Libro bianco

Rischi dei sistemi legacy di controllo accessi

Genetec™

Sommario


1 2 3
4 5 6
7 9

Sintesi

Molte organizzazioni impiegano ancora sistemi di controllo accessi che risalgono a 15 anni fa o più. I sistemi di controllo più datati possono sembrare ancora sufficienti per consentire l'accesso e l'uscita dei dipendenti, ma tali tecnologie sono vulnerabili alle minacce informatiche.

Le soluzioni di controllo accessi più recenti e sicure dal punto di vista informatico includono la crittografia end-to-end e l'autenticazione avanzata, oltre a ulteriori funzionalità che permettono di difendersi dai malware e dagli attacchi informatici. Un approccio moderno e unificato al controllo accessi può rendere la tua organizzazione più resiliente alle minacce informatiche, offrendo allo stesso tempo vantaggi che vanno ben oltre il blocco e lo sblocco delle porte.

1

Introduzione

In tutto il mondo, i criminali informatici sono alla ricerca di lacune nella sicurezza per accedere a edifici, sistemi di sorveglianza e dati sensibili da vendere sul mercato nero o usare per estorcere denaro alle organizzazioni. Le vittime pagano un prezzo molto elevato; dal 2020 al 2021, il costo medio di una violazione dati è aumentato da 3,86 a 4,24 milioni di dollari[1], ma alcune aziende hanno subito danni per decine di milioni. Nel 2021, un'azienda si è vista richiedere un riscatto di 70 milioni di dollari[2], la cifra più alta mai pretesa in un attacco informatico.

I computer e i server non sono gli unici dispositivi vulnerabili alle minacce informatiche. Quando si tratta di cybersecurity, qualsiasi dispositivo collegato a Internet o a una rete locale (LAN) può essere a rischio.

Le vulnerabilità nei sistemi legacy di controllo accessi possono creare punti deboli in grado di mettere a rischio la cybersecurity della tua organizzazione. Le nuove minacce informatiche possono sfruttare queste vulnerabilità a qualsiasi livello: di credenziali, di controller e di server o di workstation.

Se un hacker viola la tua rete per accedere a dati sensibili come le informazioni proprietarie o le informazioni private dei clienti, l'impatto di una violazione al sistema di controllo accessi può causare danni ben oltre le porte. Le conseguenze non sono solo economiche, ma possono colpire anche la tua reputazione e quella dei tuoi dipendenti, la privacy dei clienti e altro ancora.

Perché il tuo sistema possa proteggerti, dev'essere protetto a sua volta. Per questo motivo, le imprese, gli enti governativi, gli istituti formativi e le organizzazioni della sicurezza pubblica stanno abbandonando le soluzioni proprietarie a favore di soluzioni di controllo accessi sicure. Cercano una piattaforma di sicurezza fisica unificata e sviluppata pensando alla cybersecurity.

[1] https://www.ibm.com/security/data-breach
[2] https://www.welives`ecurity.com/2021/09/30/eset-threat-report-t22021/

L'impatto di una violazione al sistema di controllo accessi nel caso in cui un hacker sia riuscito ad arrivare a dati sensibili come le informazioni proprietarie o le informazioni private dei clienti, può causare danni che vanno ben oltre le semplici porte.

2

Vulnerabilità di cybersecurity nei sistemi legacy di controllo accessi

La maggior parte dei sistemi di controllo accessi odierni si basa sul protocollo Internet (IP) ed è connessa a Internet tramite una rete locale. I sistemi basati su IP sono potenti, ma quelli più datati non offrono funzionalità di cybersecurity vitali per difendersi dall'evoluzione delle minacce informatiche.

Il tuo sistema di controllo accessi è forte solo quanto il suo anello più debole. I criminali informatici possono sfruttare i punti deboli dei sistemi di controllo accessi, delle credenziali, dei controller, dei server o delle worsktation connessi alla rete. Se qualcuno riesce a violare la rete, può accedere ad altri sistemi dell'edificio, visualizzare o rubare informazioni sensibili dagli archivi interni o lanciare attacchi mirati a disattivare i sistemi chiave.

