International SecurityLigue

CoESS

Cyber-Physical Security e Infrastrutture Critiche

Proteggere le nazioni e le società nell'era dei sistemi connessi e delle minacce ibride

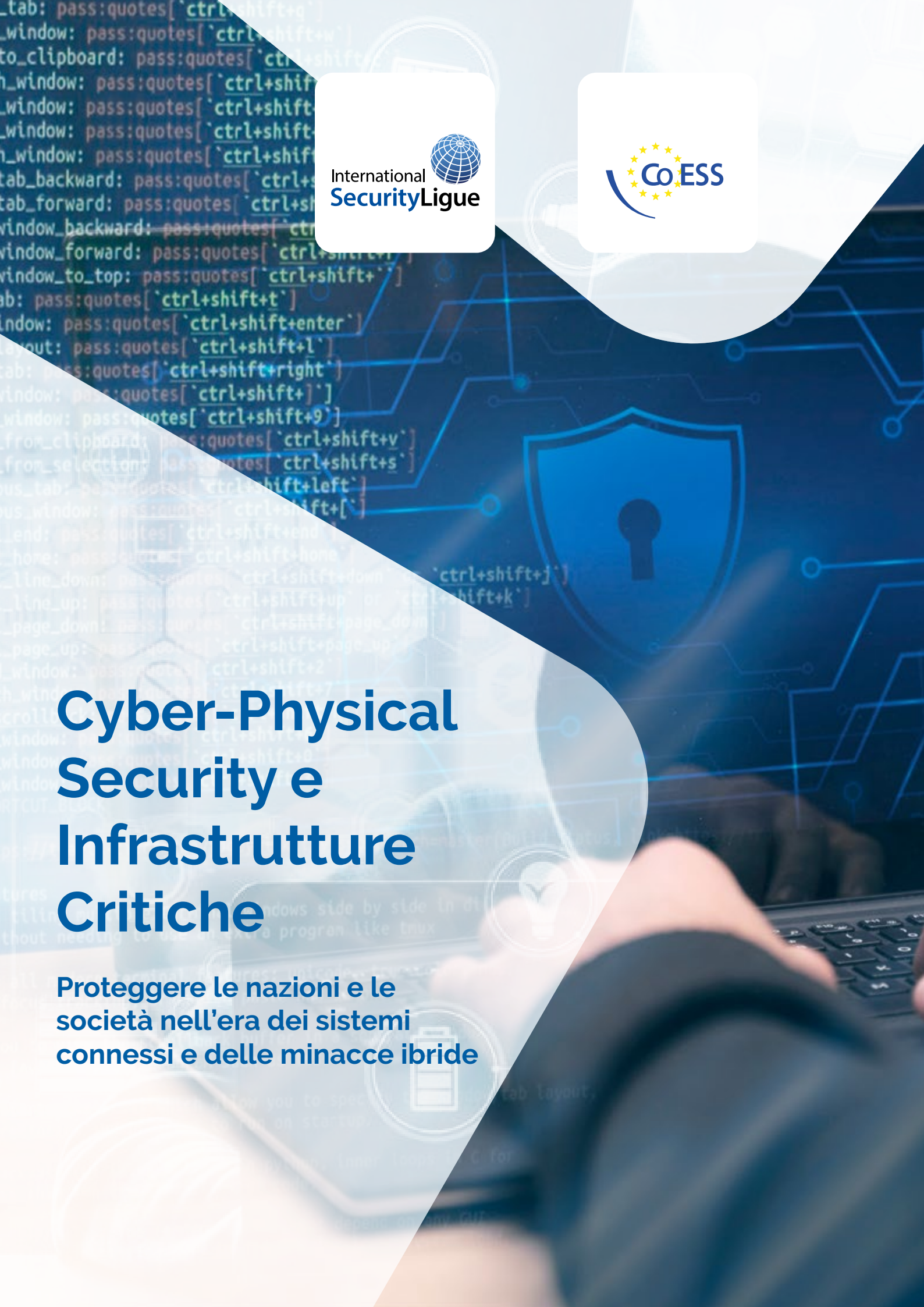


Tabella dei contenuti

Ogni giorno la stampa riporta notizie di attacchi informatici contro organizzazioni e aziende, e le infrastrutture critiche sono un obiettivo importante, soprattutto nel settore energetico, ma anche in quello finanziario, della sanità, delle comunicazioni e in altri settori.

Prefazione

La maggior parte degli attacchi comporta l'intervento umano, intenzionale o meno, e ha conseguenze nel mondo fisico; tuttavia, la sicurezza informatica e quella fisica sono ancora gestite separatamente, creando vulnerabilità. Questo libro bianco esplora la frontiera sempre più sottile tra questi due mondi e descrive come un approccio olistico possa aiutare a proteggere le organizzazioni e a renderle più resilienti.

Se l'attuale conflitto in Ucraina mette in evidenza gli attacchi informatici condotti in un contesto di guerra, va sottolineato che essi avvengono anche in altre regioni che vivono tensioni e conflitti latenti, come in Medio Oriente tra Iran e Arabia Saudita. Tutti ricordano l'attacco Stuxnet nel 2010, ma chi sa che era attivo dal 2009 e che aveva già infettato una dozzina di aziende prima di attaccare le centrifughe dell'impianto di arricchimento di uranio per materiali nucleari iraniane? Stuxnet era diverso da qualsiasi altro virus o worm precedente.

Anziché limitarsi ad assumere il controllo dei computer presi di mira o a rubare informazioni da essi, l'attacco si è spinto oltre l'ambito digitale, distruggendo fisicamente le apparecchiature che quei computer controllavano. Poi, in risposta a Stuxnet, c'è stato l'attacco alla Saudi Aramco da parte di Shamoon nel 2012, che ha compromesso 30.000 computer. Infine, dal 2016 al 2018, ci sono stati numerosi attacchi alle reti delle infrastrutture critiche saudite e alle agenzie governative.

Esempi simili si trovano in tutte le parti del mondo.

Gli attacchi informatici sono una delle armi strategiche a disposizione nei conflitti convenzionali e lo sono da molto tempo. Costituiscono un modo primario in cui gli Stati, le organizzazioni e gli individui possono danneggiare altri Stati, organizzazioni ed individui, che si tratti di un ambiente pubblico o privato. Sebbene i computer siano i bersagli dell'infezione, l'azione umana ha dimostrato di essere un fattore costante in questi attacchi.

Magnus Ahlqvist
Presidente della International Security Ligue

Vinz Van Es
Presidente della CoESS

Va quindi sottolineato che la protezione dell'accesso alle informazioni e ai sistemi è e rimarrà tridimensionale, dovendo considerare la protezione fisica, il fattore umano e la protezione digitale. È ormai chiaro che non ha senso cercare di proteggere, e tanto meno di reagire a un attacco con un approccio isolato. Allo stesso modo, la protezione delle organizzazioni dalle minacce del mondo digitale, in particolare dagli attacchi informatici, può essere realizzata solo con un approccio olistico.

Anche le conseguenze degli attacchi informatici sono tridimensionali: infrastrutture informatiche neutralizzate o distrutte; produzione industriale o servizi bloccati o annientati, con potenziali incidenti industriali gravi; infine, in termini umani, feriti o morti e perdita di posti di lavoro.

Che sia per incidente, negligenza o dolo, il ruolo dell'uomo è eminentemente presente nello sviluppo e nella diffusione degli attacchi informatici. In quanto tale, il fattore umano è una costante che deve essere pienamente integrata in una strategia di protezione in grado di proteggere sia da un "vettore involontario" sia da un "vettore malevolo" (minaccia esterna o insider). Proprio perché la dimensione umana non può essere dissociata dalla strategia di difesa delle organizzazioni, la nozione di Cyber-Physical Security è diventata essenziale.

La promozione del concetto di Cyber-Physical Security (o Sicurezza Cyber-fisica), oggetto di questo Libro Bianco, rappresenta una risposta ragionevole e critica alla minaccia odierna. È stato redatto da esperti di tutto il mondo sotto l'egida dell'International Security Ligue e della Confederazione dei Servizi di Sicurezza Europei (CoESS), unendo le forze per proteggere le persone, le organizzazioni e le infrastrutture dagli attacchi combinati che continueranno ad accadere, purtroppo.

Sezione I.
Cyber-Physical Security

A. Introduzione - Creare connessioni

Questo Libro Bianco, progetto congiunto dell'International Security Ligue e della Confederazione dei Servizi di Sicurezza Europei (CoESS), si propone di contribuire a rafforzare le infrastrutture critiche mondiali in un periodo di crescente complessità e di aumento delle minacce.

È suddiviso in due sezioni. La sezione I fornisce un quadro di riferimento e un contesto sulla lotta per la protezione delle infrastrutture critiche (IC). Il documento esplora il significato di IC, le ramificazioni dei sistemi connessi, l'aumento delle minacce cyber-fisiche ed esplora la convergenza della sicurezza per contrastarle.

La Sezione II esamina in modo più approfondito specifiche questioni di Cyber-Physical Security, fornendo una guida per l'elaborazione di soluzioni complete alle sfide attuali e future.

Perché questo libro? Perché ora?

Le infrastrutture critiche del mondo sono un obiettivo più importante e più vulnerabile che mai, il che richiede un approccio globale alla protezione che allinei la sicurezza fisica e quella informatica. Ora che molte minacce e soluzioni tecnologiche si intersecano tra le due discipline, è naturale che la missione di protezione debba subire una trasformazione.
È in gioco la sicurezza delle nazioni e dei cittadini. Considerato l'attuale contesto di minacce, il mondo richiede una maggiore attenzione da parte del governo e del settore privato ai problemi di sicurezza; ed investimenti costanti nelle soluzioni. Richiede inoltre la collaborazione tra le due entità.

"Una maggiore collaborazione e partnership tra il settore pubblico e quello privato è senza dubbio la direzione da seguire. Non possiamo

permetterci il lusso di non concentrarci più sulla difesa collettiva. Dobbiamo considerarlo uno sport di squadra", ha spiegato Jen Easterly, direttore dell'Agenzia statunitense per la sicurezza informatica e delle infrastrutture, rivolgendosi ai leader economici del mondo a Davos 2022.

"In fin dei conti, non è un problema che risolveremo noi. Si tratta di un problema persistente, su cui dovremo lavorare tutti insieme in tutto il mondo".

Le minacce alla sicurezza che le infrastrutture critiche devono affrontare oggi non sono di tipo informatico o fisico: sono entrambe. E, altrettanto spesso, le contromisure non sono né l'una né l'altra. Ma questa convergenza non ha stimolato una grande rivoluzione nelle modalità di gestione della sicurezza.

La collaborazione è imperativa all'interno di strutture critiche, dove in genere esiste una complicata suddivisione delle responsabilità per i diversi aspetti della protezione. Ora potrebbe essere insufficiente, dato che l'entità delle minacce è cresciuta e le minacce si sovrappongono, affrontare la sicurezza solo a livello funzionale, gestire le minacce ed impiegare le contromisure reparto per reparto. È necessaria una cooperazione a tutti i livelli, con le principali parti interessate che lavorano insieme per sostenere la sicurezza generale e con una comprensione collettiva di ciò che è più critico da proteggere.

La posta in gioco è alta e le soluzioni devono essere complete e orientate al processo, in grado di combattere le minacce attuali e di fornire una piattaforma per quelle future. La sicurezza delle infrastrutture critiche non è una soluzione che può essere implementata, è un processo che deve essere alimentato e che richiede denaro, impegno, pianificazione strategica a lungo termine e una visione olistica.

B. Definizione delle infrastrutture critiche e dei bisogni di protezione

Che cos'è un'infrastruttura critica? Il termine è altamente descrittivo e allo stesso tempo ambiguo.

Le infrastrutture critiche sono generalmente considerate come i beni fondamentali di cui le nazioni hanno bisogno per far funzionare le società; i sistemi che sono alla base di ciò di cui le persone hanno bisogno per vivere e le aziende per operare. Questi sono i cespiti e i sistemi che, se distrutti o interrotti, avrebbero un impatto negativo sulla vita delle imprese. Un impatto debilitante sulla sicurezza, sull'economia, sulla salute e sulla salvaguardia di una nazione. In poche parole, è il fondamento della civiltà e il punto di partenza per la prosperità.
Il termine si è evoluto. A causa dei progressi tecnologici e della crescente preoccupazione che le infrastrutture critiche possano essere oggetto di attacco, si è assistito a un ampliamento del contesto in cui vengono considerate le infrastrutture critiche. Oltre a garantire semplicemente l'adeguatezza delle opere pubbliche, le infrastrutture critiche sono ora osservate nel contesto della sicurezza nazionale. In generale, ciò ha ampliato il numero di settori infrastrutturali e di tipologie di beni riconosciuti come critici.

Ma quali settori debbano esattamente rientrare nella definizione di infrastruttura critica è un'area grigia, che si riflette nella disparità globale dei settori e dei beni che le nazioni includono in tale definizione.
Alcuni settori sono ampiamente e storica-

mente inclusi, come i sistemi idrici e l'energia; altri sono stati aggiunti più di recente, come l'IT e le telecomunicazioni; e altri beni sono fondamentali ma non sempre inclusi, come ospedali e banche.
Inoltre, i settori delle infrastrutture critiche contengono molti beni fisici con diversi livelli di importanza e l'identificazione di quelli che dovrebbero essere considerati critici è un fattore che complica il raggiungimento della "giusta" definizione.
Secondo Jen Easterly, direttore dell'Agenzia statunitense per la sicurezza informatica e delle infrastrutture, il numero di settori industriali che dovrebbero essere inclusi nella discussione globale sulle infrastrutture critiche deve essere ampliato. Il settore delle comunicazioni ne è un esempio: pur non rientrando sempre tra le infrastrutture critiche è una parte integrante dell'economia di ogni paese, alla base delle operazioni di tutte le imprese, organizzazioni di pubblica sicurezza e governo. **"Le infrastrutture critiche sono le reti, i sistemi e i dati su cui facciamo affidamento ogni ora di ogni giorno, e cioè l'acqua, l'energia, le telecomunicazioni, l'assistenza sanitaria, i trasporti: sono tutte quelle cose che sostengono le nostre vite quotidiane",** ha spiegato a Davos 2022.

La definizione di "infrastruttura critica" adottata dalle nazioni è significativa. Soprattutto, orienta e concentra le strategie di sicurezza dei governi e la spesa per le attività di protezione. Le nazioni impiegano maggiori energie e risorse per proteggere le risorse ritenute critiche.
La definizione è importante anche perché molte infrastrutture critiche sono di proprietà privata.
In molti paesi, il settore privato possiede la maggior parte delle infrastrutture critiche, con fino all'85% di tutte le infrastrutture critiche in mani private, il che significa che la vulnerabilità delle nazioni è in gran parte fuori dal loro controllo immediato. Pertanto, la definizione di infrastruttura critica è cruciale perché:

- può incoraggiare questi operatori a riconoscere la criticità del loro ruolo nella società e la necessità di investire nella protezione per il bene del paese e dei suoi cittadini;
- facilita la condivisione di informazioni sulla sicurezza tra l'industria privata e governi, che è fondamentale per aumentare la consapevolezza delle vulnerabilità e affrontarle; e
- funziona come base per l'imposizione degli obblighi di sicurezza del governo, compresi i requisiti di protezione, su infrastrutture che sono in gran parte private.

Le infrastrutture critiche sono gli elementi essenziali che consentono alle persone di vivere la loro vita quotidiana, e i governi devono definire il termine di conseguenza. Le infrastrutture critiche comprendono più settori commerciali di quanto comunemente riconosciuto, un fatto che i governi devono riconoscere se vogliono rafforzare la sicurezza delle nazioni e garantire la resilienza delle società.

- La definizione di "infrastruttura critica" è importante e influenza la definizione delle priorità di sicurezza, l'allocazione delle risorse e la regolamentazione.
- Il numero di settori industriali che fanno parte della discussione globale sulle infrastrutture critiche è destinato ad espandersi.

C. Ambienti operativi connessi

Mentre le infrastrutture critiche sono le fondamenta che permettono alle persone di condurre la loro vita quotidiana, i sistemi connessi sono alla base di molte delle infrastrutture critiche che fanno funzionare le nazioni. C'è una crescente interconnessione di tutto ciò su cui le persone fanno affidamento, dalla fornitura di elettricità ai servizi finanziari.
L'efficienza spinge a collegare rapidamente i sistemi, consentendo l'automazione e una maggiore produttività, funzionalità migliorate e costi più bassi. Le aziende considerano la connettività come un fattore di differenziazione competitiva, alimentando un'accelerazione del processo.
Non si tratta di attirare solo i gestori privati di infrastrutture critiche, ma anche i governi. Isolare i sistemi informatici e fisici l'uno dall'altro significa perdere l'opportunità di ridurre l'inquinamento, di diminuire il consumo energetico e di tenere il passo in un mondo sempre più digitalizzato e connesso. La connettività digitale consente alle nazioni di gestire popolazioni in crescita e di soddisfare le richieste di standard di vita più elevati.
Ad alimentare questa rivoluzione sono internet, l'Internet delle cose (IoT) e il suo sottoinsieme, l'Industrial Internet of Things (IIoT), e le relative tecnologie di connettività wireless come il 5G e il Wi-Fi. Secondo stime prudenti, sono oltre 30 miliardi i sensori, le piattaforme e i dispositivi che compongono questa vasta rete di confluenza e condivisione di dati.
IoT è un termine generico che si riferisce all'insieme di oggetti fisici presenti nell'ambiente - computer, dispositivi, elettrodomestici, vei-

coli, dispositivi indossabili, sensori e così via - che contengono tecnologia incorporata per comunicare tra loro e trasmettere dati. È visibile nelle fabbriche che utilizzano sensori per tracciare con maggiore precisione i materiali e coordinare la logistica della catena di approvvigionamento; nelle persone che indossano dispositivi per monitorare le attività, la salute e la forma fisica; nelle aziende minerarie che utilizzano attrezzature pesanti controllate a distanza per poter operare in modo più efficiente in luoghi isolati e pericolosi senza mettere a repentaglio l'incolumità dei lavoratori; ai distributori di asciugamani di carta per i bagni che segnalano quando devono essere riempiti. Gli esperti prevedono un futuro in cui quasi tutto è un nodo di una rete, e il futuro è ben avviato.

