare sempre connessioni crittografate

Qualunque sia il vostro settore, tutti i dati devono essere protetti con la crittografia. Inoltre, è opportuno crittografare le connessioni di tutte le reti, anche locali o "interne". I protocolli di autenticazione criptano le informazioni prima che siano inviate in rete e riducono drasticamente le probabilità di un attacco, che si serve di un codice dannoso per intercettare le trasmissioni non crittografate.

Protocolli sicuri

- L'autenticazione HTTP Digest (accesso) è uno dei metodi utilizzabili da un server web per verificare le credenziali e l'identità di un utente, come il nome utente o la password.
- HTTPS (HyperText Transfer Protocol Secure) è il protocollo di crittografia dei dati più comune. HTTPS è identico a HTTP, con la differenza che i dati trasferiti vengono crittografati ulteriormente tramite Secure Sockets Layer (SSL) o Transport Layer Security (TLS).
- SRTP (Secure Real-Time Transport Protocol) cripta il flusso video per una maggiore protezione delle immagini. Se si utilizza un VMS o una scheda SD per l'archiviazione locale dei video, verificare che anche questi siano crittografati.

Dettagli >

Proteggere il perimetro della rete

Sapete usare bene i firewall e i filtri? Proteggendo la rete in modo strutturale, potete supportare altri strumenti per implementare le procedure ottimali di cybersecurity. L'uso della segmentazione di rete (ad esempio le VLAN, Virtual Local Area Network) sui dispositivi per la sicurezza fisica riduce il rischio di intercettazioni di informazioni sensibili e attacchi ai singoli server e dispositivi connessi. Inoltre, le ACL (Access Control List) possono aiutare a controllare i movimenti sospetti. Prima di investire sui nuovi dispositivi, chiedete al produttore un elenco delle porte di rete, per verificare che la soluzione funzioni nell'intera rete.

Una corretta manutenzione è molto importante per la salute generale del sistema

Manutenzione di sistemi e processi

Una corretta manutenzione è molto importante per la salute generale del sistema. I dispositivi e i registri devono essere monitorati regolarmente per rilevare qualsiasi tentativo di accesso non autorizzato. Con tecnologie che si evolvono a passo spedito, si sommano nuovi aggiornamenti, funzionalità e prassi da seguire; dunque, è opportuno documentare le procedure di manutenzione per fare in modo che siano comprese da tutti.

Un software di gestione dei dispositivi come AXIS Device Manager può aiutare le aziende ad acquisire in tempo reale un inventario completo di tutti i dispositivi e i software connessi in rete. L'applicazione esegue una scansione dell'intera rete e acquisisce tutte le informazioni più importanti, come numero di modello, indirizzi IP e MAC, versione del firmware e stato dei certificati.

Gestione del ciclo di vita: perché è importante

Come sappiamo, la protezione di una rete è pari a quella dei dispositivi connessi. Mentre le aziende adottano un approccio a livelli per proteggere le reti, necessitano anche di un modo efficace per gestire il ciclo di vita delle loro risorse fisiche. Spesso, però, trascurano gli aggiornamenti anche quando è disponibile un nuovo firmware, perché non hanno una visione d'insieme delle loro tecnologie.

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 una 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 tecnologia nuova e più efficiente? Ad esempio, una telecamera IP può funzionare per 15 anni, ma la sua durata effettiva è inferiore perché il panorama della cybersecurity cambia velocemente.

Gestione proattiva delle risorse

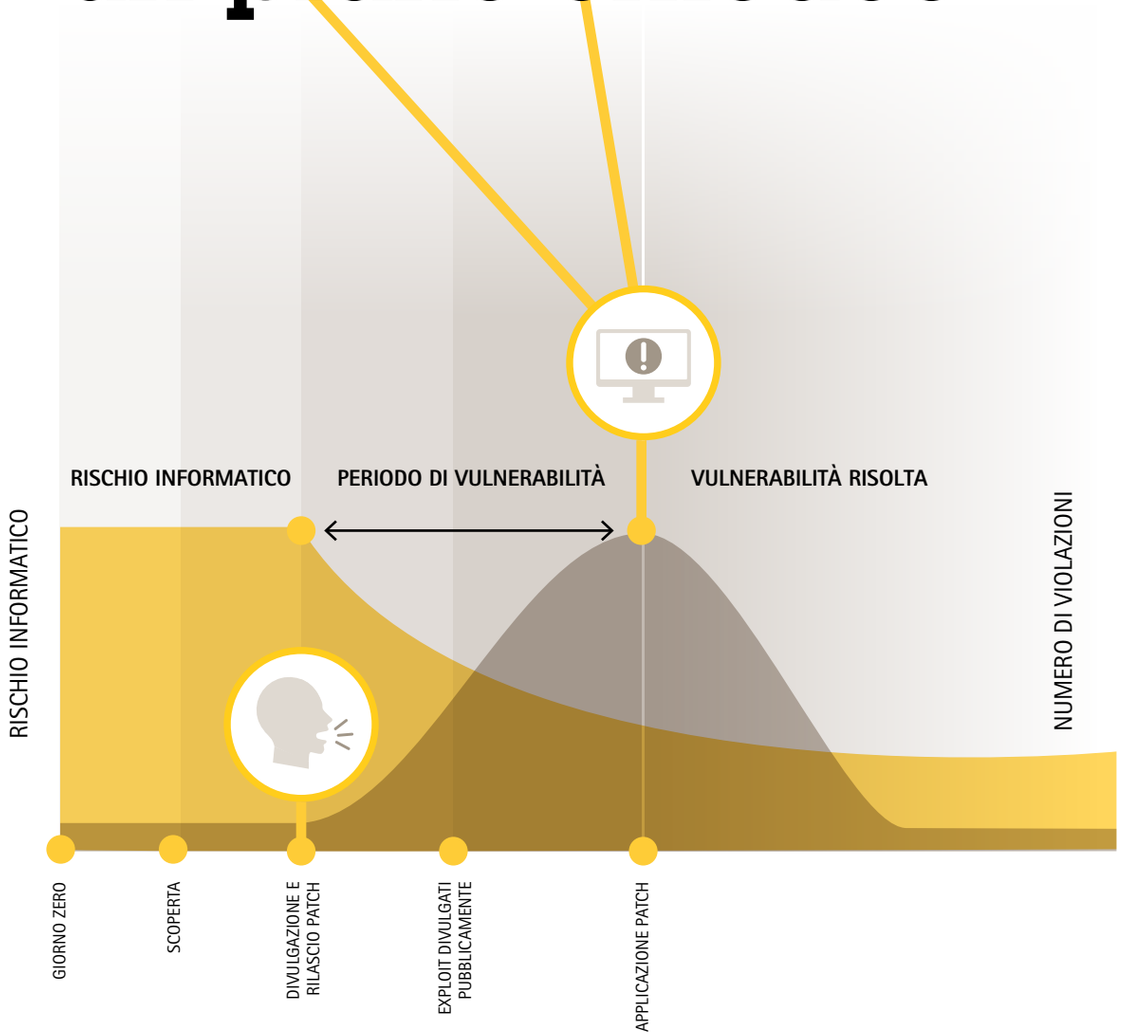
La gestione del ciclo di vita tiene conto del ciclo di vita funzionale ed economico delle risorse fisiche. Alle aziende serve un quadro chiaro di tutte le tecnologie utilizzate, in modo da poter monitorare le reti e i dati critici e garantire che siano al sicuro da minacce e vulnerabilità.