Le minacce più comuni alla cybersecurity che colpiscono i sistemi di controllo accessi includono:

- **Attacchi man-in-the-middle**: quando un criminale informatico accede a una rete per ottenere informazioni scambiate tra dispositivi, ad esempio i codici di apertura di una porta o i nomi utente e le password per accedere a un dispositivo.
- **Attacchi di tipo skimming e relay**: quando un criminale usa il proprio lettore per accedere alle informazioni sulla carta di una vittima e clonarle senza il suo consenso.
- **Attacchi al controller**: quando un criminale sovrascrive il firmware di un controller, rendendo il dispositivo inutilizzabile.

Se qualcuno riesce a violare la rete, può accedere ad altri sistemi dell'edificio, visualizzare o rubare informazioni sensibili dagli archivi interni o lanciare attacchi mirati a disattivare i sistemi chiave.

3

Vulnerabilità a livello di credenziali

I sistemi di controllo accessi usano le credenziali degli utenti per determinare chi può accedere ad aree specifiche. Esistono molti tipi diversi di credenziali, tra cui codici PIN, app per smartphone, impronte digitali e carte o chiavi elettroniche.

I criminali informatici possono rubare le credenziali degli utenti con gli attacchi skimming, usando i propri lettori non autorizzati per accedere alle informazioni senza che gli utenti ne siano consapevoli. In alternativa, se riescono ad accedere alla rete, possono intercettare i dati delle credenziali inviati e archiviarli per usarli in seguito. Possono usare questi dati per effettuare lo "spoofing" (clonazione) di alcuni vecchi tipi di carte o chiavi elettroniche ancora diffusi. Numerose credenziali datate, come le carte a prossimità, possono essere copiate molto facilmente con dispositivi economici reperibili online.

Anche alcune credenziali comunemente usate nei sistemi di controllo accessi legacy con carte di prossimità a 125 kHz o a banda magnetica presentano vulnerabilità note. Molti di questi sistemi comunicano usando il protocollo Wiegand, che è diventato lo standard di settore dalla sua invenzione nel 1974. Purtroppo, gli hacker hanno scoperto come manomettere i lettori di carte più comunemente usati per accedere alle informazioni sensibili.

Le comunicazioni Wiegand sono unidirezionali, quindi, se il lettore viene manomesso, il controller non riceve una notifica a meno che non sia connesso a un interruttore antimanomissione. Inoltre, i dati inviati tramite un sistema basato su Wiegand non sono criptati, quindi, anche se si utilizzano credenziali sicure, è comunque possibile ottenere informazioni sensibili.

Per mitigare il rischio di attacchi man-in-the-middle, cerca un sistema che offra un protocollo bidirezionale sicuro tra il lettore e il controller, ad esempio OSDP2. In questo modo, se qualcuno

La vulnerabilità più comune a livello di credenziali, comunque, è l'errore umano. Ad esempio, condividere codici PIN o chiavi elettroniche, smarrire le carte, bloccare o tenere aperte le porte.

cerca di rubare le credenziali manomettendo il lettore o sostituendolo con uno non autorizzato, non potrà comunque accedere alle informazioni sensibili. Il protocollo bidirezionale notificherà anche gli operatori del tentativo di manomissione del sistema, in modo che il team di sicurezza possa rispondere rapidamente e neutralizzare la minaccia.

La vulnerabilità più comune a livello di credenziali, comunque, è l'errore umano. Condividere codici PIN o chiavi elettroniche, smarrire le carte, bloccare o tenere aperte le porte sono avvenimenti frequenti, apparentemente di poca importanza, che possono avere un grande impatto sulla sicurezza di un edificio.

Scegliere credenziali avanzate sicure o sistemi biometrici è il miglior approccio per ridurre le vulnerabilità a livello di credenziali. Anche migliorare l'igiene informatica può aiutare a ridurre i rischi legati all'errore umano. Assicurati che tutti i membri del personale ricevano formazione, avvisi e promemoria, a supporto di una cultura del lavoro che favorisca e rafforzi una buona igiene informatica. Questo requisito andrebbe esteso ai partner con cui lavori, perché se subissero violazioni queste potrebbero impattare anche la tua sicurezza. Chiedi a tutti i partner software di descrivere le misure da loro previste per garantire che il personale rispetti le procedure consigliate di igiene informatica. È buona norma anche includere la cybersecurity tra i requisiti richiesti quando cerchi nuovi partner software o fornitori di hardware di rete.

