#05

ICT Security MAGAZINE

INDUSTRIAL CYBER SECURITY

PREFAZIONE DI

RENATO MAZZONCINI

CEO di a2a

2024

QUADERNI DI CYBER INTELLIGENCE

WWW.ICTSECURITYMAGAZINE.COM

WWW.SOCINT.ORG

WWW.AIPSA.IT

IN COLLABORAZIONE CON:

aipsa

ASSOCIAZIONE ITALIANA PROFESSIONISTI SECURITY AZIENDALE

ICT Security MAGAZINE

QUADERNI DI CYBER INTELLIGENCE

La presente collana, frutto della collaborazione tra ICT Security Magazine e la Società Italiana di Intelligence (SOCINT), inaugura una serie di contenuti volti ad arricchire e approfondire il dibattito scientifico sulla Cyber Intelligence.

in collaborazione con:

aipsa
ASSOCIAZIONE ITALIANA PROFESSIONISTI SECURITY AZIENDALE

ICT SECURITY MAGAZINE

1° rivista italiana di sicurezza informatica, attiva da oltre 20 anni, dedicata in forma esclusiva alla cyber security e alla business continuity, si pone l'obiettivo di coinvolgere i più importanti attori del settore, aziende e istituzioni pubbliche, per la diffusione degli elementi conoscitivi legati a tutti gli aspetti della information security.

SOCIETÀ ITALIANA DI INTELLIGENCE

SOCINT è un'associazione scientifica senza fini di lucro, il cui obiettivo è quello di promuovere la cultura e lo studio dell'intelligence in Italia.

AIPSA

L' A.I.P.S.A. ha come scopo istituzionale di valorizzare l'ordinamento professionale del Security Manager, formare ed aggiornare gli associati, diffondere la cultura della Security ed approfondire lo studio delle sue problematiche di ordine tecnico, funzionale, giuridico e legislativo. Per attuare i propri fini l'Associazione è entrata a far parte di numerosi e diversificati organismi attraverso i quali realizza le sinergie necessarie al raggiungimento degli obiettivi strategici di volta in volta indicati in programmi triennali.

Indice

PREFAZIONE

Oggi la cybersecurity è una priorità strategica per tutte le organizzazioni, indipendentemente dalle loro dimensioni e dal settore di attività in cui operino.

Le tecnologie si sono evolute a tale velocità che abbiamo perso di vista alcuni dei pericoli che portano con sé: non è più il tempo in cui la sicurezza poteva essere ridotta a mero vantaggio competitivo o a una questione di compliance, rappresentando al contrario un autentico fattore critico per il successo.

LE ATTUALI SFIDE DELL'INDUSTRIAL SECURITY

Nel mondo industriale – in particolar modo per le *multiutility* – la situazione è particolarmente delicata: in questo contesto un attacco informatico può infatti avere serie conseguenze sulla produzione e la distribuzione di energia, con ricadute molto gravi sulla continuità del servizio erogato a cittadini, imprese e Pubbliche Amministrazioni, nonché sul piano economico e di reputazione aziendale.

La crescente complessità degli impianti industriali, che sfruttano sempre più l'automazione e le opportunità di *smart monitoring* offerte dai sistemi di controllo basati sui dati (ICS/SCADA) per migliorare l'efficienza dei processi produttivi, ha comportato una significativa estensione delle superfici di rischio.

Il risultato è un aumento esponenziale degli

attacchi informatici mirati alle infrastrutture industriali. In questo scenario, l'Italia si sta dimostrando particolarmente fragile: nel 2023 siamo stati il terzo Paese al mondo (e il primo in Europa) maggiormente colpito da attacchi *malware*[1].

Nell'80% dei casi le vittime sono PMI[2], realtà più "fragili" e meno strutturate nelle quali sembra ancora persistere una scarsa cultura della cybersecurity, insieme a un'insufficiente consapevolezza rispetto al grado di strategicità da attribuirle.

Tuttavia, lungi dal riguardare soltanto piccole e medie imprese, il problema finisce per interessare l'intero ecosistema; specie considerando il ruolo centrale che le PMI rivestono entro le lunghe e complesse catene di fornitura di servizi essenziali come le *Utilities*.

In questo settore, infatti, i frequenti attacchi cyber contro un singolo anello della *supply chain* possono avere conseguenze importanti sul servizio finale.

LE PRINCIPALI MINACCE PER IL MONDO INDUSTRIALE

Pur variando a seconda delle tecniche impiegate e delle vulnerabilità sfruttate, le conseguenze di un attacco informatico possono essere davvero serie, arrivando a mettendo a repentaglio la privacy di dipendenti e clienti attraverso il furto (ed eventuale divulgazione successiva) di dati sensibili.

Qualora gli effetti includano l'interruzione o il rallentamento della produzione, ne derivano anche ingenti perdite economiche e rilevanti danni d'immagine per l'azienda erogatrice.

Nel contesto degli impianti industriali e a maggior ragione nel mondo delle *Utilities,* dove tutto è ulteriormente aggravato dalla natura stessa dei servizi erogati, possono poi verificarsi conseguenze ben più gravi.

Ad esempio, senza dover rievocare casi eclatanti come Stuxnet o Triton, è facilmente immaginabile che il blocco di un servizio di fornitura idrica o elettrica possa finire per compromettere la sicurezza individuale, nazionale o addirittura globale; un rischio che gli analisti di *intelligence* sottolineano già da diversi anni[3].

LA CYBERSECURITY SECONDO A2A

Considerato quanto la crescente digitaliz-

1. Stepping ahead of risk, Trend Micro 2023 Midyear Cybersecurity Threat Report

2. Il Sole24Ore (dati al settembre 2023)

3. Expert sees 'extreme uptick' in cyberattacks on utilities, RTO Insider (2018)

zazione e interconnessione dell'Industria 4.0 abbia reso il settore più vulnerabile agli attacchi informatici, esistono ormai diversi framework dedicati.

Ne sono un esempio le linee guida del National Cybersecurity Center of Excellence (parte del NIST statunitense) per le infrastrutture idriche[4] e analoghi documenti che evidenziano, tra le altre cose, la rapida evoluzione delle tecniche usate dai *Threat Actor* e la conseguente necessità di mettere in sicurezza ogni singolo nodo delle *supply chain* sottostanti ai processi industriali[5].

In questo contesto il contributo del gruppo A2A si è concretizzato nella creazione di un innovativo presidio di cybersecurity basato su meccanismi di *direct report* al vertice aziendale, ovvero il primo responsabile della definizione e successiva implementazione delle strategie a tutela dell'organizzazione.

Applicando un approccio olistico e trasversale che prevede la collaborazione di molti team (IT, *Operational Technologies*, Risorse Umane) diventa possibile tutelare integralmente gli asset critici da qualsivoglia rischio o minaccia, sia di natura fisica sia cibernetica.

In considerazione del ruolo strategico ricoperto dalla sicurezza informatica le scelte di prodotto prevedono, accanto agli strumenti di rilevazione e risposta in caso di attacchi già in corso, anche misure tese a diffondere una cultura della prevenzione e della riduzione del rischio cyber.

A tale scopo si prevede da un lato l'implementazione di soluzioni hardware e software innovative nonché, dall'altro, la costante formazione e aggiornamento del personale in tema di minacce informatiche.

L'impegno di A2A intende fornire a tutte le aziende, dai grandi *player* industriali alle PMI a gestione familiare, una *best practice* per la gestione della cybersecurity: ciò nella ferma convinzione che essa sia, nel contesto contemporaneo, una delle pietre angolari su cui fondare la prosperità – e soprattutto l'affidabilità – di ogni organizzazione.

Renato Mazzoncini, *CEO di a2a*

4. Cybersecurity for the Water and wastewater sector, https://www.nccoe.nist.gov/

5. Securing Defense-Critical Supply Chains, https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF

BIOGRAFIA

Renato Mazzoncini

Amministratore Delegato e Direttore Generale di A2A.
Docente del corso “Mobility - Infrastructures and Services” presso il Politecnico di Milano, dal 2015 al 2018 è stato Amministratore Delegato e Direttore Generale del Gruppo FS.
È autore del libro “Inversione a E: Comportamenti individuali e sviluppo tecnologico per la mobilità sostenibile”.

PREAMBOLO

Il mondo moderno, fortemente digitalizzato, è costantemente sottoposto a un'ampia gamma di minacce informatiche; e anche l'Italia non fa eccezione. Al contrario, nel 2022 il nostro Paese è stato il più colpito in Europa da attacchi di tipo *ransomware*: questo impone a tutti noi – e più in generale a tutti gli imprenditori, compreso chi guida una PMI – una profonda riflessione sulla cybersecurity e sulla sua gestione.

Il numero di attacchi informatici in Italia è cresciuto in modo preoccupante nel 2022, con un aumento del 138%, raggiungendo quota 13.000 attacchi all'anno. La Polizia Postale ha segnalato una "proliferazione di gruppi ostili" con un incremento del 78% dei sospettati. A dicembre gli attacchi rilevati sono stati pari a 12.947, più del doppio rispetto all'anno precedente. Questo *trend* allarmante è proseguito nel corso del 2023.

Il primo argine di difesa, per le aziende, è la valutazione delle vulnerabilità presenti nei sistemi informatici. Fragilità che devono essere indicizzate per priorità e progressivamente mitigate, al fine di minimizzare gli impatti sull'operatività e sulla sicurezza dei dati in possesso delle imprese.
Anche in questo caso, il primo passo è culturale.

È fondamentale, infatti, comprendere che la sicurezza al 100% è un obiettivo inarrivabile. La cybersecurity è un processo continuo e, ogni volta che ci si avvicina a un obiettivo, questo si sposta sempre più lontano. Pertanto le aziende devono organizzarsi per minimizzare gli effetti delle vulnerabilità dei sistemi informatici, che possono emergere nel tempo. La cooperazione tra aziende, enti di ricerca, formazione e istituzioni regolamentari può aumentare notevolmente la consapevolezza e la sicurezza del nostro "sistema" digitale.

La transizione digitale ci ha posto di fronte a nuove sfide, che non riguardano solo più la sicurezza informatica in senso stretto – applicabile al tradizionale dominio delle *Information and Communication Technologies* (ICT) – bensì anche il dominio industriale delle *Operational Technologies* (OT), la "fabbrica", le catene di produzione e i relativi sistemi di automazione (*Industrial Control Systems* - ICS) o di supervisione e controllo (*Supervisory Control and Data Acquisition* - SCADA), fino a spingersi all'I-IoT (*Industrial Internet of Things*).
Il perimetro si è spaventosamente ampliato in questo mondo che, fino a qualche tempo fa, ha ritenuto di essere immune agli attacchi: dunque ci troviamo di fronte a sistemi *legacy* che potenzialmente sono altamente vulnerabili perché difficilmente aggiornabili, per ragioni intrinsecamente tecnologiche ma anche per ragioni di processo legate alla produttività.
Occorre dunque adottare le stesse logiche di sicurezza in entrambi i dominii, salvaguardando e tenendo conto delle peculiarità dei due mondi: ad esempio nelle OT lo standard di riferimento è la IEC 62443 e la serie ISA 99, mentre nel tradizionale dominio ICT ritroviamo la classica sicurezza delle informazioni, con lo standard ISO 27001.

La sicurezza cibernetica non è, dunque, solo una questione tecnologica applicabile all'informatica, ma richiede un approccio manageriale. È fondamentale focalizzarsi sulle priorità e redigere documenti tecnici che definiscano chiaramente i requisiti da implementare, anche rispetto ai domini in cui ci si trova a operare. Non bisogna cadere nella trappola di lasciarsi guidare ciecamente dai fornitori di prodotti e servizi di sicurezza informatica; è invece essenziale avere, dai livelli più alti delle piattaforme esposte su internet fino ai rilevatori e attuatori in fabbrica, un controllo attivo e una visione strategica della propria cybersecurity.

È anche per questa ragione che la sicurezza informatica è diventata una priorità inderogabile per tutte le aziende, indipendentemente dalle loro dimensioni e dal loro business. Non è più solo un tema di compliance, privacy o messa in sicurezza dei dati sensibili: oggi la cyber security ha a che fare anche con la gestione sicura dei processi di produzione in fabbrica e, per un'impresa, una postura debole in materia potrebbe fare la differenza tra rimanere sul mercato o meno.

L'Italia deve fare fronte alle sfide crescenti delle minacce informatiche e allo stesso tempo cogliere le opportunità che una gestione avanzata della cybersecurity può offrire. Solo attraverso la costante formazione, la collaborazione tra aziende e una gestione manageriale della cybersecurity potremo proteggere i nostri dati, le nostre attività produttive e la nostra economia digitale.

In un contesto in cui gli attacchi informatici sono sempre più sofisticati e diffusi, è essenziale investire nel settore della gestione dei rischi di cybersecurity. Questo passa attraverso la formazione di nuove professionalità e l'acquisizione di competenze avanzate. Ma qui si apre un problema, soprattutto nell'ordine delle priorità di settori fondamentali come il manifatturiero e la piccola-media industria.

Se guardiamo agli ultimi dati diffusi dal sistema Excelsior-Unioncamere, infatti, tra settembre e novembre le imprese prevedono di assumere circa 1,4 milioni di persone. Di queste solo 20mila sono tecnici informatici, esperti di telecomunicazioni e di sicurezza delle reti. Un dato che non può né deve essere sottovalutato, poiché racconta di un difetto di percezione dell'importanza di questo settore. Questione di costi e di priorità, appunto. Ma il problema resta. Le piccole e medie imprese, infatti, sono spesso inserite all'interno di una *supply chain* che vede come primo anello aziende grandi e grandissime, impegnate a gestire servizi spesso strategici. La sicurezza dell'intera catena diventa dunque essenziale.

Ecco perché la migliore soluzione per le PMI potrebbe essere sviluppare forme consortili per provare ad abbattere i costi e a migliorare le loro capacità di fronteggiare le minacce informatiche, superando ostacoli oggettivi come la mancanza delle risorse professionali, organizzative e tecniche necessarie.

Alessandro Manfredini, *Presidente di AIPSA*

BIOGRAFIA

Alessandro Manfredini

Direttore Group Security e Cyber Defence del Gruppo A2A e Chairperson AIPSA (Associazione Italiana Professionisti della Security).
Ha conseguito le Lauree in Giurisprudenza all'Università Sapienza di Roma e in Scienze della Sicurezza interna ed esterna presso l'Università di Tor Vergata di Roma.

Dopo un decennio di esperienza come Ufficiale dei Carabinieri, è stato Security Manager del Gruppo Espresso e Direttore della Sicurezza Aziendale e dei Servizi Generali di Italo - Nuovo Trasporto Viaggiatori.

Tutor in conferenze, seminari, corsi di formazione anche a livello universitario, si è specializzato in Enterprise Security, protezione dei dati e Cyber Security, fraud management e modelli di organizzazione e gestione.

INTRODUZIONE

Siamo ormai giunti alla quinta edizione del nostro quaderno tematico, l'ultimo di questo anno ricco di successi.

Questa volta la Commissione *Cyber Threat Intelligence e Cyber Warfare* (di seguito Commissione), parte integrante della SOCINT (Società Italiana di Intelligence), ha voluto affrontare il tema dell'***Industrial Security***, da sempre oggetto di grande interesse per la sua natura e complessità.

Come sempre, tramite un 'approccio multidisciplinare, si cerca di affrontare il tema da tutti i punti di vista: giuridico, tecnico – della *Cyber Threat intelligence* – e infine tecnologico, in particolare per quanto riguarda la convergenza tra IT (*Information Technology*) e OT (*Operational Technology*). Il tutto con l'obiettivo di comprendere le dinamiche, i rischi e le conseguenze dell'uso di alcuni strumenti e metodologie cyber relativamente alle sfide che possono portare nei due diversi mondi.

Prima di intraprendere una lettura più approfondita del Quaderno, vale forse la pena analizzare come l'interconnessione tra IT e OT abbia contribuito ad aumentare i rischi di attacchi cibernetici anche in termini di "costi/benefici".

Henry Ford diceva: «*Una delle più grandi scoperte che un uomo può fare, una delle sue più grandi sorprese, è scoprire che può fare ciò che aveva paura di non poter fare*».

La rivoluzione industriale, in particolare nell'ultimo secolo, ci ha spinto allo sviluppo di nuove tecnologie e nello stesso tempo ha reso il nostro sistema interconnesso, legando indissolubilmente quello che potevamo definire il mondo "classico" dell'OT (cioè l'ambiente industriale) e il più moderno ambiente dell'IT. Questa trasformazione digitale però ha causato un aumento della superficie di attacco, insieme alla necessità di gestire i diversi rischi associati.

Il tema si è quindi spostato sulla complessità da gestire, dovuto proprio all'interconnessione dei sistemi e della diversa natura degli sistemi in ambito IT e OT.

Per poter risolvere la complessità dobbiamo, a mio avviso, scomporre il problema in due grandi variabili principali: la gestione della *supply chain* e l'obsolescenza delle tecnologie informatiche.

La gestione delle *supply chain* si riferisce principalmente alla gestione dei fornitori, al fine di ridurre il livello di rischio cyber associato e avere un controllo costante su "chi gestisce cosa".

L'obsolescenza delle tecnologie informatiche invece richiede maggiore attenzione, in quanto i mondi IT e OT hanno logiche, applicazioni e anche tempi di vita differenti, se consideriamo gli aspetti tecnologici e di processo. Pertanto un buon approccio legato alla gestione dei costi (inteso come ROI) può portare un valore aggiunto nella gestione delle tecnologie IT/OT.

Negli ultimi 10 anni l'esperienza ci ha insegnato che la conoscenza di informazioni di carattere cyber, intese come vulnerabilità dei sistemi IT e/o OT, è di profonda importanza: senza tali informazioni le organizzazioni si ritroverebbero sguarnite in termini di protezione, oltre a rischiare di perdere competitività sul mercato nazionale e internazionale (si vedano ad esempio i numerosi attacchi a centrali elettriche e agli operatori di telecomunicazioni).

In conclusione possiamo affermare che l'elemento tecnologico, inteso come *Cyber Intelligence* in un contesto di *Industrial Security,* ha di certo aiutato il mondo pubblico e privato nella previsione e prevenzione del

rischio cyber; ma non ha garantito invece un adeguato livello di ROI, elemento che solo un buon manager a capo della cyber-security può "assicurare".

Henry Ford: «*Abbiamo bisogno di persone brave, non solo di brave persone*».

Mattia Siciliano, *Presidente Commissione Studi Cyber Threat Intelligence & Cyber Warfare*

BIOGRAFIA

Mattia Siciliano

L'ing. Siciliano ha oltre 15 anni di esperienza in Cyber Security e Cyber Intelligence. Attualmente è Co-Direttore del Corporate Cybersecurity HUB della Luiss Business School. In passato ha lavorato come Business Director per una società internazionale con sede negli Emirati Arabi Uniti.

Partner e co-fondatore di DeepCyber, una società boutique focalizzata sulla Cyber Threat Intelligence e manager in diverse società di consulenza come EY e KPMG. Docente presso l'Università degli Studi di Napoli Federico II e la Luiss Business School. Consulente per il Ministero della Difesa (Innova Difesa), agenzie di intelligence e forze dell'ordine. Presidente della Commissione di Studio in Cyber Threat Intelligence e Cyber Warfare della Società Italiana di Intelligence.

Sicurezza cibernetica, Internet e processi industriali

Quando nel 1969 venne utilizzata per la prima volta la rete Arpanet per collegare tra loro quattro università statunitensi, mai si sarebbe immaginato un pianeta interconnesso ai livelli raggiunti oggi. Siamo ormai entrati nella Quarta Rivoluzione Industriale, cioè in un mondo in cui il più piccolo dispositivo – sia esso un computer personale, un oggetto domestico o un componente di un impianto industriale – è raggiungibile e gestibile dovunque ci si trovi: cosa che, per l'epoca, era pura fantascienza.

Questa meravigliosa evoluzione, che permette ciò che era considerata pura fantasia sino a 50 anni fa, ha permesso inizialmente di risparmiare notevoli quantità di denaro in viaggi superflui per tecnici informatici di ogni ordine e grado; ma oggi questo beneficio è esteso a ingegneri di processo per linee produttive industriali, ricercatori e qualunque altra professione che richieda l'utilizzo di un *personal computer* per poter essere svolta. Sono così sorte nuove e impegnative sfide per tutti coloro che si occupano di sicurezza cibernetica, ovvero la scienza che studia come prevenire, mitigare ad un livello accettabile i rischi connessi al mondo industriale, informatico e delle telecomunicazioni.

Oggi si sta finalmente iniziando a considerare la sicurezza cibernetica una necessità imprescindibile, sia nella pubblica amministrazione (non solo esclusivamente nel mondo militare, in cui esiste da lungo tempo) sia anche nel mondo dell'industria e dei servizi privati.

L'Italia è un paese in cui il settore industriale vale il 20% del PIL (dati Istat) e in cui la componente principale è il manifatturiero, che copre oltre il 71% con un numero di addetti superiore ai 3,7 milioni.

Attualmente l'industria fa un uso massiccio di strumenti informatici ma, soprattutto, di componenti elettronici che operano nel mondo fisico: come sensori o attuatori responsabili di effettuare misurazioni di grandezze fisiche (temperatura, pressione, portata, ecc.) e PLC (*Programmable Logic Controller*), piccoli computer in grado di elaborare i segnali digitali e analogici provenienti dai sensori e dagli attuatori; questi ultimi sono formati da CPU, memorie (RAM, ROM, EPROM o EEPROM) e schede di comunicazione per connessioni a dispositivi vari, tra cui gli standard più comuni sono RS232 e RS422/RS485.

La componente informatica che governa questi dispositivi è chiamata comunemente SCADA (*Supervisory Control And Data Acquisition*).

L'elemento che fa dialogare i sistemi industriali, sia tra di loro e sia con i tipici software informatici, è il protocollo TCP/IP, fondamento delle reti private, di internet e dei sistemi di comunicazione attuali usati in ambiente industriale. La Scala ISO/OSI è il primo riferimento per comprendere come funzionano le reti TCP/IP, di qualunque natura esse siano, tanto industriali quanto informatiche in senso stretto.

Per esempio i protocolli Profinet, ModBus, OPC UA sono protocolli applicativi che funzionano al livello 7 della Scala di riferimento ISO/OSI e che quindi possono essere trattati come i normali protocolli applicativi che usiamo anche per la parte infor-

matica, ovvero HTTP, HTTPS, SMTP, ecc.

Invece protocolli come EtherCat, che hanno alte prestazioni in termini di velocità nella trasmissione dei messaggi, possono essere anche inseriti in *frame* UDP/IP; ma solo nel caso in cui l'applicazione preveda la necessità di trasporto su lunghe distanze oppure per altre esigenze molto specifiche.

Se aggiungiamo il fatto che oggi la maggior parte delle aziende di automazione richiede di potersi collegare da remoto per effettuare interventi manutentivi, monitoraggio del funzionamento e in ultima istanza per fare manutenzione predittiva per via dello sviluppo esponenziale dell'intelligenza artificiale, la sfida per gli operatori e responsabili della sicurezza cibernetica, non solo in ambito ICT (*Information and Communication Technology*) ma anche industriale (*Operational Technology* - OT), è sempre più ardua.

La difesa e la preservazione della capacità economica aziendale, oltre alla tutela del suo *know how* o patrimonio informativo, si è di fatto estesa nella stragrande maggioranza dei casi anche alla parte industriale, obbligando manager e tecnici a riformulare i piani di continuità operativa e sicurezza cibernetica delle proprie aziende o impianti. A titolo esemplificativo – ma non esaustivo – si pensi a tutte quelle aziende in cui vengono miscelati i componenti in quantità precise e in condizioni ambientali predeterminate, per le quali sono stati necessari anni di ricerca e sviluppo oltre a milioni di euro di investimenti.

Ricercatori ed esperti di sicurezza cibernetica (sempre in numero troppo esiguo rispetto alla domanda odierna) hanno elaborato diverse strategie per mitigare i rischi provenienti dagli ambienti industriali: la cosa fondamentale da considerare è che sono tutte complementari e, di norma, attuarne una singolarmente non mitiga i rischi in senso assoluto.

La prima strategia raccomandata è avere **visibilità**. Con questo si intende la capacità di avere contezza di quali apparati ci aspettiamo di vedere installati nella nostra rete e di avere immediato avviso se ne vengono rilevati di nuovi, sapendo che tipo di segnali industriali (Profinet, ModBus, ecc.) ci aspettiamo di vedere o meno. Infatti, per raggiungere questo ultimo scopo, la maggior parte dei sistemi che fanno sicurezza cibernetica in ambito OT prevedono una fase di apprendimento del comportamento dei dispositivi sulla rete, che in tale periodo vanno a leggere i valori scritti nelle variabili dei vari protocolli rilevati, permettendo alla fine una *"detection"* molto puntuale di qualsiasi anomalia che possa essere significativa ai fini dell'integrità del processo industriale.

Un potenziale malintenzionato che abbia ottenuto un accesso alla rete industriale e voglia tentare un sabotaggio potrebbe collocare, all'interno della rete, un *malware* in grado di intercettare i messaggi e alterarne i valori nelle variabili, tanto da poter sabotare il processo, nei casi peggiori arrivando a causare danni per milioni di euro.

Il caso più famoso in tempi recenti è stato quello del *malware* STUXNET, sviluppato dal governo statunitense al fine di sabotare l'impianto di arricchimento dell'uranio di Natanz in Iran. Questo è un esempio in cui l'interconnessione dei sistemi industriali con quelli informatici ha permesso la conduzione di un attacco che ha impiegato anni per poter essere perpetrato, ma in cui l'assenza di tecnologia in grado di rilevare variazioni del con-

tenuto dei protocolli utilizzati sulla rete ha permesso all'attacco di avere successo. Questo *malware* fu realizzato per poter funzionare anche su sistemi SCADA.

La seconda strategia raccomandata è la **segregazione di rete**, ovvero la separazione della rete in più segmenti mantenendo il controllo (autorizzazione e visibilità) del traffico tra i vari dispositivi. Questo approccio è anche uno dei requisiti fondamentali del modello ISO27001 Annex A13.1, standard di riferimento per la certificazione di qualità dei sistemi informatici, considerato come il passaggio fondamentale per il miglioramento sostanziale della postura cibernetica in qualsiasi ambiente in cui ci siano sistemi informatici e/o produttivi.

La scelta oculata di tecnologie che possano fornire visibilità e bloccare messaggi dei protocolli industriali anomali è la migliore – se non l'unica – possibilità per proteggersi dagli attacchi più sofisticati che oggi il crimine organizzato è in grado di perpetrare. L'esperienza dimostra che l'utilizzo di *firewall* infrastrutturali (da non confondere con quelli del perimetro) usati per la separazione delle reti al posto dei tradizionali *Switch Layer 3* di rete migliora significativamente sia la visibilità, sia le capacità di mitigazione.

È contestualmente raccomandato l'utilizzo di tecnologie che abbiano conoscenza dei protocolli industriali specifici, in modo da bloccare efficacemente anche possibili attacchi che operino a questo livello. I sistemi di *Privileged Access Management* (PAM) sono tra le tecnologie più recentemente introdotte per monitorare e limitare attivamente quello che gli operatori con diritti amministrativi fanno sui sistemi, specialmente da remoto. Si tratta di un metodo molto efficiente per verificare con certezza le azioni eseguite e limitare le azioni eseguibili nei differenti contesti operativi.

La terza strategia raccomandata è l'utilizzo di **sistemi di sorveglianza e monitoraggio** che permettano di essere avvisati in tempo reale su tutte le anomalie che raggiungano una determinata soglia di allarme. Questo fondamentale componente del sistema di sicurezza cibernetica permette di stabilire con attenzione le soglie ragionevoli per non incorrere in falsi positivi che possono "desensibilizzare" gli operatori preposti alla sorveglianza attiva. Proprio per questo, è suggeribile dotarsi di un servizio di *Security Operation Center* (SOC) specifico per il mondo OT, in cui la fase iniziale di analisi e valutazione è fondamentale per il giusto *"tuning"* o regolazione della sensibilità degli allarmi.