Secondo l'Information Commissioner's Office (ICO) del Regno Unito:

“Il 60% delle violazioni è dovuto a vulnerabilità per le quali era disponibile una patch, che però non è stata applicata.”

Dettagli >

La speranza non è un piano efficace



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

Gli aggiornamenti e le patch sono il modo migliore di incrementare la cybersecurity ma non sono sempre disponibili per le tecnologie di vecchia generazione, che potrebbero non essere più supportate dal produttore. Dal punto di vista della cybersecurity, le tecnologie obsolete e non protette da patch comportano i maggiori rischi. È fondamentale che le aziende restino al passo delle minacce e seguano sempre le migliori prassi in ambito di cybersecurity. Un dispositivo trascurato potrebbe diventare un facile punto di accesso per gli hacker.

Un passo avanti alle minacce

Una gestione efficace del ciclo di vita può aiutare le aziende a proteggersi. Inoltre, le aiuta 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 gravissime.

Anche i dispositivi fisici devono essere aggiornati

I produttori rilasciano regolarmente aggiornamenti firmware e patch di protezione che rimediano a vulnerabilità/bug e risolvono altri problemi di prestazione, in modo che il sistema sia stabile e sicuro. Anche se le aziende comprendono che è importante applicare le patch ai sistemi operativi e alle applicazioni, spesso non aggiornano il firmware che permette all'hardware di funzionare. Dunque, i dispositivi rimangono vulnerabili ai cyber attacchi e possono causare enormi problemi, dalla perdita di dati preziosi dei clienti a sanzioni pesanti da parte degli organi normativi per non conformità.

Dettagli >

Gestione più semplice del ciclo di vita

Un programma strutturato di gestione del ciclo di vita aiuta le aziende a prepararsi adeguatamente per il futuro. Utilizza le tecnologie più appropriate e avanzate per ridurre al minimo i rischi per la sicurezza e le vulnerabilità. Un software di gestione dei dispositivi come AXIS Device Manager può aiutare le aziende ad automatizzare queste operazioni e gestire con efficienza le risorse.

Come funziona?

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. Può eseguire una scansione dell'intera rete e acquisire tutte le informazioni più importanti, come numero di modello, indirizzi IP e MAC, versione del firmware e stato dei certificati.

Il quadro completo

Con un quadro dettagliato di tutto l'ecosistema di rete, è più facile implementare 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.

Risparmiare tempo ed energie

Il software di gestione dei dispositivi aiuta le aziende a risparmiare molto tempo ed evitare lo stress nella gestione dei rischi per la cybersecurity. Questo software può essere utilizzato per la manutenzione del sistema e consente di:

- Distribuire modifiche di sistema, aggiornamenti firmware e nuovi certificati a tutti i dispositivi simultaneamente.
- 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 firmware più recente e sicura.
- Gestire i privilegi degli utenti nell'intera rete e configurare le modifiche.

Dettagli >

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 sono aggiornati con le patch, i firmware e i certificati più recenti. Oppure, sapere se un dispositivo è destinato alla rimozione qualora il produttore non lo supporti più. Queste utili informazioni possono aiutarvi a capire se il malware possa eventualmente infettare i vostri dispositivi. Accedendo a tutte le informazioni necessarie, potete risolvere altri problemi legati alle vulnerabilità prima che compromettano la vostra rete.

Sicurezza proattiva dell'ecosistema

Automatizzare i processi di gestione dei dispositivi aiuta a proteggere la rete da minacce e vulnerabilità. Le aziende, però, devono anche seguire procedure e regole di cybersecurity importanti. La vostra, ad esempio, applica regole per la sicurezza delle password? Con che frequenza devono essere cambiate? È meglio disattivare i servizi non utilizzati per ridurre l'area esposta a eventuali attacchi? Con quale frequenza viene eseguita una scansione delle vulnerabilità dei dispositivi? Applicate procedure per valutare i livelli di rischio quando un produttore rende nota una violazione? Queste sono alcune domande che aiutano a identificare e implementare misure per proteggere proattivamente l'ecosistema della vostra rete.

5 vantaggi della gestione automatizzata del ciclo di vita

1. Potete dedicarvi esclusivamente alle tecnologie critiche del vostro ambiente
2. Sapete in anticipo quando le tecnologie arriveranno a fine vita
3. Non dovete sostituire improvvisamente un componente importante del sistema
4. Potete programmare adeguatamente la sostituzione dei dispositivi
5. Potete mettere in preventivo un numero prevedibile di dispositivi ogni anno

Che cosa sono le reti zero trust?

Le reti sono sempre più vulnerabili. Sono minacciate da attacchi sempre più numerosi e sofisticati e dall'aumento esponenziale dei dispositivi connessi, ognuno dei quali è a sua volta un punto esposto ad attacchi. Per questo è emerso il concetto di "zero trust", con reti ed architetture zero trust. Per i produttori di hardware, Axis compresa, è fondamentale prepararsi a un futuro zero trust, che arriverà prima di quanto pensiamo.

Non fidarsi di niente e nessuno

Come suggerisce il nome, in una rete zero trust il presupposto è che non ci si può fidare di nessuna entità connessa alla/in rete, che si tratti di una persona o una macchina e a prescindere da dove si trovi o da come sia connessa. In realtà, 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 l'accesso minimo necessario per svolgere il loro compito.

In una rete zero trust, il presupposto è che non ci si può fidare di nessuna entità connessa alla/in rete.

Dettagli >

3 motivi per cui il firewall non basta più

Storicamente, le aziende volevano che il loro firewall fosse il più impenetrabile possibile, ma questo approccio diventa sempre più problematico per vari motivi.

1 I potenziali danni sono ingenti

Anche se un firewall sembra garantire un accesso sicuro in rete, se qualcuno riesce a violarlo può muoversi piuttosto liberamente.

2 Il firewall non basta più

Dato l'elevato numero di dispositivi connessi, proteggere il perimetro della rete con un'unica soluzione non è più fattibile.

3 Il vantaggio delle reti più "permeabili"

L'uso di servizi basati su cloud che si trovano oltre la rete e i vantaggi dei sistemi di clienti e fornitori connessi senza soluzione di continuità hanno cambiato il volto della sicurezza di rete.

