WHITE PAPER

La digitalizzazione e la cybersecurity dei sistemi di controllo degli accessi fisici

Alla scoperta dei sistemi e dei protocolli che permettono alle aziende di sbloccare il potenziale completo di controllo degli accessi e di creare un mondo più intelligente e sicuro

Agosto 2021

AXIS COMMUNICATIONS

Sommario

1 Sommario

Lo sviluppo della connettività via cloud sta cambiando l'aspetto dell'industria della sicurezza fisica e sta forzando gli installatori ad adattarsi per poter continuare a rimanere nel settore. Il controllo dei sistemi di accesso sembra spostarsi in direzione delle grandi aziende tecnologiche, aumentando così le aspettative nei confronti del valore di questi sistemi, poiché diventano ancora più intelligenti, assumono un potenziale di crescita maggiore e si basano sempre più su tecnologia Edge.

Questa evoluzione, oltre al potenziale per l'integrazione con altri sistemi aziendali, significa anche che la cybersecurity deve svolgere un ruolo ancora più importante nello sviluppo e nell'impiego dei sistemi, specialmente in quei casi che si basano su infrastrutture già esistenti. Il superamento di barriere tecniche, ad esempio l'architettura seriale, l'assenza di MAC address e altro, è un passo importante nella transizione verso sistemi di controllo degli accessi digitali che siano in grado di soddisfare i requisiti odierni e futuri.

L'implementazione e la sicurezza di un sistema digitale per il controllo degli accessi significano anche seguire le prassi migliori per garantire la miglior sicurezza possibile. Dobbiamo valutare e testare ogni componente incluso nel sistema, che si tratti di un dispositivo, un fornitore o un protocollo - devono essere tutti affidabili. Dobbiamo inoltre essere consapevoli delle minacce e di come attenuare i pericoli rappresentati da nuove vulnerabilità.

È importante prestare particolare attenzione ai fornitori, perché i loro dispositivi avranno accesso alla rete aziendale. Un fornitore serio deve rendere noti i processi usati per rendere sicuri i propri dispositivi. Può farlo pubblicando una Hardening guide, fornendo strumenti di gestione dedicati che semplificano la gestione e la protezione dei dispositivi di rete, ecc. Inoltre, un fornitore deve essere aperto e onesto in merito alla strategia da seguire per gestire le vulnerabilità scoperte.

2 Introduzione: Il futuro del controllo degli accessi

La connettività al Cloud ha presentato l'industria della sicurezza fisica con una nuova visione di come i sistemi devono essere utilizzati. Gli utenti finali e gli acquirenti chiedono soluzioni più intelligenti, integrate e destinate al business con funzionalità di sorveglianza e controllo degli accessi che vanno ben oltre quelle offerte dalle tecnologie tradizionali.

Molti fornitori hanno creato un forte business model basato su esperienza, servizio e conoscenze del settore di sicurezza fisica. Tuttavia, la connettività di rete e IoT sono in continua evoluzione, ciò richiede ai fornitori e agli installatori di sicurezza fisica di imparare il linguaggio informatico ,le piattaforme aperte, la connettività IP e l'integrazione del software per potersi adattare ai cambiamenti del mercato e per rimanere al passo coi tempi.

Sembra che il controllo stia rapidamente passando dai fornitori di sistemi di accesso elettronici alle aziende di tecnologia globale, che ora hanno il potere di plasmare la sicurezza in una direzione che ne sfida il funzionamento tradizionale. Gli edifici e le smart cities presentano grandi opportunità e molti prevedono una rapida crescita del mercato del controllo degli accessi, poiché la facilità d'uso e la ricercatezza delle tecnologie moderne portano molti benefici all'ambiente smart.

Non sorprende che l'impulso verso l'adozione del controllo degli accessi in hosting avvenga dopo che l'impatto dei giganti della tecnologia ha dimostrato il successo delle tecnologie cloud; così fortemente invocato durante la pandemia globale di COVID-19. Tali aziende hanno la portata, le dimensioni e l'immaginazione per apportare cambiamenti radicali e anche la sicurezza fisica verrà trasformata man mano che le aziende, realizzando il valore del cloud, cerchino soluzioni in hosting per prendersi cura di tutti i loro requisiti di sicurezza e aziendali.

Tuttavia, al momento molti produttori semplicemente non sono pronti per questo mercato in evoluzione e seguono ancora i business model che si basano su rigidi design brevettati. Il passaggio alle soluzioni smart di sicurezza fisica è in netto contrasto con questo approccio tradizionale, che è probabile venga messo in discussione. Mentre il cambiamento non avverrà da un giorno con l'altro, e nuove soluzioni di cloud hosting devono ancora diffondersi, questo nuovo mondo è comunque il dominio dei nuovi tecnici che entrano ora a far parte della nostra industria.