Molte delle stesse tecnologie che collegano le persone, le case e le aziende, sono utilizzate dalle infrastrutture critiche e negli ambienti industriali (IIoT), per scopi simili. Gli operatori di infrastrutture critiche stanno adottando sistemi connessi per migliorare la produttività e l'efficienza. I dispositivi tradizionalmente isolati di supervisione, di acquisizione dati e i sistemi di controllo industriale utilizzano ora l'IIoT per trasmettere i dati, dalle centrali elettriche agli impianti di trattamento delle acque.

È ormai comunemente richiesto che i computer e le altre tecnologie siano integrati nella progettazione e nel funzionamento delle infrastrutture fisiche. I computer sono stati da tempo incorporati in numerosi sistemi fisici, come i veicoli, i sistemi di riscaldamento e raffreddamento e i dispositivi di produzione, e ora sono integrati nelle infrastrutture fisiche, come si può osservare chiaramente nello sviluppo della tecnologia smart grid, in cui i computer e le tecnologie di comunicazione in rete lavorano autonomamente per risolvere i problemi della rete elettrica, gestire l'uso dell'energia e amministrare la produzione di elettricità. Il controllo automatizzato del traffico è diventata parte integrante delle infrastrutture di trasporto e i sistemi idrici "intelligenti" monitorano in modo proattivo lo stato di salute della propria infrastruttura fisica.

In futuro, il 5G e altre tecnologie a banda larga mobile potenziate faciliteranno ulteriormente le applicazioni nelle infrastrutture critiche e l'intelligenza artificiale consentirà progressi incalcolabili nell'uso efficiente dei dati dei sensori, per capire perché un'apparecchiatura si è guastata, ad esempio, o per aiutare a localizzare ed estrarre risorse naturali, o facilitare una rapida risposta alle emergenze.

La connettività delle infrastrutture critiche costituisce la base su cui saranno costruite le future "città intelligenti".

Tra i casi d'uso attuali e previsti vi sono:

- Sistemi più intelligenti, come i sistemi di riscaldamento e raffreddamento che migliorano la qualità dell'aria e riducono il consumo energetico.
- Macchine industriali in grado di raccogliere informazioni su prestazioni e avvisano quando è necessaria la manutenzione o la pulizia, riducendo così i tempi di manutenzione o di inattività non programmati.
- Sensori in grado di allertare i produttori agricoli sulle condizioni del suolo che aiutano a gestire le risorse idriche e ad aumentare la resa delle colture, oppure strade, ponti e linee ferroviarie sensorizzate che segnalano il loro stato di usura e avvisano quando hanno bisogno di riparazioni.

Gran parte del futuro progresso umano deriverà dall'utilizzo di dati provenienti da sistemi connessi. Tuttavia, questa connettività porta con sé un cambiamento epocale. In particolare, la fine della separazione tra reti informatiche e sistemi fisici, tra tecnologia operativa e tecnologia dell'informazione. Al suo posto c'è una rete complessa e interconnessa di sistemi cyber-fisici che fungono da base per le infrastrutture critiche del mondo, supportando o fornendo servizi infrastrutturali, e le basi per il futuro progresso delle società.

"Gran parte dei progressi futuri deriveranno dall'utilizzo dei dati provenienti dai sistemi connessi. Questo significherà la fine della separazione tra reti informatiche e sistemi fisici, tra OT e IT".

- La divisione tra sistemi fisici e informatici viene cancellata e sostituita da una rete interconnessa di sistemi cyber-fisici.
- I sistemi connessi consentono una maggiore produttività e capacità potenziate e servirà da base per il futuro progresso umano.

D- Minacce e vulnerabilità Cyber-fisiche

La connettività ha un costo

Sebbene i vantaggi derivanti dall'aggregazione e dall'analisi dei dati provenienti da più endpoints siano innumerevoli, quando i dispositivi sul campo comunicano con i data center della rete e i sistemi informatici sono connessi ad internet, la superficie di attacco si espande in modo esponenziale.
Con i sistemi connessi, il perimetro di sicurezza di un'azienda si estende ai dispositivi che operano al di fuori dei luoghi protetti e che possono collegarsi ai suoi sistemi critici. **La connettività evidenzia il fatto che le attività legate alla difesa sono collegate tra loro, e ciascuna rappresenta uno degli anelli di una catena. E, come ogni catena, è forte solo quanto il suo anello più debole.**

La minaccia di attacchi internet ai sistemi fisici degli operatori di infrastrutture critiche è cresciuta: le reti SCADA (controllo di supervisione e acquisizione dati) sono diventate più vulnerabili quando i gestori di questi sistemi, un tempo chiusi, hanno iniziato a consentirne l'accesso da computer con accesso a internet.
Questo può essere un problema soprattutto per le infrastrutture critiche più vecchie, hanno avvertito i relatori a Davos 2022. I sistemi di infrastrutture critiche obsolete che vengono aperti alla comunicazione e spinti verso il cloud potrebbero scontrarsi con le crescenti tensioni geopolitiche di oggi, con conseguenze devastanti per le società.
Dai recenti attacchi ai sistemi idrici israeliani e alle reti elettriche in India e Ucraina, i leader

mondiali hanno avvertito che le infrastrutture critiche sono un bersaglio maggiore e più vulnerabile che mai.
I dispositivi connessi all'interno delle infrastrutture critiche rappresentano un rischio in quanto introducono nuove vie per il potenziale sfruttamento remoto delle reti aziendali, con l'infrastruttura utilizzata per abilitare i dispositivi IoT che sfugge al controllo dell'operatore. Qualsiasi mancanza nella gestione dei dispositivi IoT, che può lasciare i dispositivi non monitorati e non protetti, rappresenta una vulnerabilità che può essere attaccata. Inoltre, con i sistemi connessi, qualsiasi strada all'interno della rete può potenzialmente portare a uno scenario catastrofico.
La maggior parte dei dispositivi IoT connessi all'azienda sono a loro volta connessi ad internet, per consentire ai fornitori di installare aggiornamenti, ad esempio. Gli autori di attacchi, utilizzando strumenti di scansione standard, possono trovare questi dispositivi e ci sono persino strumenti di ricerca che li aiutano (una sorta di Google per gli hacker IoT). Una volta trovati, connettersi a questi dispositivi e violarli tende a essere facile. Spesso non hanno alcuna protezione integrata, funzionano con sistemi operativi obsoleti, hanno password predefinite deboli e sono difficili da proteggere. **Anche se un dispositivo non è di per sé strategicamente importante, può fornire agli intrusi una via d'accesso ai sistemi che lo sono. Una vulnerabilità in un singolo dispositivo o database può compromettere intere reti e operazioni.**
La consapevolezza del rischio derivante dai dispositivi IoT è certamente cresciuta, ma la minaccia non è diminuita. In media, c'è ancora un ritardo considerevole (di parecchi mesi) tra l'annuncio di una vulnerabilità, la pubblicazione di una patch e la messa in sicurezza del dispositivo. Nel frattempo, gli hacker hanno migliorato la loro capacità di sfruttare questa lacuna.
Una tipica azienda di 5.000 dipendenti potrebbe avere fino a 20.000 dispositivi IoT e la penetrazione di dispositivi IoT è ormai significativa in tutti i settori, compresi quelli altamente regolamentati o che gestiscono dati sensibili e che possono essere considerati infrastrutture critiche, come la sanità, le infrastrutture energetiche, la pubblica amministrazione e i servizi finanziari. La presenza dell'IoT all'interno di questi settori è un motivo di preoccupazione, soprattutto alla luce di studi che suggeriscono un'incomprensione dei rischi dell'IoT e un'impreparazione a gestirli.
Se da un lato aumentano l'efficienza operativa e contribuiscono a spostare le operazioni nel mondo digitale, dall'altro qualsiasi dispositivo connesso diventa parte delle loro reti e porta con sé rischi per la sicurezza. Ad esempio, i dispositivi connessi utilizzano spesso il beaconing, ossia l'uso ripetuto della loro connettività per chiamare "casa", per una serie di motivi. Sebbene non sia intrinsecamente dannoso, rappresenta un rischio per l'operatore del dispositivo. Gli aggressori possono potenzialmente monitorare tali dispositivi per verificare l'attività di rete ed esaminare gli abitudini degli utilizzatori, e essere presi di mira se viene scoperta una crepa specifica nel dispositivo.
La sicurezza dei dati in transito dai dispositivi di campo al cloud è una priorità fondamentale, ma gli operatori devono anche essere certi che il cloud che gestisce i dati sia sicuro e che il dispositivo stesso sia sicuro. La sicurezza fisica è una parte fondamentale della sicurezza della rete e, a meno che non esista un protocollo rigoroso per adattare la sicurezza fisica man mano che vengono aggiunti dispositivi e i sistemi vengono riprogettati o riconfigurati (come spesso accade), anche le risorse di rete più fortificate possono diventare rapidamente vulnerabili.
I sistemi connessi e la crescente proliferazione di dispositivi IoT in ambienti come l'assistenza sanitaria e altre infrastrutture critiche offrono ai malintenzionati nuove possibilità di creare scompiglio o rubare dati. Gli attacchi contro i dispositivi IoT sono già comuni, dalle telecamere IP con controlli di sicurezza deboli ai contatori intelligenti con difetti di crittografia di base. I produttori di dispositivi non sempre progettano controlli di sicurezza nei loro dispositivi e, ad oggi, la fretta di distribuire i dispositivi IoT su larga scala sembra superare la preoccupazione per le loro implicazioni

in termini di sicurezza. L'Unione Europea sta lavorando a una legislazione per rendere l'IoT più sicuro (il futuro "Cyber Resilience Act") ma prima della sua adozione saranno stati immessi sul mercato molti oggetti che non saranno soggetti a questa legge.

Il problema è che molti dispositivi IoT non sono gestiti. Sono connessi alle reti, ma al di fuori della possibilità di controllo, o addirittura di visione, da parte di un operatore. Una ricerca di questi dispositivi all'interno di un sistema di gestione della sicurezza potrebbe anche non scoprirne l'esistenza.

L'esistenza di una vasta rete di dispositivi connessi nascosti solleva numerosi problemi di privacy e di sicurezza, e le persone interessate alla sicurezza devono aspettarsi che, con l'esplosione del numero di dispositivi connessi, molti di essi saranno vulnerabili agli attacchi e soggetti a conseguenze indesiderate. La segmentazione, insieme a una solida infrastruttura di rete e a politiche e procedure efficaci, può aiutare le infrastrutture critiche a resistere alla minaccia rappresentata dall'IoT, ma è possibile solo se tutti gli endpoint sono mappati e gestiti.

La connettività offre molti vantaggi, ma molte cose possono andare storte. Studi globali sulle aziende del settore energetico e dei servizi pubblici rivelano che la maggior parte di esse ha subito almeno una violazione nell'ultimo anno. Inoltre, suggeriscono una mancanza di preparazione. La maggior parte degli operatori di infrastrutture critiche non si preoccupa attivamente di individuare le minacce avanzate e persistenti, non utilizza tecnologie all'avanguardia per bloccare gli attacchi ai sistemi SCADA e si affida a una strategia di sicurezza SCADA reattiva, anziché proattiva.

Oggi è possibile distruggere un'infrastruttura premendo un pulsante, questo è il livello di criticità di cui stiamo discutendo", ha spiegato il consulente economico Pranjal Sharma, ospite di una tavola rotonda sulla sicurezza delle infrastrutture critiche di importanza sistemica al World Economic Forum Annual Meeting di Davos, Svizzera.

"Si tratta di una sfida comune a tutti i governi, a tutte le società e a chiunque si occupi di infrastrutture".

- I dispositivi connessi hanno mostrato una serie di vulnerabilità nella comunicazione e in altri componenti che li rendono suscettibili di attacchi remoti.
- L'esplosione del numero di dispositivi aggiunti ai sistemi in rete sta moltiplicando esponenzialmente i rischi per la sicurezza e aumentando il numero di modi in cui gli aggressori possono entrare nei sistemi cyber-fisici.
- Con la connettività, la superficie delle minacce si estende al di fuori dei luoghi protetti e può collegarsi a sistemi operativi e fisici critici.

E. Minacce "ibride" o "miste"

Immaginate gli hacker di rete che scaricano milioni di litri di acque reflue a migliaia di chilometri di distanza manomettendo le valvole controllate da remoto tramite IP. Oppure la debole sicurezza fisica di un edificio, combinata con la connettività delle postazioni di lavoro non occupate, che offre a un avversario un'opportunità economica, efficace e anonima di violare la rete di distribuzione di un'azienda energetica.

Queste minacce, nate dal collegamento in rete delle infrastrutture critiche, possono assumere diversi nomi, tra cui minacce convergenti, ibride o miste. **Esse derivano da penetrazioni fisiche non autorizzate che portano alla violazione di informazioni o di sistemi operativi, oppure da hacking di rete che creano un danno fisico.**

Mentre alcuni scenari fantasiosi sono strettamente legati alle trame dei film, come l'hackeraggio a distanza del dispositivo pacemaker di un primo ministro, gli attacchi connessi sono reali e rappresentano un rischio crescente. Gruppi estremisti e attivisti discutono attivamente sull'utilizzo di attacchi misti contro le infrastrutture critiche, tra cui impianti energetici e di pubblica utilità, sistemi di trasporto ed edifici aziendali; tra gli obiettivi interessanti vi sono i sistemi vitali, come quelli degli impianti che regolano valvole, temperatura e pressione.

La crescente tendenza a collegare i sistemi di controllo industriale ad altre reti è una delle principali preoccupazioni legate alla sicu-

rezza informatica delle infrastrutture critiche e il rischio è stato messo in evidenza sia da esempi reali di attacchi interconnessi, sia da test di sicurezza, come quello condotto in Australia dal più grande fornitore di tecnologia del mondo.

Nello scenario del test, i ricercatori si sono introdotti nella gestione operativa della sede dell'azienda, da cui hanno potuto accedere a numerosi pannelli di controllo, compresi quelli denominati "allarmi attivi" e "console di allarme "e hanno facilmente decifrato le password criptate dei dipendenti, comprese quelle degli amministratori. Gli intrusi hanno potuto vedere praticamente tutto dell'edificio, dalle planimetrie alla disposizione delle tubature dell'acqua, e se l'attacco fosse stato malevolo avrebbero potuto installare malware per ottenere l'accesso ad altri sistemi di controllo degli edifici collegati a quello compromesso. Il tutto sfruttando un'unica vulnerabilità non protetta nella piattaforma del sistema di gestione dell'edificio.

Gli esempi nel mondo reale sono numerosi: nel 2017, un virus è penetrato nella rete della più grande compagnia di trasporto marittimo di container al mondo attraverso il software di contabilità obsoleto di un singolo computer, causando l'interruzione delle operazioni di ospedali, aziende elettriche, aeroporti, banche e agenzie governative e paralizzando l'industria del trasporto marittimo globale per oltre una settimana. Nel 2019, gli hacker hanno sfruttato una vulnerabilità del firmware per causare il riavvio continuo del firewall di un operatore della rete elettrica, con conseguente interruzione delle comunicazioni. Nel giugno 2020, un gruppo di 19 vulnerabilità note come Ripple20 ha colpito milioni di dispositivi connessi, tra cui dispositivi domestici intelligenti, apparecchiature della rete elettrica, sistemi sanitari, apparecchiature industriali, sistemi di trasporto, apparecchiature di comunicazione mobile e satellitare e dispositivi di aerei commerciali.

I test di penetrazione spesso evidenziano l'attenzione immediata che le minacce convergenti meritano. In un caso, ad esempio, un'azienda di servizi pubblici ha ingaggiato un Red Team per valutare se i suoi sistemi fisici potessero essere vulnerabili a un attacco di rete. I ricercatori hanno scavato nelle liste di distribuzione dell'organizzazione per ottenere gli indirizzi e-mail dei dipendenti che avevano accesso alle reti di supervisione, controllo e acquisizione dati (SCADA) e hanno inviato loro e-mail su una potenziale riduzione di benefici. Diversi destinatari hanno cliccato su un link a un sito Web che prometteva ulteriori informazioni al riguardo, che ha scaricato sul computer dell'utente un malware che ha dato al Red Team la possibilità di prenderne il controllo. In meno di un giorno, la società di servizi ha visto come gli autori di attacchi potevano ottenere l'accesso per interrompere, danneggiare o alterare la produzione e la distribuzione di energia di un'intera regione. In un secondo test, i ricercatori, fingendosi addetti alla manutenzione, sono riusciti ad entrare in una struttura controllata e ad accedere a un computer connesso ma non presidiato, dal quale avrebbero potuto sferrare qualsiasi tipo di attacco.

A complicare il quadro della sicurezza c'è il fatto che **la maggior parte degli operatori di infrastrutture critiche ammette di non essere sicuro di aver mai subito una violazione della sicurezza fisica che ha portato a un attacco alla rete o un attacco alla rete che ha causato un'interruzione del mondo fisico.** Questa incertezza è probabilmente una delle ragioni per cui i responsabili della sicurezza, sia dal lato fisico che da quello informatico, non sono riusciti ad affrontare in modo esaustivo le minacce.

Cosa potrebbe comportare un attacco connesso?