Lo standard di riferimento per la sicurezza informatica in ambito industriale è IEC 62443 (precedentemente ISA99) dell'International Electrotechnical Commission (IEC). Dal 2002, la International Society of Automation (ISA) si occupa di queste tematiche e di inoltrare proposte di aggiornamenti all'American National Standards Institute (ANSI).

A tale proposito, la quarta strategia raccomandata è adottare un **modello di gestione** in linea con lo standard IEC 62443. Questo standard è destinato sia ai *system integrator* sia agli utenti finali, sia anche ai costruttori di componenti. Ognuno ha una serie di controlli da implementare, che indica il livello di maturità del sistema.

La sicurezza della *Supply Chain* è considerata universalmente come il nuovo elemento fondamentale ai fini del controllo della postura di sicurezza cibernetica di un'organizzazione. La scarsa cultura

in questo ambito nelle aziende che trattano automazione industriale è purtroppo assai comune: veicolare un *malware*, anche per scarsità di procedure, è assai semplice. Adottare processi in linea con quanto previsto da questa norma è caldamente raccomandato.

Le organizzazioni più virtuose oggi si stanno dotando di servizi di "Security Operation Center" specifici il mondo Operational Tecnology, che vengono comunemente chiamati SOC OT. Questo servizio che richiede una fase di analisi ed avvio, permette a regime di incrementare l'efficacia della prevenzione degli attacchi cibernetici sugli ambienti produttivi, sfruttando le capacità di apprendimento delle sonde vengono posizionate sulle reti produttive, i modelli di intelligenza artificiale ed i firewall con capacità di intervento sui protocolli industriali. Con l'introduzione della direttiva europea NIS 2 entrata in vigore il 18 gennaio 2023 e che dovrà essere recepita dagli Stati membri entro il 18 ottobre 2024, l'adozione di servizi di questo tipo si renderà sempre più necessaria al fine di soddisfare quanto previsto dalla direttiva.

Possiamo dunque affermare che il controllo della propria postura di sicurezza cibernetica deve essere tra le prime aree di investimento per le aziende produttive del nostro tessuto industriale, in considerazione del fatto che il valore delle potenziali perdite economiche date dalla somma di danni emergenti e lucro cessante appare sproposito rispetto agli investimenti che potrebbero essere richiesti per gestire la postura cyber in modo corretto, **senza contare le sanzioni a cui si andrebbe incontro qualora le normative attuali e quelle annunciate dovessero essere violate.**

Raccomandiamo, quindi, un'attenta valutazione dei rischi e una corretta assegnazione di risorse al fine di gestire questo importante elemento a tutela degli interessi comuni del mondo industriale.

Gabriele Minniti, *esperto di Sicurezza Informatica e Sicurezza delle informazioni*

BIOGRAFIA

Gabriele Minniti

È un informatico specialista in Sicurezza Informatica e Sicurezza delle informazioni con oltre 15 anni di esperienza. Ha conseguito molteplici certificazioni internazionali in ambito tecnologico ed ha lavorato in Germania ed Inghilterra per importanti aziende costruttrici di tecnologie per la Sicurezza Informatica. Nel corso della sua carriera è stato chiamato sia come consulente che come docente per entità afferenti al comparto della Difesa. Fondatore di WhySecurity srl, oggi si occupa di supporto ad indagini difensive collaborando con investigatori privati, svolge analisi di rischio economico connesso al rischio informatico e offre servizi SOC a favore dei propri clienti.

CYBER CRIME CONFERENCE

17-18 APRILE 2024

AUDITORIUM DELLA TECNICA, ROMA

Iscriviti alla newsletter di ICT Security Magazine
per conoscere l'agenda e partecipare alla
12ª Edizione della Cyber Crime Conference

Sicurezza aziendale: geopolitica e intelligence a supporto del ciclo attivo e passivo nella definizione di un'analisi di risk management

Partendo da una visione complessiva che vede l'*intelligence* inserirsi perfettamente all'interno dei processi decisionali aziendali – e perciò declinabile come metodologia generale che trova una sua naturale collocazione tra le varie fasi di tali processi – anche l'elemento geopolitico assume una rilevanza strategica di prim'ordine e concorre pienamente a supportare lo sviluppo di un percorso di selezione delle informazioni, di un processo di analisi e di un processo decisionale propri del ciclo dell'*intelligence*[1].

In un contesto globalizzato dove le aziende operano e si confrontano con *competitor* internazionali, soprattutto le dinamiche geopolitiche rappresentano una delle variabili che maggiormente determina il successo o l'insuccesso del business, oltre che la sua sicurezza. Tali dinamiche sono a loro volta caratterizzate da elementi geografici che nel loro insieme condizionano le scelte degli Stati e, a cascata, coinvolgono persone e società che in questi scenari sono attori non secondari. Volendo scomodare Jared Diamond e quanto scrisse a fine anni '90 nel suo "*Armi, acciaio e malattie. Breve storia del mondo negli ultimi tredicimila anni*", tutte le attività umane che hanno forgiato la storia sono state rese possibili dalla geografia e dall'ecologia, dando dei vantaggi ad alcuni popoli rispetto ad altri; più in generale la geografia non solo le ha rese possibili ma soprattutto le ha condizionate, decidendo i destini dei popoli[2].

Conclusa questa prima parte introduttiva sulla geografia – dove abbiamo descritto l'effetto deterministico del terreno nel rapporto uomo/territorio – e venendo a una definizione generale di geopolitica, possiamo prendere a modello quella presentata dall'enciclopedia online Treccani, dove essa viene descritta come "*il complesso di problemi politici che traggono origine da fatti d'ordine territoriale, specie quando si consideri lo Stato come un organismo che nasce, si sviluppa e decade, e che, al pari degli esseri viventi, ha bisogno di uno spazio vitale*"[3]. Secondo questa definizione, la geopolitica è una disciplina che connette l'elemento geografico all'evoluzione delle scelte politiche di uno Stato, che necessariamente influiscono, a vari livelli, sull'agire dei diversi soggetti che ope-

1. PRESIDENZA DEL CONSIGLIO DEI MINISTRI, Dipartimento delle Informazioni per la Sicurezza, Il linguaggio degli organismi informativi. Glossario intelligence, Gnosis, De Luca Editore Srl, Roma 2019.

2. JARED DIAMOND, Armi, acciaio e malattie. Breve storia del mondo negli ultimi tredicimila anni, Giulio Einaudi editore s.p.a., Torino, prima edizione 1998.

3. https://www.treccani.it/enciclopedia/geopolitica/

rano soprattutto in contesti globali. Soggetti che, come le aziende, escono dai confini degli Stati nei quali hanno sede o sono comunque fortemente condizionati da eventi extra nazionali; i quali, solo a una prima analisi alquanto superficiale, sembrano riguardarle in parte. Lo studio e la comprensione dei fenomeni geopolitici diventa perciò un metodo fondamentale per le aziende per orientarsi nel mondo, comprendendo e anticipando le conseguenze dei comportamenti politici che hanno effetti sulle loro attività, sia a livello macro che a livello più circoscritto. La geopolitica va quindi ascritta tra gli strumenti di analisi che possiamo ritrovare all'interno del bagaglio metodologico che è proprio dell'*intelligence*, uno strumento che ne affina ulteriormente le capacità previsionali riducendo, per quanto possibile, quel grado di incertezza (e di rischio!) che pur sempre le organizzazioni devono affrontare nella loro quotidianità operativa.

Ma in che termini la geopolitica può influenzare il business e i rischi connessi? Per rispondere possiamo partire prendendo in considerazione i due estremi di un'organizzazione aziendale, ovvero il ciclo attivo e il ciclo passivo. Infatti, nella definizione delle strategie aziendali legate alla parte delle vendite (**ciclo attivo**) e a quella degli approvvigionamenti (**ciclo passivo**), l'elemento geopolitico diventa determinante per definire delle strategie di business e valutarne una parte dei rischi, all'interno di quello che abbiamo definito il ciclo di *intelligence* aziendale, al fine di ridurre al minimo gli effetti negativi di fattori esogeni. Infatti l'uso stesso delle mappe, caratteristica propria della geopolitica, contribuisce solo in parte a spiegare e ad anticipare gli eventi che portano a dei cambiamenti nei rapporti tra gli attori statuali. Questo processo analitico, con una buona approssimazione, ci permette di fotografare gli interessi delle comunità quando queste si muovono all'interno di un territorio finito e, conseguentemente, ci aiuta a comprendere l'intersecarsi degli interessi dei popoli con quelli dei loro vicini (relazione territorio/uomo), necessitando però di un maggior approfondimento analitico.

A livello aziendale, entrando nell'ambito della *business intelligence* (organizzazione interna del lavoro, quindi ciclo passivo) e della *competitive intelligence* (analisi per il ciclo attivo), lo studio dell'evolversi dei rapporti uomo/territorio sopra descritti può sostenere solo una parte del processo decisionale, agendo però sulla base di valutazioni fatte con metodo scientifico. La geopolitica assume perciò un ruolo determinante ai fini di una evoluzione integrata del concetto stesso di *intelligence* economica, diventando in ultima analisi uno strumento (non l'unico ovviamente) di valutazione degli eventi comuni, sia per gli Stati che per le aziende. In questi termini, con un approccio di insieme molto più simile e complementare nell'elaborare la comprensione dei rischi e delle opportunità, entrambe le entità possono muoversi con una condivisione di obiettivi maggiore, e quindi indirizzarsi verso quello che possiamo definire il "sistema Paese"[4]. Una geopolitica che contribuisce significativamente alla fase in cui si vede Stato e aziende "fare sistema", poiché pone le basi per un metodo di analisi condiviso, accomunando di conseguenza entrambi nella medesima percezio-

4. MARCO AREZZINI, LARIS GAISER, Cyber spazio e Intelligence economica – Vademecum alle priorità contemporanee dell'intelligence italiana, Il Cerchio, Iniziative Editoriali, Rimini, 2019.

ne di quelli che sono gli interessi per la propria sopravvivenza.

Entrando maggiormente in dettaglio circa gli effetti che gli eventi geopolitici producono sulle aziende, si rende necessaria l'esigenza di attingere al bagaglio delle esperienze, abbandonando per un attimo quello legato alla teoria geopolitica. In questi termini possiamo facilmente calarci nella contemporaneità, prendendo ad esempio gli eventi (attuali per chi scrive) che stanno condizionando il biennio 2022/2023 e che condizioneranno per molti anni gli equilibri tra Stati, imponendo anche alle aziende un cambiamento epocale nel modo stesso di fare business. Laddove vediamo una geopolitica essere il punto di incontro tra la **storia**, la **geografia** (territorio e risorse) e la **strategia** (intesa come volontà e relativo piano di azione per raggiungere degli obiettivi), ecco che la guerra in Ucraina, stravolgendo questi elementi, assume per le aziende il significato di un cambiamento geopolitico epocale che condizionerà la loro stessa esistenza, al pari di altri eventi chiave che hanno segnato le prime due decadi del XXI secolo, se non con un impatto ancora maggiore.

LA GEOPOLITICA A SUPPORTO DEL RISK MANAGEMENT

Ma in che misura le aziende possono difendersi per ridurre al minimo gli effetti di situazioni di questa natura? Esistono delle prassi che possono supportare le organizzazioni nella tutela del ciclo attivo e di quello passivo?

Una risposta a questa domanda potrebbe prendere forma partendo da una analisi di *risk management*[5] aziendale "arricchita" con elementi di analisi geopolitica, utili per meglio comprendere i rischi ai quali le aziende vanno incontro. Partendo da uno schema classico di *risk management*[6], come prima cosa identifichiamo subito la necessità di strutturare tutte le nostre argomentazioni ponendoci come obiettivo l'inserimento dei sopra citati elementi di analisi in ogni fase che caratterizza il processo di gestione del rischio e di tutte le relative sottocategorie. Fatte queste considerazioni, lo schema generale dovrebbe assumere i seguenti connotati:

---

5. "Processo di gestione del rischio finalizzato a identificare, monitorare e quindi gestire l'eventualità di un evento che potenzialmente determina effetti negativi su un determinato sistema (azienda, stabilimento, territorio, impianto, mercato finanziario, Stato o altro) e ad assicurare il mantenimento delle condizioni che consentono di preservare il sistema e di raggiungere i suoi obiettivi".
Definizione Treccani online:
https://www.treccani.it/enciclopedia/risk-management_%28Lessico-del-XXI-Secolo%29/#:~:text=%E2%80%93%20Processo%20di%20gestione%20del%20rischio,assicurare%20il%20mantenimento%20delle%20condizioni.

6. In rete si trovano diversi esempi che ne descrivono le caratteristiche salienti, ad esempio:
https://www.zerounoweb.it/techtarget/searchsecurity/risk-management-cose-come-si-fa-esempi-e-vantaggi-per-le-aziende/.

FASE 1

Identificazione del rischio:

- Categoria
- Processo/aspetto
- Evento potenziale
- Potenziali cause
- Valutazione dell'impatto dell'evento (danni).

FASE 2

***Risk assessment*:**

- Analisi del rischio inerente (rischio intrinseco)
  - Probabilità del rischio
  - Impatto
  - *Risk rating* (matrice rischio)
- *Control assessment* (controllo attuale/situazione esistente/azioni in essere)
- Analisi del rischio residuo
  - Probabilità del rischio
  - Impatto
  - *Risk rating* (definizione delle priorità).

FASE 3

Trattamento del rischio:

- Opzione trattamento
- Piano d'azione
- Riferimento/piano obiettivi
- Responsabile dell'attività
- Scadenza/*Deadline.*

FASE 4

Monitoraggio e riesame del rischio:

- **Individuazione/Scelta dei** metodi di monitoraggio/revisione
- Registrazione del progresso e conformità
- Stato
- Valutazione dell'efficacia ed eventuali note.

Fase 1. Nella parte di **identificazione del rischio**, limitatamente ai cicli attivo/passivo come da premessa iniziale, possiamo individuare le categorie *business* per la parte commerciale (ciclo attivo) e la categoria *business continuity* per la parte approvvigionamenti (ciclo passivo). Circa l'indicazione dell'evento potenziale, quindi il rischio, volendo distinguere i due cicli possiamo far emergere una serie di rischi comuni ad entrambi e altri specifici per l'uno o l'altro ciclo. Già in questa prima fase la geopolitica ci viene in aiuto, dando modo di identificare anche rischi che un'analisi meno attenta avrebbe tralasciato. Nello specifico, prendendo ad esempio un'azienda manifatturiera, la geopolitica perde il suo valore determinativo (quello che genericamente viene chiamato "rischio geopolitico") per assumere invece un valore esplicativo, contribuendo perciò alla definizione stessa dei rischi in base a valutazioni che si basano sull'analisi geopolitica

degli eventi passati, di quelli attuali e di quelli potenzialmente verificabili. Per le aziende del comparto OT/IT, dove il fattore tempo ha maggiore rilevanza rispetto ad altri settori per quanto riguarda l'evoluzione tecnologica, il contributo della geopolitica assume un ruolo se vogliamo ancor maggiore in termini di supporto alle analisi. Alla luce di ciò, la suddivisione in cicli si delinea quindi nel modo seguente:

Rischi afferenti il ciclo attivo (es. cliente o distributore): rischio paese (stabilità politica), rischio esposizione finanziaria, rischio tasso cambio valuta (se contratto non in Euro o Dollari), rischio indiretto su tasso di cambio (importatore costretto a interrompere il rapporto causa svalutazione della moneta nazionale), rischio interruzione flussi finanziari che alimentano la commessa/produzione (costi iniziali commerciali, amministrativi e di progettazione, poi per impegno risorse per acquisto materiali, soprattutto se lavorazione su commessa: elevato livello di customizzazione del prodotto che riduce la capacità di virare un prodotto da un cliente ad un altro), rischio domanda variabile, rischio concorrenza, rischio introduzione nuova tecnologia, rischi legali, rischio regolamenti più restrittivi, rischio trasporti, rischio aumento costi (materie prime, logistica, energia), rischi IT e sicurezza informatica, rischi obsolescenza tecnologica (soprattutto OT/IT), rischi legati alla sicurezza del personale in loco (installatori se parliamo di ordini a commessa - *travel security*), rischio terrorismo, rischio catastrofi naturali, rischio pandemie e rischi politici generali (che amplificano i rischi precedenti).

Rischi afferenti il ciclo passivo (es. fornitore): rischio paese (stabilità politica), rischio esposizione finanziaria, rischio tasso cambio valuta (se contratto non in Euro o Dollari), rischio indiretto su tasso di cambio (fornitore costretto ad interrompere il rapporto causa svalutazione della moneta nazionale), rischi qualitativi sul prodotto (soprattutto in presenza di scarsa automazione e di un mercato del lavoro dinamico che crea una potenziale perdita frequente di personale qualificato in attività a scarso valore di automazione), rischio interruzione della catena di fornitura (interruzione della catena produttiva, anche subfornitori), rischi legali, rischio regolamenti più restrittivi, rischio trasporti, rischio aumento costi (materie prime, logistica, energia), rischi IT e sicurezza informatica, rischi obsolescenza tecnologica (soprattutto OT/IT nella *supply chain*), rischio terrorismo, rischio catastrofi naturali, rischio pandemie, rischi politici generali (che amplificano i rischi precedenti).

Sempre nella fase 1, una volta individuato il rischio, il *risk management* prevede un successivo passaggio che porta all'individuazione delle potenziali cause del rischio. In questa fase l'analisi geopolitica permette di scandagliare in maniera più approfondita i vari elementi che determinano o meno il verificarsi di un dato evento. A conclusione della prima fase, il successivo passaggio è rappresentato dalla valutazione dei principali impatti dell'evento di rischio che va poi ad introdurre la seconda fase: il *risk assessment*.

Fase 2. Nella parte di *risk assessment* il primo passaggio operativo è dato dall'analisi del rischio inerente, con relativa identificazione di 3 parametri, di cui il terzo è la risultante dell'interazione dei primi due:

Probabilità

RATING	POTENZIALE RISCHIO PER LA PRESENZA	Probabilità
QUASI CERTO	Probabile che si verifichi più volte all'anno	>90%
PROBABILE	Probabile che si verifichi una volta l'anno	50%-90%
POSSIBILE	Può darsi che si verifichi una volta ogni pochi anni	10%-50%
IMPROBABILE	Si potrebbe verificare una volta in 5 anni	5%-10%
RARO	Potrebbe verificarsi una volta in 10 anni	<5%

Impatto

RATING	IMPATTO
CATASTROFICO	**La società potrebbe chiudere l'attività. Obiettivi di business non raggiunti**
RILEVANTE	**Impatto significativo sulle attività/azienda. Alcuni obiettivi di business non raggiunti**
SIGNIFICATIVO	**Notevole impatto sulle attività/azienda. Alcuni obiettivi di business non raggiunti**
CONTENUTO	**Alcuni impatti che possono essere facilmente risolti**
TRASCURABILE	**Impatto non visibile**

***Risk rating* (matrice rischio scala 1-25)**

IMPATTO	RARO	IMPROBABILE	POSSIBILE	PROBABILE	QUASI CERTO
	PROBABILITA				
CATASTROFICO (5)	TOLLERABILE (5)	ALTO (10)	MOLTO ALTO (15)	MOLTO ALTO (20)	MOLTO ALTO (25)
RILEVANTE (4)	BASSO (4)	TOLLERABILE (8)	ALTO (12)	MOLTO ALTO (16)	MOLTO ALTO (20)
SIGNIFICATIVO (3)	BASSO (3)	BASSO (6)	TOLLERABILE (9)	ALTO (12)	ALTO (15)
CONTENUTO (2)	MOLTO BASSO (2)	BASSO (4)	TOLLERABILE (6)	TOLLERABILE (8)	ALTO (10)
TRASCURABILE (1)	MOLTO BASSO (1)	MOLTO BASSO (2)	BASSO (3)	TOLLERABILE (4)	TOLLERABILE (5)
	RARO (1)	IMPROBABILE (2)	POSSIBILE (3)	PROBABILE (4)	QUASI CERTO (5)
	PROBABILITÀ				

Il successivo passaggio della fase 2 è rappresentato dal *control assessment*, ovvero la verifica delle azioni che l'azienda ha posto in essere relativamente alla presa in carico dei rischi individuati (fotografia di come viene trattato il rischio). Il successivo passaggio, l'analisi del rischio residuo, rielabora i parametri di rischio inerente (possibilità, impatto e *risk rating*) alla luce dell'impatto che tali azioni producono, mitigandone gli effetti. I risultati di questo processo portano alla classificazione di un dato rischio riconducendolo al contesto aziendale che, nel nostro caso, circoscriviamo al ciclo passivo e al ciclo attivo dell'azienda.

Conclusa la seconda fase, con la **fase 3** si passa allo step successivo della nostra analisi di *risk management*: il trattamento del rischio. La prima azione di questo processo è indicata come opzione trattamento, ovvero la valutazione di come procedere nel trattare il rischio residuo risultante del *risk assessment*, che possiamo così riassumere:

- evitare/eliminare;
- ridurre;
- condividere;
- trasferire;
- accettare.

Soprattutto con riferimento alle prime 4 opzioni, il passaggio successivo è quello che descrive il *piano d'azione* eventuale. In tale fase può essere associata un'attività di miglioramento che, ove richiesta, si pone l'obiettivo di implementare la gestione del rischio residuo e di ridurne ulteriormente gli effetti negativi sul business. Nella fase 3 vengono anche individuati dei referenti interni dei piani d'azione e definita una *timeline* per la loro esecuzione.

Un ultimo passaggio – la **fase 4** dello schema proposto sopra – riguarda la fase di monitoraggio e riesame del rischio e rappresenta in un certo senso la fase più delicata del *risk management*. Vista la dinamicità degli eventi esterni, è proprio in questa fase che la geopolitica entra nuovamente in gioco, in quanto rappresenta lo strumento di analisi che meglio si adatta al mutare di questi. Infatti, un'analisi geopolitica mirata ha la capacità di comprendere la dinamicità degli eventi esterni e di contribuire a ridurne gli effetti negativi, supportando una corretta gestione del rischio nella fase di monitoraggio.

LA GEOPOLITICA A SUPPORTO DEL RISK MANAGEMENT

A conclusione di questa breve descrizione del *risk management*, viene ora da chiedersi in che modo l'analisi geopolitica può essere utile per sostenere le attività di una azienda, diventando quindi strumento indispensabile all'interno del ciclo di *intelligence* aziendale. Anche in questo caso è necessario ricorrere al piano dell'esperienza, descrivendo in breve quelle che possono essere delle situazioni tipo.

Con riferimento alla guerra russo-ucraina, se facessimo un passo indietro rispetto alla data di inizio delle ostilità, con l'invasione russa ai danni dell'Ucraina del 24 febbraio 2022 (quindi il periodo a cavallo tra la fine del 2021 e l'inizio del 2022), possiamo ritenere che allora fosse possibile ipotizzare l'inizio di un conflitto armato? Ovvero: riferendoci sempre all'ambito di ciclo attivo e passivo, un'azienda con delle attività in territorio ucraino o in quello russo (o in entrambi), nel periodo antecedente l'inizio della guerra possedeva degli elementi validi per poter valutare il rischio inerente, il rischio residuo, ma soprattutto avviare una fase di monitoraggio e riesame del rischio, se già operativi in quell'area?

La risposta a questa domanda si può individuare soprattutto partendo dalla fase 4 di monitoraggio e riesame del rischio. Infatti gli eventi del periodo preso in considerazione potevano sicuramente rientrare nell'ambito della fase 2, limitatamente alla valutazione del rischio inerente (ad esempio il "rischio paese" generico) e del rischio residuo ("*che effetti avrebbe sulla mia attività?*") anche senza dover ricorrere ad un'approfondita analisi geopolitica. Al contrario, nel caso del monitoraggio e riesame del rischio (fase 4), una simile analisi si sarebbe resa necessaria per sviluppare un corretto *risk assessment* che tenesse conto dell'evolversi della situazione. A sostegno di questa tesi si potrebbe portare ad esempio un tipico caso di azienda manifatturiera chiamata a realizzare un impianto "chiavi in mano". Nel monitoraggio costante del rischio, l'analisi geopolitica può assumere una valenza importante per aiutare il *management* aziendale nella gestione del progetto e anche a definire un'eventuale *exit strategy* che possa limitare al minimo gli effetti di un rischio im-

minente (soprattutto se già presenti sul territorio con attività in fase di avanzamento). Se volessimo prendere in esame il rischio di interruzione dei flussi finanziari, partendo dal fatto che l'esecuzione di un progetto chiavi in mano per la fornitura di impianti prevede degli stati di avanzamento, anche per la parte relativa ai pagamenti si deve considerare che una struttura-tipo di contratto disciplina diversi passaggi. Un caso tipico è quello che prevede, ad esempio, il pagamento del 10% alla firma del contratto, un ulteriore 20% all'approvazione progetto, un 60% al FAT (*Factory Assembling Test*) e infine un 10% al SAT (*Site Assembling Test*)[7]. Indipendentemente dal tipo di copertura finanziaria (L/C, garanzia bancaria o assicurazione del credito, solo per citarne alcune), l'azienda che realizza il progetto si assume comunque numerosi rischi – approvvigionarsi dei materiali, impegnare risorse umane, progettare ed eseguire degli impianti (con un elevato livello di customizzazione, perciò non facilmente rivendibili ad altri soggetti in caso di interruzione del rapporto con il cliente), condividere *know-how* tecnico – per i quali è previsto il pagamento solo al completamento dell'attività. In uno scenario simile, la fase di realizzazione degli impianti risulta essere quella a più alto tasso di rischio, essendo la più onerosa in termini di investimento per chi produce: si acquistano i materiali, si entra in fase di esecuzione e realizzazione degli impianti e ci si prepara per i FAT. Nell'ipotesi in cui dovesse saltare il collaudo finale l'azienda si troverebbe in uno scenario di:

- esposizione finanziaria verso fornitori (ed esposizione interne legata al costo sostenuto per finanziare l'attività svolta dei propri dipendenti)
- interruzione dei flussi finanziari (mancato incasso dell'attività svolta).

Nel contesto della guerra in Ucraina, pur trovandoci in un caso di forza maggiore solitamente previsto nelle clausole dei contratti, un evento geopolitico di questa portata ha un tale impatto che solo una valutazione sostenuta da competenze geopolitiche avrebbe potuto ridurne gli effetti. Infatti, con l'evolversi dello scenario di crisi a fine 2021, un'azienda coinvolta in quel mercato (o anche in quello russo, considerando le possibili sanzioni in risposta a una potenziale invasione) avrebbe potuto gestire il rischio con un certo anticipo rispetto all'inizio del conflitto, se sostenuta da una puntuale analisi geopolitica. Agendo sul monitoraggio e riesame del rischio (fase 4 del processo di *risk management*), se si fosse ritenuto il rischio come "molto alto" nella scala di *rating* (impatto "catastrofico", probabilità "quasi certa") già a partire da fine 2021, i mesi antecedenti all'inizio delle ostilità sarebbero serviti per cercare di completare un eventuale stato di avanzamento in corso; oppure per interrompere l'attività prima di iniziarne uno nuovo, mettendo in sicurezza le proprie risorse finanziarie. Specificatamente nel settore OT/IT – soprattutto se riferito al ciclo passivo e ai rischi connessi all'obsolescenza tecnologica nella *supply chain* – avere un fornitore strategico in un'area caratterizzata da una situazione simile a quella del territorio ucraino di fine 2021 (con l'aggravante del

7. Il peso percentuale si riferisce alla sola esecuzione degli impianti. La necessità di prevedere altre attività legate alla messa in funzione degli stessi (service) modificherebbe i valori percentuali in considerazione del valore complessivo del progetto.

fattore tempo connesso all'evoluzione tecnologica specifica di questo settore) avrebbe richiesto una capacità di analisi più attenta rispetto ad altri settori e, quindi, un ricorso ancora maggiore all'analisi geopolitica nella fase di monitoraggio del rischio.