Il futuro del controllo degli accessi, e l'intera sicurezza fisica, pertanto saranno basate su aspettative di maggiore valore. I sistemi di controllo degli accessi diventeranno punti di raccolta dati e i door controller diventeranno dispositivi I/O intelligenti. I codici QR per la gestione dei visitatori e il riconoscimento facciale biometrico per un controllo degli accessi senza intoppi verranno sempre più gestiti come analisi all'interno di una telecamera o sensore. Il futuro del controllo degli accessi si prospetta interessante per coloro che sono pronti ad accettarlo e a plasmarlo; una vera opportunità per innovare, per un mondo più intelligente e sicuro.

In questo documento esploriamo quegli aspetti che sono particolarmente importanti per il controllo degli accessi, comprese molte delle caratteristiche di questi sistemi. Inoltre esamineremo delle considerazioni sulle migliori prassi seguite dai fornitori, con informazioni e suggerimenti per gli utenti finali per dare loro fiducia nel mettere in discussione i fornitori e per prendere decisioni migliori in merito agli acquisti.

3 Le sfide di un mercato del controllo degli accessi in continua evoluzione

Quando ci concentriamo sui sistemi di controllo degli accessi (PACS), tendiamo a pensare ai fattori di rischio in termini di considerazioni riguardo alla concessione o al blocco dell'entrata fisica. Adottare un approccio equilibrato al design di un sistema di controllo degli accessi fisici è una considerazione importante basata sulla valutazione di possibili minacce.

Al giorno d'oggi, con edifici che sono protetti sempre più spesso da soluzioni elettroniche di controllo degli accessi sempre più sofisticate, questi sistemi rappresentano un modo rapido ed efficiente per gestire gli accessi per tutta l'impresa, lasciando un'impronta digitale che, se necessario, può essere esaminata e controllata, e possono essere integrati completamente con altri sistemi come gestione del personale e gestione dei visitatori.

L'unificazione dei sistemi fornisce informazioni importanti per aiutare il processo decisionale non solo per l'azienda ma anche per la sicurezza. Oltre al controllo degli accessi, diventa importante valutare attentamente la maturità informatica del sistema. Poiché i criminali diventano sempre più sofisticati e le minacce continuano a crescere, la sfida sta nell'attenuare il rischio di credenziali di accesso clonate, minacce interne o attacchi informatici lanciati da remoto.

Tuttavia, l'architettura stessa presenta un problema. Molti sistemi di controllo degli accessi tradizionali sono costruiti su infrastrutture obsolete. Tecnologie di sicurezza convergenti usano regolarmente questa infrastruttura, perciò la sfida per i venditori sta in parte nell'adattare l'hardware per collegare queste reti aziendali e in parte nel realizzare l'importanza della cybersecurity e del settore sicurezza in evoluzione che supportano la necessità di valutare attentamente e proteggere dai rischi per un'azienda.

Le considerazioni in merito a cybersecurity devono essere fattori chiave nello sviluppo dei nuovi sistemi di sicurezza. Le tecnologie di controllo degli accessi svolgono un ruolo importante in qualsiasi soluzione di sicurezza fisica e pertanto devono essere costruite in base a principi di cybersecurity riconosciuti, segnalazione di incidenti e buona prassi. È importante riconoscere che l'integrità di un sistema è forte solo quanto l'anello più debole. **Un sistema che non è preparato ad accettare questo fatto** costituisce un potenziale rischio di esposizione. Se non può dimostrare di essere pronto ad accettare, informare e mettere

in pratica azioni di recupero comunemente riconosciute, questo avrà un impatto negativo sull'abilità di fornire i necessari livelli di sicurezza fisica per i quali è stato progettato.

3.1 Credenziali per la cybersecurity (cyber-maturity)

Il coinvolgimento sempre maggiore dell'industria informatica sta cominciando a cambiare il modo in cui le tecnologie vengono valutate, utilizzate e mantenute. Una considerazione importante per gli stakeholder IT è la valutazione delle credenziali di cybersecurity di un'azienda, con particolare attenzione alle conoscenze in merito a cybersecurity da parte del fornitore. Queste conoscenze vengono anche dette "cyber maturity": dimostare una certa maturità in ambito di cybersecurity significa conoscere adeguatamente i vari pericoli e le procedure di mitigazione dei rischi. La ricca documentazione e le direttive relative alla cybersecurity, che sono state sviluppate per le telecamere di rete, possono anche essere utilizzate nei sistemi di controllo degli accessi, dato che le sfide, le valutazioni e le spiegazioni del rischio informatico e il potenziale per un attacco sono ugualmente rilevanti per questi prodotti.

3.2 Il futuro dell'architettura dei sistemi di sicurezza

I moderni sistemi di controllo degli accessi sono collegati tramite cavi di rete e connettori RJ45. Le reti forniscono potenza per i controller di accesso, nonché per la comunicazione tra i dispositivi e i sistemi di gestione centrale. La forza portante nei sistemi di controllo degli accessi è il passaggio a sistemi basati su TCP/IP. Dall'introduzione del primo vero door controller abilitato IP (AXIS A1001) nel 2013, PACS ha continuato ad evolvere, e ora fornisce una vasta gamma di caratteristiche avanzate che non sarebbe stato possibile ottenere facendo solo affidamento sulla tecnologia precedente.