I ricercatori che studiano le possibili conseguenze strategiche ed economiche degli attacchi alle infrastrutture critiche spesso esprimono la preoccupazione che gli operatori non abbiano una capacità di elaborazione creativa e una determinazione analoga a quella degli avversari. Mentre le infrastrutture critiche hanno fatto molto per rafforzare sia la sicurezza fisica che i sistemi di rete, per resistere ai danni che hacker occasionali o giovani facinorosi potrebbero infliggere, è stata

prestata poca attenzione alla protezione da schemi più insidiosi che gli aggressori determinati potrebbero escogitare.
Molte di queste vulnerabilità riguardano strategie di attacco e aspetti dei sistemi informatici che in precedenza non sembravano particolarmente importanti dal punto di vista della sicurezza. Ad esempio, la maggior parte delle difese delle reti informatiche mira a proteggere le informazioni finanziarie e personali durante le trasmissioni via Internet; ma i terroristi, ad esempio, sono più propensi a condurre attacchi fantasiosi su dati stabili. Tali attacchi potrebbero passare inosservati per diverse settimane e sono progettati per massimizzare i danni reali dell'infiltrazione informatica.
L'accesso fisico non autorizzato ai server di rete è forse l'esempio più classico di minaccia ibrida e, sebbene oggi la maggior parte dei server sia ben protetta, con forti controlli sull'accesso fisico, le falle nella sicurezza persistono e la protezione deve essere continuamente aggiornata per far fronte alle nuove minacce. Data la loro criticità, è necessario implementare soluzioni di sicurezza forti per limitare l'accesso fisico ai locali dei server, ad esempio richiedendo un'autenticazione a due o tre fattori, compresa la biometria, e i controlli devono essere mantenuti attraverso test di penetrazione fisica delle sale dei server di rete e di altri luoghi contenenti componenti di rete critici, come gli armadi di cablaggio di rete.
Il fatto che la soluzione della continuità nella sicurezza fisica possa diventare un vettore della minaccia ne esemplifica ulteriormente la pericolosità. Anche se sono progettati per fornire protezione, i dispositivi di sicurezza connessi possono creare vulnerabilità di rete critiche. Ad esempio, una tipica ricerca rivela l'esistenza di quasi 300.000 telecamere di sorveglianza collegate a internet.
Quando i dispositivi di sicurezza, come le telecamere di videosorveglianza o i pannelli di controllo degli accessi, sono collegati alla rete di un'organizzazione, gli attacchi denial-of-service (DoS) contro la rete possono rendere inutilizzabili tali sistemi e dispositivi, oppure gli aggressori remoti possono potenzialmente ottenere un accesso non autorizzato ad essi e funzionare come utenti autorizzati. **L'attacco alla rete può avere conseguenze reali, con gli aggressori che possono usarli come trampolino di lancio per attaccare i sistemi di controllo industriale o per rendere possibile l'infiltrazione fisica in un ambito di infrastruttura critica.**
Gli operatori delle infrastrutture critiche devono valutare se le loro difese di rete sono eccessivamente focalizzate su singole minacce e vulnerabilità banali e se le strategie devono essere ampliate per proteggere da minacce creative miste.

Queste possono includere:

- Inserimento di malware per alterare le specifiche di fabbricazione e
- altri processi aziendali. Ad esempio, un attacco a un produttore critico potrebbe avere come conseguenza macchine che prendono fuoco dopo essere rimaste in funzione per un determinato periodo di tempo, o prodotti difettosi.
- Alterare le informazioni per provocare isteria nell'opinione pubblica. Gli avversari potrebbero prendere di mira qualsiasi sistema sensibile nel settore sanitario, ad esempio per alterare i dati medici come i dosaggi o i programmi di trattamento. E poi annunciarlo al pubblico per diffondere panico e sconvolgere i mercati finanziari.
- Ottenere l'accesso fisico ai sistemi per alterare i codici e creare il caos pubblico.
- In un caso reale, hacker si sono infiltrati nel sistema semaforico di una città, hanno manipolato i codici di programmazione e hanno causato pericolosi rallentamenti del traffico in tutta la città.
- Compromettere le stazioni di ricarica vulnerabili dei veicoli elettrici per mettere in crisi la rete energetica più ampia.

La tecnologia interconnessa è un vettore di minaccia per gli attacchi convergenti alle in-

frastrutture critiche; e la vulnerabilità deriva principalmente dall'incapacità delle infrastrutture critiche globali di esaminare come si intersecano le minacce fisiche alla sicurezza informatica. I trasformatori collegati in rete, per esempio, sono progettati per resistere a rischi operativi come fulmini, uragani e fluttuazioni dell'alimentazione di rete, ma sono estremamente vulnerabili agli attacchi fisici intenzionali. **I security manager di entrambe le discipline della sicurezza - informatica e fisica - devono esaminare come le vulnerabilità della sicurezza fisica possano provocare violazioni del sistema e come gli attacchi informatici possano creare danni fisici.**
Gli operatori delle infrastrutture critiche devono fare di più per tenere conto della crescente portata delle minacce emergenti e della combinazione di minacce fisiche e di Cybersecurity.
Sebbene le minacce miste cyber-fisiche non siano nuove, gran parte delle infrastrutture critiche mondiali non sono preparate a gestire minacce cosi stratificate. Ogni volta vengono scoperte enormi vulnerabilità in aziende di infrastrutture critiche che affermano di essere pienamente conformi a tutti gli standard esistenti.

- La tendenza a collegare i sistemi di controllo industriale ad altre reti è una delle principali preoccupazioni per la sicurezza delle infrastrutture critiche.
- Un'intrusione fisica o di rete può creare uno scompiglio incalcolabile, dal controllo di interi sistemi di edifici intelligenti, all'interruzione dei servizi di base di cui le società hanno bisogno per funzionare.
- Le minacce fisiche e quelle della sicurezza informatica oramai si intersecano: la vulnerabilità in un'area fornisce agli aggressori un mezzo per recare danni all'altra.

OBIETTIVI	VULNERABILITÀ	OPPORTUNITÀ
Distruggere o perturbare le infrastrutture critiche ha conseguenze debilitanti nella sicurezza, l'economia, la salute o la salvaguardia di una nazione.	Sistemi e tecnologie interconnesse forniscono un'ampia e vulnerabile superficie di attacco.	Gestione della Sicurezza a compartimenti stagni Crea lacune nella sicurezza che possono essere sfruttate.

F. Vulnerabilità nella gestione della Sicurezza a compartimenti stagni (silos)

Quando due cose vengono unite per formare un nuovo insieme, il punto più debole è spesso la colla che tiene insieme le due metà. Questo è un aspetto che i criminali sanno e sfruttano, quindi è comprensibile il motivo per cui le minacce miste/ibride sono diventate una fonte primaria di debolezza della sicurezza nelle infrastrutture critiche mondiali. Inoltre, è il motivo per cui i silos di responsabilità della sicurezza che esistono nelle infrastrutture critiche sono la causa principale di vulnerabilità non riconosciute e di minacce non mitigate.

La sicurezza è un mosaico: comprende la sicurezza fisica, la sicurezza operativa, la sicurezza informatica e sottoinsiemi come la sicurezza delle persone e la risposta alle crisi. Un gruppo può essere responsabile della protezione dei dipendenti e dei visitatori, mentre un altro della gestione delle strutture, un altro ancora della sicurezza delle persone; poi un altro effettua pattugliamenti, indaga sui reati e risponde agli incidenti.

Le minacce alla sicurezza delle infrastrutture critiche si intersecano con tutte queste discipline e con altre. Un fatto che è generalmente compreso; tuttavia l'obiettivo di una gestione olistica della sicurezza non è stato raggiunto da molti gestori di infrastrutture. Perché?

Alla radice del problema ci sono i silos della sicurezza, ed è facile comprendere come si siano evoluti. Si è assistito a una rapida espansione del tipo di risorse da proteggere, dai tradizionali asset fisici a quelli intangibili,

come informazioni, dati e reputazione. Con la formazione di nuovi requisiti di protezione, sono stati creati nuovi team per sviluppare strategie ed implementare soluzioni. Ma quando si sono formati i nuovi team, in genere si sono concentrati solo sull'area emergente del rischio e hanno elaborato strategie indipendenti dalle altre funzioni di sicurezza e senza tenere conto del loro allineamento con le strategie esistenti, comprese quelle dei team che sovrintendono alla sicurezza fisica. Ognuno affrontava la propria parte di rischio senza pensare a come l'intero "puzzle della sicurezza" si componeva.
È necessario eliminare le barriere tra le funzioni di sicurezza, poiché la vulnerabilità risiede spesso nella mancanza di coordinamento tra i vari gestori della sicurezza, tra cui la sicurezza fisica, l'IT e altri. Inoltre, i limiti di un anello debole in un sistema connesso possono riverberarsi su tutte le sue parti; un fatto che sottolinea la necessità di tenere conto delle interdipendenze nelle discipline di protezione.
Per rafforzare lo scudo protettivo contro le minacce alla sicurezza, tutti i reparti che svolgono attività di riduzione dei rischi devono collaborare più strettamente, cosa che decenni di "sicurezza isolata" rendono difficile.

Quali sono alcuni degli ostacoli?

- La prospettiva è spesso al centro dei problemi. A seconda delle aree funzionali in cui gli operatori lavorano, l'idea stessa di cosa significhi "sicurezza" varia, complicando la capacità di creare una visione più ampia della sicurezza che la sostituisca. La creazione di una nuova mentalità – in modo che quando le organizzazioni pensano alla strategia di sicurezza, si possa pensare ad ampio spettro a ciò che essa significa - richiede nuovi approcci.
- Le soluzioni per la sicurezza fisica, operativa e informatica sono spesso molto diverse tra loro, con differenze di progettazione, funzionalità, implementazione, manutenzione e gestione.
- L'abbattimento dei silos di sicurezza è una sfida dalle molte sfaccettature che comprende questioni tecniche, organizzative e di competenze. Ad esempio, quando all'infrastruttura IT vengono aggiunti sistemi o dispositivi speciali, il proprietario o l'utente finale devono assicurarsi che le informazioni necessarie siano fornite al personale esperto del sistema, affinché possano essere di aiuto per l'integrazione nell'infrastruttura IT e quali figure saranno necessarie per la gestione dei sistemi, le connessioni e i processi di modifica.
- Possono mancare le persone chiave per portare avanti i progetti di connettività. Mentre Il personale addetto ai progetti cyber-fisici può concentrarsi doverosamente sui propri aspetti, spesso manca un'analisi di ampio respiro su come massimizzare i benefici e minimizzare i rischi derivanti dalla connessione di vari sistemi e dispositivi speciali. Oppure i rischi possono rimanere irrisolti perché coloro che fanno la formazione sui sistemi non sono ben preparati sui rischi derivanti dalle minacce ibride.
- Quando non si capisce chi è responsabile per quali dati e processi relativi a sistemi connessi ed integrati, possono essere vanificati aspetti importanti della pianificazione che potrebbero contribuire a collegare diverse aree funzionali.
- Se i diversi dipartimenti resistono al coordinamento per paura di perdere potere (guerre per il territorio), può essere impossibile raggiungere una cooperazione sulle questioni di sicurezza.

È ormai assodato che i criminali hanno bisogno di moventi, mezzi e opportunità. **Mentre i sistemi connessi forniscono agli aggressori motivati i mezzi per condurre attacchi ibridi alle infrastrutture critiche, sono le funzioni di sicurezza isolate a fornire l'opportunità: le vulnerabilità e le lacune nella sicurezza emergono quando la sicurezza fisica e quel-**

la informatica sono gestite in modo isolato l'una dall'altra. Pertanto, non c'è niente di più importante per la sicurezza delle infrastrutture critiche del mondo che evolvere verso un approccio più sistematico e completo alla prioritizzazione e alla protezione delle risorse.

- I silos della sicurezza, in cui gli aspetti della sicurezza sono gestiti in modo isolato, rimangono una debolezza diffusa.
- La vulnerabilità risiede spesso nella mancanza di coordinamento tra i vari responsabili della sicurezza.
- Affrontare il rischio di minacce ibride richiede uno sforzo dedicato per poter abbattere e superare gli ostacoli al coordinamento derivanti dalla gestione della sicurezza isolata.

CATEGORIE	ESEMPI
Efficienza	Eliminare doppio lavoro
produttività	sfruttare le competenze
conformità	migliorare il processo decisionale esecutivo
agilità	massimizzare il rendimento (ROI) dalle soluzioni
risparmi sui costi	migliorare lo scambio di informazioni
allineamento strategico	dare priorità alle spese per la sicurezza
resilienza	
responsabilità	
consapevolezza dei rischi	

G. Vantaggi della Sicurezza convergente

Quando il gestore di un'infrastruttura critica tratta le minacce alla sicurezza in modo isolato all'interno di specifiche funzioni aziendali, anziché affrontarle da una prospettiva globale, non può:

- stabilire con precisione le priorità,
- concentrarsi sui rischi più in grado di provocare danni,
- affrontare le vulnerabilità dei sistemi Cyber-fisici connessi, e
- non può sfruttare appieno il valore degli investimenti di protezione

La convergenza strategica della sicurezza, ovvero l'approccio tattico alla sicurezza nel suo complesso anziché la mera somma delle sue parti, consente ai gestori di infrastrutture critiche di prendere decisioni più appropriate in materia di protezione e riduzione dei rischi. Piuttosto che lasciare che ogni funzione affronti i rischi da sola e sperare che esse si allineino, un paradigma basato sulla convergenza offre agli operatori delle infrastrutture una migliore comprensione del modo in cui le contromisure possono combattere le minacce. Poiché i rischi da un punto di vista operativo sono interdipendenti, la convergenza della sicurezza, eliminando questi silos, è in grado di affrontare meglio le minacce.
Da un punto di vista organizzativo, un approccio di convergenza ai rischi legati alla sicurezza produce un valore significativo, inserendo in un costrutto comune diverse valutazioni del rischio – sopralluoghi in sito, audit IT e così via. Il sistema normalizza le discussioni sul rischio, in modo che i dirigenti possano prendere decisioni con una comprensione completa del rischio stesso. Si tratta di un aspetto imperativo, poiché lo stesso livello di protezione, o lo stesso livello di spesa per la sicurezza, non può essere mantenuto contemporaneamente per ogni unità aziendale, tanto meno per ogni componente all'interno delle unità aziendali.

Un approccio di convergenza incoraggia inoltre gli operatori a riconoscere che la protezione nel proprio ambito non è la totalità della sfida della sicurezza, ovvero che la sicurezza nella propria funzione è solo una parte della più ampia necessità di proteggere le operazioni e garantire la resilienza. Sarà sempre importante per i dirigenti di funzione concepire solide misure di sicurezza fisica o di protezione dell'IT e la garanzia che i loro dipartimenti le attuino efficacemente; ma il passaggio a una "sicurezza" che comprenda la protezione da tutti i rischi non routinari aiuta tutti coloro che operano in discipline diverse a riconoscere il valore del lavoro di squadra e della cooperazione interdipartimentale.

La convergenza della strategia di sicurezza fisica ed informatica contribuisce inoltre a far sì che le infrastrutture critiche raggiungano un obiettivo più ampio della semplice sicurezza: quello di garantire la resilienza operativa. Al di là della sicurezza specifica nel paradigma rischio-contro-misura, la sicurezza è un elemento tra i tanti necessari per garantire operazioni ininterrotte.
Questo riconoscimento - dal punto di vista operativo è in qualche modo irrilevante sapere se il danno è causato dal terrorismo o da un tornado - può aiutare a far sì che la cybersecurity e la sicurezza fisica lavorino in rapporti più stretti con altri elementi del puzzle della resilienza: risposta ai disastri, gestione delle crisi, recupero delle attività, salute e sicurezza, IT e altri.
Le storie di successo legate alla convergenza abbondano. Alcune aziende attive nel campo delle infrastrutture critiche stanno aderendo alle normative integrando il controllo degli accessi logici e fisici; altre stanno risparmiando decine di migliaia di euro all'anno riducendo la duplicazione della gestione dei database; altre stanno trasformando innumerevoli ore di video inguardabili in dati che vengono condivisi e sfruttati per migliorare i processi operativi; altre stanno implementando soluzioni singole per problemi simili e coordinando i processi di reportistica e registrazione.
Un approccio congiunto alla sicurezza fisica ed informatica aiuta a ridurre i costi razionalizzando progetti di sicurezza storicamente eterogenei; migliora la produttività e la velocità del lavoro eliminando le duplicazioni; elimina le costose funzioni di supporto agli utenti e riduce i costi di manutenzione; elimina le inefficienze, come le duplicazioni delle indagini condotte dalle risorse umane, l'IT e la sicurezza fisica; e aumenta la capacità di dimostrare a chi è fuori dall'organizzazione che l'organizzazione stessa soddisfa i requisiti di sicurezza fisica e di cybersecurity.

I valori di un approccio di sicurezza convergente includono:

- Un budget per la sicurezza che rifletta le priorità della sicurezza stessa. Quando la spesa per la sicurezza si trova all'interno di una struttura di budgeting a blocchi infatti, il problema è che i fondi per la sicurezza finiscono nelle mani di dipartimenti per i quali la sicurezza non è una preoccupazione primaria. Un approccio convergente garantisce che le decisioni sulla spesa per la sicurezza rimangano nelle mani dei leader della sicurezza.
- Sfruttare le competenze. Le competenze specialistiche sono presenti in tutte le direzioni, e un approccio coordinato alla sicurezza rende più facile sfruttare e massimizzare le competenze dei diversi dipartimenti per il bene della missione comune. La combinazione delle competenze durante le indagini, ad esempio, le rende più efficienti ed efficaci.
- Garanzia normativa. Una maggiore standardizzazione delle politiche e procedure aiuta l'operatore di un'infrastruttura critica ad aderire agli standard di gestione per facilitare la conformità alle normative. Un approccio centralizzato alla sicurezza garantisce anche la responsabilità, che è un elemento centrale della maggior parte delle normative. Un modello di sicurezza convergente concentra la responsabilità della sicurezza in un'unica sede.

- Sviluppo del personale e produttività. Quando un sistema è sviluppato in modo da unificare tutti coloro che svolgono funzioni di sicurezza, si aprono percorsi di carriera per il personale e vengono creati spazi per l'innovazione e per massimizzare le competenze delle persone.
- Migliori metriche. Quando le funzioni di sicurezza sono integrate nelle varie attività di diversi reparti, gli obiettivi e le misure di sicurezza spesso riflettono solo le esigenze di sicurezza dei singoli reparti. In un modello coordinato, le metriche di sicurezza possono aiutare a promuovere miglioramenti della sicurezza a beneficio dell'intera operatività e ad allinearsi agli obiettivi dell'intera organizzazione, non delle sue varie unità.