In conclusione – osservando come le aziende operino in un contesto di globalizzazione, inserite perciò in un processo di interdipendenze economiche, sociali, culturali, politiche e tecnologiche i cui effetti hanno una rilevanza planetaria – dalle valutazioni appena esposte emerge la necessità di acquisire maggiori competenze geopolitiche all'interno delle aziende stesse. In questi termini l'analisi geopolitica si inserisce nel processo decisionale, non solo a supporto del ciclo di *intelligence* ma anche contribuendo al monitoraggio e al riesame dei rischi nel *risk management* aziendale: così delineandosi quale strumento indispensabile per valutare con metodo scientifico il continuo mutare delle condizioni in cui le aziende si trovino a operare.

Massimiliano Alzetta, *Sales e Marketing Director presso Lamitex S.p.A*

BIOGRAFIA

Massimiliano Alzetta

Massimiliano Alzetta svolge la funzione di Sales e Marketing Director presso Lamitex S.p.A, azienda attiva nel settore dell'interior design. Precedentemente è stato Vice Sales Director di Maddalena S.p.A. Laureato in Relazioni Internazionali e successivamente in Politica Internazionale e Diplomazia con lode presso l'Università degli Studi di Padova, ha concluso un corso di perfezionamento in Intelligence e sicurezza nazionale presso l'Università degli Studi di Firenze e conseguito un master in Intelligence & ICT con lode presso l'Università degli Studi di Udine. Da sempre attento al mondo dell'intelligence, soprattutto in ambito aziendale, fa parte della SOCINT sin dagli inizi ed è membro della Commissione CTI e Cyber Warfare.

Le infrastrutture critiche all'intersezione tra dispositivi cyber-fisici e Cyber Threat Intelligence

«Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life» (Biden Administration, Executive Order on Improving the Nation's Cyber Security, 2021)

«Because ICS manage physical operational processes, the increasing convergence of information technology (IT) and operational technology (OT) creates opportunities for exploitation that could result in catastrophic consequences, including loss of life, economic damage, and disruption of the National Critical Functions (NCFs) upon which society relies» (Krebs, Director CISA 2020:ii)

FRAMEWORK GENERALE DI RIFERIMENTO

I sistemi di controllo industriale (*Industrial control systems*) ICS/OT (*Operational technology*) costituiscono, ormai da diversi anni, uno dei target principali degli attori malevoli.

Numerosi e significativi attacchi informatici si sono concentrati, difatti, su infrastrutture critiche e sistemi industriali e, tra questi, il più alto profilo di minacce è stato quello dell'attacco *ransomware* portato alla Colonial Pipeline[1], avvenuto nel 2021.

Nonostante gli sviluppi recenti, connotati da una forte consapevolezza sia dei decisori politici che dei *board* aziendali, con l'adozione conseguente di stringenti misure di difesa e resilienza, la sicurezza informatica, all'interno della Pubblica amministrazione e delle infrastrutture critiche, sembra costituire tuttora un *vulnus* evidente come testimoniano tutti gli attacchi sin qui avvenuti. La numerosità di questi eventi – ovvero gli attacchi alle strutture critiche, in primo luogo sanitarie ma

1. Colonial Pipeline trasporta 2,5 milioni di barili al giorno di benzina, gasolio, jet fuel e altri prodotti raffinati attraverso 5.500 miglia (8.850 km) di oleodotti e trasporta il 45% delle forniture di carburante della costa orientale degli Stati Uniti. La società subiva un attacco ransomware da parte di DarkSide la quale aveva iniziato le proprie operazioni di cybercrime a partire dal 10 agosto 2020. Cfr. <https://www.bleepingcomputer.com/news/security/darkside-new-targeted-ransomware-demands-million-dollar-ransoms/>. È da evidenziare che nel comunicato stampa pubblicato su un sito del dark web (8/10/2021) DarkSide spergiurava di non attaccare ospedali, scuole, organizzazioni, nonprofits oppure obiettivi governativi. Il lancio del ransomware avveniva con le seguenti affermazioni: «we are a new product on the market, but that does not mean that we have no experience and we came from nowhere. We received millions of dollars profit by partnering with other well-known cryptolockers. We created DarkSide because we didn't find the perfect product for us. Now we have it». Tutti i siti riportati in questo articolo sono stati visitati il 27 agosto 2023.

anche imprese private di ogni ordine e grado – non ha fatto che rendere di pubblica evidenza quello che si poteva facilmente ipotizzare già in precedenza. Vale a dire che esisteva un problema di messa in sicurezza di tali infrastrutture.

Non è sfuggito a nessuno, difatti, come la cybersecurity sia assurta, quasi all'improvviso, a una tra le più importanti priorità collettive: dapprima durante la crisi pandemica legata al Covid-19 (vale qui evidenziare, a solo titolo esemplificativo, il *data breach* occorso alla Regione Lazio) e all'utilizzo pervasivo della modalità lavorativa dello *"smart working"* (Paliotta 2022) e, in un momento successivo, a seguito dell'invasione da parte della Federazione Russa dell'Ucraina, con la conseguente attività di *cyber warfare* messa in atto dai principali attori *nation-state*. Non è un caso che tutto ciò sia arrivato all'attenzione delle più alte cariche dello Stato e abbia fatto segnare, nell'agosto del 2021, l'atto di nascita dell'Agenzia per la cybersicurezza nazionale (ACN).

Gran parte della complessità delle imprese che operano con sistemi ICS/OT deriva dal bilanciamento della rapida evoluzione tecnologica con un crescente livello di sofisticazione e conoscenza tecnica, da parte degli autori delle minacce, relativi a reti, componenti dei sistemi di controllo, protocolli industriali, dispositivi hardware, ecc. Del resto questi sistemi misti, definiti in letteratura come cyber-fisici, costituiscono il punto di intersezione laddove sistemi informatici e fisici si incontrano. L'elemento centrale è, pertanto, la connessione di Internet e dei computer con il mondo fisico dei dispositivi e dei sensori (Lee *et alii* 2015). I nuovi sistemi ICS/OT così creati sono in grado, infine, di controllare, ottimizzare e configurare in modo autonomo i propri parametri di funzionamento. Tutto ciò è avvenuto all'interno di un quadro generale di digitalizzazione spinta (Zong *et alii* 2017), ancora *in fieri*, che in Germania (Acatech 2013) e Italia (Paliotta 2018) è conosciuto con il nome di Industria 4.0 (Zezulka *et alii* 2016), il quale è vieppiù caratterizzato dall'uso crescente dei sensori dell'internet delle cose (Internet of things o IoT), delle macchine intelligenti (Brynjolfsson & McAfee 2011), dei *big data* (Kitchin 2014) e dell'intelligenza artificiale (AI).

A livello definitorio e in prima approssimazione, così come si può desumere da uno dei primi documenti istituzionali, quello messo a punto dal National Institute of Standards and Technology (NIST), nel 2011: «Industrial control system (ICS) is a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations such as skid-mounted Programmable Logic Controllers (PLC) often found in the industrial sectors and critical infrastructures» (Stouffer *et alii* 2011:2-1).

È intorno alla prima decade del nuovo millennio che forti preoccupazioni sulla sicurezza degli ICS/OT, in particolare nel contesto delle infrastrutture critiche nazionali, iniziano pubblicamente a palesarsi, seppur i primi documenti e interviste[2] sono da farsi rinvenire addirittura a qualche decennio prima (Lüders 2006). Ma è solo nel 2010, quando scoppia, in maniera eclatante, il caso

2. Cfr. Interview with Joseph Weiss, Cyberwar Frontline, Public Broadcasting Service (PBS), March 5, 2003, <http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/interviews/weiss.html>.

Stuxnet[3] (Langner 2011) che la sicurezza degli ICS/OT entra in maniera diffusa nel discorso pubblico e governativo e acquisisce la rilevanza odierna (Stouffer *et alii* 2011; 2013; 2015). In questo contesto, già nel 2013, il Presidente Barack Obama emetteva un *Executive Order* al riguardo: «The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats».

DIFFERENZE PRINCIPALI TRA SISTEMI ICS/OT E SISTEMI IT

I sistemi ibridi ICS/OT, sviluppatisi all'intersezione tra componente digitale e fisica, si caratterizzano in maniera distintiva nei confronti dei sistemi IT tradizionali a cui sono spesso paragonati. «A modern ICS is a complex system that depends on many different components and technologies to monitor and control physical processes; along with many of the managerial, administrative, and regulatory responsibilities associated with this task. The heart of ICSs *are operational technology (OT) which supports availability and safety of critical processes. Modern-day ICSs have incorporated information technology (IT) based on the system functions desired in the overall system*» (Hahn 2016:51).

V'è da asserire, invero, che le differenze sono assai cospicue, soprattutto dal punto di vista della cybersecurity, come viene evidenziato in Figura 1. In linea generale, i sistemi IT si concentrano sui dati a riposo o in transito; mentre quelli ICS/OT monitorano e gestiscono dati che apportano modifiche in tempo reale ai dispositivi a cui sono collegati, mediante input fisici e azioni fisiche controllate.

È intorno alla metà degli anni Novanta del secolo scorso che iniziava la convergenza tra sistemi OT e IT, intesi questi ultimi come la tecnologia relativa allo sviluppo, manutenzione e utilizzo di computer, software e reti per l'elaborazione e la distribuzione di dati. «In the past, because industrial control systems used proprietary hardware and software, this interconnection focused primarily on just being able to communicate. The introduction of Ethernet and Microsoft Windows into industrial control systems in the mid-1990s, followed by the development of OPC interfaces, greatly simplified this problem, but at the cost of exposing the ICS to security

3. «Stuxnet is a sophisticated worm designed to target only specific Siemens SCADA (industrial control) systems. It makes use of an unprecedented four 0-day vulnerabilities - attacks that make use of a security vulnerability in an application, before the vulnerability is known to the application's developers. It also uses rootkits - advanced techniques to hide itself from users and anti-malware software - on both Windows and the control computers it targets. It employs two stolen digital certificates to sign its drivers, and its creators needed a large amount of knowledge of its targeted systems. It was discovered in June 2010, but an early version appeared a year earlier. It is widely suspected of targeting Iran's uranium enrichment program, since it is rather specific about what it attacks, and this matches the Iranian Natanz enrichment plant» (Mueller & Yadegari 2012:1).

threats previously known only to IT systems»[4].

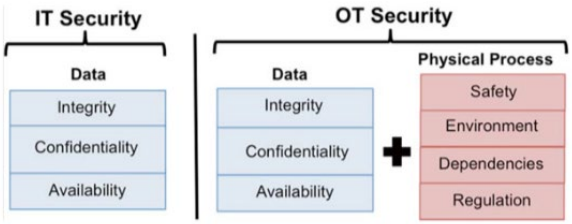


Figura 1. Operational requirements of OT versus IT

Fonte: Hahn 2016:53

In maniera dettagliata, in un blog di cui qui si riportano brevi stralci[5] ma a cui si rimanda per un approfondimento complessivo, anche dal punto di vista della cybersecurity, tali differenze sono state catalogate in 10 aspetti principali:

1) **Obiettivi di sicurezza –** i sistemi IT hanno l'obiettivo primario di proteggere i dati (confidenzialità) mentre, al contrario, quelli ICS/OT di preservare l'integrità del processo produttivo e la disponibilità dei suoi componenti[6]: la confidenzialità dei dati è senz'altro importante, ma la perdita di produzione si traduce in un'immediata decurtazione di reddito[7].

2) **Segmentazione della rete –** le reti ICS/OT possono essere viste come intranet industriali con due requisiti di sicurezza prioritari. Innanzitutto, dalle reti ICS/OT non dovrebbe essere consentito l'accesso a Internet o alla posta elettronica. In secondo luogo, queste dovrebbero essere difese rigorosamente dalle reti di altri impianti, in particolare da quelle con accesso a Internet. Le reti ICS/OT spesso dispongono di sistemi di input/output (I/O) remoti collegati all'ICS/OT tramite modem su reti pubbliche, reti pubbliche virtuali (VPN) e collegamenti satellitari, mentre le reti IT non lo sono.

3) **Network topology –** molti sistemi IT sono di grandi dimensioni rispetto a un tipico ICS/OT e contengono *data center*, intranet e reti Wi-Fi. I sistemi ICS/OT, invece, sono spesso piccoli[8] e dispongono solo di un database di configurazione e uno sto-

4. <https://blog.isa.org/top-10-differences-ics-cybersecurity>.

5. Ibidem.

6. «A control system has several unique attributes. Number one, a control system must be absolutely highly reliable. It can't shut down very often. So, unlike a business system where you can shut it down over the weekend, the system that controls the power plant must have almost 100 percent reliability or some form of backup to maintain the 100 percent reliability. It is extremely important», Interview with Joseph Weiss, cit.

7. Quando la Colonial Pipeline è stata attaccata nel maggio 2021, la società ha pagato l'equivalente di oltre 4 milioni di dollari in bitcoin poche ore dopo la richiesta di riscatto, anche se circa 2,3 milioni di dollari sono stati successivamente recuperati dalle forze dell'ordine.

8. «Operational technologies are also increasingly commoditized, prevalent, and used in applications that may be smaller in scale than industrial processes, which further contributes to cybersecurity risk.

rico relativo a dati/eventi. Questi sistemi, inoltre, rimangono relativamente statici per anni.

4) **Partizionamento funzionale –** l'approccio più comune adottato dai sistemi IT è dividere il sistema in varie partizioni amministrative per limitare al meglio l'accesso degli utenti alle risorse informative; i gruppi creati vengono utilizzati per controllare l'accesso a questi computer e ai loro oggetti (file, cartelle, eseguibili, ecc.)

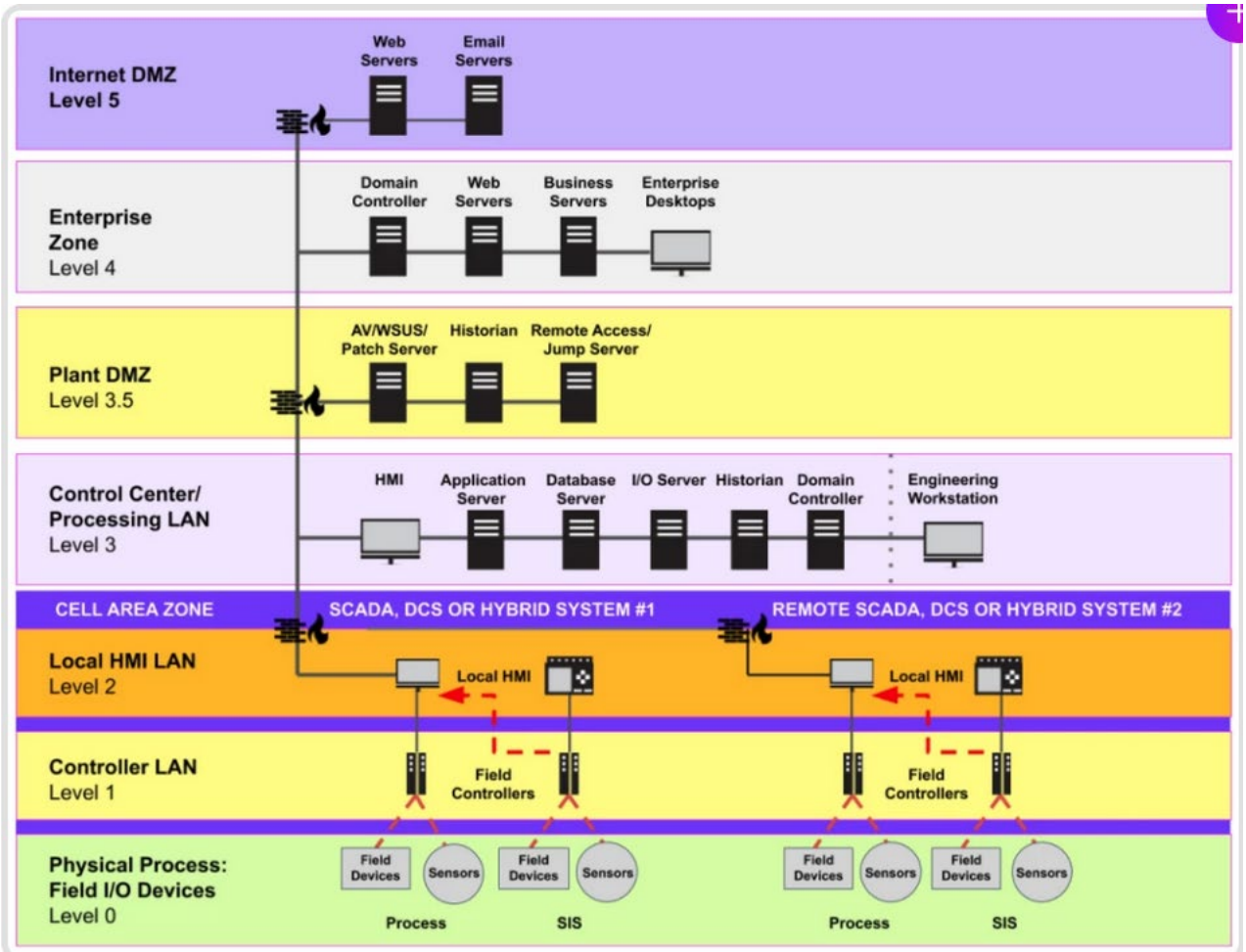


Figura 2. Essentials of the Purdue Model

Fonte: https://claroty.com/blog/ics-security-the-purdue-model

These applications are growing exponentially and migrating into domains not previously automated or connected to the internet (e.g., automobiles, medical devices, smart buildings and homes, pipelines, aviation). Adding to the ICS risk topography is the deployment of 5G networks, which reduces reliance on traditional network routers, thus limiting the ability of security providers to monitor for and prevent malicious traffic» (CISA 2020:4).

attraverso la definizione di elenchi di controllo di accesso (ACL). Il partizionamento degli ICS/OT è molto diverso in quanto è suddiviso in diversi livelli (0, 1 e 2), come definito dal modello di riferimento Purdue[9]. Il livello 0 rappresenta il processo fisico, il livello 1 il controllo e monitoraggio e il livello 2 il controllo di supervisione. I sistemi IT, in genere, non dispongono delle policy, delle procedure e degli strumenti per gestire la rete di livello 2 così come i *controller* e i dispositivi I/O di livello 1.

5) **Componenti fisici -** i sistemi IT sono composti principalmente da reti, *workstation* e server standardizzati a cui si può accedere e che si possono amministrare. Al contrario, gli ICS/OT sono sistemi proprietari strettamente integrati, composti da componenti generalmente realizzate su misura ed estranei ai sistemi IT.

6) ***User accounts* -** gli account del sistema operativo IT vengono utilizzati per autenticare l'utente durante l'accesso e per identificare a quali risorse del sistema operativo lo stesso può accedere. Il sistema ICS/OT è un sistema distribuito completo composto da applicazioni di configurazione, funzionamento e manutenzione, database e giornale di eventi. Essi utilizzano quasi sempre controlli di accesso basati su ruoli (ad es. operatori, ingegneri di processo e di manutenzione) per concedere/negare l'accesso a dati e ai dispositivi di controllo.

7) **Sistemi strumentati di sicurezza (SIS) -** gli ICS/OT spesso includono SIS integrati, ma distinti, relativi alla sicurezza dell'impianto. Questi sono responsabili del mantenimento del funzionamento del processo ponendo lo stesso in uno stato sicuro quando vengono rilevate minacce alla sicurezza. I sistemi IT non dispongono di sistemi analoghi al SIS.

8) **Software non testato -** i sistemi IT sono, in genere, sistemi aperti che consentono di eseguire software standard e di evolversi nel tempo. Gli ICS/OT, invece, sono generalmente sistemi chiusi e implementati su una specifica configurazione hardware e del sistema operativo.

9) ***Patching* -** i sistemi IT dispongono normalmente di un software di gestione delle *patches* che installa automaticamente gli aggiornamenti di sicurezza dopo il loro rilascio. D'altra parte, non è raro che le *patches* vengano rinviate o posticipate a tempo indeterminato negli ICS/OT in quanto la loro implementazione richiede test, approvazione, pianificazione e convalida per garantire un controllo sicuro e ripetibile. Inoltre, poiché il ciclo di vita de-

9. Il Modello Purdue è lo standard per la costruzione di un'architettura di rete ICS/OT che supporta la sicurezza OT separando i livelli della rete. Questa separazione consente di mantenere un flusso gerarchico dei dati tra i vari livelli. Se implementata correttamente, le imprese possono stabilire un "vuoto d'aria" tra i sistemi ICS/OT e i sistemi IT, il quale consente di applicare controlli di accesso efficaci senza ostacolare le operazioni.

gli ICS/OT è piuttosto lungo[10], per molti sistemi non più recenti le *patches* non sono più disponibili (ad esempio, ci potrebbero essere ICS/OT ancora in funzione che eseguono Windows NT e Windows XP).

10) **Inconvenienti legati alla sicurezza –** le misure di sicurezza accettabili nei sistemi IT potrebbero non essere accettabili negli ICS/OT, soprattutto quelli che diminuiscono le prestazioni dei processi produttivi oppure quando sono legati al tempo di esecuzione.

Quelle sin qui individuate costituiscono alcune differenze principali tra i sistemi industriali IT e ICS/OT, le quali determinano requisiti di sicurezza diversi per la risposta agli incidenti, all'ambiente e alla sicurezza, alla progettazione del sistema, al rilevamento delle minacce e all'architettura di rete. Questo perché, in buona sostanza, i sistemi IT sono relazionati al mondo dei dati digitali, mentre quelli ICS/OT al mondo cyber-fisico.

VETTORI DI ATTACCO E CYBER THREAT INTELLIGENCE

In generale, gli attori malevoli fanno uso di specifici vettori – come Internet o l'ingegneria sociale – per compromettere i sistemi sotto attacco. Un attacco primario può anche generare un attacco secondario, il cui obiettivo è installare *malware* che possa essere utilizzato come *pivot* per altri attacchi. Non si può non ricordare qui che anche l'accesso da remoto, ampiamente utilizzato durante la crisi pandemica da Covid-19 per permettere di lavorare in *"smart working"*, può essere considerato un vettore.

Anche il cosiddetto processo di convergenza tra sistemi IT e OT costituisce un ampio vettore di attacco e, in questo senso, i possibili percorsi di attacco possono essere di tre tipi se si adotta uno schema come quello della Figura 3.

Essi includono:

1) colpire direttamente i sistemi ICS/OT;

2) compromettere i sistemi IT da cui dipendono i sistemi ICS/OT;

3) sfruttare la crescente convergenza tra sistemi IT/OT per far leva, successivamente, su un attacco più ampio.

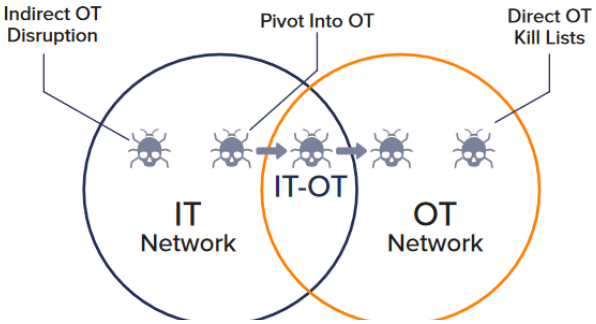


Figura 3. The Threat Landscape. Varieties of Industrial Ransomware

Fonte: DarkTrace 2021:3.

10. «Risk to traditional ICS once predominantly arose from human error and accidents, natural disasters, and acts of physical sabotage. Traditional ICS can have 30-year lifecycles and are purpose-built, stand-alone systems designed for reliability rather than security» (CISA 2020:4).

1) ***Ransomware* che colpiscono direttamente i sistemi OT.** Esistono almeno 7 famiglie di *ransomware* che contengono comandi progettati per interferire o bloccare specificamente i processi ICS/OT. La maggior parte dei ceppi, compreso EKANS, contiene 20-30 comandi che mirano ai processi ICS/OT all'interno di una "lista di eliminazione dei processi" di oltre 1.000 voci. CLOP è l'unico ceppo noto che attacca circa 150 processi ICS/OT da una *kill list* contenente 1.425 comandi. I comandi aggiuntivi utilizzati da CLOP includono processi che supportano la supervisione dei controllori logici programmabili (PLC) e dell'interfaccia uomo-macchina (HMI). Se presi di mira, potrebbero compromettere la capacità di un ingegnere di visualizzare e controllare la produzione (DarkTrace 2021:3).

2) ***Ransomware* che colpiscono indirettamente gli OT tramite la compromissione degli IT.** Il *ransomware* può anche interrompere indirettamente gli ecosistemi ICS/OT compromettendo i sistemi IT vitali su cui si basa l'OT stesso, compresi i sistemi IT che svolgono un ruolo di monitoraggio della sicurezza e garantiscono la visibilità delle operazioni. Questo percorso di attacco è stato utilizzato anche nel caso Colonial Pipeline, in quanto il *ransomware* non ha mai infettato direttamente i dispositivi OT, ma la società ha deciso di interrompere preventivamente le operazioni per evitare potenziali problemi di sicurezza (*ibidem*).

3) ***Ransomware* che sfruttano la convergenza dei sistemi IT/OT.** Il *ransomware* può sfruttare intenzionalmente la convergenza IT/OT: lo riporta DarkTrace rispetto a un incidente che ha coinvolto un impianto di gas naturale negli Stati Uniti, nel 2019, in cui l'attaccante ha infettato dapprima i sistemi IT tramite ingegneria sociale (e-mail di *phishing*) per poi effettuare un *pivoting* e passare all'OT. Quando il *ransomware* si è diffuso, sono stati compromessi sia i dispositivi IT che quelli OT. Sebbene i PLC responsabili delle operazioni non siano stati direttamente colpiti, ciò ha compromesso la visibilità delle operazioni, tanto che la società ha deciso di interrompere le operazioni per due giorni al fine di evitare potenziali effetti distruttivi (*ibidem*).

Gli attori malevoli prendono di mira i sistemi ICS/OT non mediante singoli incidenti e *data breaches*, quanto piuttosto attraverso una campagna di sforzi che consente loro l'accesso e fornisce informazioni sufficienti per poter avere un effetto distruttivo sui processi e sulle attività delle infrastrutture critiche. Comprendere a che punto è l'avversario nella sua campagna di penetrazione dei sistemi aziendali può consentire ai difensori di prendere decisioni più informate in materia di sicurezza e gestione del rischio. Ed è proprio in questo caso che può essere d'aiuto il framework della *Cyber Kill Chain* (Hutchins *et alii* 2011), adattata per i sistemi ICS/OT in quanto «this knowledge of the adversary's operations can help defenders appreciate the attacker's possible intent, level of sophistication, capabilities and familiarization with the ICS, which together work

to unveil the potential impact of the attack on an organization» (Assante & Lee 2015:1). Per portare a termine un vero e proprio attacco cyber-fisico, piuttosto che un attacco caratterizzato da spionaggio, interruzione dell'ICS/OT o furto di proprietà intellettuale, è necessario che gli avversari inizino un attacco in due fasi, così come mostrato in Figura 4.

La prima fase di un attacco informatico ai sistemi ICS/OT è il tipo di attività che ha lo scopo di ottenere l'accesso alle informazioni, conoscere il sistema e fornire meccanismi per sconfiggere le protezioni del perimetro interno od ottenere l'accesso agli ambienti di produzione. È importante sottolineare che un attore malevolo può eseguire la Fase 1 anche contro una rete di fornitori o partner, ottenendo così informazioni vitali per condurre in porto il proprio attacco.