> **"Una volta all'interno della rete, una perdita di dati che può causare danni irreparabili è un rischio concreto, mentre i malintenzionati possono rimanere attivi per settimane o mesi prima di essere scoperti (o non essere scoperti affatto).**
>
> Wayne Dorris, Regional Architecture & Engineering Manager, Axis Communications

Dettagli >

Zero trust: come funziona

La filosofia zero trust prevede tecniche come la sicurezza perimetrale granulare e la microsegmentazione della rete. La prima si basa su utenti e dispositivi. Utilizza la loro posizione fisica e altri dati identificativi per determinare se le loro credenziali di accesso alla rete siano affidabili. La seconda prevede l'applicazione di vari livelli di sicurezza a specifiche parti della rete in cui risiedono i dati più critici.

Un ulteriore livello di sicurezza

Consentire alle persone di accedere solo alle parti della rete e ai dati necessari per svolgere il loro lavoro offre vantaggi evidenti in termini di sicurezza. Ma segnalare le anomalie di comportamento associate a queste identità aggiunge un ulteriore livello di protezione. Ad esempio, un amministratore potrebbe avere ampio accesso alla rete per la manutenzione dei server di ricerca e sviluppo o di quelli finanziari.

Semaforo rosso

Se le credenziali dello stesso amministratore fossero utilizzate per scaricare file o dati critici nel cuore della notte e inviarli all'esterno della rete, scatterebbe subito il semaforo rosso. In una rete zero trust, è possibile utilizzare ulteriori autenticazioni, oppure segnalare l'attività anomala in tempo reale e portarla all'attenzione del centro operativo di sicurezza per un'indagine.

Le anomalie di comportamento possono far pensare che le credenziali di sicurezza siano state trafugate, che un dipendente sia insoddisfatto o che qualcuno cerchi di accedere per spionaggio aziendale.

Dettagli >

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 diversi fattori.

Accettazione o rifiuto di ogni richiesta

In parole semplici, il policy engine confronta ogni richiesta di accesso alla rete e il suo contenuto 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

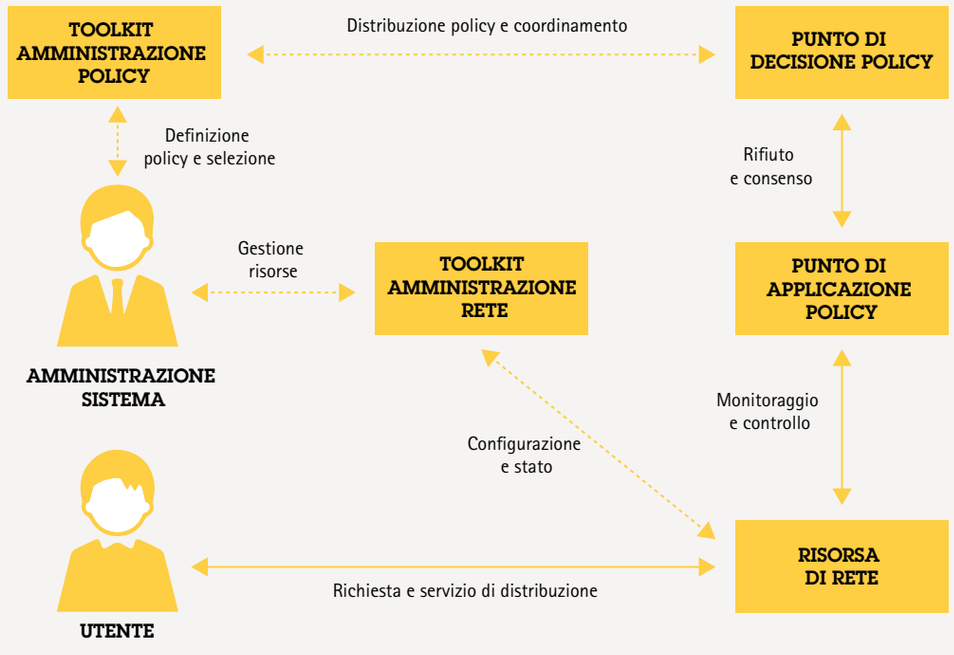
Affinché un policy engine funzioni, le aziende devono definire attentamente regole e criteri all'interno dei principali controlli di sicurezza, come firewall di nuova generazione (NGFW), gateway di sicurezza per e-mail e cloud e software di prevenzione delle perdite di dati (DLP). Questi controlli si 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: descrizione generale



Policy engine: presente e futuro

Attualmente, 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 multi-fattore, 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.

Dettagli >

Reti zero trust e videosorveglianza

Tra le entità che si connettono a una rete ci sono ovviamente le persone; oggi, però, il maggior numero di connessioni di rete è legato ai dispositivi. Tra questi vi sono le telecamere di sorveglianza e i dispositivi di rete associati. Poiché le aziende si spostano verso architetture di rete zero trust, sarà essenziale che i dispositivi di rete rispettino il principio "fidarsi mai, verificare sempre".

Ironia della sorte

Ironia della sorte, una telecamera di sorveglianza pensata per proteggere fisicamente l'azienda potrebbe causare vulnerabilità informatiche. Anche in questo caso, i metodi tradizionali di protezione dei dispositivi non sono più sufficienti. Così come i malintenzionati possono rubare le credenziali di un dipendente, possono compromettere il certificato di sicurezza dei dispositivi. In una rete zero trust, occorrono nuovi approcci affinché i dispositivi possano dimostrare la loro attendibilità in rete.

Una soluzione sorprendente

Una tecnologia in grado di fornire una prova immutabile di attendibilità dei dispositivi connessi è la blockchain. Per molti, la blockchain è associata alle criptovalute, dunque ha una cattiva reputazione. Di per sé, tuttavia, la blockchain è un registro distribuito (Distributed Ledger) e aperto che può registrare transazioni tra due parti in modo efficiente, verificabile e permanente. Le aziende possono adottare blockchain private da utilizzare per le radici di attendibilità dell'hardware e definire chiavi di attendibilità immutabili tra i dispositivi.

Le previsioni indicano che si utilizzeranno più di

75 miliardi

di dispositivi IoT entro il 2025

Perché la tecnologia blockchain funziona

Per come è strutturata la blockchain, nessuna transazione dati della catena può essere scambiata senza l'autorizzazione dei nodi di consenso di tutte le transazioni precedenti, che sono collegati crittograficamente. Dunque, integrando le chiavi di attendibilità delle parti identificabili di un dispositivo nella blockchain, si creano credenziali immutabili per il dispositivo stesso.

Intelligenza artificiale: una sfida nel cyberspazio

Dopo ogni progresso tecnologico, sicuramente i malintenzionati ne valuteranno le capacità di supportare i loro obiettivi criminali. Quando i cybercriminali preparano attacchi ransomware o il furto di informazioni finanziarie – o quando gli stati-nazione cercano di fermare le infrastrutture critiche degli avversari (se non peggio) – le nuove tecnologie possono essere un'arma in più a loro disposizione.

Queste organizzazioni sono finanziate proprio come le normali aziende. Possono innovarsi con le nuove tecnologie, come l'intelligenza artificiale (AI), il machine learning (ML) e il deep learning (DL). La differenza è che non sono ostacolate da norme nazionali o internazionali, né da leggi e questioni morali o etiche.