Per migliorare la sicurezza, le finanze e l'efficienza, gli operatori delle infrastrutture critiche del mondo devono adottare un meccanismo per ottenere visibilità sull'intero spettro delle minacce che devono affrontare, e coordinare le attività di protezione.

- Un approccio congiunto alla sicurezza fisica ed informatica consente un allineamento strategico delle due funzioni e riduce i rischi.
- Dalla convergenza della sicurezza derivano spesso altri vantaggi, tra cui una maggiore produttività, efficienza e conformità alle normative.

H. Framework della Sicurezza Convergente

La maggior parte delle organizzazioni dispone di una moltitudine di funzioni specialistiche finalizzate alla loro protezione. La sfida consiste nell'unificare, allineare ed integrare la gestione di questa miriade di attività legate alla protezione. Per molti operatori dei sistemi critici del mondo, questo richiede una nuova prospettiva nella leadership, che serva a superare i silos di responsabilità della sicurezza che possono portare a vulnerabilità non riconosciute.

Una difesa ottimale delle risorse richiede la fusione di sicurezza fisica ed informatica, ma qual è il modello di questa nuova miscela di sicurezza?

Un approccio comune di difesa richiede il riconoscimento del fatto che la sicurezza è davvero una responsabilità condivisa da molte parti, per questo sono state sviluppate diverse utili strategie e quadri di riferimento che le organizzazioni possono seguire per unificare e coordinare le loro attività.

Un approccio strutturato è importante per consentire la comunicazione tra le funzioni di sicurezza, identificare i rischi e le vulnerabilità fisiche ed informatiche collegate, allineare le politiche di sicurezza, gli obiettivi e le spese, e coordinare la risposta agli incidenti.

Ogni organizzazione deve seguire un processo e adottare i componenti del framework che meglio si adattano ai rischi che deve affrontare, alle normative a cui deve attenersi e ai propri obiettivi aziendali e operativi. Ma mentre il "come" varierà tra le diverse organizzazioni di infrastrutture critiche, l'obiettivo di migliorare il coordinamento tra le funzioni di sicurezza dovrebbe essere universale.

Un framework di convergenza efficiente fungerà da veicolo per coordinare le numerose sfaccettature della gestione dei rischi, che comprende la sicurezza fisica e la sicurezza informatica, e aiuterà a organizzare e allineare i diversi programmi di autoprotezione. Una volta adottato un framework di convergenza della sicurezza, è più probabile che le attività di sicurezza che ne derivano riconoscano che la protezione delle infrastrutture critiche è come un ecosistema che richiede che le attività difensive lavorino insieme per difendere collettivamente gli interessi di tutte le parti interessate.

Senza un processo definito per riunire le molte fette della torta della protezione, è più probabile che si creino lacune nello scudo di sicurezza. Seguendo un quadro di riferimento che guida la convergenza della sicurezza, le infrastrutture critiche possono essere più proattive nella loro difesa, piuttosto che risolvere semplicemente la falla che è stata esposta più di recente. Un framework di sicurezza convergente efficace significa anche:

- Chiarire le responsabilità ed incoraggiare la responsabilizzazione,
- ridurre al minimo le guerre di territorio,
- aumentare il profilo dei problemi di sicurezza all'interno dell'organizzazione, e
- servire come strumento per comunicare agli stakeholders interni riguardo l' "ecosistema di protezione" e le sue interdipendenze.

Per i vantaggi sopra descritti, è utile che gli operatori delle infrastrutture critiche adottino un approccio globale alla sicurezza e creino una struttura che serva ad unificare le attività di protezione. Poiché il cambiamento sistemico può essere scoraggiante, alcuni operatori trovano utile avviare un allineamento della sicurezza cyber-fisica. concentrandosi sui benefici specifici derivanti dal miglioramento del coordinamento tra le attività di protezione, come la formazione incrociata o l'eliminazione della duplicazione degli sforzi. Sebbene questo possa fornire una via per il coordinamento, i primi passi devono anche includere la volontà di condurre un'onesta autovalutazione, secondo Felipe Bayon, amministratore delegato del Gruppo Ecopetrol, la principale compagnia energetica colombiana che gestisce oleodotti, raffinerie e linee di trasmissione in tutte le Americhe.

Nel corso del World Economic Forum tenutosi a Davos nel gennaio del 2022, Bayon ha dichiarato di aver condotto di recente un esercizio di questo tipo, esaminando con attenzione la propria posizione di sicurezza rispetto all'attuale contesto di rischio. Di conseguenza, "ci siamo resi conto che dovevamo fare un passo avanti e alzare il tiro", ha detto. Ad esempio, gli operatori devono valutare se dispongono delle competenze, dell'esperienza e delle capacità giuste per avviare un approccio più coordinato alla sicurezza.
Inoltre, questo approccio richiede un'ampia partecipazione. La creazione di un approccio integrato alla sicurezza è un'impresa significativa che coinvolge molti fornitori, sistemi, parti interessate e sedi. Quindi un'azienda deve raccogliere il sostegno per un progetto di tale portata.

Come si è detto, non esiste un unico quadro di riferimento che possa essere adatto a tutte le operazioni di infrastruttura critica e le aziende sono consapevoli che debbono affrontare l'integrazione delle funzioni di resilienza in modi diversi. In alcuni casi, il nesso di coordinamento può essere la gestione del rischio. In altri casi, può essere la continuità operativa, un dipartimento combinato di sicurezza fisica e informatica o qualche altra disciplina.

Indipendentemente dalla struttura particolare, un paradigma efficace ha in genere diversi elementi in comune.

In primo luogo, è probabile che si tratti di un processo dall'alto verso il basso, in grado di esercitare una guida e un controllo su tutti gli aspetti della sicurezza, indipendentemente da quale sia il reparto in cui è inserito. In

questo modo si garantisce che qualcuno sia responsabile di tutti gli aspetti della sicurezza e che ognuno di essi venga svolto in modo corretto in conformità con i principi aziendali e gli obiettivi strategici di protezione.

Parte della convergenza consiste nel considerare gli individui e le funzioni che svolgono attività di sicurezza e nel combinare "lavori simili" in un modello centralizzato. Le responsabilità precedentemente separate si allineeranno in genere sotto una sorta di organizzazione centrale per la sicurezza con autorità di bilancio e operativa. Questo gruppo può quindi consolidare e dare priorità alla spesa per la sicurezza dell'organizzazione, trovare il modo di estrarre il massimo valore dalle nuove tecnologie, allineare politiche e procedure, stabilire obiettivi e monitorare i progressi attraverso metriche di sicurezza a livello aziendale, fornire una supervisione della sicurezza e riferire ai principali stakeholders.

Un'altra caratteristica probabile è un ruolo più significativo della gestione del rischio per guidare le attività. Una gestione che si concentri sull'aspetto proattivo del rischio in modo preventivo a livello di organizzazione; eliminando la frammentazione e le inefficienze della risposta ai singoli eventi di sicurezza quando si verificano.

Un'altra componente necessaria è la governance e la supervisione delle attività di sicurezza. Mentre la gestione della sicurezza aiuta a garantire che gli aspetti funzionali della sicurezza - politiche, processi e simili - operino in modo efficace, un ulteriore livello di governance aiuta l'organizzazione a lavorare insieme per creare una cultura della responsabilizzazione, che consenta una gestione efficace della sicurezza in tutta l'azienda. È importante notare che la struttura faciliterà una gestione della sicurezza sempre efficace, fornendo le basi per affrontare i rischi; anche se tutto ciò che la riguarda sta cambiando. L'evoluzione della tecnologia, l'interdipendenza tra tecnologie e rischi, i cambiamenti nel valore relativo delle risorse aziendali sta infatti creando un ambiente di minaccia molto dinamico.

Un quadro di riferimento efficace comprende anche:

- Identificare i principi guida di base - inclusione, trasparenza, conformità, etica, misurazione e reportistica e gestione del rischio - a cui tutti coloro che gestiscono elementi di rischio per la sicurezza sanno di doversi attenere.
- Affrontare in modo ponderato le questioni dei ruoli, delle responsabilità e della separazione dei compiti. Un processo per l'assegnazione, la valutazione e la garanzia che tutti gli aspetti della sicurezza siano affrontati eviterà le lacune di protezione non affrontate.
- Costituire una piattaforma su cui costruire il coordinamento futuro. L'idea che il rischio abbia due componenti - fisica ed informatica - non coglie tutte le complessità del rischio e può sminuirne l'importanza. La convergenza della strategia di sicurezza fisica ed informatica può essere parte di un processo che incoraggia un approccio integrato al rischio e che sia completo come richiesto dall'organizzazione.

Uno sforzo integrato per mitigare i rischi legati alla sicurezza è fondamentale per un approccio più strategico e solido alla sicurezza delle infrastrutture critiche. Esso fornisce una struttura per preparare le organizzazioni a gestire tutti gli aspetti della sicurezza, indipendentemente dal dipartimento che ne ha la responsabilità, dal tipo di minaccia o dal modo in cui cambia. Riconosce che per difendere le infrastrutture critiche in un'epoca di sistemi connessi, minacce ibride e avversari determinati, è necessario un approccio più completo, progressivo e proattivo.

- Le entità che si occupano di infrastrutture critiche dovrebbero adottare un framework per unificare, allineare ed integrare la sicurezza fisica ed informatica e facilitare un migliore coordinamento con altre funzioni di resilienza.
- Comprensione e assegnazione delle responsabilità, allineamento strategico e supervisione sono elementi critici di uno schema efficace.
- Uno sforzo integrato per mitigare i rischi legati alla sicurezza è fondamentale per proteggere la sicurezza delle infrastrutture critiche in un mondo di rischi interdipendenti.

Informazioni sull'autore:
Garett Seivold è un giornalista professionista specializzato in sicurezza che scrive per l'International Security Ligue.

Sezione II.
Problemi nella Physical-Cyber Security

1. Analisi prospettica dell'industria della Sicurezza Privata

Sfide per le professioni della Sicurezza Privata nei prossimi dieci anni

Il mondo della Sicurezza Privata si è evoluto notevolmente, spinto dalle minacce alla sicurezza in continuo aumento e, d'altro canto, da un ravvicinamento ogni giorno maggiore alle forze di sicurezza interne.
L'evoluzione del settore della sicurezza privata - e quindi la sua capacità di contribuire a proteggere le infrastrutture critiche del mondo - è caratterizzata da due forti tendenze.

Un ampliamento del campo di competenza

La prima è un ampliamento irreversibile del campo di competenza delle Società di Sicurezza Private a livello nazionale, con un quadro normativo adeguato. Le minacce alla sicurezza e alla salute aumentano di giorno in giorno e le Forze dell'Ordine a livello nazionale e locale sono costrette a concentrarsi su una serie di compiti prioritari. Ciò significa che la Sicurezza Privata sarà sempre più presente nello spazio pubblico e che alcune attività, come la registrazione dei reati, i furti nei negozi, la violenza contro le persone che visitano i centri commerciali, potrebbero essere affidate a loro. Questo è già il caso per il trasporto ferroviario, così come è già possibile per le Società di Sicurezza effettuare (in alcuni casi e con una specifica autorizzazione di una amministrazione dello Stato) la loro missione di sicurezza nello spazio pubblico. Anche se ci vuole tempo, a causa di freni istituzionali o reazioni corporative, la tendenza è confermata.
Le Società di Sicurezza Private (SSP) forniscono già servizi di protezione e sicurezza a un'ampia gamma di aree ed edifici pubblici: centri commerciali, ristoranti, cinema, stadi, aeroporti, treni, trasporti pubblici urbani, centri ricreativi, località balneari e montane, ecc.

La crescente diffusione delle tecnologie

La seconda tendenza è un mix tecnologico sempre più forte.

Sebbene si sia parlato molto della guardia giurata del futuro come una "guardia aumentata", non c'è dubbio che saranno molto meglio equipaggiate. Le nuove tecnologie faciliteranno le loro missioni consentendo loro di comprendere meglio l'ambiente in cui operano. **Avranno accesso a informazioni in tempo reale e l'integrazione dei dati consentirà alla gestione operativa di liberarsi dalle incombenze amministrative, in modo da essere ancora più presente sul campo e più vicina ai suoi clienti.**

L'intelligenza artificiale nel campo del riconoscimento comportamentale e facciale integrerà la formazione attualmente fornita agli agenti poiché la formazione sarà un fattore determinante nella capacità degli agenti di sicurezza di evolvere in un mondo protetto da tecnologie di sicurezza più efficaci. Il rilevamento di comportamenti "a rischio o non conformi" aiuterà a evitare situazioni di conflitto o di criminalità. La rilevazione dei suoni (urla, grida, rumori specifici) migliorerà anche la velocità e l'efficienza degli interventi per rendere gli spazi pubblici, come i centri commerciali, più sicuri e piacevoli.

Nei centri commerciali, ad esempio, i Security Headquarters diventeranno veri e propri centri operativi dedicati, ancor più di oggi, al supporto degli agenti dislocati e alla protezione delle aree tecniche.

Le aziende di sicurezza privata dovranno costruire un'offerta di sicurezza ibrida (uomo-tecnologia) per i propri clienti, guidata da piattaforme di ipervisione digitale, in grado di gestire le operazioni di sicurezza e di fornire un valore aggiunto significativo in termini di gestione degli eventi o delle crisi. Analizzando le informazioni raccolte e gli eventi gestiti, questi strumenti forniscono una capacità predittiva che consente di anticipare i tempi e i luoghi in cui potrebbero verificarsi eventuali incidenti. I servizi vengono quindi programmati di conseguenza e le squadre di sicurezza vengono impiegate gestendo le risorse umane nel modo più accurato possibile.

Oltre a questi sviluppi tecnici, il settore della sicurezza privata sta subendo anche dei cambiamenti strutturali.

La concentrazione delle aziende è in aumento e molte di esse si stanno muovendo verso l'integrazione di un'offerta diversificata. **Le aziende di sicurezza privata devono ora coprire uno spettro più ampio della catena del valore, dalle competenze commerciali all'integrazione dei sistemi di sicurezza, oltre alla tradizionale offerta di sicurezza umana, sempre più professionale ed efficiente.** Pertanto, oltre alle competenze umane richieste dai clienti, devono impegnarsi in un approccio olistico alla loro offerta di sicurezza. Devono posizionarsi nei confronti dei loro clienti allo stesso modo con cui misurano la portata dei loro rischi; quindi di anticipare i loro problemi di sicurezza e di trovare insieme a loro soluzioni adeguate. Infatti, la minaccia alla sicurezza è tridimensionale e deve essere affrontata come tale.

Un approccio olistico, partnership innovative

L'approccio olistico ci permette di combinare il know-how nella sicurezza umana con la capacità di integrare tecnologie innovative per soddisfare le esigenze del cliente, compresa la dimensione della cybersecurity. Siamo convinti che questa evoluzione porterà alla creazione di valore condiviso tra le aziende di sicurezza e i clienti; offrendo a questi ultimi una qualità di servizio che va oltre quella attuale.

Informazioni sull'autore:
Jean-Philippe Bérillon è un esperto di sicurezza con una profonda esperienza in diverse regioni del mondo e settori, tra cui l'energia e la sicurezza privata. È responsabile della sicurezza del Gruppo DPD e presiede il Comitato CoESS per la protezione delle infrastrutture critiche.

2. Verso una visione integrata nella governance della Physical-Cyber Security delle organizzazioni

I costi della criminalità informatica sono in costante aumento e la semplice analisi degli attacchi mostra che tutti i vettori vengono utilizzati per penetrare le difese di aziende o istituzioni, con una forte creatività.

Cybersecurity Ventures prevede che i costi globali della cybercrime cresceranno del 15% all'anno nei prossimi cinque anni, raggiungendo i 10,5 trilioni di dollari all'anno entro il 2025.

I sistemi informatici amministrativi o industriali sono ancora i bersagli crescenti di questi criminali dello spazio digitale; ma i sistemi di sicurezza elettronica non vengono risparmiati. **In un mondo sempre più interconnesso, le organizzazioni con funzioni convergenti di sicurezza informatica e fisica sono più resilienti e meglio preparate ad identificare, prevenire, mitigare e rispondere alle minacce.**

L'obiettivo umano rimarrà il preferito, sia che si tratti di un dipendente, di un consulente o di un appaltatore dell'azienda; e per le stesse ragioni le società di sicurezza privata non hanno altra alternativa oggi che rafforzare la formazione dei propri agenti, sensibilizzare e preparare gli operatori dei loro SOC (Security Operation Centre) e la loro operatività dei PC agli attacchi informatici. La qualità del servizio così offerto porterà a qualifiche più elevate del personale e quindi un servizio di sicurezza migliorato. Ed è anche per questo motivo che il cammino verso una maggiore integrazione delle tecnologie di sicurezza e di sorveglianza nell'offerta combinata di sicurezza privata e tecnologia umana, ne è oggi la perfetta espressione.
I sistemi di videosorveglianza, il controllo degli accessi, i robot di sorveglianza e i droni sono, o saranno, i prossimi obiettivi dei cybercriminali.

Tutto ciò dimostra la convergenza tecnica tra sicurezza informatica e sicurezza fisica. Ma se prescindiamo dall'aspetto tecnico e ci concentriamo sull'aspetto organizzativo, possiamo notare che le organizzazioni operano ancora in silos. Tuttavia, è nella natura stessa della sicurezza informatica e di quella fisica e umana essere trasversale, avendo un impatto su tutti gli aspetti di un'azienda, compresi strategia, produzione, sviluppo commerciale, catena di approvvigionamento, personale ed esperienza del cliente.