Questa fase è caratterizzata dalle seguenti attività:

1) pianificazione (*reconnaissance*, attività volta a ottenere informazioni su qualcosa attraverso l'osservazione o altri metodi di rilevamento);

2) preparazione (*weaponization* o *targeting*: con il primo termine si intende la modifica di un file altrimenti innocuo, come un documento, allo scopo di consentire ulteriori azioni dell'avversario, mentre con *targeting* si intende il processo di analisi e definizione delle priorità degli obiettivi e di abbinamento di azioni letali e non letali a tali obiettivi per ottenere gli effetti desiderati);

3) intrusione cyber (*delivery*; *exploit*; *install* o *modify*: la consegna ha a che fare con un'interazione dell'avversario con la rete da attaccare; l'*exploit* è il vettore utilizzato per eseguire azioni dannose; l'installazione di una funzionalità dell'attore malevolo o la modifica di funzionalità esistenti del difensore costituiscono ulteriori possibili attività dell'attaccante);

4) gestione e attivazione (*command & control* - C2: vale a dire l'utilizzo di una connessione di rete tramite una funzionalità precedentemente installata);

5) sostegno, radicamento, sviluppo ed esecuzione (*act*: comprende moltissime azioni dell'attore malevolo, tra le quali, a solo titolo esemplificativo, la scoperta di nuovi sistemi o dati, il movimento laterale all'interno della rete, l'installazione e l'esecuzione di funzionalità aggiuntive, l'avvio di tali funzionalità, la cattura delle comunicazioni trasmesse come le credenziali degli utenti, la raccolta delle informazioni desiderate, l'esfiltrazione di tali dati e le tecniche anti-forensi quali la cancellazione delle tracce lasciate nell'attacco, ecc.).

La Fase 1 può essere considerata completata quando l'aggressore è riuscito a compromettere la sicurezza di un ICS/OT ed è in grado di passare alla Fase 2. È in questa fase, dunque, che l'attaccante deve utilizzare le conoscenze acquisite nella prima fase per sviluppare e testare in modo specifico una sua funzionalità in grado di attaccare in modo significativo l'ICS/OT.

La Fase 2 è caratterizzata dalle seguenti attività:

1) sviluppo e messa a punto dell'attacco (*develop*: l'attore malevolo sviluppa una nuova funzionalità su misura per colpire una specifica implementazione ICS/OT. Questo sviluppo avverrà molto probabilmente mediante l'esfiltrazione dei dati)

2) validazione (*test*: l'attaccante deve testare la sua funzionalità su sistemi simili o configurati allo

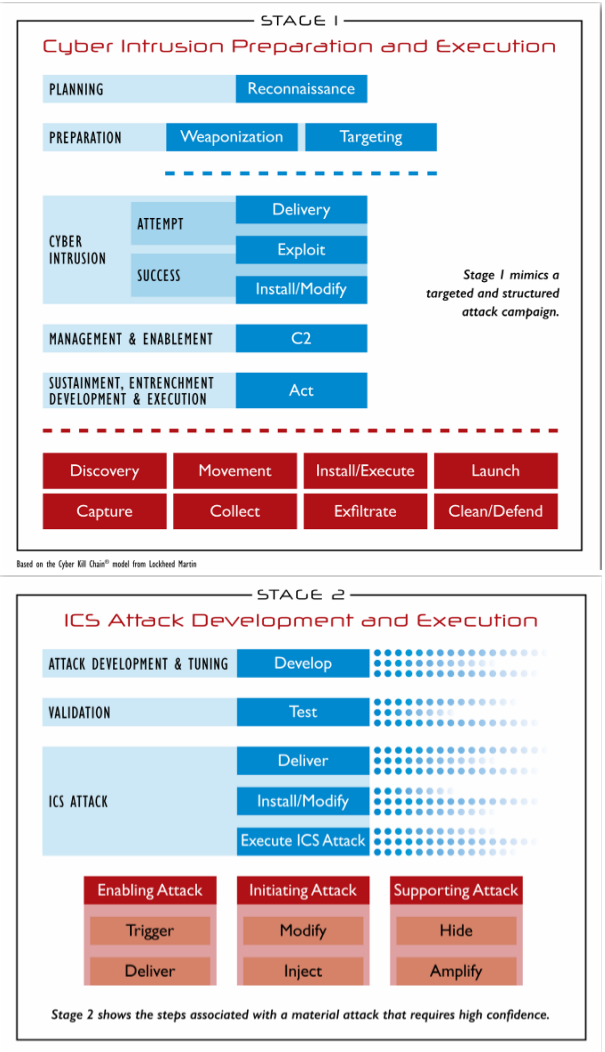


Figura 4. The Industrial Control System Cyber Kill Chain

Fonte: Assante & Lee 2015:2,8

stesso modo, se vuole che la funzionalità abbia un impatto significativo e affidabile)

3) attacco (*delivery*; *install /modify*; *execute*: l'ultima fase è l'aggressione in cui l'avversario porta la funzionalità nel sistema, la installa o modifica la funzionalità del sistema esistente e poi esegue l'attacco, che a sua volta può avere molte sfaccettature – es. attacchi preparatori o concomitanti – che non è possibile qui dettagliare).

Dalle brevi esemplificazioni sin qui presentate, si evidenzia come i sistemi ICS/OT debbano affrontare sfide di cybersicurezza peculiari, derivanti dalla convergenza degli ambienti di tecnologia operativa (OT) e tecnologia dell'informazione (IT). In questo contesto la *Cyber Threat Intelligence* (CTI) svolge un ruolo fondamentale, consentendo alle imprese di rilevare e contrastare in modo proattivo le minacce emergenti, le vulnerabilità e le campagne di attacco; le aziende possono rafforzare, pertanto, le proprie capacità di risposta agli incidenti informatici, provvedere alla mitigazione proattiva dei potenziali rischi, migliorare le strategie di gestione del rischio e promuovere una cultura proattiva della sicurezza. Una CTI specifica per i sistemi ICS/OT enfatizza, infatti, la fornitura di informazioni tempestive e utilizzabili consentendo alle società di identificare le minacce emergenti, le vulnerabilità *zero-day* e le campagne di attacco in corso, anche mediante l'utilizzo del modello ICS *Cyber Kill Chain*.

CONCLUSIONI

Da sempre, i sistemi ICS/OT sono soggetti a costanti minacce generate da attori malevoli. Questi utilizzano molteplici vettori per sferrare un attacco informatico. In questo contesto, anche le continue innovazioni tecnologiche non possono non rappresentare degli emergenti vettori di attacco da un lato ma, dall'altro, anche degli indispensabili ausili da utilizzare per la difesa proattiva: «The large-scale use of *newer technologies - such as 5G cellular networks, artificial intelligence, pervasive machine-to-machine communications, and advanced data analytics - both advantages and additional uncertainties and may significantly*

change the ICS risk landscape» (CISA 2020:ii).

Ciò impone una stretta collaborazione con i fornitori di tecnologia – non solo ICS/OT – per sviluppare, incentivare e condividere tecnologie innovative nel campo della cybersecurity che potranno ridurre le barriere di implementazione nelle infrastrutture critiche, *in primis* l'utilizzo dell'intelligenza artificiale. Sempre in ottica proattiva e predittiva, bisognerà anche migliorare la qualità e la fedeltà dei *big dati* raccolti, i quali consentiranno di avere prodotti analitici di alta qualità e orientati all'azione quotidiana.

In conclusione, come si è cercato di mettere in evidenza in questo breve testo, con l'evoluzione dei nuovi framework di attacco, dei dispositivi *legacy*, delle opzioni tecnologiche e dei vincoli di risorse, la sfida più grande per la sicurezza delle tecnologie e dei processi dei sistemi ICS/OT è l'integrazione della tecnologia *legacy* e obsoleta con i moderni sistemi IT. Ciò implica una maggiore consapevolezza di questa situazione, la quale si deve riflettere nella messa a punto di una serie di policy aziendali e, in generale, tale *awareness* deve assurgere alla massima priorità dei vertici societari. Entro tale panorama la condivisione delle informazioni sulle minacce principali, grazie alla *Cyber Threat Intelligence*, così come le strategie innovative basate sull'intelligenza artificiale, potrebbero essere implementate anche nelle organizzazioni nazionali, prevedendo un maggiore sviluppo del partenariato pubblico-privato e anche una migliore osmosi tra agenzie nazionali e infrastrutture critiche.

Achille Pierre Paliotta, *Ricercatore senior della Struttura Mercato del Lavoro dell'INAPP (ex ISFOL).*

RIFERIMENTI BIBLIOGRAFICI

Akademie der Technikwissenschaften (ACATECH) (2013), Recommendations for implementing the strategic initiative Industrie 4.0. Securing the future of German manufacturing, *Acatech Report*

Assante M. J., Lee R. M. (2015), The Industrial Control System Cyber Kill Chain, SANS Institute, October, pp. 24 <*https://na-production.s3.amazonaws.com/documents/industrial-control-system-cyber-kill-chain-36297.pdf*>

biden administration (2021), Improving the Nation's Cybersecurity, Executive Order (EO) 14028 of May 12, <*https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/*>

Brynjolfsson E., McAfee A. (2011), *Race Against the Machine. How the Digital Revolution is Accelerating Innovation, Driving Productivity, and Irreversibly Transforming Employment and the Economy*, Lexington (MA), Digital Frontier Press

Cybersecurity and Infrastructure Security Agency (cisa) (2020), Securing Industrial Control systems. A Unified Initiative FY 2019-2023, Arlington (VA), Cybersecurity and Infrastructure Security Agency, July

DarkTrace (2021), Defending Critical Infrastructure Against Ransomware, Cambridge (UK), DarkTrace, pp. 12, <*https://www.cisa.gov/sites/default/files/ICSJWG-Archive/QNL_JUN_21/DT_WP_Ransomware_Industrial_Web_Eng_S508C.pdf*>

Hahn A. (2016), *Cyber-security of SCADA and Other Industrial Control Systems*, in Colbert E. J. M & Kott A. (eds.) Cyber-security of SCADA and Other Industrial Control Systems, Fairfax (VA), Springer International, pp. 51-68

Hutchins E. M., Cloppert M. J. Amin R. M. (2011), Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Bethesda (MD), Lockheed Martin Corporation, pp. 14

Kitchin R. (2014), *The Data Revolution. Big Data, Open Data, Data Infrastructures & Their Consequences*, London (UK), Sage

Langner R. (2011), Stuxnet. Dissecting a Cyberwarfare Weapon, *IEEE Security & Privacy*, v. 9, n. 3, pp. 49-51, May-June

Lee J., Bagheri B., Kao H.-A. (2015), A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems, *Manufacturing Letters*, vol. 3, pp. 18-23

Lüders S. (2006), CERN tests reveal security flaws with industrial network devices, *The Industrial Ethernet Book 35* (CERN-OPEN-2006-074), pp. 12-23

Mueller P., Yadegari B. (2012), The Stuxnet Worm, University of Arizona, <*https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf*>

Obama administration (2013), Improving Critical Infrastructure Cybersecurity, Executive Order (EO) 13636 of February 12, *Federal Register*, v. 78, n. 33, Tuesday, February 19, <*https://www.govinfo.gov/content/pkg/FR-2013-02-19/pdf/2013-03915.pdf*>

Paliotta A. P. (2018), La web news coverage di Industria 4.0 in Italia e Germania, *INAPP Paper*, n. 14, pp. 23, dicembre

Paliotta A. P. (2022), Cyberspazio e sicurezza digitale nel lavoro agile emergenziale, in Zucaro R. (a cura di), Verso lo smart working. Un'analisi multidisciplinare di una sperimentazione naturale, *INAPP Report 30*, pp. 132-147

Stouffer K. A., Falco J. A., Scarfone K. A. (2011), Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC), *Special Publication (NIST SP) - 800-82*, Gaithersburg (MD), National Institute of Standards and Technology

Stouffer K. A., Falco J. A., Scarfone K. A. (2013), Guide to Industrial Control Systems (ICS) Security, *Special Publication (NIST SP) - 800-82 Rev 1*, Gaithersburg (MD), National Institute of Standards and Technology

Stouffer K. A., Pillitteri V., Abrams M, Hahn A. (2015), Guide to Industrial Control Systems (ICS) Security, *Special Publication (NIST SP) - 800-82 Rev 2*, Gaithersburg (MD), National Institute of Standards and Technology

Zezulka F., Marcon P., Vesely I., Sajdl O. (2016), Industry 4.0. An Introduction in the phenomenon, *International Federation of Automatic Control (IFAC)-PapersOnLine*, vol. 49, n. 25, pp. 8-12

Zhong R. Y., Xu X., Klotz E., Newman S. T. (2017), Intelligent Manufacturing in the Context of Industry 4.0. A Review, *Engineering*, vol. 3, pp. 616-630

BIOGRAFIA

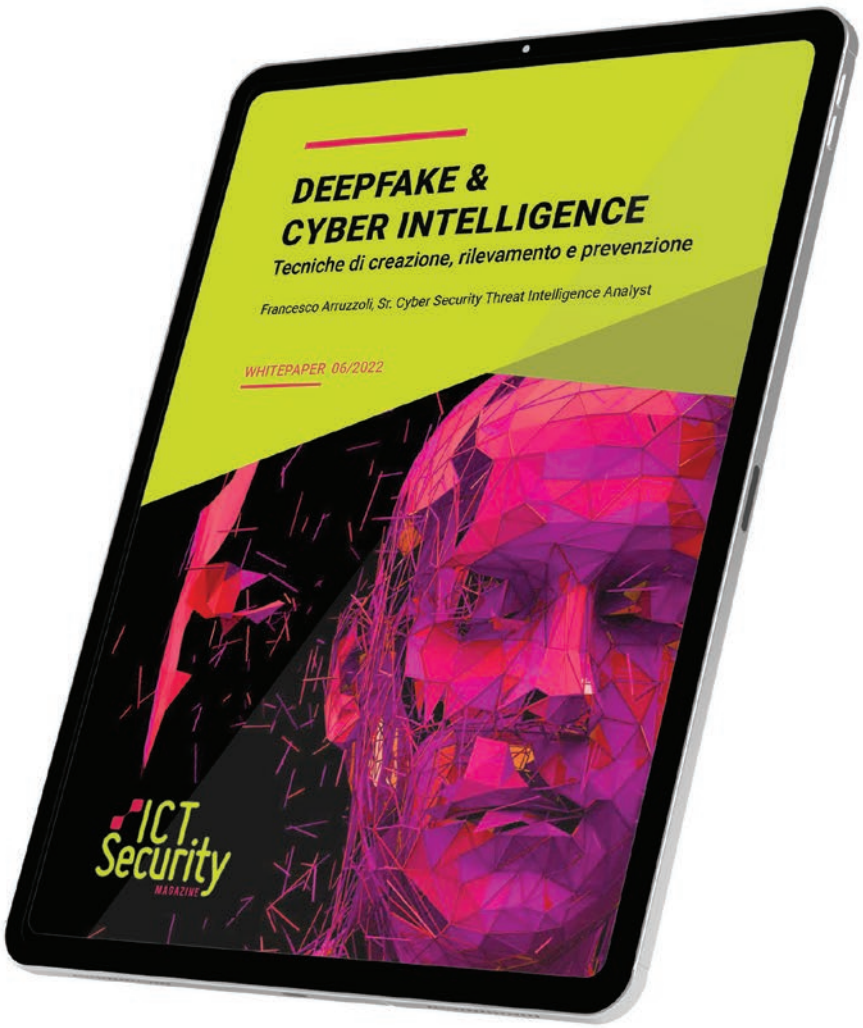
Achille Pierre Paliotta

Ricercatore senior della Struttura Mercato del Lavoro dell'INAPP (ex ISFOL). Laurea in Sociologia all'Università di Roma "La Sapienza", Master in Data Science (DS) all'Università di Roma "Tor Vergata" nel 2015 e Master in Cybersecurity (SIIS) all'Università di Roma "La Sapienza" nel 2021. Svolge studi e ricerche sull'innovazione tecnologica, sulla *cyber intelligence*, sulla cybersicurezza, sulle professioni, sull'incrocio tra domanda ed offerta di lavoro, sulla formazione continua, sull'invecchiamento attivo, sulla contrattazione collettiva e, in generale, su tematiche di sociologia economica. Sta attualmente svolgendo il I Dottorato nazionale in Cybersecurity presso IMT Lucca e IIT CNR.

White Paper

DEEPFAKE & CYBER INTELLIGENCE

Download gratuito su www.ictsecuritymagazine.com



L’obsolescenza tecnologica degli impianti industriali e le sfide per la cybersecurity

La cybersecurity degli impianti industriali è una sfida sempre più importante per le aziende che vogliono proteggere i propri dati, processi e infrastrutture da possibili attacchi informatici. Lo è anche per chi, abituato al mondo ICT aziendale tradizionale, si trova ad adattare strategie e tecnologie ad un contesto che ha, invece, le sue caratteristiche peculiari.

Un sistema di automazione e controllo industriale deve garantire il corretto funzionamento delle sue attività per tutta la durata del suo impiego sul campo. L’obsolescenza si verifica quando il produttore non fornisce più assistenza all’hardware o software e non produce più componenti di ricambio o di aggiornamento. Il mantenimento di una tecnologia obsoleta implica una serie di rischi che devono essere valutati (ad esempio la disponibilità di pezzi di ricambio, la competenza e l’affidabilità) e tra questi la cybersecurity è un aspetto fondamentale.

Un tipico ciclo di vita di un sistema di automazione come un PLC, un DCS o uno SCADA è di 10-15 anni; ma guardando lo scenario complessivo alcuni componenti possono arrivare a cicli di durata molto maggiore (figura 1). Inoltre bisogna tenere conto di quando è stata lanciata sul mercato la versione specifica del prodotto che si vuole installare, perché il suo ciclo di vita non parte da quando viene installato ma potrebbe essere iniziato da molto prima. Quindi, può succedere che il sistema di controllo scelto arrivi alla fine del suo ciclo prima di quanto si pensi.

Un altro problema che si presenta nell’impiego di sistemi commerciali è gestire il ciclo di vita del software e dei sistemi “terzi” (come i sistemi operativi Microsoft, figura 2) che hanno una durata inferiore rispetto al ciclo di vita previsto del sistema di automazione. Questo significa che, nel caso dei sistemi operativi Microsoft, il software può essere supportato per circa 10 anni se si tiene conto dell’extended support (quest’ultimo estende la durata del supporto tradizionale e prevede solo il rilascio di *patch* di sicurezza). Inoltre, bisogna considerare che l’inizio del ciclo di vita del sistema operativo raramente coincide con il lancio di un nuovo prodotto, per cui una delle componenti del sistema può diventare obsoleta anche in breve tempo.

L’aggiornamento del software, inoltre, spesso richiede la sostituzione dell’hardware del PC o del server; e i nuovi HW E SW dovranno essere compatibili con il software applicativo del sistema di automazione. È facile che prodotti degli anni 2000 siano compatibili solo con Windows XP o richiedano solo connessioni seriali per scaricare i programmi di controllo, attualmente non più presenti tra le periferiche dei PC. La necessità di sostituire o integrare i sistemi obsoleti con nuove tecnologie può quindi richiedere investimenti elevati, competenze specifiche e tempi lunghi.

Per questi motivi l’aggiornamento diventa un fattore non banale ed è comune trovare componenti obsoleti all’interno di un sistema industriale, aspetto che crea importanti limitazioni per l’appli-

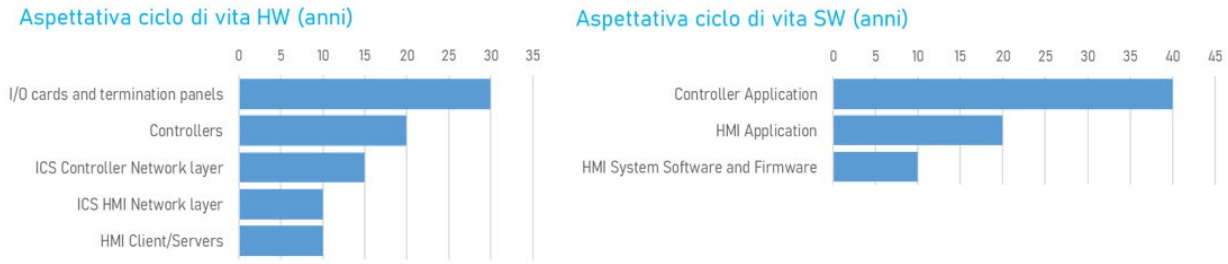


Figura 1. Aspettativa media di durata del ciclo di vita di componenti industriali (fonte: Obsolescence and life cycle management for automation systems, International Association of Oil & Gas Producers)

cazione di una strategia di cyber security efficace.

I principali rischi sono correlati ai seguenti scenari

- **Software, protocolli e interfacce vulnerabili**: l'emergere di nuove vulnerabilità, anche significative e facilmente sfruttabili, su sistemi non più supportati è una possibilità concreta. Non essendoci più supporto da parte del fornitore, si può provare ad applicare soluzioni di protezione contingenti, ma non è garantito possano avere efficacia completa. In situazioni più eclatanti e ad alto impatto, il fornitore può decidere di rilasciare ugualmente una *patch* (ad esempio è quanto accaduto da parte di Microsoft per proteggere i sistemi più vecchi dal *ransomware* WannaCry). Ma anche in questo caso molte aziende non hanno potuto o voluto aggiornare i propri sistemi e così alcuni di questi si sono ritrovati colpiti dal WannaCry anche a distanza di anni dalla sua comparsa.

Client operating systems	Latest update or service pack	End of mainstream support	End of extended support
Windows XP	Service Pack 3	April 14, 2009	April 8, 2014
Windows Vista	Service Pack 2	April 10, 2012	April 11, 2017
Windows 7 *	Service Pack 1	January 13, 2015	January 14, 2020
Windows 8	Windows 8.1	January 9, 2018	January 10, 2023
Windows 10, released in July 2015 **	N/A	October 13, 2020	October 14, 2025

Figura 2. Fine ciclo di vita per i principali sistemi operativi Microsoft

- **Risorse di sistema che diventano insufficienti**: i sistemi di protezione e monitoraggio che operano attivamente richiedono l'impiego di risorse di sistema che in alcuni casi sono appena sufficienti per far funzionare i servizi di automazione. Una normale attività di analisi o di protezione in ambiente ICT tradizionale, come un *Vulnerability Assessment* o la scansione estesa di un Antivirus, in un ambiente industriale può tramutarsi nel blocco di uno o più sistemi. L'instabilità in condizioni operative non standard facilita, inoltre, l'efficacia di attacchi cosiddetti di *"Denial of Service"* (DoS) che mirano a saturare le risorse per rendere inutilizzabili i sistemi colpiti.
- **Problemi di retrocompatibilità dei sistemi di protezione**: i sistemi di protezione e raccolta degli eventi di sicurezza evolvono nel tempo. Per far funzionare i prodotti su più versioni di un sistema operativo si devono eseguire test, verifiche e adattamenti che impiegano sforzi significativi. Di conseguenza è normale che un produttore ad un certo punto cessi di garantire la compatibilità con le versioni le più vecchie e così, su alcuni sistemi obsoleti, ci si può trovare di fronte a situazioni in cui gli aggiornamenti delle protezioni possono generare comportamenti anomali o non funzionare del tutto. È quindi sconsigliabile a priori installare le protezioni su sistemi non supportati, in quanto non vi è alcuna garanzia del loro funzionamento corretto. Questo vale anche di fronte all'ipotesi di installare versioni "vecchie" delle protezioni precedentemente supportate, in quanto non è garantito che svolgano adeguatamente la loro funzione (es. che un antivirus riesca ad aggiornare correttamente le firme sulle nuove minacce).

Negli ultimi anni, il mondo ha assistito allo sfruttamento delle vulnerabilità dei sistemi per una serie di attacchi informatici mirati a danneggiare o sabotare le infrastrutture critiche di diversi paesi, come centrali elettriche, reti di trasporto, ospedali e impianti industriali. Questi attacchi sono spesso attribuiti a gruppi sponsorizzati da governi ostili o rivali, che cercano di ottenere vantaggi strategici, politici ed economici. Quanto accaduto negli Stati Uniti nel maggio 2021 dimostra come gli effetti di un attacco cyber possano non solo determinare la chiusura di un oleodotto che rifornisce circa la metà della costa orientale USA ma, indirettamente, arrivare a mettere a rischio la tenuta del tessuto socio-economico di intere aree. La crescita degli attacchi è progressiva, fino a colpire anche settori in precedenza meno attenzionati; lo dimostra ad esempio il settore manifatturiero, che negli ultimi ha visto una crescita significativa degli incidenti cyber.

Non solo: dopo la crescita degli attacchi a fini di estorsione, il cyber spionaggio sugli impianti industriali è recentemente diventato uno strumento sempre più usato nelle guerre tra paesi, sia come strumento di aggressione che di difesa. L'obsolescenza dei sistemi e le poco consolidate pratiche di protezione sono tra i principali vettori che permettono ad attori non autorizzati di entrare negli impianti, rimanendo in ascolto e in attesa senza essere scoperti. Certi attacchi, infatti, rappresentano l'esito di compromissioni verificatesi persino più di un anno prima.

Per arginare i rischi evidenziati, occorre operare su più fronti. A livello delle singole imprese è importante intraprendere programmi che innalzino il livello di sicurezza attraverso, ad esempio:

- **segregazione dei sistemi e controllo dei flus-**

si dati: dove ci sono limitazioni nell'intervenire direttamente sui sistemi interessati, in particolare su quelli obsoleti, lo spazio di manovra non può che spostarsi nel contesto dove sono collocati. È necessario definire strette misure per la segmentazione della rete industriale e il controllo dei flussi dati. Un ruolo chiave è svolto dalla realizzazione della cosiddetta zona demilitarizzata (DMZ) a protezione del perimetro logico dell'impianto;

- **uso di sistemi di protezione "passivi"**: le misure di cybersecurity vanno impostate tenendo in considerazione le caratteristiche tipiche del contesto, favorendo ove possibile modalità di analisi "passive" o, comunque, che possano ridurre al minimo il loro impatto sull'insieme delle componenti industriali coinvolte;
- **gestione strutturata del ciclo di vita**: una corretta gestione del ciclo di vita delle varie componenti industriali deve includere gli aspetti relativi al "fine ciclo" dei vari elementi, permettendo di effettuare scelte ponderate sull'approccio al loro aggiornamento e rinnovo; in caso l'impianto sia in gestione ad un fornitore, la relazione con quest'ultimo deve essere condotta con attenzione affinché sia un elemento proattivo nella protezione e non diventi, invece, un elemento di continuità con il passato.

Ma le protezioni non bastano. All'emergere di nuove vulnerabilità, infatti, queste sono prontamente sfruttate da attaccanti sempre più capaci e rapidi, prima che sia possibile adeguare le contromisure di sicurezza adottate. È quindi importante anticiparne le mosse, per cui sono richieste capacità di *Threat Intelligence* che possono contribuire a identificare fonti, modalità e intenzioni degli attacchi informatici, nonché a fornire indicazioni per la loro prevenzione e mitigazione. Per questo negli impianti è in crescita l'adozione di sistemi in grado di fare da collettori dei dati provenienti dai vari dispositivi e di confrontarli con tempestive informazioni sulle vulnerabilità, tecniche e attività degli aggressori informatici, il tutto gestito da competenze specifiche sulla sicurezza delle tecnologie industriali che sempre più vanno a integrarsi nelle strutture tradizionali dei *Security Operation Center*.

Non solo: l'*intelligence* può operare su ulteriori e diversi livelli.

A livello strategico, può fornire una visione complessiva delle minacce informatiche e delle loro implicazioni per la sicurezza nazionale e internazionale, nonché delle opportunità di cooperazione tra gli attori coinvolti. A livello tattico può supportare la pianificazione e l'esecuzione di azioni di difesa e di risposta agli attacchi informatici – nonché la valutazione dei loro effetti – oltre a fornire informazioni specifiche e tempestive sulle vulnerabilità, le tecniche e le attività degli aggressori informatici. Questo anche a supporto dell'attività normativa in evoluzione per la creazione di sistemi industriali resilienti e la protezione, in particolare delle, infrastrutture critiche; il tutto con l'obiettivo di rafforzare la cultura complessiva della cybersecurity unitamente alla collaborazione e coordinazione tra gli attori coinvolti, sia a livello nazionale che internazionale, per migliorare le capacità di prevenzione, rilevazione e risposta agli attacchi informatici, contribuendo alla diffusione delle buone pratiche e degli standard di qualità in linea con le attuali sfide del settore industriale.