Semplicemente, cercano le opportunità offerte da queste tecnologie per raggiungere i loro scopi criminosi.

Le nuove tecnologie – compresa l'intelligenza artificiale – arriveranno sempre nelle mani dei criminali. **Per fortuna, possono anche essere utilizzate come difesa dalle aziende.**

Dettagli >

Nascosto in piena vista

Sempre più spesso, gli intrusi in rete utilizzano l'intelligenza artificiale per rendere più sofisticati i loro attacchi. Gli attacchi Distributed Denial of Service (DDoS) su larga scala fanno notizia perché mettono fuori uso siti web e servizi online di alto profilo. Com'è possibile?

Per la maggior parte dei cybercriminali, il principale obiettivo è passare inosservati il più a lungo possibile. In sostanza, si comportano come i ladri d'appartamento. Muovendosi da una stanza all'altra e stando attenti alle telecamere e agli allarmi, cercano gli oggetti di valore, poi se ne vanno con la stessa furtività con cui sono entrati. Allo stesso modo, i cybercriminali cercano di entrare, muoversi e uscire da una rete senza essere individuati.

1

Un modo per riuscirci è sembrare il più possibile un utente legittimo della rete, che può essere una persona o un dispositivo. È proprio qui che l'intelligenza artificiale e il machine learning diventano armi nuove e molto utili ai loro scopi. I cybercriminali possono infatti imparare il comportamento in rete di persone e dispositivi, sviluppare rapidamente nuovi malware o strategie di phishing e utilizzarli su larga scala.

2

Ma il modo più semplice di accedere a qualsiasi rete consiste ancora nell'indurre un utente legittimo a fare clic su un link, aprendo la porta agli intrusi. Un'e-mail falsa del capo – quasi indistinguibile per tono e stile da una vera – è spesso la chiave più efficace.

L'intelligenza artificiale (AI) è una serie di algoritmi che consente a un computer di memorizzare e analizzare l'esito di un'operazione. L'operazione viene quindi adattata alla prossima richiesta simile. Con centinaia e migliaia di richieste che si assomigliano, le sue risposte e azioni verranno ottimizzate gradualmente.

Dettagli >

Tutte le strade portano a Roma

I cybercriminali utilizzano numerosi strumenti di intelligenza artificiale per tutto il ciclo di attacco: dai "chatbot", che coinvolgono i dipendenti tramite profili sociali media falsi, alle reti neurali, che identificano i dati più utili per l'estrazione.

Una volta guadagnato l'accesso, un tecnica del genere è il movimento laterale in rete. È fondamentale, perché raramente il punto di accesso alla rete (che può essere un dispositivo non protetto in una posizione remota) è il punto di arrivo desiderato.

Pian piano, l'intruso si sposta verso aree più sensibili della rete, raccogliendo le credenziali degli utenti lungo il tragitto. Particolarmente interessanti per lui sono quelle di utenti con privilegi come gli amministratori di rete, che rappresenteranno una sorta di passepartout.

Dettagli >

Il pericoloso legame tra IT e OT

Con l'esplosione mondiale dei dispositivi connessi e della cosiddetta Internet of Things (IoT), i rischi aumentano velocemente perché la rete IT (Information Technology) è sempre più integrata con l'ambiente OT (Operational Technology).

In sostanza, la rete IT gestisce il flusso di informazioni digitali. Per contro, la OT gestisce il funzionamento dei processi fisici, dei macchinari e delle risorse fisiche di un'azienda o una sede specifica. Per chi ha l'obiettivo di fermare le operazioni o danneggiare i sistemi, più che rubare, accedere alla OT è fondamentale. Non è difficile immaginare i danni potenziali in caso di accesso ai sistemi di una centrale elettrica, una raffineria di petrolio o un ospedale.

Dettagli >

Che entrino i detective

Se pensiamo che i cybercriminali hanno la possibilità di utilizzare l'intelligenza artificiale, il quadro è agghiacciante. Tuttavia, le stesse tecnologie sono a disposizione di chi cerca di proteggere le reti dalle intrusioni. Sotto molti aspetti, chi deve difendersi è più avvantaggiato di chi attacca.

Sotto molti aspetti, chi deve difendersi è più avvantaggiato di chi attacca.

DARKTRACE

Darktrace è considerata una delle aziende più importanti del mondo che si dedicano all'intelligenza artificiale nella cybersecurity. Naturalmente, sa bene che l'IA è sempre più utilizzata dalla criminalità organizzata. Dunque, innova costantemente l'intelligenza artificiale e il machine learning per restare un passo avanti ai criminali.

Dettagli >

L'intelligenza artificiale è uno strumento di difesa, oltre che di attacco

Intervista a Jeff Cornelius, Darktrace

Nelle prossime pagine intervistiamo Jeff Cornelius, vicepresidente esecutivo di Darktrace, per sapere come l'azienda utilizza l'intelligenza artificiale e il machine learning per rimanere un passo avanti ai cybercriminali.

D **Quanto dobbiamo preoccuparci?**

"Innanzitutto, e nonostante l'impressione che possono dare i media, sviluppare l'intelligenza artificiale e il machine learning non è facile! Anche se le organizzazioni criminali e gli stati-nazione che cercano di perpetrare gli attacchi sono potenti, ci sono diversi punti a nostro favore".

"Il principale è che – grazie all'accesso fornito dai nostri clienti – riusciamo a vedere tutte le attività in rete. In questo modo, possiamo capire il comportamento di ogni dispositivo e utente. Per contro, i malintenzionati avranno sempre e solo una visuale limitata delle attività. Tutte le azioni successive al primo passo sono come movimenti alla cieca in un ambiente che noi conosciamo e loro no".

"In definitiva, i loro obiettivi comprendono attività di cui l'azienda non si occupa normalmente. Il nostro principale obiettivo è identificare e risolvere queste anomalie di comportamento in rete. Il nostro raggio d'azione deve essere ampio perché non sappiamo quando o dove può comparire un avversario, né quali possono essere i nuovi metodi o gli obiettivi specifici".

Dettagli >

Un'analogia intrigante

Intervista a Jeff Cornelius, Darktrace

D

Potrebbe chiarire?

"Per fare un'analogia, se qualcuno studiasse i miei movimenti appostandosi fuori da casa mia, riuscirebbe a farsi un quadro piuttosto dettagliato delle mie abitudini: a che ora esco di casa, che strada faccio per andare a lavorare, dove vado a pranzare e così via. Probabilmente riuscirebbe a imitare abbastanza bene alcune parti della mia vita".

"Ma se non vedesse quel che accade in casa e cercasse di imitare le mie abitudini a colazione, quasi sicuramente commetterebbe un errore, che un mio familiare individuerebbe facilmente come un'anomalia. In genere, su Internet si trovano molte informazioni su come prendere di mira qualcuno con un'astuta e-mail contenente phishing; una volta entrati, però, bisognerà sedersi a tavola con noi".

Dettagli >

Machine learning supervisionato...