Esempi di tale innovazione comprendono i lettori di codice QR per la semplificazione del controllo degli accessi touch-free, il riconoscimento facciale tramite l'integrazione con telecamere di rete, e la lettura delle targhe, tutti che interagiscono con i database PACS per decisioni basate su edge sull'approvazione o il rifiuto dell'accesso. Benefici chiave dei sistemi IP comprendono bassi costi di installazione con configurazione e gestione del dispositivo semplici. La facilità di integrazione con altri dispositivi significa una soluzione a prova di compatibilità futura che permette una facile connettività plug-and-play di nuove tecnologie di sicurezza e miglioramenti non appena sono disponibili.

3.3 La tecnologia IP contro il tradizionale controllo degli accessi

I vantaggi di IP saranno realizzati grazie a dei nuovi e moderni progetti di controllo degli accessi, specialmente nei sistemi senza contatto, che gli utenti finali si aspettano come standard. Gli utenti inoltre vogliono vedere che il controllo degli accessi si adatta all'uso di smartphone e tablet, e non solo con una credenziale per cellulari. Come farà l'industria a fornire sistemi di controllo degli accessi migliori, più utili e più economici, e potrà mantenere il passo con i cicli innovativi guidati dalle grandi aziende tecnologiche? Queste sono le sfide per il fornitore dell'industria.

Fino ad ora, queste opportunità non sono state sfruttate, probabilmente perché i sistemi di controllo degli accessi precedenti fanno affidamento a door controller installati in architettura di serie e collegati a un'unità o server centrale da cavi RS-485. La maggior parte dei sistemi sono brevettati, il che significa che il door controller è "bloccato" per permettere la gestione solo tramite software progettato dal fornitore. Questo limita l'utente finale ad un singolo fornitore di hardware e software, e la complessità di tali sistemi spesso richiede che l'installazione e la configurazione siano effettuati da personale esperto.

Quando si espandono i sistemi di accesso tradizionali, il processo è complicato dal fatto che un controller centrale tipico è progettato per accogliere un certo numero di porte, con configurazioni non corrispondenti allo standard soggette a costi elevati a causa della limitata flessibilità del sistema. Ad esempio, l'aggiunta

di una singola porta supplementare può risultare in costi molto più elevati, rendendo l'aggiunta irragionevolmente cara.

Le reti IP hanno permesso l'introduzione di architetture PACS molto più semplici e di facile installazione, con maggiore flessibilità e possibilità di personalizzazione. I professionisti IT preferiscono di gran lunga i veri dispositivi IP e il loro uso nei sistemi di controllo degli accessi basati su rete. È importante includere queste persone nel processo di progettazione futuro, poiché garantiscono l'uso di questi dispositivi IP, che sono importanti nella riduzione dei costi di espansione e saranno un requisito per i futuri progetti dei sistemi di controllo degli accessi.

3.4 Protocolli aperti

Il futuro del controllo degli accessi è legato alla volontà da parte dei produttori di condividere le proprie abilità in un protocollo aperto. La resistenza a questa apertura è ovvia, dato che molti produttori di sistemi di accesso sembrano preferire un processo che leghi gli utenti finali alle proprie soluzioni, garantendo così gli introiti futuri. Tuttavia, tale approccio non contiene valore a lungo termine. Gli utenti esigono di più dalle soluzioni e sono felici di condividere i propri dati al fine di raggiungere tale obiettivo.

I progettatori del sistema e i fornitori dell'hardware di accesso hanno le risorse o le conoscenze IT per offrire tutte le soluzioni che gli utenti richiedono come parte di un sistema di sicurezza fisica completo. Molti sembrano essere onestamente inconsapevoli del fatto che le loro offerte vengono rapidamente eclissate da nuove soluzioni innovative che minacciano sia il loro business model che la loro posizione all'interno del mercato del controllo degli accessi. Le capacità dei sistemi più recenti e la velocità delle innovazioni moderne è tale per cui siamo prossimi a non aver bisogno di un sistema di controllo degli accessi, il cui ovvio sostituto è rappresentato dalle unità I/O intelligenti.

L'apertura permette ai venditori di costruire dispositivi adatti a sistemi di controllo degli accessi su piccola scala, nei quali la semplicità è la chiave e dove i costi di acquisto e installazione devono essere competitivi. Se necessario, questi dispositivi possono essere adattati per operazioni più grandi e di complessità tecnica maggiore. Questa flessibilità è il tratto distintivo della sicurezza moderna e garantisce che i sistemi acquistati oggi saranno ancora pertinenti in futuro, anche se il business dell'utente dovesse crescere e i requisiti dovessero cambiare.

Ulteriori informazioni sull'apertura e la tecnologia aperta sono disponibili sul sito ONVIF *www.onvif.org*, creato dall'industria per favorire lo sviluppo verso degli standard aperti.

4 Barriere tecniche all'adozione

Vi sono molte considerazioni da fare in termini di connessioni tecniche, interfaccia e dispositivi che rendono possibile il controllo degli accessi. Possono esserci delle ramificazioni come risultato del passaggio da sistemi tradizionali a sistemi basati su tecnologia cloud. Le sezioni seguenti descrivono in dettaglio i punti che devono essere presi in considerazione per aiutare la tecnologia esistente, e i processi ad essa associati, ad evitare di diventare una barriera per l'aggiornamento e l'adozione di nuove soluzioni.