Michele Fabbri, *CISO di De Nora*

BIOGRAFIA

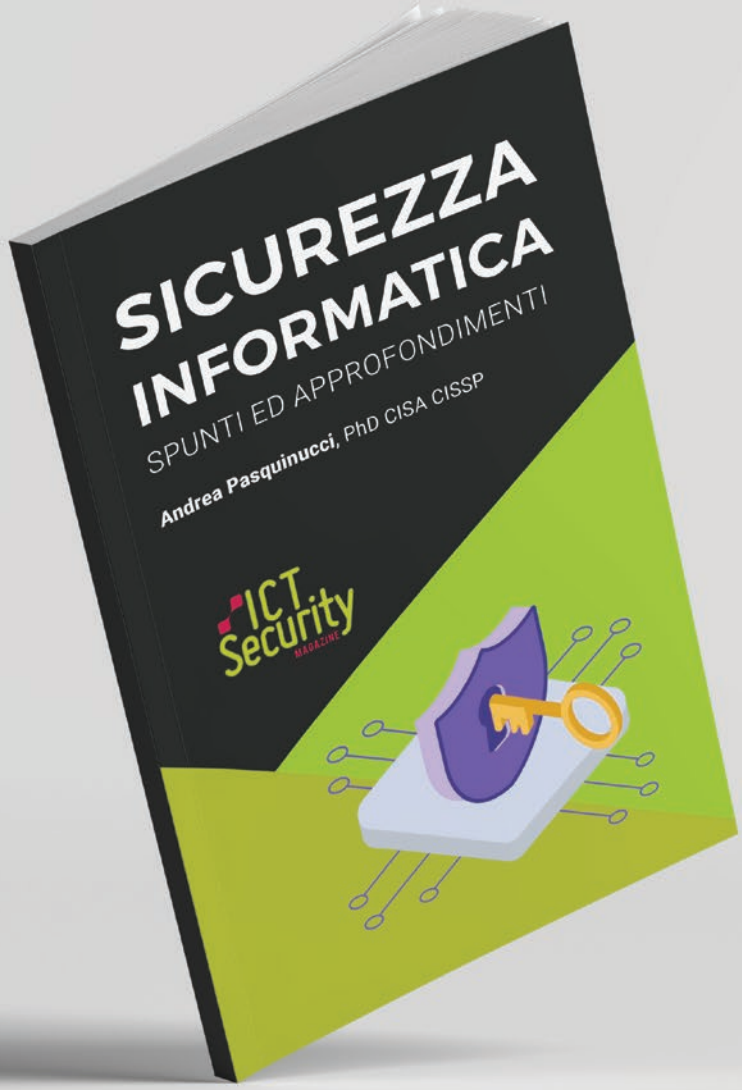
Michele Fabbri

Cyber Security Group Director - CISO presso De Nora S.p.A.
Esperto di sicurezza informatica, in oltre 25 anni ha ricoperto varie mansioni all'interno di aziende multinazionali quali Vodafone Italia S.p.A., come ICT Security Manager e Privacy & Data Protection Manager, Eni S.p.A, in qualità di Cyber Security Operations Manager e Saras S.p.A., con il ruolo di CISO.
Contribuisce alla divulgazione della cyber security tramite la sua partecipazione in vari advisory board e pubblicazioni. Attualmente è membro del direttivo dell'associazione AIPSA.

Libro in versione **cartacea** ed **eBook**

SICUREZZA INFORMATICA

SPUNTI ED APPROFONDIMENTI



Il libro è distribuito gratuitamente a tutti gli iscritti alla newsletter di ICT Security Magazine

Approcci integrati per la governance del rischio cibernetico nella Supply Chain ICT

INTRODUZIONE

La crescente dipendenza dalle tecnologie digitali e l'interconnessione delle catene di approvvigionamento hanno introdotto nuove opportunità e, contemporaneamente, esposto le organizzazioni a rischi cibernetici sempre più sofisticati. La sicurezza della *Supply Chain* ICT è diventata una priorità strategica, considerando l'ampia gamma di attacchi informatici che possono compromettere l'integrità dei dati, la continuità operativa e la reputazione aziendale.

Questo articolo si concentra sull'analisi della *governance* del rischio cibernetico, esplorando la sinergia tra gli approcci manageriali, economici, finanziari e di strategia competitiva nella gestione della sicurezza della *Supply Chain* ICT. L'obiettivo è fornire un quadro integrato per affrontare le sfide emergenti, valutare l'impatto finanziario delle violazioni della sicurezza, gestire le risorse finanziarie in modo efficiente e sfruttare la sicurezza cibernetica come fattore differenziante per la competitività aziendale.

Attraverso l'analisi degli approcci e di casi studio, si mira a fornire un contributo significativo alla comprensione di come una visione integrata degli stessi possa plasmare una *governance* del rischio cibernetico completa e adatta al contesto della *Supply Chain* ICT. In conclusione, il quadro delineato offre un'opportunità per affrontare le sfide emergenti in modo sistemico, posizionando la sicurezza cibernetica quale nuovo obiettivo di valore della strategia aziendale e della competitività nel panorama digitale globale.

BACKGROUND

Supply Chain ICT: interconnessione e complessità

La definizione di ciò che costituisce la *Supply Chain* dell'*Information and Communication Technology* (ICT) si è evoluta ampiamente nel corso dei decenni.

Dalla prima definizione che collegava la *Supply Chain* ICT alle attività online intraprese dall'azienda o dai fornitori[1] (Barlow e Li, 2007[2]; Sindhuja e Kunnathur, 2015[3]) alla più recente, che la pone

1. "E-supply chains involve organisations using online information, to perform, rather than just support, some value-adding activities in the supply chain more efficiently and effectively" (vedasi nota 2, Barlow and Li, 2007)

2. Barlow, A. and Li, F. (2007), "E-supply chains: understanding current and future opportunities and barriers", International Journal of Information Technology and Management, Vol. 6 Nos 2/3/4, pp. 286-298.

3. Sindhuja, P.N. and Kunnathur, A.S. (2015), "Information security in supply chains: a management

quale elemento principale in grado di rappresentare il tessuto vitale dell'economia digitale contemporanea, ciò che diventa interessante è l'uso di termini legati alla "creazione di valore" (letteralmente "*value creation*"[4]).

Kim e Im (2014) ritengono infatti che la *Supply Chain* ICT sia *"an effective value chain"*[5].

Riprendendo una definizione successiva a quella di Barlow and Li (2007)[6], la *Supply Chain* ICT viene presentata come *"the entire set of key actors and their organisational and process-level interactions that plan, build, manage, maintain, and defend the IT system infrastructure"*[7] (Boyson, Corsi e Rossman, 2009) e, inoltre, come "*a globally distributed and dynamic collection of people, process, and technology"* (Simpson, 2010)[8].

Caratterizzata da una rete intricata di fornitori, produttori e distributori, la *Supply Chain* ICT è, quindi, il fondamento su cui si basa la distribuzione di prodotti e servizi digitali all'interno di un'organizzazione. Purtuttavia la sua interconnessione globale, sebbene apporti notevoli vantaggi in termini di efficienza e accesso alle risorse, introduce concomitantemente una serie di sfide in termini di sicurezza cibernetica.

Per questi motivi possiamo assumere che la *Supply Chain* ICT sia un sistema aperto, dinamico e complesso.

Rischio Cibernetico: Minacce in Evoluzione

Le minacce cibernetiche si sono evolute negli ultimi 20 anni in modo esponenziale, mettendo a repentaglio la sicurezza di reti, sistemi e dati lungo tutta la *Supply Chain* ICT. Da attacchi *ransomware* a sofisticate campagne di *phishing*, le organizzazioni sono esposte a una gamma sempre più ampia di minacce. La complessità di queste minacce è ulteriormente accentuata dalla presenza di fornitori esteri, dalla globalizzazione della *Supply Chain* e dalla rapida evoluzione delle tecnologie ICT.

Relativamente a ciò, storicamente diversi sono stati i tentativi di individuare *framework* teorici per classificare i differenti rischi cyber che impattano la *Supply Chain* ICT. Ognuno di essi però, basandosi su ipotesi iniziali restrittive, non riesce a rac-

---

control perspective", Information&Computer Security.

4. Abhijeet Ghadge, Maximilian Weiß and Nigel D. Caldwell, Richard Wilding (2020), "Managing cyber risk in supply chains: a review and research agenda", Supply Chain Management: An International Journal 25/2, pp. 223–240.

5. Kim, K.C. and Im, I. (2014), "Research letter: issues of cyber supply chain security in Korea", Technovation, Vol. 34 No. 7, pp. 387-387.

6. Vedasi nota 1 e 2.

7. Boyson, S., Corsi, T. and Rossman, H. (2009), "Building a cyber supply chain assurance reference model", Science Applications InternationalCorporation (SAIC).

8. Simpson, S., Baldini, D., Bits, G., Dillard, D., Fagan, C., Minnis, B. and Reddy, D. (2010), "Software integrity controls – an assurance-based approach to minimizing risks in the software supply chain", SAFECode, June.

cogliere l'insieme completo di rischi, denotando quindi dei limiti applicativi.

Si pensi ad esempio all'approccio di Gordon and Ford (2006)[9] e di Urciuoli *et al.* (2013)[10], che classifica i rischi in *Type I* (derivanti da incidenti causati da *phishing*, furto delle informazioni e manipolazione di dati o servizi) e in *Type II* (derivanti da incidenti causati da *cyberstalking* e molestie, manipolazione o ricatto del mercato azionario e spionaggio aziendale), il cui limite è il concentrarsi solo sugli atti deliberati compiuti da attori malintenzionati.

Allo stesso modo, il National Cyber Security Centre del Regno Unito (2016)[11] classifica i rischi informatici in attacchi *targeted* (i.e., *spear-phishing*, *denial of service*, ecc.) e *untargeted* (i.e., *phishing*, *ransomware*, *scanning*, ecc.), trascurando quelli derivanti da guasti (letteralmente *physical breakdown)* o *insider threats*.

Da qui la necessità di elevare il concetto di rischio al livello di business, valutandolo attraverso un approccio che ci permetta di sviluppare una classificazione olistica dei rischi.

Obiettivi della governance del rischio cibernetico nella Supply Chain ICT

Alla luce di quanto detto sopra, l'obiettivo principale della *governance* del rischio cibernetico nella *Supply Chain* ICT è garantire l'integrità, la riservatezza e la disponibilità delle informazioni critiche attraverso un approccio che superi il limite tecnologico, che vada oltre la mera conformità normativa e che abbia caratteristiche di proattività.

La sicurezza cibernetica deve essere considerata come una componente strategica e integrata nella gestione complessiva dell'azienda, al fine di proteggere l'infrastruttura critica e mantenere la fiducia degli *stakeholder* interni ed esterni.

Nella prossima sezione esploreremo come gli approcci manageriali, economici, finanziari e di strategia competitiva possano essere sinergicamente integrati per affrontare le sfide uniche della governance del rischio cibernetico nella *Supply Chain* ICT. La combinazione di queste prospettive offrirà un quadro completo per la gestione delle minacce cibernetiche, consentendo alle organizzazioni di adattarsi dinamicamente a un panorama in continua evoluzione e di emergere come leader resilienti nell'era digitale.

GOVERNANCE INTEGRATA DEL RISCHIO CIBERNETICO

La gestione efficace del rischio cibernetico nella *Supply Chain* ICT richiede un approccio integrato che unisca prospettive manageriali, economiche, finanziarie e di strategia competitiva, di cui in Figura 1 si fornisce un diagramma di sintesi.

9. Gordon, S. and Ford, R. (2006), "On the definition and classification of cybercrime", Journal in Computer Virology, Vol. 2 No. 1, pp. 13-20.

10. Urciuoli, L., Männistö, T., Hintsa, J. and Khan, T. (2013), "Supply chain cyber security – potential threats", Information&Security: An International Journal, Vol. 29, pp. 51-68.

11. National Cyber Security Centre, UK (2016), "Common cyber attacks: reducing the impact", disponibile all'indirizzo: www.ncsc.gov.uk/white-papers/common-cyber-attacks-reducing-impact

Figura 1 - Governance del Rischio Cibernetico Integrata

Questa sezione esplorerà come tali approcci possano convergere sinergicamente per fornire una *governance* completa e resiliente del rischio cibernetico.

APPROCCIO MANAGERIALE

Leadership Strategica

L'adozione di una *leadership* strategica in materia di sicurezza cibernetica, a maggior ragione se i rischi da gestire sono quelli indotti dalla catena di approvvigionamento, implica il coinvolgimento diretto del *Top Management* nell'identificazione delle minacce e nello sviluppo di strategie a lungo termine. Questo coinvolgimento dovrebbe manifestarsi attraverso la definizione di una visione chiara della sicurezza cibernetica, l'allocazione di risorse adeguate e la promozione di una cultura di sicurezza all'interno dell'organizzazione. Inoltre, i leader dovrebbero essere attivamente coinvolti nella definizione di obiettivi chiave di sicurezza e nel monitoraggio continuo delle prestazioni[12].

Questo approccio può essere sintetizzato nei seguenti punti:

1. **Visione e impegno del *Top Management***

   Il primo passo da fare, da parte dell'organizzazione, per supportare al meglio la strategia di gestione del rischio cyber nella *Supply Chain* ICT è avere una struttura di

12. Cfr. articolo 20, Direttiva UE 2022/2555 (Direttiva NIS 2), disponibile all'indirizzo: https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022L2555&qid=1700265776948

governance chiara[13], in cui il *Top Management* è in grado di definire una visione precisa degli obiettivi di sicurezza cibernetica dell'organizzazione, allineati agli obiettivi aziendali generali[14].

Il supporto del *Top Management*, in letteratura, è sempre citato come un fattore critico per l'implementazione di una corretta strategia di *governance*[15], sebbene sia assolutamente riconosciuto per la sua importanza[16].

Ciò che quindi deve essere costruito all'interno dell'organizzazione è una nuova visione, un processo di *cultural shift*, in cui il supporto effettivo del *Top Management* si traduce nell'inseguimento di un nuovo *mindset* riguardo la sicurezza cibernetica e la gestione dei rischi nella *Supply Chain* ICT, evidenziando l'importanza della sicurezza cibernetica a tutti i livelli dell'organizzazione.

2. Leadership esecutiva e coinvolgimento attivo

Come già avviene in alcuni settori specifici – in cui le norme settoriali, ovvero l'interpretazione di esse da parte delle autorità competenti, hanno portato ad una netta posizione sull'argomento – il responsabile per l'esecuzione della strategia di sicurezza ICT deve essere coinvolto attivamente nelle decisioni strategiche dell'organizzazione, per garantire che la sicurezza cibernetica sia una considerazione fondamentale a livello manageriale.

Reich e Benbasat (2000)[17] fanno riferimento a questa visione condivisa, in cui la *leadership* e il *Top Management* aziendale condividono una visione comune del modo in cui gli obiettivi di sicurezza cibernetica contribuiranno al successo dell'impresa.

In tal senso, il *Top Management* dovreb-

13. Si noti in tal senso che la l'adeguatezza degli assetti organizzativi di cui gli Amministratori sono responsabili include la sicurezza delle reti e dei sistemi informativi.
A.TINA "Nel contesto societario anche l'implementazione di misure tecniche e organizzative adeguate e proporzionate alla gestione dei rischi posti dalla sicurezza delle reti e dei sistemi informativi utilizzati dall'impresa può essere considerata oggetto del dovere di predisposizione di adeguati assetti organizzativi dell'impresa collettiva (artt. 2086 e 2381 c.c.)" (Cybersicurezza: integrità dei processi e dei dati, in Cian – Sandei (a cura di), Diritto del Fintech, Padova, Cedam, 2020, pp. 109 ss.).

14. Cfr. requisito 5.1 (Leadership and commitment), Norma ISO/IEC 27001:2022.

15. L. Dong, D. Neufeld, and C. Higgins, "Top management support of enterprise systems implementation", J. Inf. Technol, vol. 24, no. 1, pp. 55-80, 2009

16. D. S. Preston, E. Karahanna, and F. Rowe, "Development of shared understanding between the chief information officer and top management team in US and French organizations: A cross-cultural comparison," IEEE Trans. Eng. Manage., vol. 53, no. 2, pp. 191–206, May 2006.

17. B. H. Reich, and I. Benbasat, "Factors that influence the social dimension of alignment between business and information technology objectives." MIS quarterly, vol. 24, no. 1, pp. 81–113, 2000.

be integrare la sicurezza cibernetica nei processi decisionali di ogni dipartimento aziendale, garantendo che sia una componente trasversale ed essenziale in tutte le fasi del business.

Ciò permette ai processi di sicurezza cibernetica una portata a livello di intera organizzazione, contribuendo ad allineare la visione con la strategia aziendale in tema di gestione della *Supply Chain* ICT.

3. **Gestione del cambiamento e agilità organizzativa**

La *leadership* deve essere pronta ad adattarsi rapidamente alle minacce emergenti, incorporando un approccio dinamico e agile nella gestione del rischio cibernetico.

Teece (1997)[18] si riferiva alle "capacità dinamiche" di un'organizzazione come a quelle che permettono alla stessa di integrare, costruire e riconfigurare le competenze interne ed esterne per affrontare ambienti in rapida evoluzione. In un'epoca di agilità e complessità organizzativa le competenze, come la resilienza, l'adattabilità e la capacità di far fronte alle innovazioni tecnologiche, sono fondamentali per la sopravvivenza. Allo stesso modo, le organizzazioni che adottano una cultura di fiducia (*"trust"*, come meglio specificato successivamente) e coinvolgimento possono creare una capacità di maggiore resilienza nei confronti della sicurezza informatica.

In tal ottica deve essere promossa una comprensione condivisa del cambiamento e degli scenari di rischio, per garantire che tutti siano consapevoli delle nuove minacce e delle *best practices* di sicurezza.

Una comprensione condivisa che aiuta la *leadership* a garantire risorse dedicate per l'iniziativa, a costruire team di coalizione efficaci per guidare il cambiamento nonché a fornire una visione chiara del progetto in tutta l'organizzazione.

4. **Comunicazione efficace e coinvolgimento degli *stakeholder***

La *leadership* deve comunicare chiaramente i rischi cibernetici all'intera organizzazione, fornendo informazioni trasparenti sulle minacce e sulle strategie di mitigazione e promuovendo la collaborazione tra i dipartimenti con il coinvolgimento della *Supply Chain* ICT nella pianificazione e nell'attuazione delle strategie di sicurezza.

Nello sviluppo di un processo di *"trust"*, il management svolge un ruolo importante nella comunicazione del messaggio di sicurezza informatica in tutta l'organizzazione[19] e anche al di fuori della stessa, agli *stakeholder* esterni.

18. D. J. Teece, G. Pisano, and A. Shuen, "Dynamic capabilities and strategic management," Strategic Manage. J., vol. 18, no. 7, pp. 509–533, 1997.

19. D. Dang-Pham, S. Pittayachawan, and V. Bruno, "Applying network analysis to investigate interpersonal influence of information security behaviors in the workplace," Inf. Manage., vol. 54, no. 5, pp. 625–637, 2017.

COLLABORAZIONE E COMUNICAZIONE

La collaborazione e la comunicazione sono cardini per un approccio manageriale efficace alla sicurezza cibernetica. Un'efficace gestione del rischio cibernetico richiede la partecipazione di team multidisciplinari che comprendano IT, ufficio legale, risorse umane e altri reparti pertinenti. La comunicazione dovrebbe essere chiara e diretta, con l'istituzione di canali regolari per la condivisione di informazioni cruciali sulla sicurezza. La promozione di una cultura di sicurezza attraverso la formazione e la sensibilizzazione è altrettanto importante per coinvolgere tutti i membri dell'organizzazione.

I quattro pilastri su cui si basa questo approccio sono di seguito elencati:

1. **Comunicazione efficace**

   La trasparenza nelle comunicazioni diventa un fattore abilitante concreto se si riesce a comunicare apertamente ai dipendenti e agli *stakeholder* i rischi cibernetici, spiegando in modo chiaro le minacce potenziali e le misure di mitigazione.

   Il ruolo che il management svolge nel comunicare un messaggio chiaro in tutta l'organizzazione è spesso citato in letteratura[20]. Allo stesso modo, l'esecuzione di programmi di formazione sulla sicurezza informatica per i dipendenti aiuta anche a sviluppare una maggiore comprensione della sicurezza.

   Questo porta a implementare campagne di sensibilizzazione periodiche per educare il personale sulle *best practices* di sicurezza e sulla consapevolezza delle minacce.

2. **Collaborazione interfunzionale**

   Il coinvolgimento di diverse competenze è teso a creare team di sicurezza cibernetica multidisciplinari e comitati interfunzionali che coinvolgono esperti tecnici, legali e di gestione per affrontare in modo completo le nuove sfide il cambiamento culturale (di cui abbiamo parlato nei punti precedenti).

   Un cambiamento culturale richiede un'attenzione manageriale significativa, in cui i manager non si concentrano solo su "ciò che facciamo", ma si muovono in modo incrementale verso una migliore comprensione di "come facciamo le cose", che supporta un'organizzazione più resiliente dal punto di vista informatico[21]. Lo sviluppo di un'organizzazione resiliente, in cui la *Supply Chain* è allineata all›interno di un ecosistema di rete, supporta ulteriormente tale mentalità culturale, conducendo altresì a facilitare la possibilità di organizzare esercitazioni congiunte di risposta agli incidenti che coinvolgono rappresentanti di diverse funzioni aziendali per garantire una risposta coordinata.

3. **Strumenti di comunicazione sicuri**

   L'utilizzo di strumenti sicuri e di piattaforme

20. Y. Yi, H. A. Ndofor, X. He, and Z. Wei, "Top management team tenure diversity and performance: The moderating role of behavioral integration" IEEE Trans. Eng. Manage., vol. 65, no. 1, pp. 21–33, Feb. 2018.

21. J. Loonam, J. Zweigelaar, V. Kumar, and C. Booth, "Cyber-Resiliency for Digital Enterprises: A Strategic Leadership Perspective", IEEE Trans. Eng. Manage., vol. 69, no. 6, Dec. 2022

di comunicazione implementate *ad hoc* per facilitare la collaborazione interna senza compromettere la sicurezza delle informazioni rappresenta un ulteriore vantaggio, ulteriormente accresciuto se per le comunicazioni riservate, utilizzare canali sicuri e crittografati per proteggere le informazioni da accessi non autorizzati.

4. **Gestione delle relazioni con gli *stakeholder***

   Coinvolgere attivamente fornitori, clienti e altri partner di business nella definizione delle strategie di sicurezza e nell'implementazione delle misure di mitigazione porta a stringere *partnership* più forti e a rafforzare, quando non a stabilire, rapporti regolari con le parti interessate attraverso riunioni periodiche e report dettagliati sulla sicurezza atti a garantire un dialogo costante.

APPROCCIO ECONOMICO

Analisi costo-beneficio

Negli ultimi due decenni, gli sviluppatori e i ricercatori nel campo della sicurezza cibernetica si sono resi conto che le soluzioni tecnologiche da sole non sono sufficienti a risolvere i problemi[22] e, quindi, hanno iniziato a studiarli anche da una prospettiva economica[23,24].

L'analisi costo-beneficio è uno strumento chiave per la selezione e la prioritizzazione delle misure di sicurezza cibernetica. Questa analisi dovrebbe comprendere la valutazione dei costi diretti e indiretti associati alle minacce cibernetiche, nonché i benefici attesi dalle contromisure implementate. La valutazione dovrebbe essere dinamica, tenendo conto delle evoluzioni delle minacce e delle tecnologie di sicurezza. Le organizzazioni dovrebbero mirare a massimizzare il valore di sicurezza per ogni investimento effettuato.

Gli elementi dell'analisi costo-beneficio possono essere sintetizzati in:

1. **Costi diretti**, che includono i costi associati all'implementazione di misure di sicurezza cibernetica, come l'acquisto di hardware, software e la formazione del personale, nonché la manutenzione continua delle soluzioni.

   Inoltre, si può ragionevolmente ritenere che i costi diretti incorporino altresì i costi derivanti da attività di risposta a incidenti e processi di recupero dopo una violazione[25].

2. **Costi indiretti**, che includono la stima dei costi legati alla perdita di produttività dovu-

22. Z. Rashid, U. Noor, J. Altmann, "Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem", Future Generation Computer Systems, Vol. 124, pp. 436–466, 2021.

23. R. Anderson, "Why information security is hard: An economic perspective",in: In ACSAC: Proceedings of the Seventeenth Annual Computer Security Applications Conference, pp. 358–365, 2001.

24. B. Schneier, "Secrets and Lies: Digital Security in a Networked World", John Wiley & Sons, 2011.

25. Quale semplice riferimento, anche per quanto segue, si consideri, sebbene vi siano modelli più recenti, quello presentato da Gordon e Loeb (2006).

ta a interruzioni del servizio o rallentamenti operativi causati da attacchi cibernetici e valutano i costi a lungo termine derivanti da danni alla reputazione dell'azienda, come la perdita di clienti o partner commerciali.

3. **Benefici**, derivanti dalla riduzione del rischio del verificarsi di attacchi cibernetici. La stima di questi benefici può essere complessa ma è essenziale per valutare l'efficacia delle misure di sicurezza.

   È bene notare che devono essere considerati benefici anche quelli derivanti dalla conformità a normative e regolamentazioni di sicurezza, che possono evitare multe e sanzioni.

Allo stesso modo, i metodi di analisi possono essere divisi in:

1. **Metodi quantitativi**, che cercano di assegnare valori monetari ai costi e ai benefici[26]. Ad esempio, possiamo quantificare la perdita finanziaria attesa in caso di violazione e stimare i risparmi derivanti dalla prevenzione di tale violazione.

   In questo caso, ciò che esprime il beneficio netto rispetto ai costi totali è il calcolo del *Return on Investment* - ROI[27]. Un ROI positivo indica un investimento che produce un guadagno.

2. **Metodi qualitativi**, che considerano qualitativamente il livello di rischio associato a diverse minacce e la capacità di mitigare tali rischi con le misure di sicurezza cibernetica.

   In questo caso, viene valorizzata in modo qualitativo la valutazione del valore della reputazione aziendale e la percezione di affidabilità che derivano dall'implementazione di solide pratiche di sicurezza.

Data la natura della *Supply Chain*, per le assunzioni fatte nel precedente paragrafo 2.1, l'analisi che andremo a svolgere sarà un'analisi dinamica e adattiva, che ci permette di considerare l'evoluzione delle minacce cibernetiche nel tempo. L'approccio dinamico ci permette di adattarci alle nuove minacce emergenti e di incorporare il costo e il beneficio associato all'adattamento e all'aggiornamento continuo delle misure di sicurezza per affrontare le minacce in evoluzione.

ROI degli Investimenti di Sicurezza

Il calcolo del *Return on Security Investment* - ROSI[28][29], ovverosia del ROI calcolato sugli investimenti di sicurezza, è fondamentale per misurare l'efficacia delle iniziative di sicurezza cibernetica per valutare

L.A. Gordon and M.P. Loeb, "Economic aspects of information security: An emerging field of research." Information Systems Frontiers, 8(5), pp.335-337, 2006.

26. J. Freund, J. Jones, "Measuring and Managing Information Risk: A FAIR Approach", 2015.

27. Cfr. Infra § 3.2.2

28. S. Alter, S.A. Sherer, "A general, but readily adaptable model of information system risk", Commun. Assoc. Inf. Syst. 14, 2004

29. C.D. Huang, R.S. Behara, Economics of information security investment in the case of concurrent

i valori ottenuti dagli *stakeholder* nell'ecosistema di condivisione delle informazioni sulla cibersicurezza. La metrica del ROSI consente alle organizzazioni di valutare quanto valore aggiunto ottengono rispetto ai costi sostenuti.

Inoltre, può consentire di valutare tutti gli *stakeholder* esterni nell'ecosistema di condivisione delle informazioni sulla sicurezza informatica, in linea con il processo di *"trust"* visto in precedenza, anche attraverso lo studio di incentivi[30] e specifiche metriche[31].