Intervista a Jeff Cornelius, Darktrace

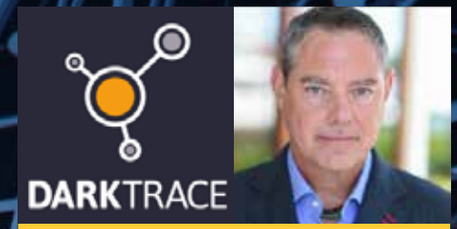
D **Ci parli del machine learning.**

"Esiste una distinzione importante tra machine learning supervisionato e non supervisionato. Il primo prevede l'addestramento dei computer con un set di dati conosciuto. Il sistema fa costantemente riferimento a questi dati per valutare se l'esito registrato sia quello previsto".

"Dal punto di vista della cybersecurity, i modelli di apprendimento si basano sul malware noto. Ed è questa la vera gara tra i criminali e la cybersecurity: i primi utilizzano il machine learning per creare nuove versioni del malware. In questo senso stiamo assistendo ad una crescita esponenziale. Le aziende che si occupano di cybersecurity cercano di stare al passo scrivendo nuovi modelli di difesa tramite il machine learning supervisionato. È un po' come il correttore ortografico, che giorno dopo giorno cerca di aggiornarsi con tutte le nuove parole o lingue che nascono. Restare al passo diventa sempre più difficile, se non impossibile".

Dettagli >

...e machine learning non supervisionato



Intervista a Jeff Cornelius, Darktrace

D

Ma esistono altri metodi?

"Sì. Anziché riferirsi alle minacce passate, gli algoritmi di machine learning non supervisionato classificano in modo indipendente i dati e individuano modelli interessanti. Analizzano i dati di rete su vasta scala ed eseguono miliardi di calcoli di probabilità basandosi solo sulle evidenze. A questo punto, iniziano a definire i comportamenti "normali" nella specifica rete da parte di dispositivi, utenti o gruppi di essi. Ogni deviazione da questo "stile di vita" suggerisce l'evoluzione di una minaccia. Questo sistema di preavviso ci consente di rimanere un passo avanti ai cybercriminali e ai malintenzionati".

Unire le forze per ridurre i rischi

Proteggere aziende, organizzazioni, infrastrutture critiche e città non è un lavoro per una sola persona. Non esiste una bacchetta magica, né una soluzione universale. Piuttosto, mantenere livelli accettabili di cybersecurity deve essere uno sforzo collaborativo tra una lunga lista di stakeholder, compresi gli utenti finali.

Cybersecurity: una questione di mentalità

Anche in questo caso si tratta sostanzialmente di unire le forze. Ogni persona all'interno di un'organizzazione deve essere considerata un membro del team di cybersecurity. È dunque opportuno:

- Investire sulla formazione dei dipendenti in ambito di cybersecurity
- Istruire i nuovi assunti
- Incoraggiare gli alti dirigenti a far rispettare le regole di cybersecurity
- Documentarsi costantemente sui nuovi pericoli per la cybersecurity e comunicarli
- Considerare la cybersecurity un requisito essenziale quando si scelgono i nuovi dispositivi di rete
- Implementare una politica Bring-Your-Own-Device (BYOD)
- Creare e applicare una strategia di risposta agli incidenti di cybersecurity

Coinvolgendo tutta l'azienda nei progetti di cybersecurity, sarete in una posizione nettamente migliore per garantire la sicurezza della rete e dei dispositivi.

Dettagli >

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 gli utenti finali:

Integratori e installatori

Devono verificare che tutti i dispositivi installati siano protetti con gli ultimi aggiornamenti e dispongano di un antivirus sofisticato. Un altro sforzo in comune con tutti gli stakeholder deve essere una strategia solida per le password, la gestione degli accessi remoti e la manutenzione dei software e dei dispositivi connessi nel tempo.

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

Aiutano a specificare i sistemi e devono anche specificarne la corretta manutenzione per tutto il ciclo di vita, oltre che essere trasparenti sui potenziali costi. 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.

Produttori di dispositivi

La cybersecurity inizia da qui. I produttori devono applicare le prassi ottimali di cybersecurity nella progettazione, nello sviluppo e nel collaudo per ridurre al minimo il rischio di vulnerabilità. Sono altrettanto importanti le funzionalità di sicurezza integrate, i chip sviluppati in-house e un attento controllo della catena di fornitura. Infine, è opportuno fornire strumenti per una gestione dei dispositivi a basso costo e automatizzata e informare i canali di distribuzione e i partner sulle vulnerabilità note.

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.

Utenti finali

Così come ogni azienda ha necessità specifiche e uniche 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 sicure da archiviare e cambiare regolarmente, assegnare permessi differenziati e installare sempre le patch e gli aggiornamenti più recenti sono solo alcuni esempi di misure da intraprendere.

Dettagli >

Partner per la protezione

Solo collaborando possiamo prepararci ad affrontare meglio minacce per la cybersecurity che si evolvono di continuo e reagire velocemente. Ogni stakeholder ha il proprio ruolo nell'implementare soluzioni sicure sotto tutti gli aspetti: dalla produzione dei dispositivi, alla progettazione, all'installazione dei sistemi, fino alla manutenzione e alla gestione delle varie soluzioni. È così che si rimane vigili.

Cybersecurity in modalità edge

Il mondo dell'edge

Nel 2021 si osserva una tendenza sempre maggiore verso l'edge computing, ovvero l'elaborazione dei dati ai "margini" della rete. Il fatto che miliardi di dispositivi **IoT** siano già connessi in rete e che il loro numero stia **aumentando rapidamente** non è di per sé una novità. Ma la natura e le esigenze di questi dispositivi hanno implicazioni serie per la cybersecurity.

IoT

IoT (Internet of Things) indica una rete di dispositivi connessi a Internet e in grado di "comunicare" tra loro. Rientrano in questa categoria gli smartphone, gli accessori indossabili, i dispositivi per la smart home come i contatori e le smart machine industriali. I dispositivi IoT utilizzano sensori e processori per raccogliere e analizzare dati acquisiti nel loro ambiente, creando azioni conseguenti.

Rapido aumento

Entro il 2025, si prevedono oltre 75 miliardi di dispositivi Internet of Things (IoT) in uso. Il loro numero triplicherà rispetto al 2019.

Dettagli >

Il mondo dell'edge

> Vi è la crescente tendenza a elaborare i dati e le analitiche direttamente sulle telecamere.

Molti dispositivi connessi alla rete richiedono o almeno beneficerebbero della capacità di rilevare istantaneamente quanto accade, decidere e agire di conseguenza.

Un esempio lampante: i veicoli a guida autonoma

Sia nelle comunicazioni con l'ambiente esterno (ad esempio con i segnali stradali) che sui sensori che rilevano i rischi (ad esempio un oggetto che spunta improvvisamente davanti all'auto), le decisioni devono essere elaborate in una frazione di secondo. Tramite la rete, l'auto invia i dati a un datacenter, che li elabora, li analizza e li restituisce. Il veicolo decide così come comportarsi: l'insieme di tutte queste operazioni ha però una latenza inaccettabile.