Il ruolo chiave del CSO

Ciò significa che la collaborazione tra Responsabile dell'Informazione - Chief Information Officer (CIO), responsabile della Sicurezza Informatica - Chief Information Security Officer (CISO) e Responsabile della Sicurezza - Chief Security Officer (CSO) - non è adeguata alle sfide della minaccia informatica. Il problema del CISO legato al CIO, che oggi è quasi la norma, può essere visto come un'organizzazione inefficiente. In quanto responsabile del controllo della sicurezza dei sistemi, la sua indipendenza dal CIO dovrebbe essere più naturale e si dovrebbe preferire un rapporto diverso, ad esempio con il CSO.

Inoltre, i CSO sono già responsabili della gestione operativa delle società di sicurezza private. Sono anche attori nel campo della definizione delle specifiche per la sicurezza fisica dei siti, i processi da elaborare e mettere in atto e l'identificazione di tecnologie appropriate per la gestione dei loro siti.
In molti casi, il CSO dirige le gare d'appalto per la manutenzione di sistemi di sicurezza elettronica, controllo degli accessi e sorveglianza, con una preferenza per le società di sicurezza che possono gestire questi sistemi e assicurarne la manutenzione e che hanno la capacità di integrare le tecnologie di sicurezza.

La scelta di affiancare il CISO al CSO è motivata dalla maggiore trasversalità della professione di CSO e dal fatto che questa trasversalità integra meglio il difficile tema dell'approccio al comportamento umano, poiché il comportamento umano è il più delle volte la parte più debole della linea di difesa che le organizzazioni devono costruire. In questo modo la collaborazione tra i due responsabili della protezione, il CIO e il CSO, si avvicinerebbe.
Le organizzazioni, grandi o piccole che siano, critiche o non critiche, possono perseguire la convergenza sviluppando un approccio che si adatta alla struttura, alle priorità e al livello di capacità specifica dell'organizzazione.

Rompere i silos

Più che una semplice osservazione, è una vera preoccupazione **il fatto che si continui a gestire le minacce fisiche ed informatiche in modo indipendente. Inoltre, dimostra l'incapacità delle organizzazioni di ripensare il proprio modello e di rivedere la propria governance in questo settore. Il fatto è che non si può fornire una buona sicurezza informatica senza una solida sicurezza degli edifici, o se i team di sicurezza informatica e fisica continuano a essere isolati.**

Quando si tratta di infrastrutture critiche, la posta in gioco è ancora più alta. Non affrontare la minaccia con un'organizzazione omogenea lascia spazio a vulnerabilità e falle che i criminali o chiunque voglia attaccare l'azienda possono sfruttare per penetrare nei siti o nei sistemi. Queste vulnerabilità sono tanto una questione di protezione dei sistemi industriali o gestionali quanto una questione di protezione dei sistemi di sicurezza, i sistemi informatici e dei dispositivi di sicurezza fisica ed elettronica.

Inoltre, gli attacchi stanno diventando combinati: minacce interne, intrusioni fisiche con neutralizzazione dei sistemi elettronici di sicurezza, attacchi informatici. È quindi necessario avere un approccio in grado di combinare le competenze per garantire un approccio globale e convergente alla sicurezza, una organizzazione sulla base di un approccio olistico per comprendere la minaccia.

È questa convergenza che consentirà alle organizzazioni di essere de-compartimentalizzate e di dare coerenza e solidità ai sistemi di protezione di cui hanno bisogno oggi.

È quindi necessario che le organizzazioni si evolvano verso una costruzione convergente della sicurezza con un'unica direzione. È infatti una governance integrata della sicurezza di cui le aziende in generale e le infrastrutture critiche in particolare hanno bisogno, cioè la sicurezza delle persone, delle reti informatiche industriali e amministrative e la sicurezza fisica dei siti.

Questo modello di organizzazione matura, che integra omogeneità e approccio olistico, garantisce una maggiore reattività ed efficienza; che si traduce anche in una cultura della sicurezza più forte nelle organizzazioni. Siamo fermamente convinti che tali organizzazioni siano in grado di fornire una difesa più efficace e una reazione più rapida ad attacchi sempre più sofisticati e combinati (fisici e digitali).

La visione di un Chief Security Officer prevede un unico responsabile di quest'area globale che diventerà un unico punto di riferimento per il management esecutivo, per le agenzie di sicurezza o per qualsiasi altro dirigente dell'organizzazione con cui avere una contatto diretto quando si è interessati a qualsiasi questione di sicurezza trasversale e urgente.

Informazioni sull'autore:
Jean-Philippe Bérillon è un esperto di sicurezza con una profonda esperienza in diverse regioni del mondo e settori, tra cui l'energia e la sicurezza privata. È responsabile della sicurezza del Gruppo DPD e presiede il Comitato CoESS per la protezione delle infrastrutture critiche.

3. Ripensare i PPP (Partenariati Pubblico-Privato) per migliorare la resilienza delle infrastrutture critiche

Il titolo di questo capitolo è leggermente fuorviante, in quanto i partenariati pubblico-privati (PPP) non sono (ancora) ambiti ben definiti. Nel contesto di questo documento, i PPP sono partnership tra un'agenzia governativa e il settore privato per la fornitura di beni o servizi al pubblico. Un recente confronto tra i quadri giuridici che regolano la sicurezza privata in Europa del CoESS mostra che solo il 40% dei 30 Paesi europei intervistati ha istituito tali partenariati. In genere, si tratta di accordi locali, quindi limitati e non soggetti a quadri o riferimenti chiari.

In un White Paper dal titolo "The Security Continuum in the New Normal" pubblicato nel 2019, il CoESS chiede la creazione di tali quadri e propone linee guida e raccomandazioni per costruire PPP di successo basati su casi concreti.

Il fatto che, finora, i PPP non beneficino di un quadro di riferimento chiaro, offre l'opportunità di integrare la dimensione dei Cyber-Physical Systems (CPS) fin dall'inizio e di raccomandare un approccio olistico che parta da zero.

La raccomandazione CoESS per i PPP esamina vari aspetti dal lato delle società di sicurezza privata, articolati intorno ai 4 valori di CoESS: Sicurezza, Conformità, Qualità e Fiducia.

Sicurezza -> Aziende legittime

- Guardie autorizzate
- Condizioni di lavoro e attrezzature adeguate
- Buon processo di selezione
- Formazione adeguata al lavoro/ all'ambiente

Conformità -> con:

- Legislazione in vigore
- Obblighi fiscali, sociali, amministrativi, contratti collettivi
- Standard e certificazioni riconosciuti

Qualità -> Seguire l'approccio di acquisto Best Value

- Selezionare i fornitori di Sicurezza Privata in base al criterio dell'offerta economicamente più vantaggiosa, non ai costi più bassi.
- Qualità > 50% e > 60% nelle Infrastrutture Critiche

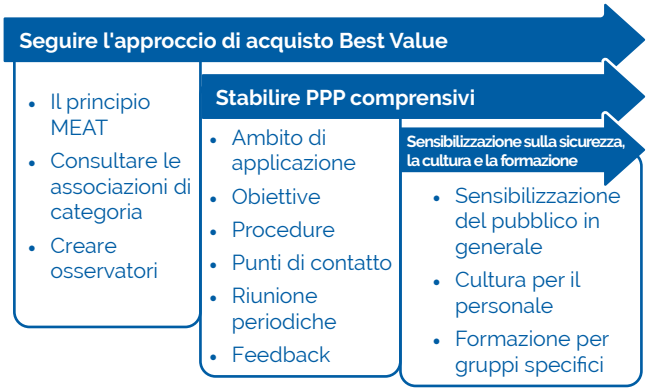
Fiducia -> Convalida da parte di un'associazione/camera pertinente e rappresentativa

- Chiara descrizione e comprensione dei ruoli
- Comunicazione

Implementazione del modello Plan DoCheck Act -> Feedback e miglioramento

- Mentalità di catena di sicurezza
- Struttura dello scambio di informazioni

Una volta istituiti, il CoESS fornisce le seguenti raccomandazioni per garantire che i partenariati funzionino:



Nota: MEAT è l'acronimo di Most Economically Advantageous Tender (offerta economicamente più vantaggiosa). Si tratta di un metodo di valutazione che può essere utilizzato come procedura di selezione, consentendo alla parte contraente di aggiudicare il contratto sulla base di aspetti dell'offerta diversi dal solo prezzo.

Per un successo dei PPP che migliorino la Cyber-Physical Security i seguenti punti meritano particolare attenzione:

- Garantire che la Società di Sicurezza Privata (SSP) sia selezionata in base a criteri di qualità e non solo di prezzo. Il CoESS è favorevole all'assegnazione dei contratti per le infrastrutture critiche in base ad almeno il 60% per criteri di qualità e ha sviluppato uno strumento per misurarli in modo oggettivo in un manuale sviluppato congiuntamente con il sindacato UNI Europa e con fondi UE.
- I criteri per misurare la qualità includono la conformità alla legislazione e alle norme e standard pertinenti, come il sistema standard per le SSP nella Protezione delle Infrastrutture Critiche, EN 17483.
- Un'accurata selezione e formazione degli agenti di sicurezza è molto importante ma non sufficiente. È stato dimostrato che le buone pratiche di gestione sono la base su cui poggia una buona sicurezza. È possibile costruire una cultura di sicurezza, un passo importante per mitigare le minacce interne, che a loro volta sono un vettore significativo di attacchi informatici. Mentre i dipendenti scontenti possono intenzionalmente portare a termine o sostenere attacchi dannosi, le minacce interne accidentali possono derivare da una formazione insufficiente; e la trascuratezza rispetto alle minacce interne può essere la conseguenza di una scarsa cultura della sicurezza.
- I ruoli e le responsabilità dei partner pubblici e privati devono essere ben descritti e capiti reciprocamente per garantire la continuità e la solidità della catena di sicurezza. Una mentalità comune della catena di sicurezza che richiede formazione e consapevolezza delle minacce cyber-fisiche è essenziale. La maggior parte degli attacchi informatici proviene dall'uomo, in modo fisico o di altro tipo, e possono essere evitati con semplici misure e campagne di sensibilizzazione.
- Determinare l'ambito, le procedure e i processi dei partner è molto importante per la sicurezza della catena; e spiegare lo scopo della sua esistenza contribuirà a garantirne la corretta implementazione.

Nel Libro Bianco, il CoESS sottolinea anche che, troppo spesso, lo "scambio" di informazioni è un esercizio unidirezionale. **Nei casi di Cyber-Physical Security, è ancora più cruciale che le Autorità Pubbliche comunichino ai SSP qualsiasi sospetto di attività dannosa o di minaccia elevata.** Senza divulgare alcuna informazione segreta, potrebbe essere molto utile inviare ai SSP avvisi tempestivi su sospette violazioni fisiche o tentativi di attacco informatico. Come sottolineato dal CoESS in diverse occasioni, il rischio di non comunicare è probabilmente più alto del sospettato rischio di divulgazione le informazioni.

In conclusione, entrambe le parti in causa nei PPP hanno molto da guadagnare adottando un approccio comune e una politica condivisa di Cyber-Physical Security nella protezione delle infrastrutture critiche. E ciò andrà sicuramente a vantaggio di entrambe le parti, oltre che della società nel suo complesso.

Informazioni sull'autore:
Catherine Piana è direttore generale del CoESS dal 2014 e di ASSA-i dal 2016 e presidente del Comitato tecnico del CEN. TC 439 "Servizi di sicurezza privata".

4. Convergenza della Physical-Cyber Security nelle Infrastrutture Critiche, ottimo! Ma che dire dell'OT?

Introduzione

La nostra società contemporanea è sempre più digitalizzata. Nel corso degli anni, questo ha portato all'umanità molti valori, prosperità e benessere. Tuttavia, anche il rovescio della medaglia, o lato oscuro che dir si voglia, sta diventando sempre più evidente. Gli incidenti di tipo digitale, dovuti sia a incidenti che a dolo, sono sempre più frequenti e quotidianamente nelle cronache. Le agenzie governative di cybersecurity, le istituzioni e gli esperti informatici mettono in guardia dalle interruzioni digitali che mettono a rischio la continuità delle organizzazioni e della società. Al giorno d'oggi, ogni processo dipende dall'infrastruttura digitale (IT) e non esistono praticamente alternative analogiche se i sistemi digitali si guastano. Anche le stesse infrastrutture critiche dipendono completamente dall'infrastruttura digitale.

Il lato positivo è che tutti gli attori della società stanno diventando sempre più consapevoli dell'interdipendenza e dei rischi. Privati, organizzazioni e governi stanno estendendo le loro difese informatiche e stanno aumentando la resilienza.

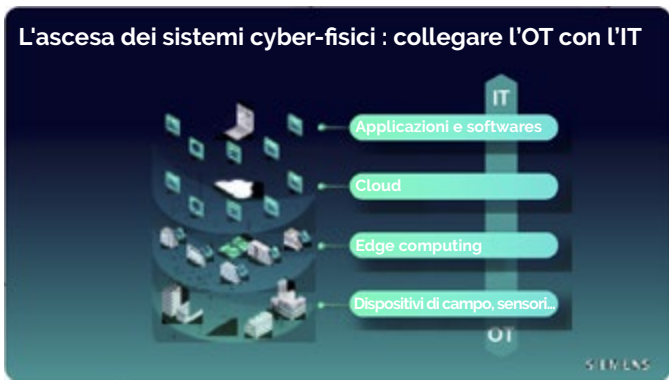
Il settore della sicurezza professionale, che si confronta con questa nuova realtà in continua evoluzione, è purtroppo ancora molto frammentato. I professionisti della sicurezza fisica si occupano principalmente di minacce fisiche, e i professionisti della sicurezza informatica di quelle informatiche. Questi due ambiti hanno un interesse comune nella gestione del rischio e condividono persino processi di gestione del rischio simili. Tuttavia, hanno un background diverso, minacce e controlli specifici e persino un linguaggio diverso. Negli ultimi anni, questi rami si sono lentamente avvicinati e hanno iniziato a familiarizzare l'uno con l'altro.

Nell'ultimo decennio, sono emerse minacce ibride, combinazioni di minacce fisiche ed informatiche si sono evolute, determinando la convergenza di questi domini.

A complicare le cose, c'è un terzo dominio di sicurezza che ha disperatamente bisogno di attenzione: la sicurezza OT. Questo documento introdurrà brevemente questo dominio e ne illustrerà alcune caratteristiche specifiche. **La sicurezza OT è strettamente correlata sia alla sicurezza informatica che a quella fisica e una strategia di sicurezza olistica non può prescindere da una sua corretta comprensione.**

OT, che cos'è?

OT è l'abbreviazione di Operational Technology. È il fratello gemello dell'Information Technology (IT). Entrambe rappresentano il mondo digitale. L'IT, come indica il nome, si concentra sulla creazione, elaborazione, archiviazione, sicurezza e scambio di tutte le forme di informazioni e dati elettronici.
L'obiettivo principale dell'OT, invece, è il controllo delle apparecchiature che influenzano il mondo reale.
Questi sistemi sono noti come sistemi di controllo industriale (ICS), sistemi SCADA, sistemi di automazione e controllo industriale (IACS), sistemi di gestione degli edifici (BMS) ecc.
Questo settore spazia dall'automazione di processo (industriale), ai sistemi di trasporto, ai sistemi di controllo dell'automazione fino alle reti intelligenti e agli edifici intelligenti. Questi sistemi sono definiti Cyber-Physical Systems e collegano il mondo digitale a sensori e attuatori fisici che interagiscono con l'ambiente fisico.
Anche i sistemi di sicurezza fisica, come la videosorveglianza, il rilevamento delle intrusioni, il controllo degli accessi e simili, fanno parte del dominio OT.



Il più delle volte, la convergenza della sicurezza fisica ed informatica si concentra sulla convergenza della sicurezza fisica e dell'IT, dimenticando il dominio dell'OT.
Il dominio OT è tradizionalmente gestito dai reparti operativi. Essi sono responsabili del mantenimento dei processi dell'organizzazione. L'obiettivo è la disponibilità del sistema e la riduzione dei tempi di inattività (non pianificati). Poiché i processi sono fisici per natura, la sicurezza delle persone e dell'ambiente è una preoccupazione primaria. L'interazione in tempo reale è essenziale per i sistemi OT, ad esempio: premendo un pulsante di arresto di emergenza, questi sistemi devono rispondere istantaneamente. Ritardi e latenze non sono accettabili.

IT vs. OT: che differenza c'è?

Il settore IT, con il suo focus sulle informazioni e i dati, si occupa principalmente della riservatezza e dell'integrità delle informazioni. La disponibilità delle informazioni è spesso meno critica; la latenza e persino i brevi tempi di inattività sono accettabili.

Nell'ambito dell'IT, la sicurezza di solito non è un argomento di cui ci si preoccupa. Negli ambienti aziendali, il reparto IT si occupa generalmente dell'IT dell'ufficio. Di solito non è a conoscenza di eventuali sistemi OT nella loro rete o semplicemente creano un "segmento di rete tecnico" separato per questo, in modo da non essere disturbati dall'OT. Nella maggior parte dei casi, l'OT non è considerato una responsabilità del reparto IT. **I professionisti OT originariamente gestivano sistemi di automazione che non erano collegati al mondo esterno** (ai tempi in cui l'IT e internet non esistevano ancora). Sono ancora convinti di gestire una centrale elettrica/processo produttivo/ponte/edificio e non gli passa mai per la testa che in realtà stanno gestendo sistemi OT che sono interconnessi con, e anche in parte costituiti da, apparecchiature IT.

Il fortunatamente crescente numero di professionisti IT che si occupano di sistemi OT non capisce o non accetta che i sistemi OT

hanno alcune caratteristiche peculiari da gestire. I professionisti IT, ad esempio, sono abituati a mantenere i loro sistemi aggiornati, aggiornare ed applicare patch ai loro software in modo regolare e molto strutturato.
L'aggiornamento del software dei sistemi OT è ovviamente possibile e consigliabile; tuttavia, potrebbe implicare la necessità di testare l'intero sistema OT da un capo all'altro per assicurarsi che tutte le caratteristiche di sicurezza non siano interessate dall'aggiornamento e funzionino come previsto. La migrazione del software di automazione dei processi di una centrale elettrica, ad esempio, potrebbe essere impossibile (non può essere spenta) o molto costosa a causa di test approfonditi. **Un numero crescente di organizzazioni, soprattutto nelle infrastrutture critiche, stanno unendo i reparti IT e OT per farli collaborare.**

E la sicurezza fisica?