4.1 Dispositivi di controllo RS-485

Una considerazione è l'uso del dispositivo di controllo RS-485 e il potenziale rischio di installare dispositivi semi-intelligenti che raramente, se non mai, sono dotati di un MAC address, rendendone difficile l'identificazione. RS-485, anche noto come TIA-485(-A) o EIA-485, è uno standard che definisce le caratteristiche elettriche dei driver e dei ricevitori da utilizzarsi nei sistemi di comunicazione seriale. La

segnalazione elettrica è equilibrata e i sistemi multipoint sono supportati. Ma RS-485 specifica solo lo strato fisico, il generatore e il ricevitore. Non controlla lo strato di comunicazioni vitale.

L'assenza di un MAC address o l'uso di un'architettura seriale non indicano necessariamente problemi di affidabilità o effetti negativi sul funzionamento di un sistema di controllo degli accessi: tali design sono il pilastro dei sistemi di controllo degli accessi da più di 30 anni. Tuttavia, la crescita delle aspettative in campo di sicurezza è difficile da visualizzare, a meno che ogni singolo dispositivo in un sistema di controllo degli accessi non sia intelligente e possa essere impostato individualmente. Noi ipotizziamo che solo sistemi completamente intelligenti e dispositivi accessibili possano offrire il valore che ci si aspetta in futuro. È da sottolineare il fatto che "completamente accessibili" non sta ad indicare dispositivi dalla cybersecurity ridotta, ma il contrario.

4.1.1 Open Supervised Device Protocol (OSDP)

Un nuovo metodo di comunicazione, accettato dall'IEC e che offre il potenziale di aumentare la sicurezza nelle comunicazioni degli accessi, è l'Open Supervised Device Protocol (OSDP), uno standard di comunicazione di controllo degli accessi sviluppato dalla Security Industry Association (SIA), l'associazione dell'industria per la sicurezza, per migliorare l'interoperabilità tra i sistemi di controllo degli accessi e i prodotti relativi alla sicurezza. OSDP usa un sistema di codifica a 128 bit, supporta installazioni multidrop e controlla le connessioni per segnalare i problemi dei lettori. Un ulteriore punto di cui prendere nota è che l'OSDP supporta i lettori di schede, gli apriporta, i contatti di allarme e le funzioni di richiesta di uscita utilizzando solo 2 cavi e non le connessioni multiple precedentemente richieste per una porta. Il sito SIA indica che: "OSDP è stato approvato come standard internazionale dalla International Electrotechnical Commission, la Commissione elettrotecnica internazionale, nel maggio 2020 e pubblicato come IEC 60839-11-5 a luglio 2020. L'OSDP della SIA continua a rimanere aggiornato per mantenere la posizione all'avanguardia nell'ambito dell'industria della sicurezza.

4.2 Valore dei dispositivi con un MAC address

Il MAC address è l'indirizzo hardware unico a livello globale di un dispositivo o adattatore di rete singolo. In relazione alla rete IT, il MAC address è importante quanto un indirizzo IP. I MAC address identificano in modo unico un computer sulla LAN e sono necessari affinché protocolli di rete come TCP/IP possano funzionare. Il MAC address è inserito direttamente nel dispositivo, e sebbene sia possibile indovinarlo tramite il sistema operativo, ciò è chiaramente sconsigliabile e l'indirizzo deve essere protetto dalla soluzione per la sicurezza.

TCP/IP e altre architetture di rete comuni di solito usano un modello Open System Interconnection (OSI), nel quale la funzionalità della rete è divisa per strati. I MAC address funzionano allo strato relativo al collegamento dati (strato 2 nel modello OSI) e permettono ai computer di identificarsi su una rete. Il filtraggio del MAC address aggiunge un altro strato di sicurezza. Prima di permettere a qualsiasi dispositivo di unirsi a una rete, il router controlla il MAC address del dispositivo e lo confronta con una lista di indirizzi approvati. Se l'indirizzo del cliente è sulla router list, l'accesso è concesso, altrimenti l'accesso viene negato.

4.2.1 Power over Ethernet (PoE)

PoE offre due benefici che sono costanti per quanto riguarda le applicazioni, il risparmio sui costi e la flessibilità del posizionamento del dispositivo. PoE trasporta dati e alimentazione nello stesso cavo; ciò significa che l'architettura del dispositivo può essere resa più semplice rispetto ai design più tradizionali. Vale la pena sottolineare che molti sistemi di controllo degli accessi vengono pubblicizzati come sistemi collegati a IP.