I *decision maker* dovrebbero valutare regolarmente il ROSI per garantire che gli investimenti in sicurezza siano allineati agli obiettivi aziendali e possano adattarsi alle mutevoli minacce cibernetiche.

Definiamo ora gli elementi che abilitano l'analisi del ROSI:

1. **Calcolo del ROSI**

   Il ROSI si calcola sottraendo il costo dell'investimento di sicurezza dai benefici ottenuti, quindi dividendo questo risultato nuovamente per il costo dell'investimento.

   La formula è:

$$ROSI = \frac{(Benefici - Costi)}{Costi} \times 100$$

2. **Costi**

   Il costo dell'investimento include il costo di acquisizione, implementazione e configurazione delle soluzioni di sicurezza, che possiamo definire "Costo iniziale", e i "Costi operativi" che coprono i costi continuativi, come manutenzione, formazione del personale e aggiornamenti.

3. **Benefici**

   A loro volta, i benefici possono essere intesi come somma di due fattori:

   (a) "Riduzione delle perdite", che includono i risparmi derivanti dalla riduzione delle perdite dovute a incidenti di sicurezza, compresi i danni finanziari diretti e le perdite di produttività;

   (b) "Prevenzione delle violazioni", che considera i benefici derivanti dalla prevenzione di violazioni, come i costi legali evitati e il mantenimento della fiducia dei clienti.

Con questi ingredienti, possiamo procedere all'analisi del ROSI che, come abbiamo visto nel paragrafo 3.2.1, possiamo affrontare attraverso l'uso di:

1. **Metodi quantitativi**

   Che ci permettono di effettuare:

   - una **"valutazione monetaria dei benefici"** attraverso il calcolo:

heterogeneous attacks with budget constraints, Int. J. Prod. Econ. 141, pp. 255–268, 2013.

30. L.A. Gordon, M.P. Loeb, W. Lucyshyn, L. Zhou, The impact of information sharing on cybersecurity underinvestment: A real options perspective, J. Account. Public Policy 34 (5) (2015) 509–519.

31. K. Campbell, L.A. Gordon, M.P. Loeb, L. Zhou, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market", J. Comput. Secur. 11 (3), pp. 431–448, 2003.

(a) delle "Stime delle perdite", che utilizza stime quantitative delle perdite finanziarie attese in caso di violazione e può derivare da modelli di valutazione del rischio;
(b) del "Valore della prevenzione", che stima il valore finanziario di prevenire attacchi e violazioni, considerando sia i costi diretti che quelli indiretti;

- una **"valutazione dei *benchmarking*"** attraverso:
  (a) l'"Analisi dei dati storici", utilizzati per confrontare l'efficacia delle misure di sicurezza rispetto a situazioni passate, aiutando a stabilire un punto di riferimento per la valutazione del ROSI;
  (b) l'"Analisi dei *benchmark* di settore", che confrontano il ROSI con i **benchmark** per determinare come si posizioni l'organizzazione rispetto agli standard del settore.

2. Metodi qualitativi

Che ci permettono di apprezzare:

- i valori di **"reputazione e affidabilità"** attraverso:
  (a) l'"Impatto sulla reputazione", che valuta qualitativamente come la sicurezza cibernetica influisce sulla reputazione del fornitore e sulla percezione di affidabilità che l'organizzazione ha dello specifico partner;
  (b) la "Fiducia del cliente", che considera la fiducia degli utenti nell'azienda come un indicatore qualitativo del successo delle iniziative di sicurezza sulla *Supply Chain* ICT;
- la capacità di "**adattabilità delle soluzioni"**, che valuta la capacità delle soluzioni di sicurezza di adattarsi a cambiamenti nel panorama delle minacce e nella crescita dell'organizzazione attraverso le caratteristiche di scalabilità e flessibilità delle stesse.

Come precedentemente detto, queste analisi hanno un senso se riusciamo a svolgerle in modo dinamico e adattivo. Per far ciò, il calcolo e la successiva analisi del ROSI devono prendere in considerazione gli scenari futuri, inclusi nuovi tipi di minacce e cambiamenti nel panorama cibernetico, nonché l'evoluzione delle tecnologie di sicurezza e l'adozione di nuove soluzioni.

Inoltre, l'analisi del ROSI dovrebbe essere periodica e adattata a nuovi dati, nuove minacce e cambiamenti nelle operazioni aziendali, incorporando il *feedback* del mercato e delle parti interessate per migliorare continuamente le strategie di sicurezza e l'efficacia delle misure.

È importante notare che il successo dei nostri investimenti di sicurezza in termini di creazione di valore diventa, specie alla luce di quanto visto nel primo punto descritto nei metodi qualitativi, co-creazione di valore[32], da affrontare su due livelli: (i) l'estrazione di valore da enormi volumi di informazioni disponibili in ambienti aperti, dinamici e complessi, come è appunto la *Supply Chain* ICT; (ii) il miglioramento delle percezioni degli utenti interni

32. S. Vicini, F. Alberti, A. Sanna, N. Notario, A. Crespo, J.R.T. Pastoriza, "Cocreating security-and-

all'azienda.

La letteratura ha indagato direttamente la sicurezza e la privacy come un'istanza di co-creazione di valore[33,34]. Nell'ambito di un approccio collaborativo in materia di sicurezza[35], proposto nel precedente paragrafo 3.1.2, la condivisione delle informazioni tra *stakeholder* interni – il cui ruolo cambia verso la partecipazione proattiva alla creazione di valore in ambito cibernetico – e *Supply Chain* ICT potrebbe favorire l'istituzione di meccanismi di prevenzione degli incidenti, aumentando i benefici e ottenendo un ROSI più alto.

APPROCCIO FINANZIARIO

Gestione delle risorse finanziarie

La gestione oculata delle risorse finanziarie richiede un approccio basato sulla prioritizzazione e sull'ottimizzazione. Le organizzazioni dovrebbero identificare le aree critiche e allocare risorse finanziarie in modo proporzionato al livello di rischio, soprattutto quando questo è associato alla *Supply Chain* ICT.

La creazione di un budget dedicato alla sicurezza cibernetica, con la flessibilità necessaria per rispondere alle nuove minacce, è cruciale. La gestione finanziaria deve essere dinamica, con una revisione periodica degli investimenti in base all'evoluzione delle minacce.

Per studiare questo approccio, utilizziamo lo stesso *workflow* pensato per il paragrafo 3.2, andando a definire preliminarmente gli elementi della gestione finanziaria, e cioè:

1. **Risorse necessarie**

   L'analisi del rischio identifica le aree a rischio elevato che richiedono investimenti finanziari significativi. Questa analisi dovrebbe basarsi sulla valutazione del rischio cibernetico e sulla prioritizzazione delle minacce.

2. **Budget dedicato**

   Attraverso l'allocazione delle risorse, l'organizzazione stabilisce un budget dedicato alla sicurezza cibernetica, tenendo conto delle priorità identificate dall'analisi del rischio. L'allocazione delle risorse dovrebbe essere proporzionata al livello di rischio e all'importanza delle risorse coinvolte, anche in termini di accordi commerciali con i partner della *Supply Chain* ICT.

Definiti gli elementi dell'analisi finanziaria, la stessa potrà essere affrontata, anche in questo caso, at-

privacy-by-design systems", 11th International Conference on Availability, Reliability and Security, ARES 2016, pp. 768–775, 2016.

33. C. Feltus, E.H.A. Proper, Conceptualization of an abstract language to support value co-creation", Federated Conference on Computer Science and Information Systems (FedCSIS), pp. 971–980, 2017.

34. C. Feltus, E.H.A. Proper, "Towards a security and privacy co-creation method", 12th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 75–80, 2017.

35. R. Garrido-Pelaz, L. González-Manzano, S. Pastrana, "Shall we collaborate?: A model to analyse the benefits of information sharing", Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security, pp. 15–24, 2016.

traverso l'uso di:

1. **Metodi quantitativi**

   Che ci permettono di calcolare:

   - il **"Costo effettivo delle soluzioni"**, attraverso la valutazione del rapporto costo/beneficio di ogni soluzione di sicurezza considerata, determinando quali soluzioni offrono il massimo beneficio rispetto ai costi sostenuti;
   - la **"Riduzione dei costi residui"**, misurata attraverso l'ottimizzazione delle risorse, garantendo che ogni investimento sia utilizzato in modo efficiente e che non ci siano sprechi finanziari.

2. **Metodi qualitativi**

   Che ci permettono di apprezzare:

   - la **"Concentrazione delle risorse finanziarie"**, attraverso l'analisi della densità di allocazione delle stesse rapportata alla *magnitude* delle aree di maggior rischio nella *Supply Chain* ICT, determinate grazie alla prioritizzazione delle minacce in fase di analisi del rischio fatta sulla base della loro gravità e probabilità di occorrenza;
   - la **"Conformità normativa"**, che deriva dall'analisi fatta per valutare la "Concentrazione delle risorse finanziarie" ma ci permette di considerare con un grado di detenzione maggiore, ovverosia con un occhio di attenzione, gli investimenti necessari per mantenere la conformità, contribuendo a evitare multe e sanzioni finanziarie.

L'ultimo passaggio è quello di rendere questa analisi dinamica e adattiva. Obiettivi che si realizzano con una revisione regolare del budget per adattarsi a nuove minacce e alla rapida evoluzione del panorama cibernetico, nonché con una flessibilità finanziaria per rispondere a incidenti di sicurezza improvvisi e alle necessità di emergenza indotta dalla indisponibilità dei servizi forniti dalla *Supply Chain*, senza compromettere altre aree operative.

ASSICURAZIONI E FINANZA STRUTTURATA

L'uso di assicurazioni contro le minacce cibernetiche e strumenti di finanza strutturata può contribuire a mitigare i rischi finanziari derivanti da violazioni della sicurezza. Le organizzazioni dovrebbero valutare attentamente le opzioni disponibili e adattarle alle proprie esigenze specifiche. Le assicurazioni possono fornire un meccanismo di trasferimento del rischio finanziario, mentre la finanza strutturata può consentire alle organizzazioni di gestire le conseguenze finanziarie attraverso strumenti come i derivati finanziari o l'emissione di *bond*.

Proviamo a valutare ora il ruolo e l'effetto che questi due elementi avrebbero sul nostro processo integrato di *governance* del rischio cibernetico nella *Supply Chain* ICT.

1. **Ruolo delle assicurazioni**

   L'azienda deve valutare attentamente il proprio profilo di rischio cibernetico per determinare la necessità di assicurazioni. Ciò, può includere una valutazione delle poten-

ziali perdite finanziarie[36] dovute a violazioni della sicurezza, svolta secondo il processo di analisi visto nel precedente paragrafo 3.3.

Tenendo conto delle potenziali perdite finanziarie, l'azienda deve strutturare la polizza assicurativa attraverso la definizione di una copertura adeguata, assicurandosi, quindi, che la polizza copra un'ampia gamma di rischi, inclusi danni finanziari diretti, spese legali, costi di ripristino e perdite di reddito dovute a interruzioni delle operazioni.

Tutto ciò può essere accelerato e meglio indirizzato grazie ad un'attenta *partnership* con assicuratori specializzati in rischi cibernetici, che comprendano le sfide uniche associate alle minacce informatiche.

2. Ruolo della finanza strutturata

Dagli anni '90, le assicurazioni sul rischio cibernetico si sono evolute per affrontare i crimini informatici emergenti come i *Data Breach* e il *ransomware*.

Purtuttavia, negli ultimi anni sono emersi nuovi veicoli di trasferimento del rischio informatico[37], come i prodotti di *capital market "cyber cat bond"*[38], annunciati nel 2023.

L'obiettivo di questa sezione non vuole essere quello di analizzare nel dettaglio le caratteristiche di questi nuovi veicoli di trasferimento del rischio ma stimolare una riflessione sulla possibilità di esplorare l'uso di derivati finanziari per mitigare il rischio finanziario derivante da perdite causate da violazioni della sicurezza cibernetica, ovve-

---

36. Ipotizzare un impatto finanziario preciso è sempre molto difficile senza informazioni dettagliate. Tuttavia, una stima approssimativa può essere fatta considerando alcune delle tipiche categorie di spese associate a violazioni della sicurezza cibernetica. In particolare, possono essere considerati, sempre attraverso un'analisi quantitativa che qualitativa, i seguenti fattori:

1. **costi legati alla risposta all'incidente,** che includono le spese per risolvere l'incidente, condurre indagini forensi, ripristinare sistemi compromessi e implementare nuove misure di sicurezza;
2. **perdita di entrate,** che derivano da clienti persi a causa della perdita di fiducia, interruzioni delle operazioni e difficoltà nell'acquisire nuovi clienti;
3. **costi legali e penali,** che includono spese per difendersi da azioni legali, multe per violazioni di normative sulla privacy e/o sulla sicurezza cibernetica, nonché eventuali risarcimenti a clienti colpiti;
4. **costi di ripristino e miglioramento della sicurezza,** che includono investimenti in nuove tecnologie, aggiornamenti dei sistemi, formazione del personale e altre misure per migliorare la sicurezza;
5. **perdita di valore del marchio**, ridotto dalla reputazione danneggiata a causa dell'incidente, influenzato dalla perdita di fiducia dei clienti e delle parti interessate;
6. **perdita di differenziazione competitiva,** difficile da quantificare, che può tradursi in perdite di quota di mercato, dovuta a mancanza di trasparenza sulla sicurezza cibernetica, che influenza negativamente la percezione del marchio rispetto ai concorrenti.

37. D. W. Woods, J. Wolff, "A History of Cyber Risk Transfer", Draft version June 2023

38. https://www.ft.com/content/a945d290-a7f1-427c-84a6-b0b0574f7376

ro esaminare la possibilità di emettere titoli garantiti da rischi cibernetici come mezzo per trasferire parte del rischio finanziario a investitori interessati.

Applicando la metodologia usata in precedenza, in questo caso, l'**analisi quantitativa** degli elementi "Assicurazioni" e "Finanza strutturata" ci permette:

- nel primo caso, di utilizzare analisi attuariali per determinare il premio assicurativo appropriato in base al livello di rischio cibernetico dell'azienda;
- nel secondo caso di analizzare la struttura del portafoglio finanziario per garantire un equilibrio tra rischi e rendimenti.

Attraverso l'**analisi qualitativa**, invece, possiamo apprezzare:

- i vantaggi derivanti dalla conformità a standard di sicurezza riconosciuti, che può portare a ridurre i premi assicurativi e migliorare la valutazione assicurativa;
- l'efficacia della strutturazione finanziaria, attraverso la verifica della flessibilità della struttura finanziaria per adattarsi a minacce cibernetiche emergenti e nuovi scenari di rischio.

APPROCCIO DI STRATEGIA COMPETITIVA

Differenziazione competitiva

La sicurezza cibernetica può diventare un elemento di differenziazione competitiva attraverso l'implementazione di misure robuste e la comunicazione attiva degli sforzi di sicurezza. Le organizzazioni dovrebbero evidenziare la loro attenzione alla sicurezza nei confronti dei clienti e dei partner commerciali, posizionandola come un valore aggiunto distintivo. La trasparenza riguardo alle pratiche di sicurezza e alle certificazioni ottenute può contribuire a costruire una reputazione di affidabilità.

Un aspetto sempre più riconosciuto nella creazione di vantaggio competitivo è quello teso a integrare la sicurezza nei processi di sviluppo del prodotto fin dalle fasi iniziali, seguendo il principio di *"security by design"*, per garantire che la stessa sia una componente essenziale delle nuove iniziative.

Questo, unito a metodologie di sviluppo agile, consente di dare un forte impulso ai processi di sviluppo messi in atto dalla *Supply Chain* ICT nonché una rapida risposta alle minacce emergenti, permettendo l'integrazione di *feedback* sulla sicurezza durante i cicli di test e produzione.

Parallelamente, lo stesso approccio può essere applicato sia alla protezione dei dati sensibili/personali – attraverso l'implementazione di una rigorosa identificazione e classificazione dei dati gestiti e/o trattati per mezzo dei beni e servizi messi a disposizione dalla *Supply Chain* ICT, garantendo che le risorse siano allocate in modo proporzionato al valore e alla sensibilità dei dati – sia alla proprietà intellettuale, implementando misure di sicurezza specifiche atte alla protezione del copyright, inclusi brevetti, algoritmi e informazioni strategiche, ovvero al *knowledge transfer*.

In questo contesto rispettare gli standard specifici del settore, quando applicabili, per garantire la conformità alle regolamentazioni settoriali, nonché ottenere certificazioni di sicurezza riconosciute a livello internazionale (come la ISO/IEC 27001) e/o

seguire linee guida come quelle dettate dal Framework NIST, permettono di migliorare la credibilità della sicurezza dell'organizzazione e migliorare la differenziazione competitiva.

Last but not least, è importante ponderare investimenti in innovazioni tecnologiche, esplorando e adottando tecnologie emergenti che possano migliorare la sicurezza cibernetica, come la *blockchain* per la tracciabilità e l'intelligenza artificiale per l'analisi predittiva delle minacce. Ciò, anche collaborando attivamente con fornitori di tecnologie avanzate per sviluppare soluzioni innovative di sicurezza, sfruttando le competenze specializzate e rimanendo all'avanguardia nelle difese cibernetiche.

Collaborazione sicura con la Supply Chain

La collaborazione sicura con i partner della *Supply Chain* ICT è essenziale per garantire la sicurezza lungo tutta la catena di approvvigionamento.

Prima di instaurare una collaborazione, è sempre fondamentale condurre una *due diligence* approfondita per valutare la maturità e la sicurezza cibernetica dei potenziali partner nella *Supply Chain*. Ciò, anche in ottica di definizione di standard comuni di sicurezza che devono essere rispettati da entrambe le parti, garantendo un livello uniforme di sicurezza nell'intera catena di fornitura.

Implementare canali di comunicazione sicuri con i partner, utilizzando protocolli crittografati, permette di proteggere le informazioni scambiate e ridurre il rischio di intercettazioni malevole. In tal senso, risulta indispensabile fornire formazione continua sulla sicurezza cibernetica ai partner nella Supply Chain per assicurare una comprensione condivisa delle minacce e delle *best practices*.

Nell'adozione di canali sicuri di comunicazione con la *Supply Chain*, l'organizzazione dovrebbe considerare l'implementazione di strategie di condivisione graduale, iniziando con informazioni meno sensibili e aumentando la condivisione man mano che la fiducia e la sicurezza crescono, tenendo sempre ben a mente l'adozione del principio del *"need-to-know"*, condividendo solo le informazioni necessarie per il raggiungimento degli obiettivi comuni e limitando l'accesso a dati sensibili.

Creare meccanismi per la condivisione proattiva di informazioni sulle minacce tra i partner, soprattutto se queste sono informazioni derivate da processi di *intelligence*, permette una risposta più rapida e coordinata agli eventi di sicurezza.

Prontezza e coordinazione, – assolutamente necessarie in situazioni di emergenza – raggiungono una maturità maggiore conducendo, inoltre, esercitazioni congiunte con la propria *Supply Chain* ICT.

In conclusione, la letteratura rileva il ruolo operativo che la sicurezza delle informazioni ha svolto negli ultimi decenni nel consentire alle organizzazioni di mantenere al sicuro le rispettive informazioni e dati.

Le organizzazioni che cercano di costruire imprese più resilienti dal punto di vista informatico, in particolare alla luce delle tecnologie digitali emergenti, devono considerare un ruolo più strategico per i loro dati.

In altre parole, i dati e la loro conseguente sicurezza diventano un *key focal point* per il management, da esplorare per sfruttarne il potenziale vantaggio competitivo, proteggendo al contempo l'organizzazione e gli *stakeholder*.

ANALISI DEI CASI DI STUDIO

L'analisi dei casi di studio fornisce una visione delle esperienze pratiche di aziende che hanno implementato strategie avanzate di gestione del rischio cibernetico nella loro *Supply Chain*. Questi casi offrono un'opportunità di apprendimento preziosa, consentendo di comprendere le sfide incontrate, le soluzioni adottate e i risultati ottenuti.

Data la funzione di integratore dei processi visti fin qui, che si vuole dare all'analisi in questo articolo, il caso di studio sarà ambientato in un contesto ipotetico.

Azienda XYZ

L'azienda XYZ, un produttore globale di dispositivi elettronici la cui *Supply Chain* ICT estesa coinvolge diversi fornitori, partner e distributori in tutto il mondo, ha subito recentemente una serie di attacchi cibernetici che hanno minacciato la continuità operativa, con potenziale impatto sulla sicurezza dei dati sensibili.

Proviamo ad applicare all'azienda XYZ una strategia integrata basata sui quattro approcci visti in precedenza:

1. **Approccio manageriale:**

   L'azienda XYZ implementa un approccio manageriale attraverso la creazione di un comitato interfunzionale per la sicurezza cibernetica. Questo comitato è responsabile della pianificazione della strategia di sicurezza e della definizione di politiche, procedure e linee guida per la gestione del rischio cibernetico nella *Supply Chain* ICT.

   Vengono inoltre sviluppati programmi intensivi di sensibilizzazione e formazione per educare i dipendenti, i fornitori e i partner sulla sicurezza informatica, che mira a creare una cultura di sicurezza condivisa in tutta la *Supply Chain* ICT.

2. **Approccio economico:**

   L'azienda XYZ conduce una valutazione economica del rischio cibernetico, identificando e quantificando le possibili perdite dovute a interruzioni operative, *Data Breach* e danni alla reputazione derivanti da incidenti alla sua catena di approvvigionamento. Questa analisi economica guida gli investimenti nella sicurezza cibernetica, anche per la gestione della *Supply Chain* ICT.

   Viene effettuato un calcolo dettagliato dei costi necessari per implementare misure di monitoraggio e difesa avanzate. L'azienda cerca di bilanciare gli investimenti in sicurezza con i benefici attesi in termini di riduzione del rischio e potenziale impatto economico.

3. **Approccio finanziario:**

   L'azienda XYZ considera l'acquisto di polizze assicurative cibernetiche per coprire i danni finanziari derivanti da violazioni della sicurezza. Questo approccio offre una copertura supplementare per ridurre l'esposizione finanziaria in caso di incidenti.

   Viene inoltre istituito un fondo di riserva finanziario dedicato alla gestione del rischio cibernetico nella *Supply Chain* ICT. Questo fondo fornisce liquidità immediata per affrontare le conseguenze finanziarie di un'indisponibilità prolungata di beni e servizi e facilitare la ripresa operativa.

4. **Approccio di strategia competitiva:**

   L'Azienda XYZ utilizza la robusta gestione del rischio cibernetico come elemento differenziante del marchio. Comunicando apertamente le misure di sicurezza adottate nella *Supply Chain* ICT, l'azienda mira a costruire la fiducia dei clienti e dei partner.

   L'azienda sviluppa inoltre partenariati strategici con fornitori e partner che dimostrano impegni significativi per la sicurezza cibernetica. Questa collaborazione sicura diventa un vantaggio competitivo, creando una rete di *supplier* più resiliente.

Risultati attesi:

L'implementazione di questi approcci integrati consente all'azienda XYZ di affrontare in modo proattivo le minacce cibernetiche, proteggendo non solo i propri interessi ma anche la sicurezza di tutta la sua catena del valore. La combinazione di strategie manageriali, economiche, finanziarie e di strategia competitiva fornisce un quadro completo per gestire il rischio cibernetico in modo efficace e sostenibile.

Proviamo ora ad ipotizzare l'impatto di una non adozione della strategia consigliata.

1. **Mancanza di *governance* manageriale**
   - Scenario: l'azienda XYZ trascura di implementare un comitato inter-funzionale per la sicurezza cibernetica e di stabilire politiche chiare con i propri fornitori.
   - Impatto: la mancanza di *governance* potrebbe portare a una risposta disorganizzata agli incidenti, provocando un'*escalation* della crisi e aumentando il rischio di danni irreparabili alla reputazione e perdite finanziarie.

2. **Sensibilizzazione inadeguata**
   - Scenario: la formazione sulla sicurezza informatica non viene prioritizzata.
   - Impatto: gli utenti potrebbero essere più suscettibili a cadere vittime di attacchi di *phishing* o a commettere errori che portano a violazioni della sicurezza, aumentando il rischio complessivo.

3. **Assenza di valutazione economica del rischio**
   - Scenario: l'azienda non effettua una valutazione economica del rischio cibernetico.
   - Impatto: senza una comprensione chiara delle possibili perdite economiche, l'azienda potrebbe investire in misure di sicurezza non adeguate o sottovalutare i reali costi di un potenziale attacco alla propria *Supply Chain*.

4. **Investimenti inadeguati in sicurezza cibernetica**
   - Scenario: la *leadership* non approva investimenti sufficienti in sicurezza cibernetica, ovvero non approva investimenti atti a migliorare il monitoraggio dei trasferimenti di dati verso la propria catena del valore.
   - Impatto: La mancanza di risorse finanziarie per misure di sicurezza avanzate potrebbe rendere l'azienda vulnerabile ad attacchi sofisticati, con

conseguenze finanziarie e operative significative.

5. **Mancanza di copertura assicurativa**
   - Scenario: l'azienda decide di non investire in polizze assicurative cibernetiche.
   - Impatto: in caso di violazione, l'azienda potrebbe affrontare costi elevati per la riparazione, la ripresa e le conseguenze legali senza il supporto finanziario di un'assicurazione cibernetica.
6. **Assenza di fondo di riserva**
   - Scenario: l'azienda non istituisce un fondo di riserva dedicato alla gestione del rischio cibernetico.
   - Impatto: in caso di incidente, l'azienda potrebbe trovarsi impreparata a gestire le spese immediate e subire danni finanziari significativi.
7. **Mancata differenziazione competitiva**
   - Scenario: l'azienda trascura di comunicare in modo trasparente le sue misure di sicurezza nella *Supply Chain* ICT.
   - Impatto: la mancanza di differenziazione competitiva sulla sicurezza cibernetica potrebbe influire negativamente sulla fiducia dei clienti e dei partner, minando la posizione dell'azienda sul mercato.
8. **Collaborazione insufficiente nella Supply Chain ICT**
   - Scenario: l'azienda non sviluppa partenariati strategici per una collaborazione sicura nella *Supply Chain* ICT.
   - Impatto: una mancanza di collaborazione sicura potrebbe rendere vulnerabile tutta la *Supply Chain*, aumentando la probabilità di attacchi mirati.

I risultati previsti in caso di non adozione delle strategie consigliate possono quindi così essere sintetizzati:

1. aumento del rischio di violazioni della sicurezza con impatti finanziari e sulla reputazione;
2. possibilità di una risposta disorganizzata agli incidenti, con tempi di ripristino più lunghi;
3. maggiore esposizione finanziaria a conseguenze legali e ripristino post-attacco;
4. diminuzione della fiducia da parte dei clienti e dei partner, con potenziali perdite di redditività;
5. riduzione della competitività sul mercato a causa della mancanza di differenziazione nella sicurezza cibernetica;
6. potenziale compromissione dell'integrità della *Supply Chain* a causa di collaborazioni non sicure.

CONCLUSIONI

Riassunto degli approcci e delle analisi

In questo articolo abbiamo esaminato gli approcci chiave alla *governance* del rischio cibernetico nella *Supply Chain* ICT, con un particolare focus sugli aspetti manageriali, economici, finanziari e

di strategia competitiva. Attraverso un'analisi approfondita di ciascun approccio, abbiamo cercato di fornire una panoramica completa delle sfide e delle opportunità che le aziende possono incontrare nel gestire la sicurezza cibernetica in un ambiente così aperto, dinamico e complesso.

Dal punto di vista manageriale, abbiamo sottolineato l'importanza della *leadership* e della cultura aziendale nel plasmare una forte postura di sicurezza. L'adozione di pratiche gestionali solide può contribuire a mitigare le minacce cibernetiche e ad aumentare la resilienza organizzativa.

Analizzando l'approccio economico, abbiamo evidenziato la necessità di valutare l'impatto finanziario delle violazioni della sicurezza cibernetica. La gestione accurata dei costi e la valutazione del ROSI possono guidare decisioni informate nella definizione di strategie di sicurezza cibernetica.