Oggi le organizzazioni e il loro management sono sempre più consapevoli dell'importanza dei sistemi informatici, dei dati e delle informazioni. La protezione di questi sistemi e dei loro contenuti ha un'alta priorità. La protezione fisica dei sistemi IT non è un problema e di solito si concentra sulla protezione fisica dei data center, delle sale con apparecchiature IT e dei componenti di rete. Per i sistemi IT, i componenti fisici sono concentrati in stanze ed edifici specifici e, quindi, sono più facili da proteggere. La sicurezza fisica è parte integrante degli standard e delle norme di sicurezza informatica. I responsabili della sicurezza fisica possono facilmente incorporare questi standard e linee guida nelle loro politiche di sicurezza. Anche i sistemi di sicurezza fisica sono prescritti e dettagliati in queste linee guida. In questo senso, la sicurezza fisica è una parte inseparabile della sicurezza informatica. Dal momento che l'IT o la cybersecurity sono oggi un argomento di discussione nei consigli di amministrazione (e la sicurezza fisica spesso non lo è), ha senso che i professionisti della sicurezza fisica salgano sul carro della sicurezza informatica per mettere la loro professione sotto i riflettori e dargli la priorità che merita.

I sistemi OT sono nascosti nel funzionamento di molte organizzazioni. Sono di estrema importanza per specifici reparti operativi e fanno parte delle loro attività quotidiane. Di solito non sono un argomento di interesse a sé stante. La configurazione fisica di questi sistemi è completamente diversa da quella dei sistemi IT. I componenti fisici dei sistemi OT controllano processi fisici e i loro componenti sono distribuiti in tutto il sito. Questi componenti non sono o solo parzialmente centralizzati e installati in ambienti meno sicuri. Prendiamo ad esempio un sistema di videosorveglianza, le telecamere sono installate tutt'intorno e persino sul perimetro esterno non sicuro dei siti, portando le connessioni di rete al nucleo dei sistemi OT letteralmente fuori dalla prima linea di difesa. La protezione fisica di questi sistemi è una sfida a causa del carattere onnipresente dei loro componenti. I reparti operativi, generalmente responsabili dei sistemi OT, mancano di consapevolezza della sicurezza e gli standard e linee guida sono meno sviluppati e implementati. Il settore OT, in particolare, ha bisogno di una prospettiva fisica per aggiornare la sicurezza.

Per concludere...

Il più delle volte la sicurezza fisica non è un argomento di primaria importanza per le organizzazioni e i loro consigli di amministrazione. Lo è invece la cybersecurity, in pratica limitata alla sicurezza informatica. Evidenziare l'inscindibile connessione tra sicurezza fisica ed informatica può aumentare la rilevanza del dominio della sicurezza fisica. **La sicurezza fisica dei sistemi OT è ancora agli albori, e questo è un'opportunità da cogliere, in particolare per le infrastrutture critiche.** Nella nostra società contemporanea, la sicurezza è di vitale importanza. Uniamo sicurezza fisica, IT e OT per costruire un ambiente perfetto.

Informazioni sull'autore:
Johan de Wit è docente presso la Delft Universityof Technology nei Paesi Bassi e lavora presso Siemens Building Technologies allo sviluppo di prodotti futuri e alla progettazione di sistemi di sicurezza.

5. Superare le barriere tra sicurezza Informatica e Fisica

La sicurezza informatica e fisica sono spesso trattate in modo isolato, il che solleva questioni quali:

- Perché una cosa così chiaramente vantaggiosa come una migliore coordinazione è così poco diffusa?
- Che cosa possono fare le organizzazioni per aiutare a superare le barriere che impediscono l'allineamento del lavoro?

Ci possono essere barriere strutturali e tecniche che impediscono una più stretta collaborazione tra sicurezza informatica e fisica, ma l'ostacolo maggiore è spesso di natura culturale. Qualsiasi sforzo di collaborazione rischia di riunire entità con culture e prospettive distinte nelle loro missioni. E questo può essere particolarmente vero per gli operatori della sicurezza. I professionisti della sicurezza informatica tendono a provenire da un mondo in cui l'innovazione è più ammirata e spesso prevale un sistema di valori libertari. Mentre la sicurezza fisica può essere composta da specialisti provenienti dalle Forze dell'Ordine o da ambienti militari e propende per una struttura di comando autoritaria.

Sebbene i leader di entrambi i dipartimenti condividano l'obiettivo di condurre le operazioni in modo sicuro, la convergenza può essere accompagnata da uno scontro di visioni, culture e competenze. Le varie entità che svolgono funzioni legate alla sicurezza all'interno delle aziende hanno tutte "punti di vista diversi, culture diverse, percorsi di carriera diversi, formazione diversa e persino vocabolari diversi", ha dichiarato un responsabile della sicurezza di un'autorità portuale negli Stati Uniti.

Il tempo ha aiutato a risolvere alcune preoccupazioni; perché se da un lato i progressi sono lenti, dall'altro c'è anche un senso di inevitabilità intorno alla rimozione dei silos di sicurezza. Anche la tecnologia ha contribuito a colmare questo divario, in quanto è diventata il cuore di molti processi di gestione della sicurezza aziendale e ha radicalmente cambiato e unito il modo in cui tutti i gruppi lavorano.

Tuttavia, per alcuni operatori di infrastrutture critiche, potrebbe essere impossibile colmare il divario tra le funzioni di sicurezza senza sforzi specifici e mirati per incoraggiare queste culture distinte a lavorare insieme in modo più efficace.

La creazione di una terminologia comune da utilizzare sia per la sicurezza fisica che per quella informatica è una strategia semplice ma popolare. Utilizzando un glossario comune di termini di gestione del rischio, i dirigenti operativi e della cybersecurity possono comunicare in modo più efficace e possono contribuire a migliorare la collaborazione in aree di coordinamento complicate, come la condivisione delle informazioni.

Quando le organizzazioni identificano i cambiamenti necessari per lo sviluppo di una strategia di sicurezza integrata, il potenziale scontro tra culture deve essere preso in considerazione.

Quando la città di Vancouver (Canada) ha intrapreso l'ultima strategia di integrazione - la fusione della sicurezza informatica e della sicurezza fisica in un'unica unità - il capo del dipartimento unificato ha spiegato che la comprensione delle diverse culture esistenti tra i gruppi è stato il fattore più critico per il successo. "Durante uno sforzo di consolidamento, è fondamentale essere consapevoli del fatto che ci sono due gruppi di persone

che possono avere o non avere una comprensione delle funzioni, degli obiettivi o delle capacità dell'altro gruppo. È fondamentale comunicare a entrambi i gruppi e spiegare a ciascuno come i due gruppi si integrano, le loro somiglianze e i vantaggi del consolidamento".
Secondo i reparti operativi delle infrastrutture critiche che hanno abbracciato pienamente la convergenza della sicurezza - e che hanno combinato le operazioni di sicurezza fisica e informatica per coordinare la strategia - le attività gestionali più importanti per attuare il cambiamento sono (nell'ordine):

- Allineamento della leadership,
- Strategia ed esecuzione della comunicazione,
- e progettazione dell'organizzazione, compresa la profilazione delle mansioni e dei ruoli.

La questione della progettazione dell'organico è particolarmente importante per diversi motivi, tra i quali il fatto che è necessario capire innanzitutto come vengono gestite le responsabilità di sicurezza prima di poter attuare un cambiamento efficace o sviluppare una strategia integrata.

Una convergenza di successo richiede una base comune di comprensione riguardo a chi fa cosa: ad esempio, chi supervisiona la risposta alle crisi in loco? Le strutture o la sicurezza? Che ne è delle politiche e degli standard? Della sicurezza o delle risorse umane? Che ruolo ha il management di linea o il consulente legale nella sicurezza delle informazioni o nelle indagini? Sebbene la convergenza sia riconosciuta come un modo per migliorare la sicurezza, di fatto molte organizzazioni non hanno una chiara comprensione del ruolo che i diversi reparti già svolgono nelle varie funzioni di sicurezza, un importante precursore del miglioramento.

La questione della progettazione delle mansioni è spinosa anche perché il personale operativo all'interno dei reparti di sicurezza tradizionale e di sicurezza delle informazioni è spesso protettivo nei confronti dei propri ruoli, responsabilità e proprietà intellettuale. Alcuni possono temere che gli sforzi di integrazione possano comportare la perdita di posti di lavoro o di autorità. I silos di sicurezza esistenti godono di diversi livelli di prestigio e autorità all'interno di un'azienda di infrastrutture critiche. L'implementazione del cambiamento tenendo conto di questi aspetti può aiutare a identificare strategie in grado di ridurre al minimo le preoccupazioni del personale e migliorare l'adesione al progetto.

L'assunzione di personale rappresenta per le infrastrutture critiche un'altra opportunità per creare un'operatività della sicurezza più coesa, selezionando candidati che abbiano competenze nei loro ambiti specifici ma che dimostrino anche la capacità di apprezzare la sicurezza in senso più ampio. Ad esempio, la tecnologia può aiutare ad unire le diverse discipline della protezione. Questo è possibile solo se il personale dispone di un sufficiente bagaglio tecnologico che gli consente d'impegnarsi ponderatamente nelle discussioni sull'utilizzo strategico e aziendale delle nuove tecnologie nell'affrontare i rischi comuni. Le infrastrutture critiche dovrebbero cercare di assumere leader che possiedano le competenze ed il background per contribuire all'obiettivo della sicurezza aziendale, oltre all'esperienza nei rispettivi settori.

Infine, anche se la strada verso la convergenza della sicurezza può essere lunga ed impegnativa, esistono approcci che possono contribuire ad avviare il processo di migliore coordinamento:

- Accettare le differenze. L'integrazione delle informazioni tra tutti gli stakeholders della sicurezza è importante, ma i progressi verso questo obiettivo possono essere incrementali. Invece di smantellare immediatamente i silos e stabilire nuove catene di comando, le aziende possono innanzitutto porre l'accento sulla costruzione di una capacità di "consapevolezza situazionale" completa, in cui i dirigenti di diversi

gruppi possano confrontare le informazioni di alto livello e cercare le tendenze. È un modo utile per dare impulso alla convergenza strategica.

- Costruire il coordinamento dei piani di emergenza. Molte infrastrutture critiche dispongono di un'unità di supervisione o di un'unità ombrello che controlla tutti i rischi per la sicurezza. In assenza di quest'ultima, tuttavia, esistono ancora delle vie per migliorare il coordinamento, ad esempio attraverso i comitati esistenti che si occupano della risposta alle emergenze e della continuità operativa. Sebbene questi comitati di coordinamento debbano spesso la loro nascita alla necessità di gestire una crisi specifica, le organizzazioni li utilizzano sempre più come strumento essenziale per mantenere la preparazione quotidiana.
- Rendere disponibili gli strumenti e i concetti di gestione del rischio in tutta l'azienda, così le risorse umane, l'IT, la sicurezza informatica, la sicurezza fisica e gli altri soggetti interessati alla sicurezza possono parlare un unico "linguaggio". Ma la gestione del rischio può offrire una terminologia universale (una sorta di esperanto) che può aiutare a superare il divario culturale. Offre un insieme di concetti che possono essere applicati sia alla sicurezza fisica che a quella informatica e utilizza strumenti rilevanti per la protezione dei beni fisici, risorse informatiche ed operazioni. È importante che la gestione del rischio metta in relazione la sicurezza con la gestione finanziaria, aiutando i dirigenti a misurare il valore della spesa per la sicurezza in relazione ai suoi benefici.
- Considerare lo sviluppo di un unico cruscotto in cui confluiscano tutte le funzioni che si occupano dei rischi per la sicurezza e che forniscono input per la misurazione delle prestazioni. Uno strumento di questo tipo può aiutare ad organizzare le varie parti della sicurezza in un insieme più ampio e fornire alla dirigenza un quadro di riferimento di alto livello dell'attuale stato di sicurezza dell'intera organizzazione.
- È probabile che qualsiasi dipartimento operativo di infrastruttura critica incontri degli ostacoli nel momento in cui si crea un maggiore coordinamento tra le funzioni di sicurezza. L'identificazione di questi probabili ostacoli e lo sviluppo di strategie per superarli dovrebbero far parte del piano di convergenza delle funzioni di sicurezza tradizionali ed informatiche in un quadro coesivo.

Informazioni sull'autore:
Garett Seivold è un giornalista professionista specializzato in sicurezza che scrive per l'International Security Ligue.

6. Valutazioni congiunte dei rischi e test di penetrazione

Le valutazioni del rischio rivestono un ruolo particolarmente importante nella definizione di una postura di protezione, in quanto sono proprio queste valutazioni di minacce, vulnerabilità e conseguenze potenziali a determinare il livello di protezione - a fronte dell'esistenza di risorse critiche - che informano un'organizzazione su quale sia il livello di mitigazione del rischio giustificato e quale sia il livello di rischio che ha senso accettare. Molte organizzazioni hanno riconosciuto l'importanza delle valutazioni dei rischi per la sicurezza e hanno capito che, per poter fungere effettivamente da base per tutti gli sforzi di mitigazione e prevenzione della sicurezza, devono essere accurate, dettagliate, frequentemente aggiornate e, cosa fondamentale, inclusive.

Esistono numerose metodologie di valutazione del rischio a disposizione delle organizzazioni, così come strumenti per misurare e valutare le diverse componenti del rischio. Non esiste un unico approccio alla misurazione del rischio che vada bene per tutti. Tuttavia, un'importante caratteristica comune è che le valutazioni del rischio devono colmare il falso divario tra sicurezza informatica e sicurezza fisica.

Gli operatori delle infrastrutture critiche possono migliorare la resilienza adottando un approccio sistematico ai rischi per la sicurezza fisica ed informatica, e adottando metodologie comuni e formali di valutazione del rischio per entrambi. Alcuni dei vantaggi:

- La condivisione delle tecniche di valutazione del rischio contribuisce a creare una coerenza nel calcolo dell'impatto dei rischi sull'impresa.
- I leader delle varie funzioni possono dare priorità e sostenere le loro specifiche raccomandazioni nello stesso modo e comunicare in modo uniforme tali rischi alla leadership esecutiva.
- L'alta dirigenza può far sì che tutti i rischi operativi siano presentati in modo analogo per la revisione, consentendo un processo decisionale più informato ed efficace.
- Le organizzazioni possono acquisire una comprensione olistica del rischio e gestire in modo corretto le priorità alle misure di protezione.

Tuttavia, non tutte le valutazioni dei rischi per la sicurezza supportano un approccio olistico alla gestione della sicurezza delle infrastrutture. Ad esempio, le valutazioni del rischio che considerano solo l'impatto diretto degli eventi di sicurezza, ignorando i loro potenziali effetti a cascata, possono oscurare le potenziali conseguenze e determinare la mancanza degli investimenti necessari nella sicurezza. Le valutazioni dei rischi per la sicurezza dovrebbero esaminare sia le conseguenze dirette di una violazione della sicurezza sia i suoi possibili impatti a valle per creare un approccio coordinato alla gestione dei rischi per la sicurezza.

Un esempio su tutti: un'intrusione fisica in un edificio non deve essere considerata solo come una debolezza nel controllo degli accessi, ma anche nella sicurezza della rete se l'ingresso non autorizzato può potenzialmente portare ad una violazione dei sistemi di dati. Questa prospettiva riconosce che singoli incidenti di sicurezza, come il furto di dati da parte di un dipendente, possono avere effetti a catena e portare a violazioni della conformità, multe, notizie sfavorevoli da parte dei media, sfiducia del pubblico, perdita di affari e altre conseguenze dannose.

La comunicazione del rischio è un aspetto importante per rendere le valutazioni dei rischi per la sicurezza più ampiamente applicabili. In particolare, mentre le valutazioni dei rischi per la sicurezza sono spesso condotti per guidare le decisioni dei professionisti della sicurezza e delle loro raccomandazioni, la comunicazione con gli altri stakeholders dovrebbe far parte del ciclo di valutazione del rischio. I risultati di identificazione, valutazione e risposta del rischio dovrebbero essere trasmessi agli utenti finali e ai proprietari dei processi operativi. Ad esempio, i risultati rilevanti di una valutazione dei rischi per la sicurezza potrebbero essere condivisi con i responsabili di piano delle centrali elettriche, per renderli più consapevoli della sicurezza, per far loro comprendere le categorie di minacce che devono affrontare e per aiutarli a capire le interdipendenze tra le vulnerabilità della sicurezza e le contromisure.

Un elemento fondamentale per una valutazione efficace dei rischi per la sicurezza a livello aziendale è un'indagine completa delle risorse in ogni sede. Senza di essa, può essere impossibile stabilire le priorità di protezione. Un'indagine sulle risorse della struttura nonché una valutazione dell'impatto dovrebbero porre domande dettagliate al fine di ottenere ciò che è davvero vitale nel complesso in ogni sito infrastrutturale, e quali sono le conseguenze di una violazione per le varie risorse. Le indagini dovrebbero chiedere: quali attività e operazioni critiche si svolgono in questa sede in questo momento? Quali risorse critiche si trovano in questa struttura? Quanto è costato sviluppare l'asset? La risorsa ha ancora valore se viene compromessa? Per essere completi, tutti le risorse - comprese le persone, le attrezzature/materiali, le informazioni, le strutture, le attività e le operazioni - devono essere sottoposti a questo livello di esame per identificarne la criticità.

Test di penetrazione

Oltre agli aspetti tecnici della sicurezza informatica, un approccio olistico richiede attenzione a ciò che i sistemi fanno, a tutti i modi in cui potrebbero essere compromessi e alle conseguenze che ne deriverebbero. La sicurezza informatica delle infrastrutture critiche non può essere garantita se la sicurezza fisica non è altrettanto solida.