5 Le caratteristiche delle procedure corrette

La gestione del controllo degli accessi è un componente importante per poter gestire in modo efficace il flusso di persone e controllare gli accessi. Le aziende necessitano di molto di più che bloccare una porta o edificare una barriera. Richiedono migliori opzioni di controllo per poter offrire un'assistenza migliore al cliente e alti livelli di sicurezza in qualsiasi momento. L'adozione di un approccio con pratiche migliori per un controllo degli accessi completo va oltre la selezione dei dispositivi corretti. Si tratta di avere la giusta architettura in posizione, di usare tecnologie di alta qualità, di seguire le procedure e i protocolli corretti, di incoraggiare il personale e gli stakeholder ad adottare i comportamenti corretti.

5.1 Gestione degli stakeholder e approccio convergente alla sicurezza

Come abbiamo visto, si tende a convergere verso la stessa infrastruttura per avere le tecnologie necessarie affinché i siti funzionino regolarmente; dunque, abbiamo anche bisogno di un processo decisionale che sia convergente. Negli esempi di maggior successo, un approccio convergente alla sicurezza ha abbattuto pareti e consentito a diversi reparti di collaborare. Questa convergenza è ancora più importante oggi, quando le tradizionali offerte per la sicurezza elettronica e fisica convivono fianco a fianco nelle reti aziendali.

Gli addetti alla sicurezza fisica devono poter contare su tecnologie che supportino i loro requisiti operativi e fronteggino i rischi associati, ma che allo stesso tempo supportino i criteri di sicurezza IT ed evitino che i dispositivi fisici diventino una porta di accesso alla rete aziendale. Se tutti gli stakeholder collaborano, è possibile creare un ambiente virtuale e fisico protetto.

5.2 Aspettative nei confronti di Partner, produttori e fornitori

È indispensabile garantire che le terze parti capiscano l'importanza di seguire le pratiche sulla sicurezza in tutto quello che fanno e che agiscano in modo da soddisfare necessità specifiche. I rapporti con le aziende esterne sono essenziali per costituire una catena di fornitura sana e instaurare rapporti di fiducia.

Ecco le considerazioni principali da fare quando si valutano le terze parti e i loro effetti sulla catena di fornitura:

- Devono capire e accettare i rischi inerenti la cybersecurity
- Devono avere un approccio maturo verso la cybersecurity con i processi e gli strumenti disponibili
- Devono capire gli effetti delle normative e delle leggi sulla loro offerta
- Devono poter dimostrare come risponderanno alle richieste degli utenti in merito alla conformità normativa
- La cybersecurity è un processo, non solo una tecnologia: dunque, devono poter descrivere la gestione del ciclo di vita in ambito di cybersecurity per proteggere l'attività di un utente.

5.3 Gestione della sicurezza: Processi dei fornitori e dell'amministrazione

Come tutti i tipi di sicurezza, anche la cybersecurity funziona solo se applicata a tutto campo. Si tratta di proteggere adeguatamente la rete di telecamere IP a ogni livello: dai prodotti e dai partner selezionati, fino ai requisiti da definire.

5.3.1 Standard e direttive

ISO 27001 – Information Security Management ISO/IEC 27001 è un sistema di gestione della sicurezza che richiede:

- L'esame sistematico dei rischi per la sicurezza delle informazioni di un'organizzazione, considerando le minacce, le vulnerabilità e gli effetti
- Lo studio e l'implementazione di una serie coerente e completa di controlli della sicurezza delle informazioni e/o altre forme di gestione dei rischi (come l'elusione o il trasferimento) per fronteggiare i rischi considerati inaccettabili
- L'adozione di un processo di gestione onnicomprensivo, per garantire che i controlli di sicurezza delle informazioni soddisfino le esigenze dell'organizzazione in modo costante.

5.3.2 Cyber Essentials Plus

Cyber Essentials è un programma finanziato dal governo e supportato dal settore per aiutare le organizzazioni a proteggersi dalle minacce online più comuni. Cyber Essentials è un indicatore efficace per le aziende che capiscono le sfide poste dalla cybersecurity, ed è una valutazione delle procedure e dei processi della società. Esaminando nello specifico:

- Configurazioni sicure
- Controllo e amministrazione degli accessi
- Protezione da malware
- Gestione delle patch
- Firewall e gateway Internet

Per i produttori di tecnologie, la prima linea di difesa deve essere la riduzione dei rischi associati ai loro sistemi. Dall'1 ottobre 2014 il governo richiede a tutte le aziende che partecipano a gare d'appalto la certificazione Cyber Essentials per la gestione di dati sensibili e personali.

5.3.3 Secure by Design, Secure by Default

Lanciato dal Surveillance Camera Commissioner nel 2019, **Secure by Design, Secure by Default** stabilisce i requisiti minimi per i produttori di sistemi e i componenti delle telecamere per la sorveglianza. Lo schema richiede ai produttori di adottare un approccio olistico per risolvere i problemi di sicurezza alla radice, anziché curarne i sintomi; lavorare a tutto campo per ridurre i danni complessivi a un sistema o a un componente.

Secure by Design, Secure by Default prevede accorgimenti tecnici a lungo termine per fare in modo che il software e l'hardware integrino le funzioni primitive di sicurezza adeguate. Un compito altrettanto difficile è garantire che le primitive siano disponibili e utilizzabili, in modo che il mercato possa adottarle da subito.