In termini finanziari, abbiamo esplorato la gestione delle risorse finanziarie come elemento cruciale della sicurezza cibernetica. Investimenti oculati possono contribuire a stabilire una solida base di difesa contro le minacce emergenti.

Infine abbiamo analizzato l'approccio di strategia competitiva, riconoscendo la sicurezza cibernetica come elemento differenziante. Una gestione efficace della sicurezza può non solo proteggere l'azienda da minacce potenzialmente dannose, ma anche conferirle un vantaggio competitivo nel mercato.

Le principali conclusioni possono quindi sintetizzarsi nei seguenti punti:

1. **Integrazione necessaria:** l'approccio migliore alla sicurezza cibernetica nella *Supply Chain* ICT richiede l'integrazione sinergica di approcci manageriali, economici, finanziari e di strategia competitiva.
2. **Comprendere la complessità:** la natura complessa delle catene di approvvigionamento richiede una comprensione approfondita delle interconnessioni tra attori e l'adozione di misure preventive adeguate.
3. **Ruolo centrale della *leadership*:** la *leadership* efficace è fondamentale per creare una cultura di sicurezza cibernetica che permei l'intera organizzazione, garantendo l'adesione e la consapevolezza a tutti i livelli.
4. **Valutazione costo-beneficio continua:** l'analisi continua dei costi e dei benefici delle misure di sicurezza è essenziale per adattare e ottimizzare le strategie in risposta alle minacce in evoluzione.
5. **Innovazione e differenziazione:** la sicurezza cibernetica non deve solo difendere, ma può anche fungere da catalizzatore per l'innovazione e la differenziazione competitiva.

PROSPETTIVE FUTURE

La sicurezza cibernetica nella *Supply Chain* ICT è un campo in continua evoluzione. Le aziende devono rimanere agili nell'affrontare le nuove minacce emergenti e nell'adattare le proprie strategie di sicurezza di conseguenza. L'adozione di tecnologie emergenti, come l'intelligenza artificiale e il *machine learning*, potrebbe offrire nuovi modi per prevenire, rilevare e rispondere alle minacce, sebbene la loro introduzione debba essere ben integrata con gli obiettivi di business al fine di evitare disallineamenti.

Inoltre, la collaborazione tra le parti interessate nella catena di approvvigionamento – inclusi for-

nitori, partner e regolatori – diventa sempre più cruciale per creare un ecosistema di sicurezza robusto.

In conclusione, la *governance* del rischio cibernetico nella Supply Chain ICT richiede un approccio olistico, basato su una *leadership* forte, valutazioni finanziarie precise e un impegno continuo per l'innovazione e la differenziazione competitiva. Solo attraverso una gestione strategica e consapevole della sicurezza cibernetica le aziende possono prosperare in un ambiente digitale sempre più complesso.

Flavio Marangi, *Partner di Balance S.r.l. e Leader della "Business Unit di Risk, Governance & Compliance"*

BIOGRAFIA

Flavio Marangi

Esperto in materia di governance dei processi di security, con particolare rilevanza per quelli in ambito Network and Information, Golden Power e Intelligenza Artificiale, ha maturato significative esperienze in attività di indirizzo, coordinamento e controllo implementate sia nel settore delle istituzioni nazionali e internazionali sia nel settore privato.

In tali ambiti, grazie ad una solida e concreta preparazione anche post-universitaria, avendo frequentato corsi di specializzazione sia nella sfera della Business Administration che in ambiente accademico e della Difesa, sorretto da un vasto network relazionale, ha gestito rapporti interistituzionali e attività di ricerca, analisi ed elaborazione di informazioni, nel settore della sicurezza e delle strategie innovative, ai fini della tutela di know-how di rilevanza scientifica e industriale.

Utilizzo dell'intelligenza artificiale nella cybersecurity dei sistemi industriali

Gli attacchi cibernetici ai sistemi industriali sono diventati sempre più sofisticati e pericolosi con l'evoluzione dell'Industria 4.0.

L'Industria 4.0 ha l'obiettivo di creare un ambiente industriale per ecosistemi di produzione in tempo reale, fabbriche intelligenti e sistemi autonomi. I progetti legati all'Industria 4.0 utilizzano tecnologie dell'informazione come l'Internet delle cose (IoT), il *cloud*, i *big data* e l'intelligenza artificiale (IA). La capacità di connettere i sistemi industriali alla rete ha portato a numerosi vantaggi in termini di efficienza, produttività, manutenzione e monitoraggio; ma ha anche aumentato esponenzialmente la superficie esposta alle minacce cyber. Sistemi e processi industriali sono così diventati un nuovo obiettivo primario; in particolare, i sistemi di controllo industriale (ICS) sono diventati uno dei principali target per i cyber criminali.

Questi sistemi sono responsabili del monitoraggio e del controllo dei processi industriali, come la produzione di energia, la gestione delle forniture idriche e l'automazione delle fabbriche. Proteggere i sistemi di controllo industriale dai cyber attacchi è una priorità per garantire la sicurezza di *asset* che vanno oltre l'operatività di un'azienda, potendo arrivare al blocco di intere nazioni o addirittura a pericoli per la vita umana.

Rimane nella storia dei cyber attacchi quello del 23 dicembre 2015 in Ucraina, quando il *malware* Blackenergy ha disconnesso alcune sottostazioni elettriche della rete elettrica nazionale, causando un *black out* di diverse ore nella maggior parte del Paese; precedenti attacchi che hanno utilizzato il *malware* BlackEnergy erano stati attribuiti a Sandworm Team, gruppo criminale piuttosto noto per azioni contro sistemi SCADA/ICS. Più recentemente, a maggio del 2021, un altro attacco ha fatto molto riflettere la comunità degli esperti di sicurezza: quello in cui un *ransomware* ha interrotto tutte le operazioni della Colonial Pipeline, il più grande gasdotto degli Stati Uniti. L'azienda ha dichiarato di aver pagato 4,4 milioni di dollari per ripristinare la propria attività.

I sistemi di controllo industriale (ICS - *Industrial Control System*) sono comunemente definiti come un sottoinsieme delle tecnologie operative (OT - *Operational Technology*) che regolano i processi industriali; e comprendono a loro volta i sistemi noti come SCADA (*Supervisor Control and Data Acquisition*), introdotti a partire dagli anni '60 per monitorare le linee di produzione e oggi spesso associati a infrastrutture su larga scala denominate DCS (*Distributed Control System*), ampiamente utilizzate nell'industria di processo (Fig.1).

Storicamente, gli ICS non sono stati progettati con caratteristiche di sicurezza *"by design"* e la convergenza di ambienti OT con le tecnologie dell'IT (*Information Technology*) nell'Industria 4.0 ha portato con sé le vulnerabilità dei sistemi IT: ad esempio la capacità di gestione remota ha connesso i sistemi ICS alla rete Internet, così esponendoli ai rischi del mondo esterno.

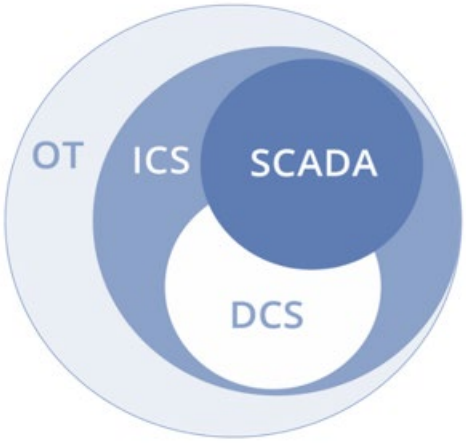


Figura 1

I sistemi OT hanno, poi, delle peculiarità che rendono difficile l'utilizzo delle misure di protezione tipiche dei sistemi IT: ad esempio la quantità di informazioni scambiate in rete, estremamente elevata ma con pacchetti di informazioni di dimensioni limitate (dell'ordine di pochi *byte*) e provenienti da un gran numero di fonti.

Questo significa che alcuni meccanismi, come la crittografia utilizzata per le classiche trasmissioni di dati IT o la firma digitale (usata per evitare l'alterazione dei dati), risultano di difficile adozione perché potrebbero introdurre un *overhead* elevato e un ritardo inaccettabile nell'elaborazione dei dati e per il controllo dell'*hard real-time*; in altre parole il requisito per garantire il tempo massimo di esecuzione per ogni *task*, essenziale per il controllo di processi industriali che il più delle volte operano a ciclo continuo (24x365).

In questo scenario anche l'utilizzo dei sistemi antivirus e le attività di *patching* risultano complessi da introdurre e applicare. Il tutto è reso ancora più complesso dal fatto che questi sistemi abbiano un *setup* molto ampio e una durata di vita di oltre dieci anni.

Va considerato inoltre che i sistemi ICS sono sempre più presenti in ambienti cyber-fisici o CPS (*Cyber-Physical Systems*), tra i più significativi nello sviluppo dell'informatica.

Nei CPS c'è una combinazione di processi fisici in rete integrati con componenti cibernetici, sensori e attuatori che interagiscono nel ciclo di monitoraggio e nel processo decisionale della linea di produzione: interazioni, queste, che diventano essenziali nei processi uomo-macchina e macchina-macchina tipici dello *smart manufacturing* e della produzione "intelligente".

Infine, mentre i sistemi IT sono stati progettati per interagire con un operatore umano, i sistemi OT devono principalmente interfacciarsi con "sistemi fisici", dovendo considerare elementi come reazioni chimiche, liquidi, variazioni di temperature, movimento di oggetti, etc.

Un attacco con iniezione di dati falsi, che mira a compromettere le misure di supervisione e acquisizione dati (SCADA) e a disturbare il funzionamento del sistema, è tra le cyber minacce più temute negli ambienti OT.

La valutazione dei rischi di sicurezza, nell'ambiente industriale, deve considerare non solo gli aspetti digitali ma anche quelli fisici. Questo approccio è essenziale per proteggere le persone, l'ambiente e le infrastrutture critiche dalle minacce informatiche. Nell'ambito operativo, la probabilità e l'impatto non sono gli unici due fattori da considerare: la relazione con il mondo fisico è il terzo parametro chiave nella formula della cybersecurity per l'OT.

Questo parametro aggiuntivo modifica drasticamente la valutazione del rischio e include dettagli preziosi per gli operatori, la cui postura di sicurezza è principalmente focalizzata sulla vita umana e

sugli impatti per l'ambiente, ovvero *asset* che non vengono quasi mai presi in considerazione nell'IT.

A titolo esemplificativo si riporta in Fig. 2 un macro esempio di architettura IT/OT integrata:

Gli attacchi informatici agli ICS possono essere mirati od opportunistici. I primi hanno come obiettivo immediato l'infrastruttura fisica, mentre i secondi includono un attacco contro un sistema industriale come sottoprodotto, piuttosto che come obiettivo principale.

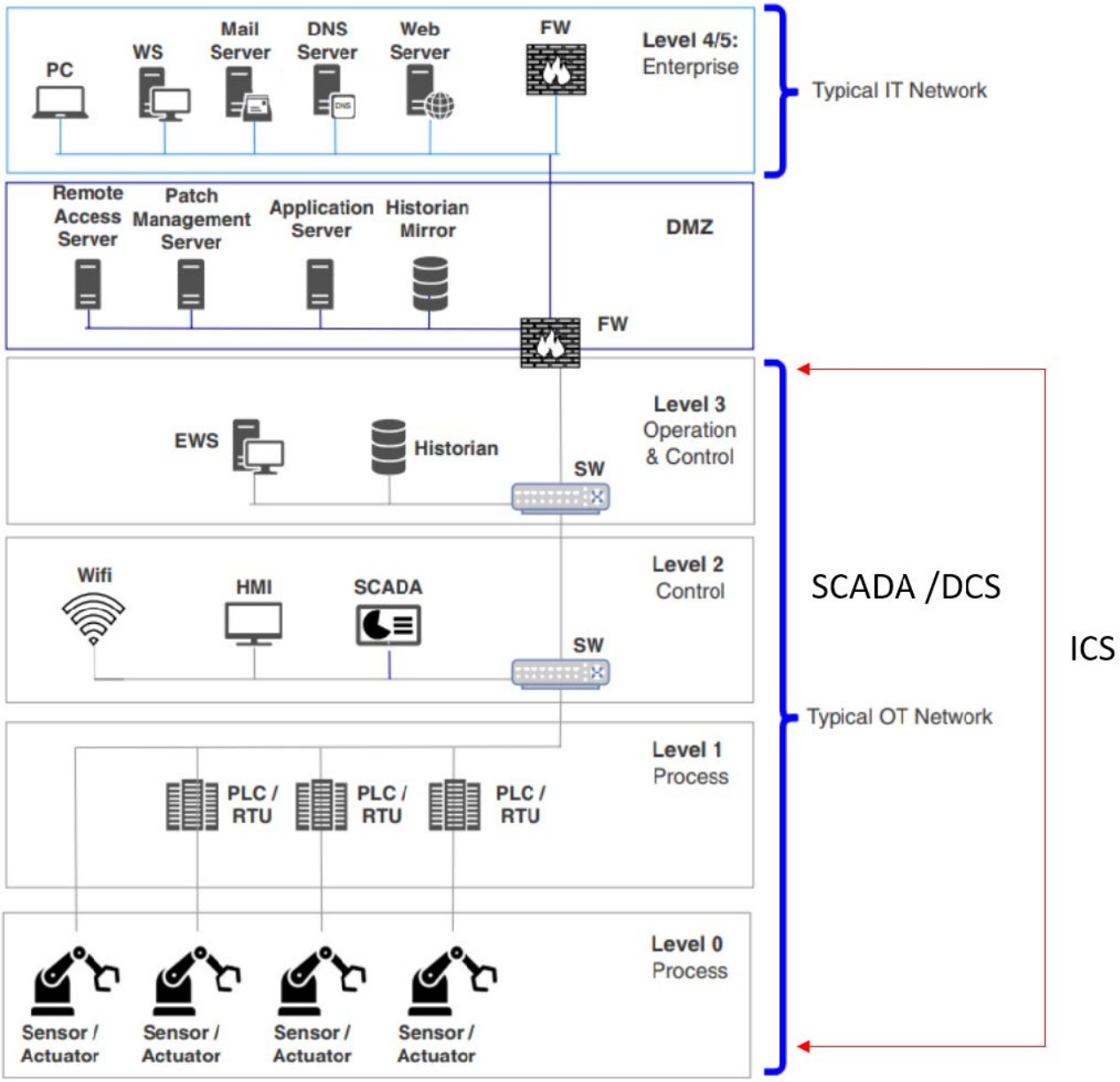


Fig. 2

ICS Architecture based on PERA model (Williams, 1994)

La MITRE Corporation ha recentemente rilasciato un quadro MITRE ATT&CK per ICS[1] per modellare i percorsi di attacco verso l'OT, sotto forma di tattiche, tecniche e procedure. Alcune delle tattiche del quadro ATT&CK per ICS ricompaiono nella matrice ATT&CK generale; altre sono uniche per i sistemi di controllo industriale.

Tra le tattiche uniche vi sono l'inibizione delle funzioni di controllo, la compromissione del controllo dei processi e una categoria che elenca le varie forme di impatto che gli attacchi informatici ICS possono avere. Gli attacchi di solito non vengono eseguiti in un'unica fase e con un'unica tecnica o procedura. Al contrario, si basano su un insieme di tecniche eseguite in una sequenza nota come *kill chain*.

Il quadro MITRE ATT&CK per ICS aiuta a identificare le specifiche tecniche e procedure che possono essere utilizzate in ciascuna fase della *kill chain* per gli attacchi agli ICS. L'utilizzo di un quadro come ATT&CK for ICS permette agli operatori di sistemi di controllo industriale di comprendere meglio le minacce, di identificare le vulnerabilità e di adottare misure preventive e di mitigazione.

Inoltre, l'impiego della *Threat Intelligence* nell'utilizzo del MITRE ATT&CK aiuta a fornire una visione più completa e dettagliata dell'ambiente di sicurezza, consentendo di aggiornare il *framework* in modo più preciso e dinamico, permettendo di:

1) identificare le tecniche usate dagli attaccanti: la *Threat Intelligence* fornisce informazioni sulla modalità di attacco utilizzata da ciascun gruppo di attaccanti, consentendo di mappare queste informazioni alla corrispondente tecnica nel framework MITRE ATT&CK;

2) prioritizzare la mitigazione: la *Threat Intelligence* fornisce informazioni sulla gravità degli attacchi e la probabilità di successo, consentendo agli amministratori di prioritizzare la mitigazione delle tecniche di attacco più pericolose in base allo scenario e alla tipologia di organizzazione;

3) diminuire i casi di falso positivo: la *Threat Intelligence* fornisce informazioni sui comportamenti di attacco specifici, consentendo di ridurre gli errori dovuti a falsi positivi nelle analisi di sicurezza;

4) fornire un contesto strategico: la *Threat Intelligence* fornisce un quadro più completo circa il contesto strategico, consentendo di comprendere la natura dell'attacco, la motivazione degli attaccanti e le implicazioni per l'organizzazione.

In questo complesso scenario, che vede le problematiche di sicurezza legate al mondo ICT sommarsi a quelle specifiche del settore OT, un valido aiuto nella prevenzione e contrasto a queste tipologie di attacchi cyber viene da soluzioni basate sull'intelligenza artificiale[2].

L'intelligenza artificiale è un approccio innovativo che conferisce soprattutto capacità di apprendimento al sistema. L'utilizzo di algoritmi di *deep*

1. MITRE Corporation; https://attack.mitre.org/matrices/ics/

2. Cyber-attacks detection in industrial systems using artificial intelligence-driven methods; 22 giugno 2022; autori: Wu Wang,Fouzi Harrou, Benamar Bouyeddou, Sidi-Mohammed Senouci, Ying Sun.

learning e *machine learning* permette di sviluppare sistemi di rilevamento delle intrusioni (IDS) per combattere gli attacchi informatici, che possono compromettere sistemi di tipologia OT; ad esempio la capacità di analizzare in *real time* traffico intenso ma di ridotte dimensioni nonché di analizzare la corretta configurazione dei parametri dei sensori e attuatori di un sistema SCADA o, ancora, di un PLC rispetto al suo comportamento operativo.

Proprio per le peculiari ed eterogenee caratteristiche architetturali degli ambienti OT, con un approccio basato su sistemi IA in grado di utilizzare contemporaneamente modelli diversi di *deep learning* (DL) e *machine learning* (ML), è possibile creare un sistema *deep ensemble*.

L'*ensembling* è un approccio di ML che combina diversi modelli predittivi per ottenere una migliore performance di previsione rispetto a un singolo modello.

Il concetto di base dell'*ensembling* è che la fusione delle previsioni di più modelli può ridurre la varianza delle previsioni individuali e migliorare stabilità e accuratezza complessiva del modello predittivo, magnificando così i punti di forza dei vari modelli, che si completeranno tra loro; mentre molte debolezze degli stessi si elimineranno a vicenda.

Questo metodo innovativo di rilevamento delle anomalie utilizza un insieme di modelli di *deep learning* per identificare e rilevare attacchi informatici nei sistemi SCADA/ICS. Il modello *deep ensemble* combina e apprende in modo dettagliato le caratteristiche delle attività dannose, permettendo di distinguerle dalle attività normali. Il principale vantaggio dei modelli di *deep learning* utilizzati è che non si richiede una progettazione delle funzionalità né si assumono ipotesi sulla distribuzione dei dati, rendendo quindi questi sistemi molto interessanti anche per il rilevamento degli attacchi informatici in ambito ICT.

Esistono diverse tecniche di *deep learning* che possono essere utilizzate per contrastare i cyber attacchi.

Rilevazione degli attacchi: le reti neurali possono essere addestrate per rilevare attività sospette o anomale nella rete, come intrusione o attacchi DDoS. Questi modelli possono essere addestrati utilizzando *dataset* etichettati contenenti esempi di attività normali e attività malevole.

SVM (*Support Vector Machine*): algoritmi di apprendimento automatico che possono essere usati per rilevare attacchi basati sulle caratteristiche del traffico di rete. L'SVM è in grado di distinguere tra traffico normale ed eventuali anomalie, che possono essere indicatori di un attacco in corso.

Riconoscimento di *malware*: l'utilizzo di reti neurali per riconoscere i modelli di codice dannoso può essere utile per rilevare e isolare i *malware* prima che possano causare danni significativi.

Tra i principali modelli di IA utilizzati:

Reti neurali convoluzionali (CNN) - si tratta di una rete neurale progettata per elaborare input memorizzati in *array*. L'architettura delle CNN è composta da tre tipi di strati: strati di convoluzione, strati di raggruppamento e strati di classificazione. Le CNN possono essere utilizzate per monitorare l'integrità del sistema industriale, in quanto possono analizzare flussi di dati provenienti da sensori all'interno dell'ambiente e rilevare anomalie o violazioni dei parametri di sistema, garantendo un

continuo monitoraggio dell'integrità del sistema stesso. Le CNN possono anche essere allenate per rilevare tentativi di *hacking* e manipolazione dei dati, potendo analizzare i *log* di sistema e i flussi di dati per identificare comportamenti anomali o attività sospette all'interno della rete industriale. Anche l'ambiente fisico può essere controllato attraverso le reti CNN, allenandole a rilevare intrusioni o accessi non autorizzati; tramite l'analisi di immagini o video provenienti da telecamere di sicurezza o droni, le CNN possono rilevare anomalie o comportamenti sospetti all'interno dell'ambiente industriale.

***Autoencoder* profondi (DAE)** - sono reti neurali in grado di analizzare e codificare dati compressi, presentando la versatilità dell'apprendimento non supervisionato. L'*encoder* e il decodificatore sono i componenti fondamentali dell'*autoencode*: un'applicazione adatta alla sicurezza dei dispositivi IoT, ai sistemi di intrusione e al rilevamento dei guasti dei sensori. Gli *autoencoder* di *denoising* sono un tipo di algoritmo di apprendimento automatico che può essere utilizzato nel campo della cybersecurity, in particolare nel contesto dei sistemi di controllo industriale. Negli ICS, i DAE di *denoising* possono essere utilizzati per rilevare anomalie nelle letture dei sensori e in altri flussi di dati, che potrebbero indicare una minaccia alla sicurezza informatica. Addestrando l'*autoencoder* in condizioni operative normali, esso può imparare a distinguere tra dati normali e anomali; se rileva un input che si discosta significativamente dalla distribuzione normale, può segnalarlo come potenzialmente anomalo e indicativo di un problema di cybersecurity. Gli *autoencoder* di *denoising* possono essere utilizzati anche per il rilevamento e la diagnosi dei guasti nei processi industriali, il che può aiutare a prevenire le minacce alla cybersecurity attenuando gli effetti di guasti o malfunzionamenti delle apparecchiature. Identificando i potenziali problemi prima che si aggravino, i team di cybersecurity possono rispondere in modo proattivo e prevenire interruzioni su larga scala.

***Deep Belief Network* (DBN)** - modello generativo probabilistico che funziona con una combinazione di reti di apprendimento multistrato, supervisionate e non supervisionate. I DBN possono essere addestrati su set di dati su larga scala provenienti da attacchi informatici noti e utilizzati per estrarre informazioni preziose sui vettori di attacco, sulle tecniche e sulle vulnerabilità dei potenziali bersagli. Questi dati possono essere utilizzati per sviluppare strategie di *Threat Intelligence* e di risposta agli incidenti, sviluppare contromisure efficaci e migliorare la sicurezza informatica complessiva.

Rete neurale ricorrente (RNN) - modello di apprendimento automatico adattato alle reti neurali, per imparare a mappare ingressi e uscite sequenziali. Le RNN sono in grado di analizzare il comportamento del software e rilevare gli schemi che indicano la presenza di *malware*. Addestrandosi su un ampio set di campioni di *malware* noti, le RNN possono identificare automaticamente *malware* nuovi o sconosciuti in base al loro comportamento.

***Generative Adversarial Network* (GAN)** - utilizza l'apprendimento automatico non supervisionato con due reti neurali, una delle quali svolge il ruolo di generatore e l'altra di discriminatore. La rete generatrice riceve i dati in ingresso e produce dati in uscita con caratteristiche simili ai dati reali; la seconda rete riceve i dati reali e i dati della prima rete, per verificare se i dati in ingresso siano reali o falsi. Le GAN possono essere utilizzate per generare dati sintetici, indistinguibili dai dati rea-

li da parte del discriminatore. Questi dati sintetici possono essere utilizzati per addestrare i modelli di apprendimento automatico a rilevare le minacce informatiche, in quanto forniscono un set di dati ampio e diversificato senza dover fare affidamento su dati sensibili o riservati provenienti dal mondo reale.

Inoltre le GAN possono essere utilizzate per generare esempi avversari, ossia input progettati per essere mal classificati dai modelli di apprendimento automatico. Questi esempi possono aiutare a identificare i punti deboli e le vulnerabilità dei modelli di apprendimento automatico, migliorandone la robustezza contro gli attacchi informatici. Le GAN possono anche essere utilizzate per generare dati sintetici al fine di testare, convalidare e verificare protocolli e sistemi di cybersicurezza in un ambiente controllato e simulato.

Deep Reinforcement Learning **(DRL)** - è la combinazione di reti neurali profonde e algoritmi di apprendimento. La sintesi dei due algoritmi fornisce una soluzione utile in scenari in cui il processo decisionale è complesso e richiede una combinazione di percezione, cognizione e azione. Grazie alla sua capacità di migliorare i meccanismi di rilevamento, prevenzione e risposta alle minacce, negli ultimi anni il *Deep Reinforcement Learning* ha guadagnato un'attenzione significativa nel campo della cybersecurity.

Combinando la potenza dell'apprendimento profondo con gli algoritmi di apprendimento per rinforzo, i professionisti della cybersecurity possono sviluppare sistemi intelligenti che imparano dalle proprie esperienze per identificare e mitigare le varie minacce informatiche. Uno dei principali vantaggi del *deep reinforcement learning* nella cybersecurity è la sua capacità di gestire attacchi complessi e dinamici: i sistemi tradizionali e gli approcci basati sulle firme spesso faticano a rilevare attacchi *zero-day* o che utilizzino modelli in rapida evoluzione. I modelli di *deep reinforcement learning*, invece, sono in grado di apprendere dai dati storici e di adattare le proprie strategie di difesa in tempo reale, migliorando l'accuratezza e l'efficienza nel rilevare minacce sconosciute e in evoluzione.

Le ricerche in campo di ML e DL mostrano tecniche promettenti per combattere le minacce informatiche applicando strumenti di IA per proteggere l'ecosistema industriale, i sistemi continueranno ad imparare dai tentativi di attacco: di conseguenza, trarranno vantaggio dall'analisi predittiva per affrontare la crescente complessità dei cyber attacchi. L'intelligenza artificiale aiuta il monitoraggio per identificare modelli di attività normali e anomale con caratteristiche dannose e il monitoraggio, a sua volta, rende possibile mitigare e localizzare gli attacchi.

Tuttavia, le tecnologie IA non garantiscono una sicurezza assoluta per gli ambienti industriali. Le stesse tecnologie, infatti, vengono sfruttate anche per creare nuovi tipi di minacce avanzate: ad esempio gli attori malintenzionati utilizzano modelli ML per generare *malware* sempre più sofisticati, aumentando così la portata degli attacchi.

Le soluzioni basate sull'IA offrono numerosi vantaggi nel prevenire e contrastare i cyber attacchi, ma richiedono una costante evoluzione e miglioramento che tengano in conto l'evoluzione delle minacce. La combinazione di intelligenza artificiale e competenze umane specializzate può essere la strategia migliore per affrontare le sfide della sicurezza cibernetica. Attualmente utilizzare l'IA per la prevenzione e il contrasto dei cyber attacchi

presenta, rispetto ai sistemi di difesa tradizionali, diversi vantaggi e alcune importanti sfide.

Di seguito una tabella riassuntiva dei principali vantaggi e svantaggi nell'utilizzo di queste tecnologie (Tab.1).

componente di interazione col mondo fisico è preponderante, la decisione di bloccare un sistema di produzione per isolare un attacco cyber – ad esempio – potrebbe causare enormi danni ambientali e addirittura la perdita di vite umane.