Similitudini con la videosorveglianza

Per essere proattivi anziché reattivi – prevenendo gli incidenti e non reagendo semplicemente ai fatti – un numero sempre maggiore di operazioni di calcolo e analisi deve svolgersi direttamente sulla telecamera. Ma con l'aumento dei dispositivi che funzionano in modalità edge, e il ruolo sempre più critico di questi dispositivi per la sicurezza, vi sono numerose conseguenze che esamineremo nelle prossime pagine.

Dettagli >

Dispositivi proprietari dedicati

Avere software e hardware dedicati e ottimizzati – ovvero progettati per la specifica applicazione – è fondamentale con questa crescente tendenza verso l'edge computing. I dispositivi connessi dovranno avere maggiori capacità di calcolo ed essere prodotti tenendo a mente la cybersecurity fin dai componenti essenziali.

È qui che diventano importanti i chip proprietari integrati. Ad esempio, i dispositivi Axis utilizzano un "system-on-a-chip" brevettato che li protegge dai cyber attacchi, dovuti ad esempio a un firmware non autorizzato che crea un backdoor. Nella sua ultima versione, il processore ARTPEC-7 è progettato specificamente per la videosorveglianza di oggi e di domani, dando sempre la massima priorità alla sicurezza.

Progettato specificamente per la videosorveglianza, l'ultimo chip Axis ARTPEC-7 ha prestazioni oltre 50 volte superiori all'originale. Controllando la progettazione e la produzione dei chip, Axis può creare prodotti ottimizzati al meglio per le esigenze dei clienti, affrontando anche fattori esterni che si evolvono come i pericoli per la cybersecurity.

> **"ARTPEC-7 ci consente di dare alle telecamere una qualità d'immagine estremamente alta, ma anche ottime prestazioni, una buona efficienza nel consumo di banda e la capacità di eseguire le analitiche in modalità edge.**
>
> Stefan Lundberg, Expert Engineer, Axis Communications

Dettagli >

Dispositivi edge e fiducia

La fiducia si presenta sotto varie forme:

- **Fiducia che le aziende raccolgano e utilizzino i dati in modo responsabile**
- **Fiducia che dispositivi e i dati siano protetti dai cybercriminali**
- **Fiducia che i dati siano precisi e che la tecnologia funzioni come previsto**

I dispositivi edge saranno il punto in cui questa fiducia si consoliderà o verrà a mancare.

La fiducia in tutta la catena di fornitura sarà fondamentale. Mentre integrare chip-spia nell'hardware è una possibilità piuttosto remota, è relativamente semplice installare un "backdoor" su un dispositivo tramite un aggiornamento firmware successivo a quello di produzione.

Dettagli >

Dispositivi edge e fiducia

In tutto il mondo si continuerà a parlare di privacy personale. Anche se è possibile utilizzare tecnologie come l'anonimizzazione e il masking dinamico in modalità edge per tutelare la privacy, gli atteggiamenti e le normative non sono coerenti tra regioni e Paesi. Nel quadro normativo internazionale, le aziende che operano nella sorveglianza devono navigare a vista.

La cybersecurity è più importante che mai

Con il maggior numero di processi e analisi dei dati che si svolgono sul dispositivo, la cybersecurity diventerà ancora più importante. Nonostante i numerosi e sofisticati cyber attacchi, molte aziende non riescono ancora a implementare gli aggiornamenti firmware, neanche i più semplici. Per proteggere un sistema, è fondamentale gestire i singoli dispositivi e l'intero ciclo di vita della soluzione di sorveglianza con regole chiare sull'hardware, il software e gli utenti.

I rischi della non-compliance

Negli ultimi anni, aziende come British Airways e Marriott International sono state multate pesantemente perché non hanno rispettato le normative. Il rischio di penali ha sconvolto il mondo del business e condiziona il modo in cui le aziende spendono il budget per la cybersecurity.

Le aziende rischiano anche attacchi mirati come ransomware, malware e phishing. Questi possono causare l'interruzione dei sistemi, perdite di dati, disagi operativi, pubblicità negativa, perdita di clienti e di profitti.

Che cos'è la compliance?

Spesso si pensa che il termine compliance si riferisca alla conformità alle norme di governo e agli standard internazionali. Tuttavia, è vero solo in parte. Le aziende devono anche implementare e seguire controlli interni e prassi ottimali, garantendo che anche i partner con cui trattano siano conformi.

Oggi, le aziende hanno la responsabilità di garantire che i dati dei clienti siano protetti adeguatamente.

Le aree da considerare sono tre:

1. **Compliance normativa**
   Normative istituzionali come il GDPR e standard o framework internazionali come ISO o NIST
2. **Compliance interna**
   Policy aziendali interne e best practice
3. **Compliance esterna**
   Compliance all'interno della catena di fornitura

Dettagli >

L'obbligo di rispettare la legge

Le leggi come il Regolamento generale sulla protezione dei dati (GDPR) dell'Unione Europea sono concepite per regolamentare l'uso dei dati personali dei consumatori da parte di organizzazioni, aziende e governi. Per quanto riguarda la cybersecurity, queste leggi toccano molto da vicino le soluzioni di sicurezza utilizzate dalle aziende.

Anche se il GDPR è una legge che vale per l'Europa, ha ripercussioni sulle aziende di tutto il mondo. Ad esempio, le società statunitensi che archiviano dati in Europa devono rispettare il GDPR. Allo stesso modo, se un'azienda ha un contratto con terze parti che trattano dati, queste devono rispettare il GDPR. Negli Stati Uniti, i 50 stati hanno norme diverse per la tutela dei dati: questo complica e allunga i tempi di gestione dei lavori interstatali.

La governance interna costa di più

Gli hacker non badano alle norme: guardano un'azienda determinandone le specifiche vulnerabilità e i punti di esposizione. Le aziende possono anche spendere tutto il budget a disposizione per la cybersecurity. Tuttavia, l'obiettivo deve essere una protezione sufficiente che non impedisca l'innovazione. È un'opera di bilanciamento e dipende dalla propensione di un'azienda al rischio. Alcune aziende implementano controlli ancora più rigorosi di quelli imposti per legge, perché in caso di violazioni ai sistemi informatici devono dimostrare che hanno adottato le giuste cautele.

Compliance nella catena di fornitura

Le aziende con catene di fornitura complesse hanno anche altri requisiti ai fini della compliance. Ad esempio, le aziende con sede in Europa che lavorano con il governo degli Stati Uniti devono rispettare standard come la Cybersecurity Maturity Model Certification, che richiede una certificazione sulla gestione interna delle procedure di cybersecurity. Nella peggiore delle ipotesi, anche le terze parti (come i fornitori) possono essere responsabili di non-compliance e incorrere in una parte delle sanzioni.

Benché gli obblighi esterni siano importanti, si consiglia che le policy interne delle aziende siano ancora più rigide. Questo perché è responsabilità dell'azienda garantire la conformità e la protezione dei dati contro qualsiasi violazione.