Per supportare le sue tecnologie, Axis ha allineato l'approccio "Secure by Design, Secure by Default" al codice di condotta National Cybersecurity Strategy:

- Richiesta password
- Indicatore di sicurezza della password
- Crittografia HTTPS
- 802.1x

- Accesso remoto DISABILITATO (attraversamento NAT)

6 Guide e strumenti (processi per i fornitori)

Quando si parla di assicurare la sicurezza di una rete, le organizzazioni spesso impiegano diversi sistemi di controllo tecnici per creare una "difesa multistrato", il che aiuta a limitare i singoli punti di vulnerabilità e di esposizione. Tuttavia, un importante processo che viene spesso trascurato è il "system hardening", ovvero la modifica delle impostazioni predefinite affinché il sistema sia più protetto dai pericoli per la sicurezza delle informazioni. Questo processo inoltre aiuta anche a ridurre le vulnerabilità intrinseche di tutti i sistemi.

6.1 Guide "hardening" per i produttori

Il rafforzamento del sistema dovrebbe essere applicato a tutti dispositivi collegati a una rete, come workstation, server e dispositivi connessi. Poiché il produttore conosce la configurazione del proprio sistema meglio degli altri, deve fornire ai partner e agli utenti le informazioni necessarie per proteggere l'integrità dei dispositivi e dell'installazione finale. La hardening guide deve fornire consigli tecnici a tutte le persone che utilizzano le soluzioni di videosorveglianza. Deve indicare una configurazione di base e dare informazioni complete su come affrontare minacce che si evolvono di continuo.

Tutti i fornitori devono impegnarsi ad applicare le prassi ottimali di cybersecurity nella progettazione, nello sviluppo e nel collaudo dei dispositivi per ridurre al minimo il rischio di vulnerabilità che potrebbero essere sfruttate per un attacco. Tuttavia, proteggere una rete, i dispositivi e i servizi che supporta richiede una partecipazione attiva in tutta la catena di fornitura, così come nell'azienda/organizzazione dell'utente finale. Un ambiente sicuro dipende dai suoi utenti, dai processi e dalle tecnologie. Una buona guida all'hardening deve seguire usi di base come i CIS Controls - Versione 6.1. Questi comandi erano conosciuti in precedenza come SANS Top 20 Critical Security Controls.

6.2 Gestione dei dispositivi

Un gestore dei dispositivi è uno strumento che fornisce un modo semplice, economico e sicuro di gestire i dispositivi collegati. Offre agli installatori e agli amministratori di sistema uno strumento altamente efficiente per gestire tutte le principali attività di installazione, sicurezza e manutenzione.

Inventario dispositivi / Sistema di gestione risorse

- Regole per account e password
- Installazione efficiente delle applicazioni e degli aggiornamenti firmware
- Applicazione dei controlli per la cybersecurity: gestione HTTPS e caricamento certificati IEEE 802.1x, gestione account e password
- Gestione del ciclo di vita dei certificati - Gestione di tutte le principali attività di installazione, di sicurezza e operative
- Configurazione rapida e semplice dei nuovi dispositivi, impostazioni di backup e ripristino
- Adatto a sistemi di tutte le dimensioni, mono e multi-sito

6.3 Le sfide associate a OEM/ODM

Gli OEM (Original Equipment Manufacturer) sono aziende che rivendono prodotti di un'altra azienda con il proprio nome o marchio. Gli ODM (Original Design Manufacturer) sono aziende che progettano e realizzano prodotti che successivamente vengono commercializzati con il marchio di un'altra azienda. Tali aziende permettono all'azienda che presta il marchio di entrare in produzione senza dover avviare una fabbrica.

Gli OEM/ODM offrono diversi vantaggi a livello imprenditoriale. Il primo è che eliminano tutti i rischi e i costi di produzione, consentendo alle aziende di concentrarsi sulla vendita e sul marketing. È uno dei principali motivi per cui molti produttori di telecamere di sicurezza si affidano a OEM o ODM per realizzare prodotti con il loro marchio.

Questo metodo di lavoro pone però una serie di sfide: una delle principali è ovviamente la cybersecurity. Se i prodotti di un produttore sono vulnerabili, questo può avere un effetto su tutti i rivenditori e i partner nella catena di fornitura. Inoltre, avere una visione chiara della catena può essere molto difficile. Dato il gran numero di OEM e ODM, un utente finale che ha eseguito le opportune verifiche e rifiutato le tecnologie di un determinato produttore potrebbe ritrovarsi a utilizzarle senza rendersene conto.

6.4 Microprocessori per CPU

I chip per CPU generici installati sui dispositivi vengono presi di mira dagli hacker, che identificano molte vulnerabilità. Uno dei principali motivi è che, partendo da una sola vulnerabilità, possono procedere a cascata. Tra gli esempi recenti ci sono "Meltdown" e "Spectre", due attacchi side-channel contro i moderni microprocessori per CPU che permettono di accedere illegalmente ai dati utilizzando un codice senza privilegi.