Vantaggi dell'IA nella cybersecurity	Sfide per l'utilizzo dell'IA nella cybersecurity
Rilevamento e risposta rapida: l'IA può analizzare grandi quantità di dati in tempo reale per identificare modelli sospetti o attività anomale, consentendo una risposta immediata al cyber attacco.	Falsi positivi e falsi negativi: l'IA può generare allarmi erronei o non rilevare correttamente alcune minacce. È necessario un costante lavoro di perfezionamento dell'algoritmo per ridurre i falsi positivi e negativi.
Adattabilità: l'IA può apprendere in modo autonomo e migliorare continuamente le sue capacità di rilevamento e difesa, adattandosi alle nuove minacce e ai nuovi metodi utilizzati dagli aggressori.	Malintenzionati che sfruttano l'IA: gli aggressori possono utilizzare l'IA per eseguire attacchi più sofisticati e sfuggire alla rilevazione, creando una sorta di "corsa agli armamenti" tra i difensori e gli aggressori.
Automazione dei processi di sicurezza: l'IA può automatizzare compiti ripetitivi come il monitoraggio del traffico di rete, l'analisi dei *log* e la gestione delle vulnerabilità, riducendo l'onere sui team di sicurezza.	Bisogno di *expertise* specializzata: l'implementazione di soluzioni basate sull'IA richiede competenze tecniche avanzate, che potrebbero non essere facilmente disponibili o accessibili a tutte le organizzazioni.
Identificazione delle minacce sconosciute: l'IA può individuare e mitigare le nuove minacce cibernetiche prima che siano ampiamente riconosciute dai sistemi di difesa tradizionali.	Costi elevati: l'implementazione e la gestione di sistemi di difesa basati sull'IA possono richiedere investimenti significativi in termini di infrastruttura, risorse e personale specializzato

Tab.1

In conclusione va sottolineato che queste tecnologie rivelano anche diversi problemi etici nella loro implementazione, come la mancanza di un codice morale per le macchine. Il processo decisionale può infatti avere impatti significativi, che l'Intelligenza Artificiale potrebbe non avere la capacità di valutare.

Tale incapacità di prendere decisioni che tengano conto di questioni etiche rappresenta senz'altro la principale sfida: poiché negli ambienti industriali la

Francesco Arruzzoli, *Resp. R&D e Centro Studi Cyber Defense Cerbeyra*

BIOGRAFIA

Francesco Arruzzoli

Con oltre 30 anni di esperienza nell'ambito della sicurezza delle informazioni Francesco Arruzzoli è Sr. Cyber Security Threat Intelligence Analyst presso la Winitalia di cui è cofondatore. Responsabile del Centro Studi Cyber Defense Cerbeyra presso il polo di cyber security del Gruppo Vianova, coordina le attività di R&D, analisi delle cyber minacce e progettazione di nuove soluzioni per la cyber security di aziende ed enti governativi. Progettista di sistemi esperti, software developer, network e system engineer, è stato tra i primi ethical hacker italiani certificati. Autore di libri ed articoli sue riviste del settore, in passato ha lavorato per multinazionali, aziende della sanità italiana, enti governativi e militari. In qualità di esperto di Cyber Intelligence e contromisure digitali ha svolto inoltre attività di docenza presso alcune università italiane.

Quaderno di Cyber Intelligence #2

CYBER CRIME

White paper gratuito su www.ictsecuritymagazine.com

Progettazione di sicurezza in Operational Technology: applicazioni militari dello standard ISA-62443

BREVE INTRODUZIONE ALLO STANDARD ANSI/ISA-62443

Lo standard tecnico ANSI/ISA-62443 (anche noto come IEC-62443) rappresenta un pilastro fondamentale nella protezione delle infrastrutture critiche e dei sistemi di automazione e controllo industriale (IACS). Questa serie di standard, sviluppata dal comitato ISA99 dell'International Society of Automation (ISA) in collaborazione con la International Electrotechnical Commission (IEC), offre linee guida dettagliate e metodologie approfondite per la progettazione, l'implementazione, l'operatività e il mantenimento di sistemi di controllo industriale sicuri e affidabili.

Lo standard ISA-62443 si distingue per il suo approccio olistico alla sicurezza, integrando principi di ingegneria, gestione del rischio e tecnologie di sicurezza avanzate, definendo un quadro completo per affrontare le vulnerabilità e le minacce sempre più sofisticate e pervasive che affliggono i sistemi industriali moderni: una delle caratteristiche distintive di ISA-62443 è infatti la sua capacità di adattarsi a una vasta gamma di settori industriali, compresi il manifatturiero, l'energia, l'acqua, i trasporti ed altri ancora.

In ambito di infrastrutture critiche della Difesa, nell'aprile 2021 il NATO ENSEC COE[1] – centro di eccellenza per la sicurezza energetica della NATO – e il comitato di standard ISA99 – dedicato alla Sicurezza dei Sistemi di Automazione e Controllo Industriale – hanno sottoscritto un protocollo d'intesa per la cooperazione nello scambio di informazioni e la possibile collaborazione su risorse didattiche e attività: il NATO ENSEC COE si è subito interessato all'applicazione dello standard ANSI/ISA-62443 durante uno studio sul rischio cibernetico dei sistemi di controllo industriale utilizzati nel sistema di oleodotti NATO dell'Europa Centrale NATO-POL[2], al fine di migliorare la sicurezza, l'affidabilità e le prestazioni delle tecnologie fondamentali che sostengono la sicurezza dell'Alleanza e degli Stati membri.

Tra gli obiettivi primari dello standard ISA-62443 vi è garantire la disponibilità, l'integrità e la confidenzialità delle informazioni e dei sistemi di controllo nelle infrastrutture industriali secondo un concetto di triade C.I.A. invertita, introdotto dallo stesso standard per enfatizzare l'importanza della disponibilità nei sistemi di controllo industriale, dove il tempo di inattività può avere conseguenze significative tanto sulla produzione quanto sulla sicurezza. Nel cuore dello standard ISA-62443 risiede il concetto di *Security Level* (SL), che stabilisce i requisiti di sicurezza per i sistemi di automazione industriale in base alla loro capacità di resistere ad attacchi di intensità

1. https://www.enseccoe.org/en/about/6

2. https://it.wikipedia.org/wiki/Oleodotto_NATO_Petroleum,_Oil_and_Lubricant

e motivazione variabile; tale classificazione (riportata nel dettaglio al paragrafo **Adozione nel contesto delle infrastrutture militari critiche**) serve come guida per gli operatori industriali, consentendo loro di implementare misure di sicurezza proporzionali al livello di minaccia valutato. In aggiunta, lo standard introduce il concetto di *Security Level Target* (SL-T), che indica il livello di sicurezza che si aspira a ottenere per tutelare i sistemi IACS (*Industrial Automation & Control Systems*) dalle minacce individuate attraverso l'analisi dei rischi.

DEFINIZIONE E DETERMINAZIONE DEI SECURITY LEVEL TARGET (SL-T): OSTACOLI E CONSIDERAZIONI

Citando lo standard tecnico ANSI/ISA-62443-3-2-2020:

"There is no prescribed method for establishing SL-T. Some organizations choose to establish SLT based upon the difference between the unmitigated cyber security risk and tolerable risk. Whereas others elect to establish SL-T based on the SL definitions provided in Annex A of this document and ISA-62443-3-3. Another approach, if a risk matrix is used (see Annex B for examples), is to qualitatively establish the SL. Starting from a reasonable estimate of SL (can also be none) the cyber security risk is evaluated by the risk matrix taking into account the countermeasures implied by the SL. If the risk is not acceptable, then the SL is raised (this means additional countermeasures are added) until the cyber security risk is acceptable. The SL derived from this analysis becomes SL-T."[3]

Appare evidente l'assenza di un metodo fisso, definito dallo stesso standard, che consenta di stabilire il *Security Level Target* (SL-T) di un IACS: alcune organizzazioni potrebbero scegliere di adottare un approccio basato unicamente sulla differenza tra rischio non mitigato e rischio tollerabile, altre di seguire le definizioni fornite nella norma ISA-62443-3-3, queste ultime oggetto di analisi nel successivo paragrafo.

Alcuni metodi prevedono l'uso di una matrice di rischio: si parte da una **stima di SL** e si valuta il rischio usando la matrice, aggiungendo contromisure finché il rischio non sia ritenuto accettabile derivando quindi un livello di sicurezza target (SL-T). Tale flessibilità nell'approccio potrebbe consentire alle organizzazioni di adattare SL-T alle proprie esigenze specifiche; occorre tuttavia notare come la stessa flessibilità sia in grado di portare a interpretazioni soggettive e, potenzialmente, ad incoerenze nella determinazione di SL-T tra diverse parti coinvolte all'interno di un'organizzazione.

In una prima progettazione di tipo *"greenfield"* (termine proveniente dallo standard che si riferisce a una nuova installazione o a un nuovo sistema che viene progettato e implementato da zero, senza vincoli derivanti da tecnologie o infrastrutture esistenti), risulta essenziale considerare le seguenti situazioni che potrebbero emergere e influenzare il processo di definizione di un *Security Level Target* (SL-T).

- **Mancanza di dati reali:** in un progetto non ancora avviato, potrebbero mancare dati

3. (ANSI/ISA-62443-3-2-2020)

reali sulla performance degli impianti o sulla vulnerabilità degli asset. Senza dati concreti, qualsiasi valutazione del rischio sarà basata su stime e ipotesi, rendendo difficile stabilire un SL-T accurato e affidabile.

- **Variabilità delle specifiche:** le specifiche del progetto potrebbero cambiare durante le fasi di progettazione e sviluppo. Questi cambiamenti potrebbero influenzare significativamente il livello di sicurezza richiesto; conseguentemente, l'assegnazione di un SL-T in questa fase e mediante la conduzione del solo *risk assessment* potrebbe portare a discrepanze tra le specifiche iniziali e i requisiti di sicurezza finali.
- **Mancanza di specifiche nell'implementazione delle contromisure di sicurezza:** durante la fase di progettazione, potrebbe sorgere incertezza riguardo all'implementazione concreta delle contromisure di sicurezza. L'assenza di dettagli sull'attuazione pratica potrebbe compromettere le valutazioni dei rischi, conducendo a scelte basate su scenari ideali piuttosto che sulla realtà effettiva.
- **Variazioni nella complessità:** la complessità del sistema potrebbe variare durante la progettazione. Un sistema inizialmente progettato come "semplice" potrebbe diventare più complesso a causa di requisiti aggiuntivi o di modifiche nel progetto. Tali variazioni potrebbero influenzare il livello di sicurezza richiesto, rendendo difficile stabilire un SL-T *"baseline"* che sia definitivo o duraturo nel tempo.
- **Rischio di sovra o sotto-stima:** in assenza di dati concreti e dettagli sull'implementazione, il rischio di sovrastimare o sottovalutare il livello di sicurezza richiesto potrebbe aumentare. Tra le dirette conseguenze si avrebbe un eccesso di spesa per contromisure di sicurezza non necessarie o, al contrario, una protezione insufficiente contro le minacce reali.
- **Mancato coinvolgimento degli *stakeholder*:** nelle fasi iniziali del progetto, specie quelle precoci, potrebbe non essere coinvolto un numero sufficiente di *stakeholder*. Senza il coinvolgimento di tutte le parti interessate, le valutazioni del rischio e gli SL-T proposti potrebbero non riflettere appieno le esigenze – anche in termini di *compliance* – e le "preoccupazioni" di tutte le parti coinvolte nel progetto.

ADOZIONE NEL CONTESTO DELLE INFRASTRUTTURE MILITARI CRITICHE

Nel contesto delle infrastrutture militari critiche legate alla *Operational Technology*, argomento centrale del presente contributo, l'assegnazione del livello di sicurezza (SL-T) è un processo complesso che richiede una considerazione accurata delle minacce, delle specifiche dottrine e normative militari e delle esigenze operative. L'approccio del *risk assessment* "tradizionale" mediante fogli o modelli pronti all'uso, sebbene ampiamente utilizzato in contesti come quello delle *utilities*, potrebbe non soddisfare completamente le esigenze delle organizzazioni militari coinvolte.

Di seguito vengono esaminate – seppur non esaustivamente – le ragioni principali per cui un approccio più specializzato e orientato alla *cy-*

ber threat intelligence, oltre che specificamente adattato alle minacce e alle precipue esigenze militari, è essenziale nella progettazione e implementazione di sistemi e infrastrutture OT nell'ambito della difesa.

1. **Classificazione delle informazioni sensibili:** considerato che le organizzazioni militari trattano anche informazioni altamente sensibili e/o classificate, un *risk assessment* tradizionale potrebbe non tener conto delle minacce particolari legate alla sicurezza nazionale e alle operazioni militari. La classificazione delle informazioni potrebbe rendere inadeguate alcune metodologie di valutazione del rischio utilizzate nel contesto civile e industriale.

2. ***Advanced Persistent Threat***: le organizzazioni militari affrontano minacce avanzate e persistenti da attori statali e non statali. Queste minacce spesso superano le tradizionali capacità di valutazione del rischio, richiedendo approcci più sofisticati e orientati all'*intelligence* per poter essere efficacemente identificate e mitigate.

3. **Necessità di contromisure specifiche:** le dottrine militari richiedono contromisure specifiche e altamente specializzate per affrontare minacce particolari. Un *risk assessment* generico potrebbe non identificare adeguatamente queste esigenze specifiche, portando ad una protezione insufficiente contro minacce complesse.

4. **Gestione delle operazioni tattiche e strategiche:** le implementazioni nell'ambito delle operazioni militari possono richiedere una gestione delle risorse e delle operazioni altamente dinamica e flessibile. Un approccio basato su *risk assessment* tradizionale, seppur mirato alle infrastrutture critiche, potrebbe non essere sufficientemente adattabile alle mutevoli condizioni del teatro operativo o alle esigenze tattiche e strategiche in rapida evoluzione.

5. **Riservatezza delle capacità tecniche:** alcune capacità tecniche utilizzate in contesti militari sono altamente riservate. La divulgazione di queste informazioni, quando possibile, durante un processo di valutazione del rischio potrebbe compromettere la sicurezza e l'efficacia delle operazioni militari.

6. **Possibili minacce interne:** le minacce interne, come *insider* non affidabili o infiltrazioni nemiche, sono una preoccupazione diffusa in diverse organizzazioni; tuttavia, nel contesto militare possono avere implicazioni particolarmente gravi per la sicurezza nazionale. Le esigenze specifiche delle organizzazioni militari, incluse la riservatezza delle informazioni e la necessità di operare in ambienti ad alto rischio, richiedono un approccio più specializzato e orientato all'*intelligence* per identificare e affrontare tali minacce in modo efficace.

7. **Rispetto delle direttive governative e normative militari:** le organizzazioni militari devono naturalmente conformarsi a

direttive governative[4] e normative militari specifiche, che potrebbero richiedere approcci di sicurezza unici e non facilmente adattabili a modelli di valutazione del rischio generici.

In aggiunta, per quanto concerne le definizioni dei quattro livelli di sicurezza presenti nello standard tecnico ANSI/ISA-62443-3-2-2020, di seguito riportate:

"ISA-62443-4-2 [10] defines SLs in terms of four different levels (1, 2, 3 and 4), each with an

increasing level of security. SL 0 is implicitly defined as no security requirements or security

protection necessary.

SL 1: *Protection against casual or coincidental violation*

SL 2: *Protection against intentional violation using simple means with low resources, generic skills and low motivation*

SL 3: *Protection against intentional violation using sophisticated means with moderate*

resources, IACS specific skills and moderate motivation

SL 4: *Protection against intentional violation using sophisticated means with extended*

resources, IACS specific skills and high motivation."

È chiaro che le definizioni dei quattro livelli di sicurezza fornite dallo standard ISA-62443-4-2, basate unicamente sulle capacità delle minacce e sulle risorse necessarie per compromettere la sicurezza del sistema, risultano piuttosto generiche e potrebbero presentare limitazioni rilevanti se applicate al contesto militare. L'assenza di dettagli specifici rischia di "spingere", "forzare" i decisori verso un'assegnazione "automatica" di SL 4 a tutte le casistiche rientranti in tale contesto, a causa della percezione di minacce esterne complesse, altamente motivate o non completamente comprese, dando così origine a varie problematiche, di seguito elencate.

- **Sovraccarico di risorse:** l'assegnazione deliberata di SL 4 ad ogni IACS potrebbe portare a un eccessivo dispendio di risorse, finanziarie e umane, per implementare e gestire misure di sicurezza sofisticate anche in situazioni che non richiedono tali livelli di protezione.

- **Difficoltà nell'identificare le minacce prioritarie:** con la deliberata e indiscriminata assegnazione di SL 4, gli enti potrebbero avere difficoltà a identificare e dedicare risorse alle minacce più gravi e specifiche, perdendo di vista le priorità di sicurezza.

- **Rischio di non conformità:** l'assegnazione indiscriminata di SL 4 potrebbe portare a non conformità con direttive, normative e requisiti specifici dell'ambito militare.

- **Mancanza di adattabilità e interoperabilità:** un'assegnazione generica del massimo SL potrebbe mancare di adattabilità alle mutevoli minacce e a esigenze operative specifi-

4. Direttive PCM-ONS 3/2019, PCM-ANS/COMSEC-256 (B), PCM-ANS/TI-001÷005 e 008, PCM-ANS 6/2006 et al.

che, incluse quelle di interoperabilità, poiché non terrebbe conto dei contesti operativi variabili e delle minacce emergenti.

- **Eccessiva complessità:** l'implementazione generalizzata di misure di sicurezza al massimo livello potrebbe portare a una complessità eccessiva nei sistemi militari, rendendo difficile la gestione operativa e la manutenzione delle infrastrutture.

La mancanza di dettaglio nelle definizioni degli SL potrebbe, quindi, portare a un'applicazione inefficace e/o poco adattabile delle misure di sicurezza nel contesto militare. Risulta pertanto fondamentale – al fine di scongiurare inefficienze operative, spreco di risorse e una protezione inefficace contro le minacce reali e prioritarie – una personalizzazione o reinterpretazione (anche estesa) dei quattro *Security Level*, così da poterli adattare alle minacce specifiche, alle dottrine militari e alle esigenze operative di ciascun ente. Tale personalizzazione consentirebbe una maggiore flessibilità nell'adozione di contromisure mirate, riducendo al minimo la spesa e l'utilizzo delle risorse senza tuttavia compromettere l'efficacia della sicurezza. Inoltre, permetterebbe di reagire in modo tempestivo alle minacce emergenti e di adattare continuamente le strategie di sicurezza, garantendo una protezione dinamica e adeguata in un panorama estremamente mutevole come quello militare.

OPERATIONAL TECHNOLOGY E DIFESA: UN MODELLO DI SICUREZZA ADATTIVO

Per massimizzare tanto l'efficienza quanto l'efficacia nella metodologia di progettazione e implementazione dell'*Operational Technology* in infrastrutture militari critiche, in accordo anche con lo standard tecnico ISA-62443, è cruciale l'adozione di obiettivi tecnici strategici, specialmente nelle nuove implementazioni (*greenfield* secondo ISA-62443). Tali obiettivi dovrebbero essere di natura dinamica e personalizzabile per rispondere alle necessità specifiche di ogni organizzazione militare. Obiettivi ad alto livello potrebbero abbracciare vari ambiti, alcuni dei quali elencati di seguito.

Identificazione delle minacce e delle vulnerabilità

Conduzione di un'analisi approfondita per l'identificazione delle minacce specifiche che potrebbero essere affrontate nelle operazioni militari in corso o future, critiche e non; conseguente valutazione delle vulnerabilità delle infrastrutture militari, inclusi sistemi di comunicazione, reti informatiche, protocolli di comunicazione e infrastrutture fisiche.

Valutazione del rischio

Adozione di una metodologia di valutazione del rischio specifica che tenga conto delle minacce e delle vulnerabilità identificate e che tenga inoltre in considerazione parametri quali: la sensibilità delle informazioni, la criticità delle operazioni e l'impatto potenziale di un attacco sulle missioni e operazioni militari in corso e/o future, nonché sulle capacità dell'ente e sulla sicurezza nazionale.

Definizione delle metriche di sicurezza

Sviluppo e definizione di metriche specifiche per

la valutazione della sicurezza delle infrastrutture militari. Ciò potrebbe includere indicatori di performance operativa, tempi di ripristino in caso di attacco, capacità di ripristino automatico[5], densità di valore[6] e capacità di resilienza. Potrebbe essere valutata anche l'inclusione di indicatori di performance derivanti da dati storici esistenti, anche se collezionati nel contesto dell'*information technology*, come ad esempio il tempo medio di rilevamento (MTTD) e di risposta (MTTR).

Coinvolgimento delle parti interessate

Sviluppo di un piano di dettaglio che preveda e descriva il coinvolgimento e lo "*scope* di autorità" (opzionalmente anche di "autorevolezza") di tutte le parti interessate: compresi vertici e reparti militari, organi di vigilanza, agenzie di informazione per la sicurezza, organismi di certificazione, *vendor*, *system integrator* e professionisti della sicurezza.

Adattamento alle dottrine e normative militari

Incorporazione di specifiche dottrine e regolamenti militari che governano la sicurezza e la protezione delle infrastrutture critiche all'interno delle analisi di rischio. È altresì fondamentale includere tassonomie, definizioni e standard pertinenti, anche quando si tratta di standard interni all'organizzazione.

Personalizzazione degli SL

Rielaborazione delle definizioni di *Security Level* derivanti dallo standard per calibrarli in modo specifico in base alle minacce e alle necessità proprie del settore Difesa. Ad esempio, potrebbe rivelarsi necessaria l'introduzione di processi valutativi supplementari o criteri di assegnazione per ciascun SL, che considerino le operazioni erogate o supportate – anche marginalmente – da determinati IACS, nonché la gestione di informazioni sensibili o classificate e le minacce emerse da entità ostili, inclusi potenziali scenari di conflitto armato.

Validazione e aggiornamento continuo

Validazione programmata delle valutazioni del rischio condotte attraverso esercitazioni e simulazioni, per assicurare che esse siano realistiche e rappresentino le minacce attuali; costante aggiornamento delle valutazioni del rischio al fine di riflettere l'evoluzione delle minacce e delle tecnologie.

Implementazione di contromisure specifiche

Implementazione di contromisure di sicurezza specifiche che siano in linea con il livello di sicurezza target identificato, partendo dalla *baseline* di "controlli" e requisiti di sicurezza definiti per ciascun *Security Level* dallo standard ANSI/ISA-62443; sorveglianza continua dell'efficacia

5. e.g. CVSS v4.0, Metrica "Recovery": describes the resilience of a system to recover services, in terms of performance and availability, after an attack has been performed.

6. e.g. CVSS v4.0, Metrica "Value Density": describes the resources that the attacker will gain control over with a single exploitation event. It has two possible values, diffuse and concentrated.

delle misure di sicurezza per garantire aggiustamenti tempestivi in relazione a minacce o vulnerabilità di recente scoperta.

Collaborazione e condivisione

Lavoro sinergico con entità, organizzazioni militari e istituti di ricerca specializzati in *Operational Technology* per lo scambio di *expertise* e approcci ottimali. Questo interscambio di esperienze è fondamentale per affinare le tattiche di protezione e personalizzare i livelli di sicurezza (SL) in modo più efficace.

Cyber Threat Intelligence

La *Cyber Threat Intelligence* (ambito intenzionalmente ampliato rispetto ai precedenti) permette l'analisi approfondita delle minacce emergenti e delle vulnerabilità sistemiche, fornendo dati critici per la valutazione del rischio e l'adozione di misure di sicurezza adeguate, attraverso processi di identificazione e classificazione sistematica; può pertanto contribuire significativamente alla determinazione dei *Security Level Targets* (SL-T) necessari per la protezione delle risorse strategiche. Si richiama infatti l'attenzione del lettore su come l'efficienza nell'uso delle risorse risulti imprescindibile in tale ambito, dove il capitale – sia umano che tecnologico – deve essere impiegato in maniera ottimale: ottimizzazione delle risorse che passa attraverso una gestione strategica basata su informazioni affidabili, permettendo di allocare l'investimento delle capacità difensive in modo proporzionato al grado di rischio rilevato. La capacità di identificare con precisione le minacce più rilevanti consente di allocare le risorse in maniera oculata, concentrando gli investimenti sulle aree di maggiore rischio e importanza. Questo approccio mirato non solo massimizza l'efficacia delle misure protettive implementate ma riduce anche l'inefficienza derivante dall'utilizzo eccessivo o mal diretto di risorse (tempo, manodopera, budget, attrezzature, etc.) per affrontare minacce di minore entità o improbabili (fenomeno noto come *"overprovisioning"*).

Mirko Caruso, *Esperto in sicurezza delle informazioni e conformità delle infrastrutture critiche*

TABELLA RIEPILOGATIVA

Fase	Descrizione
Identificazione delle minacce e vulnerabilità	Conduzione di un'analisi approfondita per individuare minacce specifiche e valutare le vulnerabilità del sistema.
Valutazione del rischio	Adozione di una metodologia specifica considerando minacce, vulnerabilità, *likelihood*, impatto potenziale e parametri critici.
Definizione delle metriche di sicurezza	Sviluppo di metriche specifiche per valutare la sicurezza delle infrastrutture militari, considerando vari aspetti.
Coinvolgimento delle parti interessate	Definizione del coinvolgimento e dell'autorità di tutte le parti interessate, comprese organizzazioni ed enti esterni.
Adattamento alle dottrine militari	Incorporazione delle dottrine e normative militari nelle analisi di rischio, tenendo conto di esigenze specifiche.
Personalizzazione dei *Security Level*	Rielaborazione delle definizioni di SL per adattarle alle minacce e alle necessità uniche del settore Difesa.
Validazione e aggiornamento continuo	Esercitazioni programmate e aggiornamenti costanti per garantire la realismo delle valutazioni e tener conto dell'evoluzione delle minacce.
Implementazione di contromisure specifiche	Applicazione di misure di sicurezza mirate, partendo dai controlli definiti per ciascun *Security Level*.
Collaborazione e condivisione	Lavoro sinergico con entità specializzate in *Operational Technology* per scambio di *expertise* e approcci ottimali.
Cyber Threat Intelligence	Utilizzo della CTI per analizzare le minacce emergenti e fornire dati critici per la valutazione del rischio e la definizione dei *Security Level Targets*.

BIOGRAFIA

Mirko Caruso

Security Governance Engineer presso la società pubblica PagoPA S.p.A., Docente ospite presso i Dipartimenti di Matematica e Informatica e di Ingegneria Elettrica, Elettronica e Informatica dell'Università di Catania, Ufficiale della R.S. delle FF.AA.

Background nella gestione della sicurezza delle informazioni e nella conformità delle infrastrutture critiche, Security Assessor PCI-DSS, membro e collaboratore della OWASP® Foundation. Ricercatore indipendente presso il Berkman Klein Center di Harvard per il progetto Lumen. Contributor del Domain-based Message Authentication, Reporting and Conformance.

ISACA CISSP e Cisco Certified Network Security Professional.

Nelle Hall of Fame del Gruppo TIM e di American Express per la responsible disclosure di vulnerabilità critiche.

Si è recentemente occupato della progettazione e implementazione di un framework per la gestione del rischio OT (Operational Technology) conforme allo standard ISA 62443 per un Ente afferente il Ministero della Difesa.

FORUM ICT SECURITY

23-24 OTTOBRE 2024

AUDITORIUM DELLA TECNICA, ROMA

Iscriviti alla newsletter di ICT Security Magazine
per conoscere l'agenda e partecipare alla
22ª Edizione del Forum ICT Security

White Paper

RANSOMWARE
Innovazione e redditività del cyber-crime

Download gratuito su www.ictsecuritymagazine.com

CYBER CRIME CONFERENCE

17-18 APRILE 2024

AUDITORIUM DELLA TECNICA, ROMA

Iscriviti alla newsletter di ICT Security Magazine
per conoscere l'agenda e partecipare alla
12ª Edizione della Cyber Crime Conference