La Redazione


# Sicurezza cyber dei sistemi di sicurezza fisica: un must

**"È noto che i sistemi di sicurezza fisica possano essere porte aperte all'hacking, soprattutto se si tratta di tecnologie proprietarie datate, dunque non progettate per difendere da minacce informatiche in costante evoluzione e aggiornamento. Genetec Inc.[1] ha rilasciato un e-book rivolto agli operatori del settore con domande e consigli per mettere in sicurezza (cyber) i sistemi di sicurezza dei propri clienti.**

[1] Genetec Inc. offre soluzioni conformi e resilienti dal punto di vista informatico.
Per saperne di più:
**https://www.genetec.com/it/blog/cybersicurezza**


**Per essere resilienti occorre predisporre strategie di cybersecurity incisive e scegliere partner affidabili che offrano strumenti automatizzati per mitigare le minacce**

Partiamo da alcune domande base per determinare se un sistema di sicurezza fisica può mettere in pericolo la sicurezza informatica del cliente finale:

1) Conosci le conseguenze finanziarie e operative di una violazione delle informazioni dei clienti per una falla nella sicurezza di una telecamera o di un dispositivo che gestisci?

2) Quanto tempo impiega il tuo team ogni mese per aggiornare software e firmware e per gestire le procedure di cybersecurity nei tuoi sistemi?

3) Puoi stabilire e mantenere password ad elevato livello di sicurezza e limitare efficacemente l'accesso ai dati? Puoi offrire funzionalità single sign-on con più livelli di autenticazione?

4) I tuoi sistemi legacy consentono di adottare i più recenti metodi di crittografia o di implementare funzionalità di cybersecurity per fronteggiare l'evoluzione delle minacce?

5) Se un cliente o le forze dell'ordine ti richiedono di visualizzare le riprese video, puoi condividere le registrazioni in modo sicuro tutelando l'identità delle persone inquadrate?

Una volta che ci si è confrontati con questi 5 aspetti preliminari, è ora di implementare almeno tre misure di cybersecurity per rendere un'installazione di sicurezza fisica più resiliente. Naturalmente più livelli di sicurezza verranno messi in campo, maggiore sarà la sicurezza dell'attività.

## Tre misure di cybersecurity essenziali

1) Livello 1: crittografia. Criptando le informazioni o il testo leggibile per nasconderlo agli utenti non autorizzati, aiuta a proteggere i dati di sicurezza fisica inviati dai dispositivi di sicurezza (telecamere, lettori di controllo accessi e sensori IoT) da e verso i server e le workstation client. NB - In particolare per la videosorveglianza, è essenziale usare metodi di crittografia robusti sia per

## Impatto economico e legale di una violazione

i dati in transito che per quelli a riposo. Nonostante i dati in transito siano generalmente considerati più vulnerabili, i malintenzionati attaccano sempre il punto d'ingresso più debole.

2) Livello 2: autenticazione. L'autenticazione è il processo di convalida dell'identità di utenti, server o applicazioni client che viene eseguito prima di concedere loro l'accesso alle risorse protette. Lato client, l'autenticazione può includere varie tecniche come nomi utente e password o token di sicurezza. Lato server, la conferma di affidabilità di una parte terza avviene solitamente tramite certificati digitali. NB - Usare più forme di autenticazione rafforza ulteriormente la sicurezza. Oltre ai nomi utente e alle password, considerare l'uso di app di autenticazione per smartphone, dispositivi biometrici o token fisici di sicurezza come YubiKey o una smart card.

**Tipologie di attacco: spyware, ramsomware, denial of service (DdoS), forza bruta, man in the middle, phishing**

3) Livello 3: autorizzazione. E' un processo che permette di definire privilegi specifici per gli utenti, che limitano ulteriormente chi può accedere alle applicazioni e cosa può vedere o fare al loro interno. L'autorizzazione nei sistemi di sicurezza può anche indicare quali tipi di informazioni possono essere condivise internamente o esternamente e quando è possibile farlo, oltre a definire per quanto tempo possono essere conservati i dati. NB – E' possibile automatizzare la distribuzione di questi privilegi con un'integrazione Microsoft Active Directory nei sistemi di sicurezza: non solo semplifica la configurazione dell'autenticazione, ma garantisce anche che, quando un dipendente lascia l'azienda, i suoi privilegi vengano revocati di default.

## Vendor affidabili

Ovviamente la prima strategia per assicurarsi che i sistemi di sicurezza fisica siano in grado di garantire la cyber security è rivolgersi a brand affidabili. E anche se tutti i player oggi dichiarano di mettere in campo soluzioni e procedure di cybersecurity, ci sono 10 domande che possono aiutare a valutarne la loro reale affidabilità.