La maggior parte dei dispositivi, dagli smartphone all'hardware dei datacenter, potrebbe essere in qualche modo vulnerabile. I maggiori produttori di sistemi operativi hanno realizzato patch che limitano i problemi, anche se alcune parti devono essere installate dai produttori OEM perché contengono elementi specifici per ogni piattaforma. Il National Cybersecurity Centre (NCSC) consiglia di applicare al più presto le patch ai dispositivi.

6.5 Strategia per il firmware

Il firmware con firma digitale è importante per gli utenti finali e riduce i rischi di manomissione dei dispositivi durante la logistica e/o la distribuzione. La firma digitale, detta hash, viene applicata al firmware in fase di distribuzione. Un processore calcola l'hash e caricherà solo un'immagine firmware che abbia la stessa hash confermata da un certificato riconosciuto.

6.6 Gestione delle vulnerabilità

La costante ascesa del cyber crime e dei suoi rischi costringe molte aziende/organizzazioni a prestare più attenzione alla sicurezza delle informazioni. La gestione delle vulnerabilità deve rientrare negli sforzi compiuti da un'azienda per controllare i rischi in materia di sicurezza. Questo processo consente di avere sempre un quadro delle vulnerabilità in ambiente IT e dei rischi correlati. Solo identificando e riducendo le vulnerabilità è possibile impedire agli hacker di penetrare nelle reti di un'azienda e di rubarne le informazioni.

I fornitori devono fare in modo che la gestione delle vulnerabilità sia presente in tutte le operazioni, con processi per rilevare e rimediare alle vulnerabilità in tutti i sistemi e per prevenire l'introduzione di nuove vulnerabilità in caso di modifiche o utilizzo di nuovi sistemi. Tutte le questioni inerenti i rischi accettati dal

fornitore devono essere comunicate e concordate con l'utente finale. Se non si implementa questo principio, gli hacker potrebbero sfruttare le vulnerabilità dei sistemi per attaccare un'azienda e i suoi fornitori.

Le patch di protezione e gli aggiornamenti contro le vulnerabilità devono essere installati con una procedura approvata e tempestiva, per prevenire qualsiasi violazione alla sicurezza. I sistemi dei fornitori che per qualsiasi motivo non sono aggiornabili devono prevedere misure per proteggersi dalle vulnerabilità. Tutte le modifiche devono essere svolte secondo i processi di gestione del fornitore.

6.7 Notifiche di sicurezza

Le notifiche di sicurezza aiutano a ridurre i rischi dovuti a vulnerabilità note. Le notifiche di sicurezza possono riferirsi a rapporti ufficiali di vulnerabilità CVE (Common Vulnerability and Exposure) o di altro tipo, e includono una descrizione della vulnerabilità, una valutazione del rischio, raccomandazioni e informazioni su quando sarà disponibile un aggiornamento all'assistenza. La maggior parte dei produttori adotta un modello di vendita indiretta e ha un programma di partnership.

Le notifiche di sicurezza consentono ai clienti che non aderiscono al programma di partnership di un produttore di ricevere notifiche sulla cybersecurity al più presto e quando vengono comunicate nel canale di vendita. Si tratta di uno strumento molto utile per gli utenti finali che hanno installato dispositivi ma potrebbero non avere un contratto con l'azienda che ha eseguito l'installazione.

6.8 BSIMM (Building Security in Maturity Model)

BSIMM è una struttura per stabilire la sicurezza di un software stabilita per aiutare le aziende a confrontare la sicurezza del proprio software con quella di altre alternative disponibili. BSIMM aiuta a valutare i processi, le attività, i ruoli e le responsabilità nelle seguenti aree:

- Revisioni relative a design e architettura
- Revisione dei codici
- Test delle vulnerabilità note
- Strumento di scansione standard per riscontrare vulnerabilità CVE nei pacchetti open source

6.9 LTS (Long-Term Support).

LTS (Long-Term Support) è una politica di gestione del ciclo di vita dei prodotti che prevede il mantenimento di una versione stabile del software per un periodo più lungo rispetto all'edizione standard. Il firmware Long Term Support deve essere aggiornato solo con patch che risolvono problemi di stabilità, prestazioni e protezione. I produttori forniscono un firmware LTS per un massimo di 10 anni dall'introduzione del dispositivo sul mercato.

Il supporto LTS deve essere parallelo ma indipendente rispetto al supporto software attivo esistente. Uno dei vantaggi del supporto LTS è che mantiene l'integrazione con terze parti correlate con la versione originale del firmware.

6.10 Apprendimento e collaborazione

Uno dei principali punti da considerare quando si sceglie un partner tecnologico è la formazione e l'assistenza che offre. Con l'evolversi delle criticità nel settore, soprattutto in ambito di cybersecurity, i produttori devono affrontare la materia in modo proattivo fornendo materiali e contenuti. Alcuni esempi:

- Corsi gratuiti in aula sulla cybersecurity
- Corsi online sulla cybersecurity
- Test rapidi online sulla cybersecurity
- Guida alla protezione avanzata
- Regole sulle vulnerabilità
- Buona prassi per la cybersecurity
- Concetti e terminologia sulla cybersecurity

7 Creare un profilo di igiene informatica: passi successivi e considerazioni

Una buona igiene informatica comprende l'identificazione, la prioritizzazione e la risposta ai rischi che minacciano i servizi e i prodotti chiave dell'azienda. L'implementazione di buone prassi per la sicurezza dell'igiene informatica aiuterà a prevenire violazioni dei dati e configurazioni errate dei sistemi, nonché a minimizzare i rischi associati per l'azienda. È inoltre importante ottenere un accordo degli stakeholder sulle aree principali a rischio, per concentrarsi sugli obiettivi principali per la gestione del rischio.