Gestire i diritti di accesso è un altro processo soggetto a errori, se le informazioni sono gestite e monitorate manualmente. Scegli partner che possano anche fornire una soluzione unificata per la gestione dei diritti di accesso basata su ruolo e status utente e non sull'individuo. In questo modo, potrai automaticamente aumentare, ridurre, aggiungere o revocare i diritti di accesso di interi gruppi di persone al variare delle necessità. Ad esempio, quando una dipendente va in maternità, cambia ruolo o lascia l'azienda. Quando lo stato della dipendente cambia nel database collegato, cambiano anche i suoi diritti d'accesso, eliminando il rischio che qualcuno usi una vecchia carta per accedere ad aree in cui non dovrebbe più entrare. Il sistema permette anche di revocare velocemente gli accessi nel caso in cui una carta o altre credenziali vengano smarrite o rubate.

4

Vulnerabilità a livello di controller

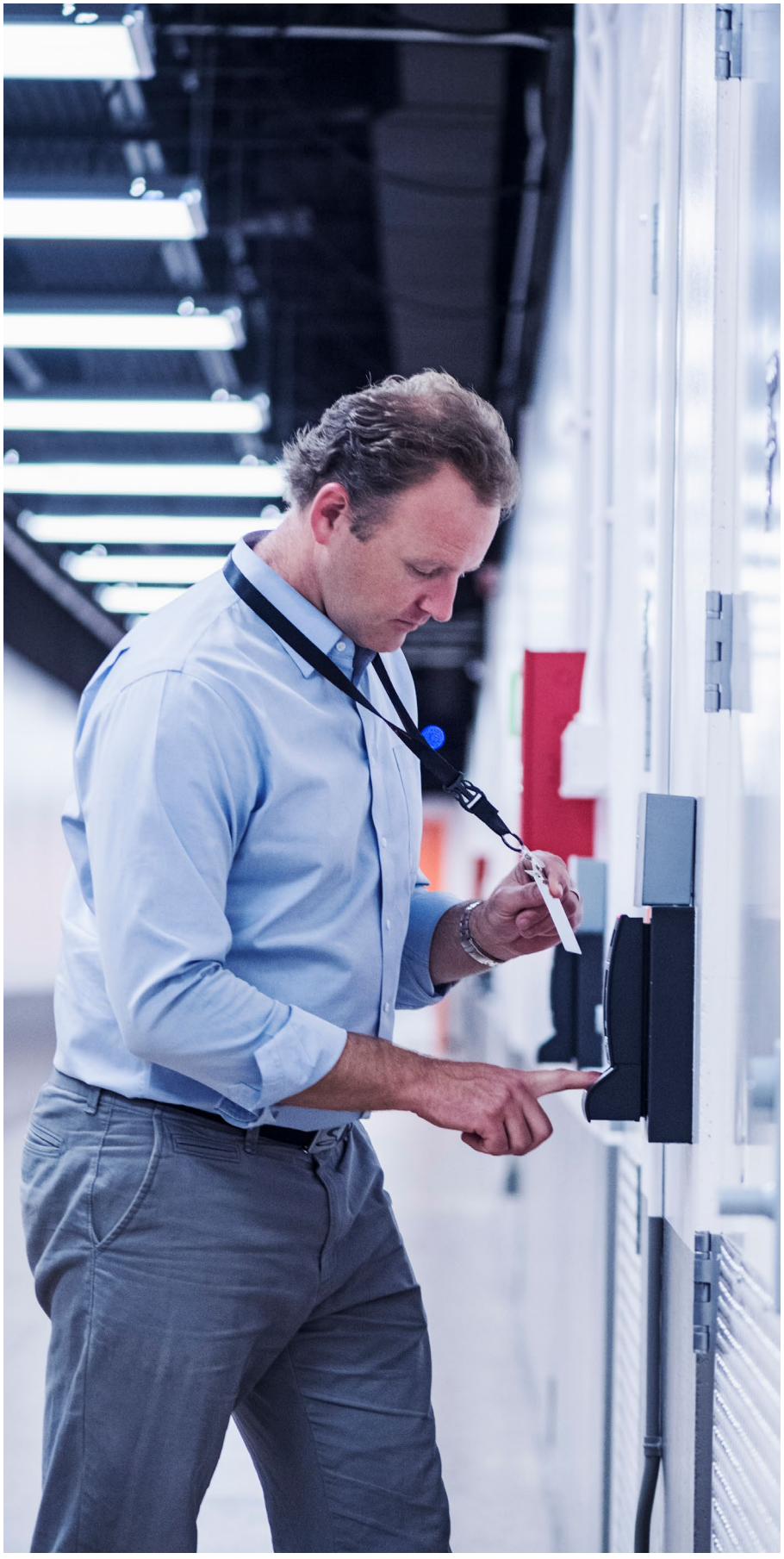
I pannelli di controllo, o controller, leggono le credenziali e le confrontano con una lista consentita sul server di controllo accessi. Se le credenziali corrispondono, invia un segnale alla serratura della porta per aprirla o per negare l'accesso.