1) Il fornitore monitora proattivamente le nuove minacce emergenti e il loro potenziale impatto su operation, dati e persone?

2) Prevede una strategia completa per colmare le lacune e le vulnerabilità di sicurezza?

3) Quali direttive applica per quanto riguarda la cybersecurity?

## Come controllare la sicurezza informatica della supply chain?

Occorre anzitutto assicurarsi che ogni dispositivo, così come i server utilizzati per archiviare i dati e ospitare le console di monitoraggio, siano aggiornati all'ultima versione del firmware e del software raccomandata. La modifica delle password predefinite e l'istituzione di un processo per cambiarle frequentemente è una pratica fondamentale. Anche il miglioramento della progettazione della rete per segmentare i dispositivi più vecchi può ridurre il potenziale di attacchi crossover. Per determinare il rischio dei sistemi di sicurezza fisica, occorre condurre una valutazione, creando e mantenendo un inventario di tutti i dispositivi connessi alla rete e della loro connettività, versione del firmware e configurazione. La valutazione deve includere modelli e produttori che destano preoccupazione, come quelli elencati dal governo USA nel National Defense Authorization Act (NDAA) come "ad elevato rischio informatico". Occorre inoltre creare un elenco di tutti gli utenti che sono a conoscenza dei dispositivi e dei sistemi di sicurezza. Nel processo di revisione occorre individuare i dispositivi e i sistemi da sostituire. Un approccio efficace consiste nell'unificare i dispositivi e il software di sicurezza fisica e informatica su un'unica piattaforma ad architettura aperta con strumenti e pannelli di gestione centralizzati. La U.S. Cybersecurity and Infrastructure Security Agency raccomanda di far lavorare i team di sicurezza informatica e fisica insieme, in modo da sviluppare un programma di sicurezza completo basato su una comprensione comune di rischi, responsabilità, strategie e pratiche.

4) Le soluzioni che offre sono sviluppate con più livelli di sicurezza, ad esempio tecnologie avanzate di crittografia e autenticazione?

5) Come protegge i dati dell'azienda e la privacy dei clienti?

6) Lavora con partner che a loro volta riconoscono l'importanza di sicurezza e protezione dei dati? Valuta e seleziona attentamente i partner per assicurarsi che mantengano i massimi livelli di cybersecurity e conformità?

7) Quali misure prende per informare e assistere i suoi clienti con le procedure di cybersecurity?

8) È trasparente circa le vulnerabilità e condivide strategie e soluzioni per risolverle rapidamente?

9) Aderisce agli standard per la sicurezza, come ISO 27001? Dispone di certificazioni da altri enti normativi o associazioni internazionali?

10) Si sottopone a controlli di terze parti e svolge test di penetrazione per identificare e risolvere i problemi di sicurezza?

**Gli strumenti e i servizi unificati possono segnalare le potenziali vulnerabilità e aiutare a semplificare gli aggiornamenti, limitare gli accessi e i privilegi degli utenti, fornire indici di sicurezza**

## Protezione duratura

Per garantire la cybersecurity nella sicurezza fisica non basta difendersi dagli attacchi: occorre studiare una strategia che duri nel tempo, stabilendo un rapporto di fiducia con clienti e partner. Per farlo, è necessario valutare, rivalutare e aggiornare continuamente le misure di protezione dei dati e della privacy. Ecco un piccolo memo.

1) Avere consapevolezza delle minacce informatiche: non fare affidamento solo sulle informazioni di altri professionisti IT o della sicurezza, restare al passo con i nuovi rischi e le più recenti strategie di mitigazione e formare i dipendenti su cosa fare e cosa non fare in modo che diventino altrettanto consapevoli.

2) Effettuare una valutazione dei rischi e un inventario delle risorse per attivare i meccanismi di cybersecurity ideali. Fare un elenco dei computer, dei dispositivi IoT, dei tipi di dati e così via può aiutare a mantenere livelli più elevati di cybersecurity.

3) Restare al passo con le patch e gli aggiornamenti di sistema - Le patch possono risolvere le vulnerabilità della sicurezza e mitigare rischi potenzialmente elevati. Valutare di impiegare strumenti automatizzati che informino degli aggiornamenti software o firmware, così da non perdere mai l'opportunità di mantenere la resilienza dei sistemi di sicurezza.

4) Implementare l'autenticazione a due fattori. Non affidarsi solo alle password: possono essere facilmente rubate o condivise.

5) Definire un piano di recupero dalle violazioni - È essenziale disporre di un sistema di sicurezza fisica che rilevi le potenziali compromissioni, ed è altrettanto importante definire un piano di recupero dalle violazioni.