Anche se non si tratta di una lista esaustiva, le considerazioni seguenti aiuteranno a migliorare l'efficienza nella gestione delle minacce informatiche.

7.1 Fornitori

Controllo delle registrazioni e delle certificazioni

Rivedere le registrazioni e certificazioni appropriate, ad es. chiedere prova della registrazione ISO9000 e di altre certificazioni di qualità. Determinare se i prodotti del fornitore sono stati progettati per essere usati su una rete aziendale.

Ricerca di prove di buona prassi

Assicurarsi che un fornitore scelto possa dimostrare buona prassi in cybersecurity. Devono offrire una guida per la cybersecurity avanzata che descriva le misure di sicurezza fisiche e informatiche e le buone prassi per aiutare a rendere sicura la rete.

Verificare il fornitore

Eseguire una attenta verifica prima di impegnarsi all'acquisto. Controllare le clausole contrattuali per accertarsi che siano chiare. Da un punto di vista finanziario, è importante chiedere cosa succederebbe al prodotto e all'assistenza se la società dovesse avere dei problemi.

Determinare le risorse per un'assistenza continua

Stabilire se il fornitore ha le risorse per continuare a creare le soluzioni di cui pensate di aver bisogno in futuro. Verificare che il fornitore sia delle dimensioni, della portata e delle capacità giuste per supportare i requisiti della vostra azienda in futuro.

Definire le necessità dell'azienda per il futuro

Concentrarsi sulle necessità dell'azienda per il futuro. I dispositivi e le soluzioni intelligenti hanno la capacità di migliorare e garantire il futuro dell'azienda, perciò è importante assicurarsi che il fornitore soddisferà o supererà le aspettative, con un accordo sulla manutenzione e un'assistenza continua.

Verificare le pratiche etiche dell'azienda

Controllare che vengano seguite pratiche etiche e sostenibili. Una partnership basata su fiducia e obiettivi comuni è una base importante per la longevità. Il fornitore segue dei sistemi di gestione ambientale, un programma di responsabilità sociale (Corporate social responsibility, CSR) o una politica di approvvigionamento etico?

7.2 Prodotti e sistemi

Eseguire le procedure di controllo adeguate

Eseguire procedure di controllo tecniche sul sistema e sui componenti principali per accertarsi che funzioni e che non vi siano fattori nascosti che potrebbero comprometterne il funzionamento futuro. Accertarsi che le informazioni sulla valutazione e l'attenuazione del rischio siano chiare e disponibili.

Controllare il contratto di manutenzione

Verificare che cosa è incluso come parte di un contratto, ad esempio se il contratto di assistenza e manutenzione comprende gli aggiornamenti del software del produttore e del firmware.

Proteggere i dispositivi collegati

Accertarsi che il sistema di sicurezza fisico collegato alla rete sia protetto. I sistemi di sicurezza devono essere impiegati con in mente la cybersecurity: cambiare lo username e la password predefiniti, installare il firmware più recente, utilizzare una codifica (idealmente HTTPS), disabilitare l'accesso remoto.

Richiedere una dichiarazione di sicurezza del progetto

Il fornitore deve essere in grado di fornire una dichiarazione di sicurezza del progetto come prova dello stato di sicurezza di qualsiasi dispositivo collegato alla rete.

Valutare l'intelligenza del sistema

I dispositivi collegati che sono completamente intelligenti sono quelli collegati a rete con un MAC address e che sono parte essenziale dell'architettura del sistema. I dispositivi senza un MAC address non sono intelligenti e non possono essere identificati, gestiti o protetti singolarmente.

Valutare la conformità con GDPR/Legge sulla tutela dei dati personali

Accertarsi che i prodotti e i sistemi supportino la capacità di conformarsi alla normativa GDPR, entrata in vigore nel 2018, e all'aggiornamento della legge sulla tutela dei dati personali del 1998.

T10168631/IT/M3.2/2108

Informazioni su Axis Communications

Axis consente un mondo più intelligente e più sicuro creando soluzioni per migliorare la sicurezza e le prestazioni aziendali. Come società di tecnologie di rete e leader nel settore, Axis offre soluzioni nella videosorveglianza, controllo degli accessi, interfono e sistemi audio. Queste sono ottimizzate da applicazioni di analisi intelligente e supportate da formazione di alta qualità.

Axis ha circa 4.000 impiegati dedicati in più di 50 paesi e collabora con partner di tecnologia e integrazione di sistema in tutto il mondo per offrire soluzioni di clienti. Fondata nel 1984, Axis e con sede a Lund, in Svezia