Alcuni vecchi tipi di controller contengono chiavi segrete per decriptare le informazioni nei lettori stessi, alcuni dei quali potrebbero trovarsi al di fuori del perimetrio di sicurezza. I criminali informatici che accedono ai controller possono quindi ottenere le chiavi d'accesso ai tuoi edifici.

I controller richiedono aggiornamenti firmware regolari per garantire una sicurezza aggiornata. È importante garantire che il team di sicurezza verifichi la disponibilità di aggiornamenti e li installi regolarmente.

Infine, un'azione semplice ma importante per garantire la sicurezza dei controller è assicurarsi di cambiare le password predefinite con qualcosa di unico e difficile da indovinare.

I controller richiedono aggiornamenti firmware regolari per garantire una sicurezza al passo coi tempi. È importante che il team di sicurezza verifichi la disponibilità di aggiornamenti e li installi regolarmente.



5

Vulnerabilità a livello di server o workstation

I server archiviano e gestiscono l'elenco di credenziali approvate e fornite agli individui e successivamente comunicano con i controller per autenticare i dati delle credenziali. Queste informazioni devono essere trasmesse su una rete. Se i dati non sono criptati, i criminali informatici che accedono alla rete possono ottenere credenziali e ad altri dati sensibili.

I dati delle credenziali acquisiti dai lettori e archiviati nei server dovrebbero essere protetti da metodi robusti di crittografia, autenticazione e autorizzazione. La maggior parte delle vulnerabilità a livello di server è legata a:

- Utenti non autorizzati che approfittano di metodi di autenticazione deboli.
- Autorizzazioni troppo ampie per gli utenti, che permettono alle persone di apportare modifiche al sistema o di accedere a dati che dovrebbero essere riservati.
- L'efficacia del server nel gestire l'autenticazione degli utenti per garantire che solo le persone approvate possano visualizzare le informazioni sensibili.

I dati delle credenziali acquisiti dai lettori e archiviati nei server dovrebbero essere protetti da metodi robusti di crittografia, autenticazione e autorizzazione.

6

Procedure consigliate di cybersecurity per i sistemi di controllo accessi

La tecnologia di controllo accessi ha subito una grande trasformazione negli ultimi anni. Il tradizionale mercato proprietario ha lasciato il passo a uno più aperto. I clienti non sono sempre legati a un solo fornitore e, come risultato, le aziende stanno sviluppando prodotti e servizi più innovativi. Queste nuove soluzioni più sicure dal punto di vista informatico offrono la crittografia end-to-end e l'autenticazione avanzata, oltre ad altre funzionalità per difendersi da attacchi informatici e malware.

Per migliorare la cybersecurity della tua rete

- Aggiorna il tuo sistema: i sistemi più datati non sono progettati per affrontare le minacce odierne.
- Usa credenziali intelligenti e/o mobili e gli ultimi protocolli di comunicazione per proteggere i dati trasmessi tramite Internet.
- Informa i dipendenti sulle procedure consigliate di cybersecurity e assicurati che venga spesso ricordato loro di aggiornare le password.
- Usa un sistema di gestione dell'identità per garantire che gli utenti possano accedere solo alle aree e ai dati necessari per il loro ruolo e il loro stato attuale.
- Crea reti locali separate per i dispositivi che archiviano o condividono informazioni altamente sensibili, in modo che non sia possibile accedervi dalla tua rete generale.

Molte organizzazioni preferiscono un approccio ibrido che permette di sfruttare la scalabilità e la flessibilità del software e delle opzioni di archiviazione dati del cloud, mantenendo allo stesso tempo la gestione locale di alcuni server.