Dettagli >

Quali normative seguire?

Restare aggiornati sulla compliance richiede un lavoro costante. Le norme sulla cybersecurity e sulla gestione dei dati che valgono per la vostra azienda dipendono in genere dal vostro settore. Tuttavia, diverse normative possono interessare più settori e Paesi.

Le aziende devono sempre essere al corrente delle linee guida e delle modifiche imminenti che possono riguardare alcune leggi. Esaminando le minacce e gli attacchi più recenti e comprendendo le nuove leggi e norme sulla compliance, le aziende possono determinare le modifiche da apportare per garantire il superamento dei nuovi controlli di conformità.

Audit di sicurezza informatica

Dopo aver identificato le normative che l'azienda deve rispettare, è necessario valutare la compliance a livello generale. Con un audit interno di sicurezza informatica, è possibile valutare i processi di governance adottati dall'azienda in questo campo. In generale, le aziende devono condurre un audit di sicurezza informatica a cadenza annuale. Tuttavia, si consiglia di monitorare costantemente tutti i controlli per rimediare tempestivamente a eventuali lacune. Alle aziende si consiglia anche di documentare regolarmente questa valutazione continua dei controlli di sicurezza, che potrà essere utilizzata per i futuri audit.

Alcuni elementi da considerare durante un audit di sicurezza informatica:

- **Gestione dei rischi:** quale procedura adotta la vostra azienda per identificare e gestire i rischi associati alla compliance normativa? Ad esempio, come vengono comunicati i rischi e quali processi sono in uso per garantire che siano sempre valutati?
- **Processo di audit interno:** le aziende devono definire un processo di audit interno per monitorare costantemente la compliance. Ad esempio, quali processi applicate per identificare, valutare e controllare le variazioni alle prassi di cybersecurity?
- **Formazione su sicurezza e privacy:** i dipendenti hanno la preparazione necessaria per identificare lacune nella sicurezza IT? Ad esempio, avete un programma di formazione contro il phishing via e-mail? Un programma di formazione però, non basta: saranno i controlli interni a determinarne l'efficacia. Se un'area è ad alto rischio per un'azienda, questa dovrà effettuare i controlli ogni tre mesi anziché una volta all'anno.

Dettagli >

Monitoraggio della compliance

È possibile utilizzare i risultati di un audit interno per preparare un piano di monitoraggio della compliance. Il piano può essere utilizzato per valutare in modo continuativo gli sforzi complessivi di un'azienda ai fini della compliance e affrontare tutti i rischi identificati dall'audit. I rischi più pericolosi per la vostra azienda devono avere la priorità. Valutando i controlli di compliance previsti dalla vostra azienda, potete identificare le lacune normative dei vostri controlli di cybersecurity.

Nel determinare chi abbia la responsabilità di monitorare i rischi per la cybersecurity, i ruoli devono essere assegnati in base alle competenze richieste. È possibile ottimizzare l'assegnazione dei ruoli chiedendovi quali dipendenti abbiano le competenze necessarie e quali attività di monitoraggio dei rischi possano essere combinate.

Siete aggiornati?

I produttori rilasciano regolarmente gli aggiornamenti firmware ogni volta che emergono vulnerabilità e vengono adottate nuove leggi. Tuttavia, è altrettanto importante avere una visuale chiara di tutti i dispositivi e del loro ciclo di vita, per essere pronti quando un prodotto non sarà più supportato. Gli strumenti di gestione dei dispositivi come AXIS Device Manager aiutano a garantire che i prodotti siano aggiornati e conformi. Questi strumenti inviano notifiche sul rinnovo delle licenze, sulle tempistiche di manutenzione o sulle certificazioni per aiutare le aziende a rispettare i requisiti di conformità e ad essere sempre aggiornate. Inoltre, questi strumenti possono fornire la documentazione necessaria per gli audit, se prevista.

Dimostrare la compliance

Spesso, i clienti inviano ai produttori di dispositivi questionari sul loro livello di sicurezza informatica. Le aziende devono rispondere a domande sui piani di continuità, su come implementano le certificazioni e su come proteggono i dati in rete. Condividendo prontamente tutte queste informazioni, possono tranquillizzare i clienti e dimostrare che hanno preso tutti gli accorgimenti necessari.

Dal 2008, le banche statunitensi hanno ricevuto sanzioni per **243 miliardi** di dollari

Dal 2008, le spese di gestione legate alla compliance sono aumentate del **60%**

Il costo del regulatory risk ammonta a **10.000 dollari** per dipendente

> **“ La non conformità costa molto. Se pensate che la compliance sia costosa, provate la non-compliance.**
>
> **Paul McNulty, ex viceprocuratore generale degli Stati Uniti https://youattest.com/**

Dettagli >

Documentare, documentare e documentare

La documentazione è fondamentale per poter dimostrare il rispetto delle normative. Le vostre policy interne possono prevedere domande come:

- Perché e che cosa registrate?
- Esponete cartelli al pubblico per informarlo che è registrato?
- Il sistema di sorveglianza rende riconoscibili le persone? Se sì, occorre valutare e documentare le conseguenze per la privacy. Chi ha accesso alle riprese?
- Come vengono archiviati i dati? Per quanto tempo? I dati archiviati sono protetti fisicamente e informaticamente? Come garantite che le registrazioni precedenti vengano eliminate?

Occorre anche includere la documentazione su alcuni scenari specifici. Ad esempio, in caso di intrusioni, come deve essere gestita la situazione? Chi ha la responsabilità di controllare i dati e quali procedure sono previste? Inoltre, si consiglia di segnalare ai comitati di regolamentazione qualsiasi problema identificato durante gli audit interni e gli sforzi compiuti dall'azienda per colmare eventuali lacune.

La compliance è un bersaglio che si muove

Le leggi e le norme si evolvono costantemente; dunque, è importante comprendere che anche i piani di monitoraggio della compliance più rigorosi non mettono totalmente al riparo dalle sanzioni. Le aziende devono monitorare costantemente e poter dimostrare con sicurezza la loro conformità.

È ora di agire

Senza dubbio, la compliance è una componente importante della cybersecurity e porta con sé criticità che non sono destinate a sparire. Le aziende e i consumatori aprono gli occhi e osservano i rischi, comprendendo che i sistemi e i dati sono vulnerabili agli attacchi se non si interviene rapidamente. Mentre le aziende vogliono perseguire l'innovazione e la crescita in sicurezza, devono anche contenere al massimo i pericoli del cyber crimine. D'altro canto, i consumatori vogliono che i loro dati siano custoditi al sicuro e si aspettano che le aziende si comportino di conseguenza. Le norme governative possono essere rispettate solo con un approccio collaborativo in cui rivenditori, produttori e utenti finali si assumono le loro responsabilità per una cybersecurity efficace. In questo modo, si riduce al minimo il rischio di violazioni dannose.

Senza dubbio, la compliance è una componente importante della cybersecurity e porta con sé criticità che non sono destinate a sparire.