Una volta riconosciuto, questo dovrebbe incentivare gli operatori delle infrastrutture critiche a considerare le vulnerabilità fisiche come parte di un test di penetrazione della rete. I test di penetrazione che non tengono conto delle minacce miste o ibride non possono offrire una reale garanzia di sicurezza dei sistemi di rete. È necessario condurre esercizi di penetrazione attiva che attacchino i punti di intersezione tra sicurezza fisica ed informatica e vadano oltre la scansione automatica delle vulnerabilità dei sistemi di rete.

I test di penetrazione congiunti sono anche un modo prezioso per creare alleanze e migliorare la comunicazione tra professionisti in entrambe le discipline e per migliorare il coordinamento delle strategie di protezione. Ad esempio, i risultati potrebbero evidenziare la necessità di posizionare le telecamere di sorveglianza in modo che possano essere d'aiuto negli esami forensi delle violazioni della rete (le telecamere possono aiutare a fornire prove nel caso in cui un dipendente lanci un attacco insider alla rete dalla postazione di lavoro di qualcun altro). Oppure può suggerire la necessità d'utilizzare sistemi video intelligenti per aiutare a proteggere le reti aziendali, analizzando il comportamento dei dipendenti e di altre persone che hanno accesso all'edificio (come il personale di servizio) e avvisando quando qualcuno si trattiene troppo a lungo in una stanza, ad esempio.

Molti ricercatori che conducono test di penetrazione della rete presso le infrastrutture critiche affermano che gli operatori hanno spesso un'opinione sbagliata della sicurezza delle loro reti perché trascurano i problemi di accesso fisico e spesso avvertono che sfruttare le reti aziendali attraverso un accesso fisico non autorizzato è in genere facile. Molti scoprono durante i test di penetrazione che chiunque abbia tempo, voglia e un po' di

know-how può infiltrarsi nei sistemi, osservare il traffico di rete dei sistemi industriali e persino ottenerne il controllo.
Le infrastrutture critiche devono valutare regolarmente l'efficacia della sicurezza fisica per impedire l'accesso ai sistemi tecnologici e di rete, in particolare a quelli identificati come critici. La vulnerabilità della rete può essere ridotta conducendo esercizi di penetrazione attiva per valutare se l'infiltrazione in una struttura potrebbe portare al furto di dati e se le vulnerabilità nei sistemi connessi potrebbero consentire che le intrusioni nella rete provochino danni fisici.

I risultati dei test di penetrazione nel mondo reale ne dimostrano la necessità.

- Durante i test condotti presso un'azienda, un membro del team di pen-test ha dichiarato che gli sono bastati alcuni nomi di dipendenti e un atteggiamento fiducioso per trovarsi in breve tempo in una stanza di postazioni di lavoro con decine di computer connessi ma non presidiati, da cui avrebbe potuto accedere a sistemi di dati critici.

- In un altro test, un'azienda di servizi pubblici voleva valutare la vulnerabilità dei suoi sistemi fisici ad un attacco di rete. Perciò, Il suo team ha cercato di individuare nelle liste di distribuzione gli indirizzi e- mail dei dipendenti che avevano accesso alle reti di supervisione, controllo e acquisizione dati (SCADA). Il suo team di penetrazione ha poi inviato loro messaggi di posta elettronica su un potenziale taglio dei benefici per i dipendenti e molti hanno cliccato su un link a un sito web che prometteva ulteriori informazioni al riguardo. Una volta fatto, il malware scaricato sul computer dell'utente ha permesso ai tester di controllarlo. In meno di un giorno, il team di penetrazione è stato in grado di interrompere la produzione e la distribuzione di energia dell'azienda.

- Un altro consulente in materia di penetrazione ha affermato che le aziende di solito partono dal presupposto che siccome hanno un sistema di badge, il loro centro dati è sicuro. Ma i sistemi di badge in genere non emettono un avviso quando viene cambiata l'immagine, ha spiegato, quindi nei test condotti dal red team potrebbe infiltrare nella rete di computer un client per cambiare la foto di un dipendente con quella di un membro del gruppo della sua squadra. Poi, quando l'individuo si reca in azienda e il "suo badge" non funziona, il personale lo cerca nell'elenco e vede che la sua foto è presente nel sistema, e di solito lo fa entrare con un badge temporaneo. Inoltre, poiché i sistemi di accesso raramente avvisano quando il livello di privilegio di accesso di una persona cambia, egli può concedere ai membri della sua squadra l'accesso remoto a qualsiasi parte dell'edificio. Secondo gli esperti, è molto probabile che queste intrusioni facili funzionino, e notano che le infiltrazioni di base sono spesso efficaci, come far "saltare" porte protette elettronicamente con un semplice filo di rame, o far scattare i sensori del sistema di richiesta di uscita spingendo un dispositivo che genera calore sotto la porta e tenendolo vicino al pannello della porta.

Un buon coordinamento tra sicurezza informatica e sicurezza fisica è necessario per capire se si stanno verificando attacchi convergenti, come si stanno verificando e come rispondere ed indagare. Il coordinamento tra sicurezza fisica e sicurezza informatica è anche una base necessaria per molte contromisure di successo, come l'approvvigionamento e de-approvvigionamento comune per gli utenti, sia per i sistemi informatici sia per quelli fisici; un unico processo di gestione delle identità; processi di log-off automatizzati; la segmentazione delle reti in modo che una violazione da internet non possa raggiungere i sistemi di controllo; la fornitura di controlli di accesso più severi a tutte le apparecchiature e il miglioramento del rilevamento di comportamenti e attività insoliti.

Le valutazioni congiunte dei rischi fisici ed informatici, l'uso di metodologie di valutazione del rischio simili per entrambe le discipline e la conduzione di test di penetrazione che affrontino le minacce ibride sono strategie che possono aiutare gli operatori delle infrastrutture critiche a migliorare il coordinamento tra sicurezza fisica ed informatica.

Informazioni sull'autore:
Garett Seivold è un giornalista di carriera specializzato in sicurezza che scrive per l'International Security Ligue.

7. Usare le metriche e altre attività per colmare il divario tra la strategia della Sicurezza Fisica e quella della Cybersecurity

Man mano che gli operatori delle infrastrutture critiche riconoscono le interdipendenze critiche che esistono tra le diverse attività di sicurezza, dovrebbe diventare chiaro l'enorme valore di un approccio integrato alla sicurezza, in cui le strategie per la protezione delle risorse fisiche ed informatiche non sono create in modo isolato, ma sono invece sviluppate in modo olistico.

Ma la strada per arrivarci può sembrare lunga e difficile. I silos di sicurezza esistenti possono avere radici profonde e istituire un cambio di rotta può sembrare un compito monumentale. Alcune organizzazioni possono ritenere che le strategie spesso utilizzate per raggiungere l'allineamento siano dirompenti o di portata eccessiva, come ad esempio unire la sicurezza fisica e quella informatica in un unico dipartimento, nominare un unico dirigente per la supervisione di entrambe le funzioni o creare un nuovo ente, comitato di rischio o di supervisione. In effetti, raggiungere la convergenza strategica della sicurezza non è una questione semplice. Il rischio per la sicurezza è insito in tutti i processi di un'infrastruttura critica, ma i proprietari di tali processi si consultano raramente tra loro. Le differenze culturali operative possono costituire un ostacolo incredibile alla creazione di una strategia di sicurezza coordinata, anche tra la sicurezza fisica e quella informatica. Oppure i dipartimenti che svolgono funzioni di sicurezza possono collaborare, ma incrociarsi solo occasionalmente. Per esempio, nelle assunzioni possono essere coinvolte sia la sicurezza che le risorse umane, ma la sicurezza tende a occuparsi di condurre indagini approfondite sui precedenti, mentre le risorse umane possono occuparsi di ridurre i tempi delle assunzioni.
In assenza di una fusione strutturata tra reparti che crei integrazione, non è facile che tutti si trovino sulla stessa lunghezza d'onda sulla sicurezza. Tuttavia, non tutte le strade per migliorare il coordinamento devono passare attraverso la ristrutturazione delle funzioni di sicurezza fisica ed informatica dell'organizzazione.

Esistono attività specifiche che possono aiutare le infrastrutture critiche ad allineare le molte funzioni disparate che hanno un ruolo da svolgere nella protezione, spingendo l'organizzazione verso una strategia di sicurezza più integrata. Le possibilità includono:

- Identificare nel master plan della sicurezza tutte le attività di protezione che la società conduce, e quali sono i dipartimenti e le persone responsabili per ciascuno di essi.
- Condividere le tecniche di valutazione dei rischi per la sicurezza per creare coerenza nella valutazione del rischio.
- Sviluppare processi e strumenti standardizzati per l'identificazione, la raccolta e la gestione dei dati, la segnalazione dei rischi e degli eventi di sicurezza.
- Implementare canali chiari per la segnalazione e la condivisione di informazioni sulla sicurezza e i rischi.
- Partecipare ai comitati con rappresentanti di diverse parti dell'azienda per discutere delle sfide e delle soluzioni in materia di sicurezza.
- Implementare la tecnologia che guida le soluzioni di sicurezza aziendale.
- Formalizzare la condivisione dell'intelligence e il processo decisionale collaborativo tra tutte le funzioni che hanno

responsabilità in materia di sicurezza e che hanno un impatto sulle operazioni di sicurezza.

Alcuni gruppi promuovono l'acronimo "SIMPLE" per comunicare in modo semplificato i vantaggi di un approccio convergente della gestione dei rischi per la sicurezza. Una strategia di sicurezza integrata consente alle infrastrutture critiche quanto segue:

- **(Strategic view)** Visione strategica del rischio organizzativo in tutti i dipartimenti, che si traduce in meno politiche, meno margine di errore e processi e meccanismi di reportistica più snelli.
- **(Improvement)** Miglioramento delle comunicazioni grazie all'integrazione di risorse adeguate; con il risultato di una migliore pianificazione della continuità operativa e di un'efficace gestione del cambiamento per creare una cultura organizzativa più incentrata sulla sicurezza.
- **(Mitigation)** Mitigazione del rischio poiché l'intelligence, le indagini e le tecniche di recupero in caso di disastro, sono integrate al meglio, riducendo l'esposizione e aumentando l'agilità alle condizioni.
- **(Process alignement)** Allineamento dei processi e aumento dell'efficienza; con conseguente riduzione delle riunioni e una riduzione della sovrapposizione di processi e procedure.
- **(Legislation)** Garanzia della legislazione e della conformità; con conseguente semplificazione del processo di conformità e una posizione legale e normativa migliorata.
- **(Effective evaluation)** Valutazione efficace delle procedure di revisione aziendale; con dei miglioramenti che permettono una maggiore comprensione degli obiettivi e dei metodi di attacco, riducendo al contempo le vulnerabilità.

Collegare metriche

Una visione integrata e strategica della sicurezza pone necessariamente domande di ampio respiro quali:

- Quanto mi costa la sicurezza?
- Cosa ottengo in cambio del mio denaro?
- Funziona?
- Si può migliorare?
- Si può fare a costi inferiori?

Non è possibile rispondere a queste domande basilari - alle quali l'alta dirigenza deve rispondere per stabilire le priorità e stanziare il budget per la protezione - senza un programma di metriche per la sicurezza ponderato e ben pianificato. I responsabili della sicurezza dovrebbero essere degli alleati in questo processo, dimostrando disponibilità a condividere le informazioni, ad integrare i processi e ad ammettere che altre priorità di rischio possono talvolta avere la precedenza.

I responsabili della sicurezza devono anche adottare una visione che vada oltre il rincorrere obiettivi vaghi per il loro dipartimento ed avere responsabilità su misurazioni specifiche delle prestazioni, in modo da avere una visibilità estesa sulle vulnerabilità dell'azienda. Spesso gli obiettivi per la sicurezza vengono identificati in modo troppo generico per indirizzare le attività di miglioramento; l'obiettivo della sicurezza, ad esempio, può essere visto come un obiettivo generale per fornire un ambiente sicuro e protetto. Questo può essere problematico poiché **la mancanza di chiari indicatori di performance della sicurezza e di obiettivi da raggiungere può portare a un eccesso di discrezionalità a livello operativo.** Il risultato può essere che ciò che i dirigenti aziendali desiderano dalla sicurezza non si riflette nei settori in cui gli operatori scelgono di concentrare il loro tempo, la loro attenzione e le loro risorse. Le azioni del personale di sicurezza devono corrispondere a ciò che l'organizzazione ritiene necessario per massimizzare la protezione - un aspetto

che le metriche per la sicurezza formali possono contribuire a garantire.
Le metriche per la sicurezza convergenti, se appropriate, possono migliorare ulteriormente l'allineamento. È un modo per un'organizzazione di analizzare ed affrontare in modo olistico le minacce critiche e di informare efficacemente l'organizzazione sui suoi progressi.

Ad esempio, se il furto di dati è un problema, è possibile sviluppare un programma di metriche per la sicurezza convergenti per affrontarlo, che identifichi obiettivi e misure di performance per ciascun gruppo al servizio della missione collettiva. Per quanto riguarda la sicurezza fisica, ad esempio, potrebbe essere importante rafforzare la cultura della sicurezza e migliorare l'adesione alle politiche di controllo degli accessi, quindi le metriche possono essere progettate per misurare e migliorare l'atteggiamento dei dipendenti. Per l'IT, le password deboli possono essere considerate un fattore che contribuisce al furto di dati e le metriche possono essere progettate per misurare i progressi verso una migliore applicazione dei criteri sulle password. In questo modo, l'organizzazione può misurare i progressi verso una migliore sicurezza dei dati, assicurando al contempo che sia la sicurezza informatica che quella fisica facciano parte della soluzione.

È importante definire misure di performance per la sicurezza, ma queste possono rafforzare i silos della sicurezza se gli obiettivi e le misure di sicurezza non sono stati raggiunti.

Le misure di performance riflettono solo le esigenze di sicurezza dei singoli reparti e unità. Le metriche di sicurezza dovrebbero anche essere concepite per fungere da ponte, consentendo alle organizzazioni di prendere in considerazione le minacce e rischi tra i vari reparti e allineare le misure di performance agli obiettivi organizzativi.

Quando si adotta un approccio di metriche collettive, le metriche per la sicurezza aiutano a unificare le missioni di sicurezza dei vari dipartimenti e la possibilità per l'alta dirigenza di valutare la sicurezza da una prospettiva strategica piuttosto che da un modello di rischio/correzione o incidente/contromisura.

Le metriche per la sicurezza integrate sono un modo con cui le infrastrutture critiche possono contribuire ad allineare le funzioni di sicurezza senza una ristrutturazione fondamentale, insieme alla comunicazione, il reporting, la raccolta dati e strategie tecnologiche.

Informazioni sull'autore:
Garett Seivold è un giornalista professionista specializzato in sicurezza che scrive per l'International Security Ligue.

8. Un nuovo paradigma di Sicurezza nella minacciosa era informatica – Dalla Sicurezza Fisica alla Sicurezza Convergente nella gestione delle informazioni.

Era il 2005 quando James I Chong coniò l'acronimo PSIM, dopo aver fondato la società VidSys. Un PSIM è un software che raccoglie i dati di tutte le applicazioni di sicurezza (antifurto, TVCC, controllo accessi, allarme antincendio...), consentendone il loro controllo attraverso un'interfaccia unificata, supportando il personale della Centrale di Ricezione Allarmi, della Sala di Controllo e del Centro di Comando per essere al corrente della situazione, per prendere decisioni e reagire anche prima che si verifichi una violazione della sicurezza.

Per essere più chiari, lo PSIM non è solo una piattaforma di integrazione, ma piuttosto un software intelligente che converte enormi quantità di dati in informazioni significative e fruibili. Ciò avviene filtrando e correlando i dati in base a tempo, luogo, durata, frequenza e tipo; utilizzando algoritmi sofisticati che potrebbero includere tecnologie all'avanguardia, come i Big Data e l'Intelligenza Artificiale.

Poiché lo PSIM si evolve costantemente in base alle esigenze dei clienti e dei processi aziendali, già nell'ultimo decennio ha iniziato a spostarsi naturalmente verso ciò che è stato identificato come Converged Security and Information Management (CSIM, ancora una volta un nuovo acronimo del sig. Chong). Il concetto alla base di questa evoluzione può essere facilmente ricondotto al fatto che tutte le applicazioni di sicurezza sono ora convergenti con l'IP. Di conseguenza, poiché l'anti-manomissione è intrinseca a tutte le caratteristiche dei sistemi di sicurezza, la cybersecurity e la cyber-resilienza sono state adottate dai produttori di sistemi di sicurezza e, di conseguenza, implementati nel PSIM, ora CSIM.

Ma in un'epoca in cui la sicurezza fisica e quella informatica si stanno fondendo per rispondere meglio agli attacchi combinati, è giunto il momento di ampliare la portata del PSIM/CSIM per includere la consapevolezza sulla situazione per la sicurezza di quelli che stanno diventando - o sono già - gli asset maggiormente cruciali in qualsiasi infrastruttura pubblica o privata: l'informatica e i dati. Infatti, diversi studi mostrano come sia necessario un approccio olistico per evolvere verso una piena comprensione dei rischi in continuo sviluppo che i sistemi fisici ed informatici devono affrontare.

Il CSIM, se correttamente progettato e implementato, estende le capacità del software oltre la sicurezza fisica, acquisendo e correlando i dati provenienti da più sistemi di sicurezza informatica e sistemi di gestione delle informazioni.

Con funzionalità per asset o clienti su larga scala e ampiamente dislocati, questo tipo avanzato di piattaforma può essere sfruttato efficacemente per supportare la fornitura di Servizi di Sicurezza Privati (SSP) in una varietà di casi d'uso come la protezione delle infrastrutture critiche, la sicurezza della catena di approvvigionamento, la sicurezza del pubblico e degli eventi, la gestione di edifici e impianti e così via.