- Scegli un fornitore di sicurezza in grado di dimostrare la propria conformità ai framework consolidati di controllo della sicurezza.
- Assicurati che il tuo sistema usi solo metodi comprovati di crittografia dei dati e che applichi l'autenticazione a più fattori.
- Lavora con un partner che disponga di un team dedicato a monitorare le minacce informatiche e a garantire che il software venga aggiornato di frequente e riceva le patch necessarie.

Non c'è bisogno di scegliere tra una soluzione basata su cloud o una on-premise. Molte organizzazioni preferiscono un approccio ibrido che permette di sfruttare la scalabilità e la flessibilità del software e delle opzioni di archiviazione dati del cloud, mantenendo allo stesso tempo la gestione locale di alcuni server.

7

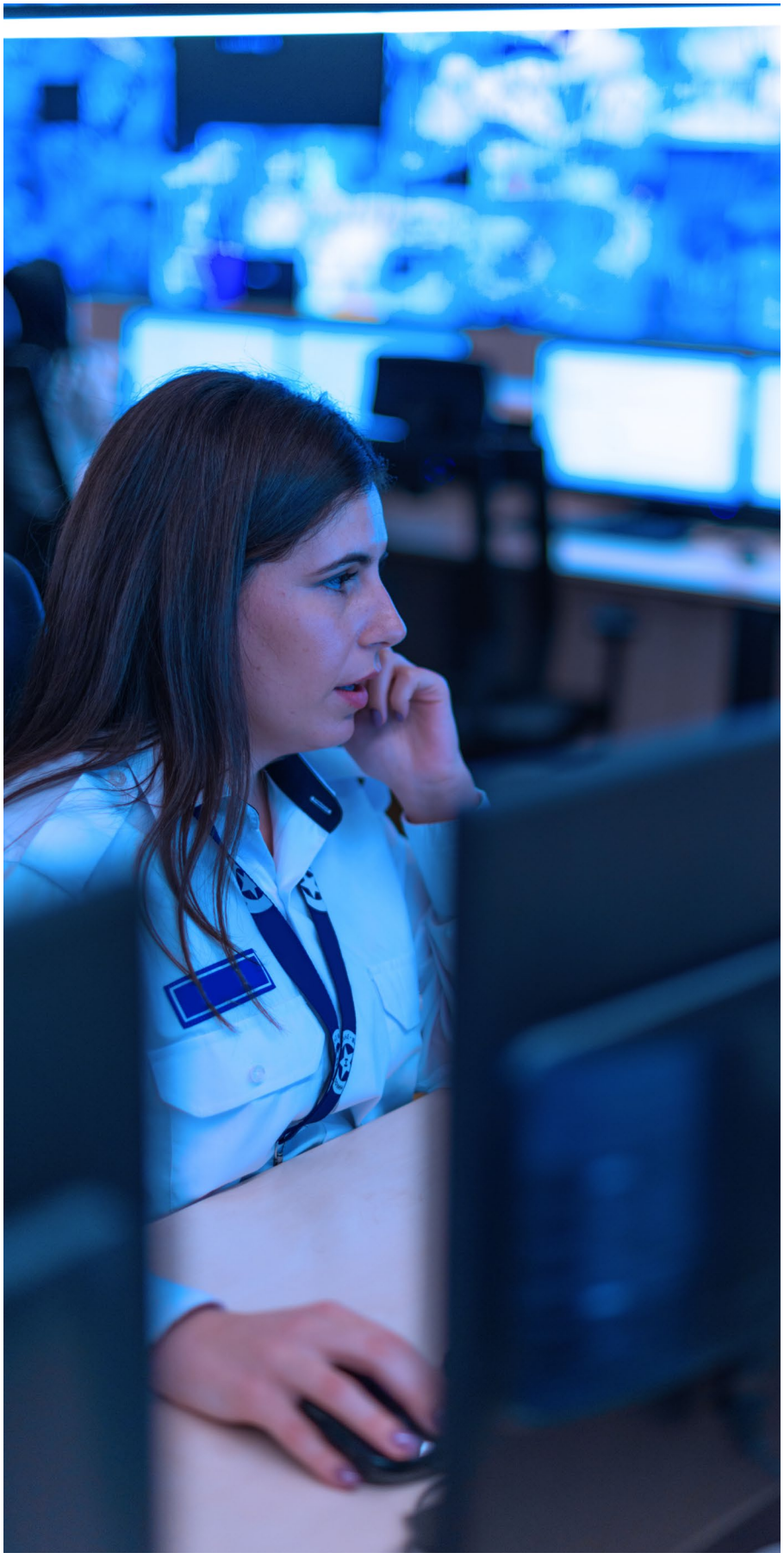
I sistemi di controllo accessi attuali non sono solamente sicuri dal punto di vista informatico