Cosa dovete sapere sul vostro fornitore di sistemi di sorveglianza e sui suoi rispettivi fornitori?

I pericoli per la sicurezza sono sempre presenti. Sorgono nuove minacce e la loro natura può cambiare nel tempo. Le aziende devono sapere che il loro fornitore di sistemi valuta costantemente e contrasta questi rischi, non solo nelle sue sedi ma anche presso i suoi fornitori.

Per le aziende è prassi comune pensare solo alla cybersecurity dei loro fornitori. 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?

- Progetta e produce dispositivi sicuri con protezione integrata?
- Condivide informazioni e strumenti per adottare tutte le cautele necessarie?
- Risponde velocemente e con aggiornamenti gratuiti se riscontra nuove vulnerabilità?
- Controlla l'intera catena di fornitura, dai componenti al prodotto finito?

"Come fanno i fornitori a controllare la loro catena?"

Dettagli >

Trovare il partner giusto

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 anche i processi di gestione dei rischi dei subfornitori, oltre alle loro infrastrutture e ai processi produttivi. Occorre organizzare visite in stabilimento, seguite da un audit, per valutare se l'azienda soddisfi i requisiti e gli standard per la qualifica dei vendor approvati. Nel valutare un potenziale nuovo partner all'interno della catena logistica, i fornitori devono svolgere analisi approfondite sulla posizione finanziaria dell'azienda e sul suo modello di proprietà.

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. Dunque, la collaborazione e la comunicazione sono intense e quotidiane, con frequenti visite in sede.

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 sono nella lista dei 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?

Dettagli >

Audit del vostro fornitore

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:

- Conformità dei processi, documentazione compresa
- Sicurezza delle infrastrutture
- Trattamento fisico in stabilimento
- Gestione inventario
- Apparecchiature di produzione
- Controllo qualità
- Registri di tracciabilità

Le revisioni aziendali trimestrali sono un altro 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:

- Gli ingressi e le uscite devono essere sorvegliati in modo continuativo; inoltre, i controlli ai varchi di accesso devono essere tracciabili e i registri dei visitatori devono essere archiviati. Alcune aree possono richiedere una sorveglianza continuativa, anche in presenza di vigilanti che proteggono la struttura e le aree circostanti.
- È necessario utilizzare scanner per individuare oggetti o materiali non autorizzati.
- I trasporti devono essere affidati solo a vettori esperti che adottano regole e controlli di sicurezza rigorosi. Gli autisti e i mezzi devono rispettare le normative di sicurezza in fase di ritiro e consegna.
- Tutte le merci trasportate per via aerea devono essere controllate ai raggi X. Una prassi comune è sigillare le spedizioni nel luogo di origine, in modo da prevenire le intrusioni anche senza rilevamento.
- Spesso, le merci in partenza e in arrivo vengono sorvegliate e documentate con le telecamere TVCC.

Dettagli >

Trasferimento dei dati e sicurezza delle informazioni

Il trasferimento dei dati nella rete della catena logistica deve essere protetto da protocolli di sicurezza, utilizzando metodi di crittografia e l'autenticazione. I subfornitori e i partner devono proteggere al massimo le informazioni per ridurre i rischi di eventuali lacune nella catena di fornitura.

Il vostro fornitore deve adottare un approccio sistematico per identificare e gestire le informazioni sensibili dell'azienda. Questo sistema deve includere persone, processi, sistemi IT e sedi fisiche, nonché rispettare la norma ISO 27001 e il Regolamento generale sulla protezione dei dati (GDPR) dell'Unione Europea. In questo modo si ha una maggiore consapevolezza e una gestione efficace dei rischi.

Sicurezza del personale

Conoscere i neoassunti è molto importante, non solo dal punto di vista della formazione, delle competenze e dell'esperienza lavorativa, ma anche da quello della sicurezza. Nei processi di selezione di Axis, ad esempio, la qualità e la sicurezza sono fondamentali. Tra i suoi approcci figurano la verifica dell'identità, la richiesta di referenze e il controllo dei precedenti penali. I nuovi dipendenti e consulenti devono firmare un accordo di riservatezza (NDA) che protegge la proprietà intellettuale e altre informazioni sensibili, sia durante l'impiego che dopo averlo lasciato.

Formare i dipendenti e ridurre i rischi

Axis si preoccupa che i dipendenti siano sempre molto attenti alla sicurezza delle informazioni. Se i dipendenti sono preparati, hanno le informazioni necessarie per sapere sempre cosa fare e quali sono i rischi. I dipendenti Axis rientrano nel nostro impegno per una sicurezza e una fiducia concrete; tutti loro seguono corsi sulla sicurezza delle informazioni e vengono invitati a prestare sempre la massima attenzione. L'accesso a informazioni, sistemi e risorse viene concesso ai dipendenti solo se ne hanno necessità per svolgere i loro compiti. I dipendenti dei fornitori e dei partner di produzione condividono informazioni, sistemi e risorse con Axis seguendo le stesse procedure.

Dettagli >

Integrità dei prodotti

Come tutti i prodotti, anche quelli di sorveglianza devono funzionare secondo il progetto e la destinazione d'uso, restando sempre integri. Questo è possibile solo se l'hardware e il firmware 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 sue apparecchiature di produzione critiche e 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.

Perché Axis?

Soluzioni per un mondo più intelligente e sicuro

Qualità in tutto ciò che facciamo: tutti i nostri prodotti sono testati accuratamente per regalare la massima tranquillità ai clienti.

Tecnologie innovative: le nostre tecnologie si uniscono all'immaginazione per aumentare le performance al pari dell'utilizzabilità. Basate su standard aperti, sono flessibili, scalabili e facili da integrare.

Sostenibilità ad ogni livello: Axis manifesta un impegno costante per uno sviluppo responsabile nei confronti dell'ambiente utilizzando materiali sostenibili. Ad esempio, l'80% delle telecamere e dei codificatori Axis è privo di PVC.

Cybersecurity: monitoriamo costantemente le minacce e le loro conseguenze, prendendo contromisure veloci e risolutive. Anche dopo l'installazione, continuiamo a rafforzare la cybersecurity dei dispositivi con aggiornamenti, nuove versioni e installazioni.

Presenza globale, competenza locale: Axis vanta il maggior numero di prodotti installati e dipendenti al mondo, con una presenza in oltre 50 Paesi. Condividendo idee ed esperienze, è sempre aggiornata sugli ultimi sviluppi.

Il potere delle partnership: grazie al suo impegno verso la partnership, 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 di rete che migliorano la sicurezza e forniscono nuove opportunità di business. In qualità di leader nel settore dei video di rete, Axis offre prodotti e servizi per la videosorveglianza e l'analisi dei video, il controllo degli accessi, intercom e impianti audio. Axis ha oltre 3800 dipendenti in più di 50 paesi e collabora con partner in tutto il mondo per fornire soluzioni ai clienti. Fondata nel 1984, Axis è una società con sede a Lund, in Svezia.

Per ulteriori informazioni su Axis, visitare il sito web www.axis.com