Con il passaggio dal PSIM al CSIM, si prevede una migliore cooperazione - se non addirittura una fusione - tra funzioni precedentemente contrastanti come la sicurezza fisica e la sicurezza informatica. Le organizzazioni coinvolte in questo processo sono spinte verso una convergenza organizzativa ed operativa che richiede la fusione delle funzioni. I

fornitori di sicurezza privata che offrono soluzioni complete in questo scenario e adottano la tecnologia CSIM, devono ampliare le loro competenze e abilità, aggiungendo la sicurezza informatica alla base delle conoscenze aziendali. Devono inoltre integrarla nella loro cultura aziendale, implementando coerentemente l'approccio olistico di cui sopra.

Le aziende di sicurezza più innovative del mondo hanno già iniziato questo processo e già sono attivi diversi fornitori all'avanguardia che possono vantare casi di successo, confermando come l'approccio olistico è la strada da seguire. Queste Società di Sicurezza Privata sono ora in grado di supportare i clienti che si trovano ad affrontare nuove minacce combinate, informatiche e fisiche, comprendendo le loro esigenze a partire dalla fase di analisi del rischio.

Informazioni sull'autore:
Antonello Villa è un imprenditore ed esperto di centrali di allarme e di monitoraggio in generale.
È anche vicepresidente di Confedersicurezza, l'associazione italiana che rappresenta le aziende di sicurezza privata. All'interno della CoESS, ha presieduto per molti anni il Comitato Monitoraggio e Telesorveglianza ed è stato membro del Consiglio di Amministrazione.

Un case-history...

... in cui l'uso di un CSIM avrebbe potuto essere utile. Il caso riguardava un famoso marchio che gestisce diversi stabilimenti a livello globale. In uno di questi stabilimenti, situato nella Repubblica Ceca, alcuni criminali hanno sferrato un attacco informatico a un server destinato alla gestione degli ordini di ritiro. Grazie alle misure informatiche in atto, comunemente supportate da un sistema di rilevamento delle intrusioni (IDS), l'attacco è stato individuato in pochi minuti, portato all'attenzione dei team IT competenti e risolto. Ma a causa della mancanza di convergenza tra sicurezza informatica e fisica e, di conseguenza, della mancata implementazione della sicurezza informatica all'interno dello strumento adottato per gestire la sicurezza fisica (un PSIM), in un lasso di tempo così breve i criminali sono stati in grado di dare l'autorizzazione a un finto operatore logistico per un prelievo fittizio. Lo PSIM è stato alimentato da dati falsi per concedere l'accesso a questo falso "operatore" e un carico completo è stato rubato. I responsabili della sicurezza non sono riusciti a bloccare questa frode perché, dal punto di vista della sicurezza generale, mancava un pezzo importante del quadro, cioè quello che descrive l'attacco informatico. Con un CSIM, questa informazione cruciale sarebbe stata condivisa tra i team IT e di sicurezza, i quali avrebbero potuto rinviare le operazioni di trasporto fino a quando il server non fosse stato nuovamente operativo, e di fornire alle forze dell'ordine competenti le informazioni giuste per identificare ed arrestare i criminali, nell'ambito di un partenariato pubblico-privato (PPP) ben consolidato.

9. Physical-Cyber Security: La legislazione e/o gli standard dell'Unione Europea possono aiutare?

Negli ultimi anni, l'Unione Europea è stata all'avanguardia nell'elaborazione di una legislazione in ambito digitale, che ha avuto un impatto e ha influenzato legislatori che vanno ben oltre i confini dell'Unione.
È il caso, ad esempio, del regolamento generale sulla protezione dei dati (GDPR), entrato in vigore nel 2018. Possiamo quindi aspettarci che anche altre legislazioni, esistenti o in corso, possano ispirare i legislatori di altre regioni del mondo.
Diverse direttive e regolamenti dell'UE sono rilevanti per l'argomento del presente Libro Bianco:

- Sotto la voce "Protezione delle infrastrutture critiche":
  - Dal punto di vista informatico, il cosiddetto "NIS1" ("Network and Information Security"). Direttiva, che sarà aggiornata a breve dal "NIS2", che prevede regole più severe.
  - Dal punto di vista fisico, la Direttiva sulla resilienza delle entità critiche ("CER"), che sostituisce la Direttiva 2008/114 sulla protezione delle infrastrutture critiche.
- Sotto la voce "Requisiti di cybersecurity per i produttori e utenti di prodotti e servizi connessi:
  - La legge sulla sicurezza informatica dell'UE
  - Legge sulla resilienza informatica dell'UE ("CRA"in corso)
  - La direttiva sulle apparecchiature radio (cosiddetta "RED" - Radio Equipment Directive)
  - La legge UE sull'intelligenza artificiale

Osservando questa complessa rete di direttive e regolamenti nel contesto della Cyber-Physical Security si può notare che: **la cybersecurity e la sicurezza fisica sono gestite separatamente nelle imprese, così come lo sono anche nella legislazione.**
Questa è la prima osservazione che il CoESS ha fatto ai servizi competenti della Commissione Europea Durante la preparazione delle proposte per le direttive CER e NIS2. Nonostante il fatto che nelle proposte fosse indicato come queste due aree dovevano essere gestite in parallelo, il legislatore non si è spinto fino ad affrontarle in un unico testo. Si tratta di un'occasione persa o solo di un segno che la situazione non era abbastanza matura?
Certo, le due direttive hanno una buona dose di riferimenti incrociati e di requisiti paralleli, ma il CoESS non ritiene che questo sia sufficiente. L'unico aspetto positivo della situazione è che ha dato l'opportunità di chiedere che le disposizioni contenute nella proposta NIS2 venissero rispecchiate nella proposta CER; in particolar modo il riferimento agli standard.
La direttiva CER adottata raccomanda agli Stati membri di utilizzare gli standard per verificare la qualità dei fornitori di sicurezza. Tuttavia, il fatto che le due direttive siano nate da servizi diversi della Commissione Europea e abbiano seguito iter diversi al parlamento europeo non è stato l'ideale.

Cosa hanno in comune i due testi:

- In una certa misura, i settori identificati come "entità critiche", facendo riferimento ai "servizi essenziali" nel NIS sono simili; anche se non del tutto uguali a quelli che i NSI definiscono "servizi essenziali";
- Questi servizi essenziali/entità critiche hanno l'obbligo di effettuare una valutazione del rischio e di adottare le misure appropriate per proteggere le entità e garantirne la resilienza;

- Gli operatori di tali servizi/entità devono segnalare gli episodi dirompenti alle autorità competenti.

Anche se dovrebbero entrare in vigore più o meno nello stesso periodo – attorno al 2024 - a seguito dei recenti atti di sabotaggio nel mar Baltico ai danni di condutture sottomarine il Consiglio ha recentemente invitato gli Stati membri ad accelerare il recepimento della Direttiva CER. La Commissione ha sottolineato che le infrastrutture energetiche e di trasporto dovrebbero richiedere particolare attenzione ed essere sottoposte a stress test.
Per quanto riguarda gli standard, durante la ricerca di quelli esistenti che potrebbero indirizzarci verso la Cyber-Physical Security, abbiamo trovato uno standard IEC, EN IEC 62443, uno standard di sicurezza informatica per le operation technolgies. Sebbene non si tratti esattamente della protezione dei Cyber-Physical Systems (CPS), l'approccio potrebbe essere utilizzato come modello per affrontarli, poiché le operation technologies (OT) sono CPS.
L'IEC 62443 è una serie di norme sviluppate da due gruppi all'interno dell'IEC, in consultazione con altri gruppi di normazione all'interno dell'ISO, tra gli altri.

L'approccio è basato sul rischio e viene applicato in un'ampia gamma di settori, tra cui:

- Reti e sistemi di utilità
- Impianti idroelettrici
- Eolico offshore
- Ferrovie, navigazione e aviazione
- Controllo degli edifici
- Automazione industriale ed "IioT"

È necessario effettuare un'analisi più dettagliata per determinare come i principi della norma IEC 62443 possano essere trasposti alle CPS in materia di sicurezza.
Sul piano fisico, il CEN TC 439 "Private Security Services", di cui il CoESS è parte attiva, sta sviluppando un intero sistema di standard per definire i criteri di qualità per i fornitori di servizi di sicurezza attivi nella protezione delle infrastrutture critiche:

- EN 17483-1:2021 "Servizi di Sicurezza Privata -CIP- requisiti generali": come indicato, questo standard fornisce i requisiti generali di sicurezza per aziende che offrono servizi in qualsiasi tipo di infrastruttura critica. Include criteri che riguardano la necessità di proteggere i dati dei clienti, ma non fa implicitamente riferimento alla protezione olistica del CPS.
- prEN17483-2 "Servizi di Sicurezza Privata – CIP- Airport and Aviation Security": è l'aggiornamento della precedente EN 16082:2011 "Airport and Aviation Security Services".
- prEN17483-3 "Servizi di Sicurezza Privata – CIP- Maritime and Port Security": è l'aggiornamento della precedente EN 16747:2015.
- futura EN17483-4 "Servizi di Sicurezza Privata – CIP - Produzione e Trasporto di Energia"
- Saranno sviluppati altri standard, molto probabilmente in materia di assistenza sanitaria e di ospedali, impianti di trattamento delle acque e altre "CI"(infrastrutture critiche) che lo richiedano.

E poi?

In futuro, questi standard dovranno includere una disposizione che richiami l'attenzione sulla necessità di adottare un approccio olistico ai Cyber-Physical Systems, ma ciò sarà efficace solo se gli operatori dell'IC (infrastrutture critiche) avranno lo stesso approccio.
Oggi più che mai, la catena della sicurezza deve garantire che ogni anello sia robusto quanto l'altro. Deve inoltre avere un approccio olistico e team multidisciplinari in cui gli specialisti della sicurezza fisica e della cybersecurity lavorino insieme per lo stesso obiettivo.

Informazioni sull'autore:
Catherine Piana è direttore generale della CoESS dal 2014 e di ASSA-i dal 2016 e presidente del Comitato tecnico del CEN. TC 439 "Servizi di sicurezza privata".

10. Tabella della legislazione UE rilevante per la Physical-Cyber Security

	Requisiti di protezione dei dati	Requisiti per la protezione delle infrastrutture critiche (Fisica ed Informatica)	
	Regolamento generale sulla protezione dei dati (GDPR)	**Sicurezza delle reti e delle informazioni 1&2 (NIS 1 & 2) Direttiva**	**Direttiva sulla resilienza delle entità critiche ("CER")**
Obiettivo	Protezione dei dati personali dei cittadini dell'UE e nuovi diritti di privacy.	Alto livello di sicurezza informatica delle entità critiche in tutta l'UE - il NIS 1 è stato aggiornato da norme più severe del NIS 2.	Alto livello di sicurezza informatica delle entità critiche in tutta l'UE - il NIS 1 è stato aggiornato da norme più severe del NIS 2.
Ambito di applicazione	Il GDPR impone obblighi di protezione dei dati a tutte le organizzazioni che raccolgono e/o elaborano dati di cittadini dell'UE.	Operatori di "Entità critiche" nei seguenti settori: NIS 1 (attuale): sanità, trasporti, mercato finanziario, energia, approvvigionamento idrico, infrastrutture digitali e fornitori di servizi. NIS 2 (aggiornamento): reti di comunicazione elettronica, reti sociali, centri dati, spazio, gestione dei rifiuti, settore chimico, servizi postali, produzione di prodotti critici, prodotti alimentari, pubblica amministrazione, ricerca. L'articolo 2 del NIS 2 e gli allegati forniscono una panoramica del tipo di entità critiche di questi settori che rientrano nel campo d i applicazione della direttiva.	Operatori di "entità critiche" nei seguenti settori: energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione e spazio. Viene stabilita una metodologia per identificare le entità critiche che rientrano nella direttiva.
Disposizioni rilevanti (non esaustive)	Il trattamento dei dati è soggetto ai principi di protezione e di responsabilità, sulla base del consenso dell'interessato (con esenzione per le attività di delle Forze dell'Ordine) I dati devono essere trattati dal titolare del trattamento in modo sicuro in base a determinate misure tecniche ed organizzative La protezione dei dati è un requisito di progettazione e predefinito in qualsiasi nuovo prodotto o attività commerciale/servizio	Il trattamento dei dati è soggetto ai principi di protezione e di responsabilità, sulla base del consenso dell'interessato (con esenzione per le attività di delle Forze dell'Ordine) I dati devono essere trattati dal titolare del trattamento in modo sicuro in base a determinate misure tecniche ed organizzative La protezione dei dati è un requisito di progettazione e predefinito in qualsiasi nuovo prodotto o attività commerciale/servizio	Gli Stati membri hanno l'obbligo di disporre di una strategia per garantire la resilienza delle entità critiche, d'effettuare una valutazione del rischio nazionale e identificare le entità critiche. Le entità critiche sono tenute a effettuare valutazione del rischio, ad adottare misure tecniche, di sicurezza e organizzative adeguate a incrementare la resilienza e segnalare alle autorità nazionali gli incidenti che causano disagi. Le misure tecniche, di sicurezza e operative comprendono la designazione del personale critico, anche tra i fornitori di servizi esterni, e il controllo qualità di tale personale in termini di qualificazione e formazione. Altre misure includono un'adeguata protezione fisica di aree sensibili, come recinzioni, barriere, monitoraggio del perimetro, apparecchiature di rilevamento, controlli di accesso, gestione della sicurezza dei dipendenti e misure di continuità aziendale.
Applicabile	Dal 2018.	NIS 1: dal 2018. NIS 2: a partire dal 2024	Dal 2024.

	Requisiti di sicurezza informatica per i produttori ed utenti di prodotti e servizi connessi			
	Legge sulla sicurezza fisica ed informatica dell'UE ("EU Cybersecurity ACT")	**Legge sulla resilienza informatica ("Cyber Resilience Act")**	**Direttiva sulle apparecchiature radio ("Radio Equipement Directive - RED")**	**Legge UE sull'Intelligenza Artificiale ("EU Artificial Intelligence Act")**
Obiettivo	Tra le altre cose, la legge sulla cybersecurity rafforza la fiducia nei prodotti "ICT" istituendo un quadro di certificazione della cybersecurity per prodotti e servizi.	Standard minimi di cybersecurity per tutti i prodotti hardware e software connessi per proteggere meglio gli utenti dalle minacce alla cybersecurity.	Garantire che le apparecchiature radio siano sufficientemente sicure. Una legge delegata del 2021 ha aggiornato la direttiva del 2014 per migliorare la sicurezza informatica dei prodotti coperti.	Regolamentazione dell'uso di sistemi di IA ad alto rischio.
Ambito di applicazione	Produttori e utenti di prodotti e servizi basati sulle TIC.	Produttori di tutti i prodotti hardware e software collegati.	Produttori e utenti di apparecchiature elettriche ed elettroniche che possono utilizzare lo spettro radio per scopi di comunicazione e/o determinazione radio - tra cui apparecchiature radio connesse ad internet, macchine, sensori, reti e IoT.	Produttori e utenti di sistemi di IA ad alto rischio identificati nell'allegato della legge europea sull'IA; comprese le tecnologie e i sistemi di identificazione biometrica.
Disposizioni rilevanti (non esaustive)	Il quadro di certificazione fornirà a livello europeo schemi di certificazione come un insieme completo di regole, requisiti tecnici, standard e procedure per prodotti e servizi basati sulle TIC. Attesterà che i prodotti e i servizi ICT che sono stati certificati in conformità a tale schema sono conformi ai requisiti specificati. L'uso di prodotti certificati può essere reso obbligatorio dagli Stati membri o dall'UE, come previsto dalla Direttiva NIS 2.	Disposizioni generali: I prodotti devono soddisfare specifici requisiti stabiliti dalla legge, da documentare con una dichiarazione di conformità UE. Tutti i prodotti coperti devono recare il marchio CE. Valutazione della conformità: per un numero specifico di "prodotti critici", una terza parte dovrebbe essere coinvolta nella valutazione della conformità. Aggiornamenti sulla cybersecurity: I produttori devono garantire la cybersecurity attraverso aggiornamenti di sicurezza costanti e gratuiti tramite aggiornamenti automatici e la notifica agli utenti degli aggiornamenti disponibili per la durata prevista del prodotto o comunque per cinque anni.	L'articolo 3 della RED in relazione alla salute e la sicurezza, e altro ancora. La legge delegata prevede inoltre che: Gli operatori di rete e i fornitori di servizi devono garantire che i loro sistemi e piattaforme sono sicuri. I produttori di apparecchiature devono assicurarsi che siano progettate tenendo conto dei principi di sicurezza. Gli utenti devono essere consapevoli dei rischi legati all'esecuzione di alcune operazioni e della necessità di effettuare i necessari aggiornamenti delle apparecchiature che utilizzano.	Le tecnologie e i sistemi di IA ad alto rischio, compreso il loro utilizzo, devono rispettare diverse disposizioni, tra cui quelle relative alla governance dei dati, alla supervisione umana e alla sicurezza informatica.
Applicabile	Sono in corso lavori su diversi schemi di certificazione, ad esempio per i servizi cloud.	Attualmente negoziato a livello di UE.	RED si applica dal 2016. I requisiti aggiornati di cybersecurity saranno in vigore dal 2025.	Attualmente negoziato a livello UE, si applicherà in modo effettivo molto probabilmente non prima del 2025.

Editori

Armin Berchtold
Segreteria generale della Lega Internazionale per la Sicurezza c/o Securitas AG Alpenstrasse 20
CH-3052 Zollikofen infoliga@security-ligue.org www.security-ligue.org

Catherine Piana
Direttore generale CoESS aisbl
56 Avenue des Arts 1000 Bruxelles Belgio catherine@coess.eu www.coess.eu

Versione italiana a cura di ConFederSicurezza e Servizi & Fondazione Asfàleia
Traduzione: Xheni Gjoni
Revisione della traduzione: Antonello Villa
Design e grafica: Mariarosaria Sardelli