Un sistema di controllo accessi unificato che impiega i più recenti standard di cybersecurity per garantire la sicurezza di comunicazioni, server e dati, come Security Center Synergis di Genetec, può non solo proteggere meglio le risorse e i dipendenti delle aziende, ma anche supportare le loro operation e i loro processi decisionali ben oltre il blocco e lo sblocco delle porte. Scegliendo un sistema di controllo accessi basato su IP con un'architettura aperta, le aziende possono effettuare in qualsiasi momento l'aggiornamento alle ultime tecnologie supportate, muoversi al proprio ritmo e rispettare i limiti del budget.

Il sistema di controllo accessi Synergis™ impiega i più recenti standard di cybersecurity per proteggere le comunicazioni, i server e i dati a tutti i livelli della tua architettura. Questa protezione avanzata, che copre dalle carte di accesso al software, ti permette di gestire i tuoi edifici in tranquillità, sapendo che sono al sicuro da occhi indiscreti.

Genetec™ Security Center è una piattaforma ad architettura aperta che unifica la videosorveglianza basata su IP, il controllo accessi, il riconoscimento automatico delle targhe (ALPR), le comunicazioni e l'analisi. Genetec sviluppa anche soluzioni e servizi basati su cloud, progettati per migliorare la sicurezza e contribuire a nuovi livelli di intelligenza operativa per governi, imprese, trasporti e comunità locali.

Security Center è una piattaforma ad architettura aperta che unifica la videosorveglianza basata su IP, il controllo accessi, il riconoscimento automatico delle targhe (ALPR), le comunicazioni e l'analisi.



8

I vantaggi dei sistemi di controllo accessi attuali vanno oltre il blocco e lo sblocco delle porte

I sistemi di controllo accessi più recenti e sicuri dal punto di vista informatico, come Synergis, possono fare molto di più che bloccare e sbloccare le porte in base a una programmazione. Possono sfruttare i dati raccolti e combinarli con altre fonti per offrire informazioni approfondite in grado di migliorare le operation di routine e rafforzare la sicurezza. Come risultato, questi sistemi offrono un ritorno sugli investimenti nettamente superiore.

Synergis si spinge oltre le porte per fornire informazioni che permettono di prendere decisioni più oculate e di migliorare le operation quotidiane. È un sistema veramente aperto e connesso a una vasta e crescente selezione di dispositivi di controllo accessi di terze parti. Aggrega e mostra i dati in formato dinamico per operare in modo più intelligente.

Ad esempio, durante la pandemia di COVID, i clienti che impiegavano Synergis sono stati in grado di installare facilmente e rapidamente nuovi lettori biometrici che hanno ridotto la necessità di contatto fisico[3], limitando la diffusione del virus. Hanno anche sfruttato i dati del controllo accessi per supportare il tracciamento dei contatti[4] nel caso in cui un dipendente fosse risultato positivo ai test virali, oltre a gestire i livelli di occupazione e i requisiti di distanziamento fisico[5] previsti dalle autorità pubbliche della sanità.

Synergis può aiutarti a proteggere non solo le porte, ma tutte le tue operation, dalla gestione dell'occupazione in tempo reale al monitoraggio delle infrastrutture remote.

I sistemi di controllo accessi acquisiscono una grande quantità di dati, ma i sistemi più datati rendono difficile raccoglierli e comprenderli. Synergis include delle dashboard che offrono una visione unificata dei dati di tutti i sistemi di sicurezza e i sensori, in modo che sia possibile prendere decisioni operative proattive anziché reattive.

Synergis può aiutarti a proteggere non solo le porte, ma tutte le tue operation, dalla gestione dell'occupazione in tempo reale al monitoraggio delle infrastrutture remote. Permette di adattarti alle nuove esigenze semplicemente modificando le impostazioni del software o aggiungendo/aggiornando l'hardware, senza bisogno di sostituire l'intero sistema. Con Synergis, puoi usare i dati del controllo accessi per consentire l'automazione degli edifici, ad esempio per spegnere le luci o regolare riscaldamento e climatizzazione in assenza di personale. Puoi anche ottenere informazioni su quali aree degli edifici vengono utilizzate più spesso, per capire la quantità di spazio effettivamente necessaria.

[3] https://www.genetec.com/podcasts/engage/episode-10-stepping-up-cybersecurity-biometrics-and-multifactor-authentication
[4] https://www.genetec.com/press-center/press-releases/2021/02/genetec-helps-westminster-property-ventures-ensure-safe-return-to-work-for-its-commercial-tenants
[5] https://resources.genetec.com/en-industry-focuses/genetec-occupancy-management-package

9

Conclusioni

Un sistema di controllo accessi unificato che impiega i più recenti standard di cybersecurity per garantire la sicurezza di comunicazioni, server e dati, come Security Center Synergis, può non solo proteggere meglio le risorse e i dipendenti delle aziende, ma anche supportare le loro operation e i processi decisionali ben oltre il blocco e lo sblocco delle porte. Scegliendo un sistema di controllo accessi basato su IP con un'architettura aperta, le aziende possono effettuare in qualsiasi momento l'aggiornamento alle ultime tecnologie supportate, muoversi al proprio ritmo e lavorare nei limiti del budget.

Vuoi saperne di più?

Scarica la nostra checklist dei 7 fattori principali da considerare prima di effettuare la migrazione a un sistema di controllo accessi basato su IP.

Scarica la checklist

Genetec Inc. è un'azienda tecnologica innovativa con un ampio portafoglio di soluzioni di sicurezza, intelligence e operazioni. Il prodotto di punta dell'azienda, Genetec™ Security Center, è una piattaforma di sicurezza fisica che unifica la videosorveglianza basata su IP, il controllo degli accessi, il riconoscimento automatico delle targhe (ALPR), le comunicazioni e l'analisi. Genetec sviluppa anche soluzioni e servizi basati su cloud, progettati per migliorare la sicurezza e contribuire a nuovi livelli di intelligenza operativa per governi, imprese, trasporti e comunità locali. Fondata nel 1997 e con sede a Montreal, Canada, Genetec serve i propri clienti in tutto il mondo attraverso una vasta rete di rivenditori, integratori, partner di canale certificati e consulenti in oltre 159 paesi.

Videosorveglianza: ottieni una maggiore consapevolezza situazionale e migliora la sicurezza della tua città con la possibilità di condividere le telecamere tra agenzie e organizzazioni, fornendo un quadro operativo comune e migliorando i tempi di risposta agli incidenti.

Controllo accessi: aumenta la sicurezza della tua azienda, rispondi in modo efficace alle minacce e prendi decisioni più chiare e tempestive con una piattaforma unificata e IP-ready, sia che si tratti di implementare un nuovo sistema di controllo accessi o di aggiornare un'installazione esistente.

Riconoscimento automatico delle targhe: automatizza il rilevamento dei veicoli di interesse, aumenta l'efficienza del monitoraggio e controllo dei parcheggi e accelera le indagini di pubblica sicurezza grazie alla possibilità di condividere i dati delle targhe con le agenzie e le organizzazioni partner, senza rinunciare alla proprietà e alla privacy.

Supporto alle decisioni operative: raggiungi una maggiore efficienza nella gestione degli incidenti e nel processo decisionale, con flussi di lavoro avanzati che guidano gli operatori nell'intero percorso, dagli avvisi, alle procedure basate su criteri, fino all'esportazione della compilazione dettagliata dei casi.

Gestione dei casi investigativi: semplifica la gestione dei casi e accelera le indagini con una piattaforma che ti consente di centralizzare le prove digitali e di collaborare in modo sicuro con investigatori, agenzie esterne e pubblico.

Servizi cloud: estendi le capacità del tuo sistema di sicurezza locale e riduci i costi IT con servizi cloud on-demand altamente scalabili, che consentono alla tua città di far fronte facilmente ai requisiti di sicurezza in rapida evoluzione e di operare con maggiore efficienza.

Genetec Inc.
genetec.com/locations
info@genetec.com
@genetec

AGGIORNATO: 01-GIU-22