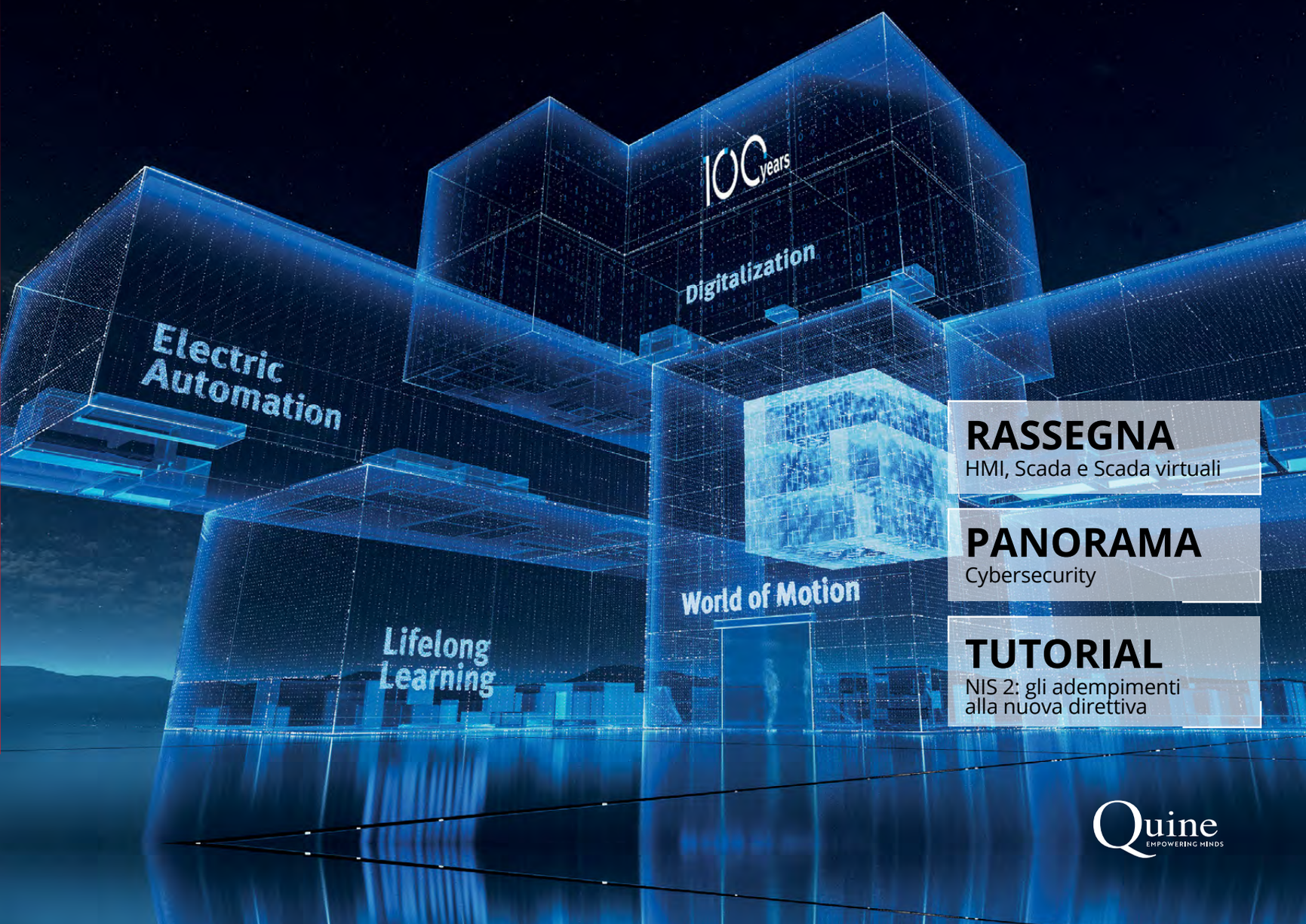
AUTOMAZIONE OGGI AO

461
APRILE
2025 ANNO 42

# SPECIALE
## IT e OT: come unire il gap

FESTO




**RASSEGNA**
HMI, Scada e Scada virtuali

**PANORAMA**
Cybersecurity

**TUTORIAL**
NIS 2: gli adempimenti alla nuova direttiva

Quine
EMPOWERING MINDS

Matteo Marino

# Strategie di cybersecurity nell'automazione industriale

**La cybersecurity è un tema cruciale, non soltanto per garantire il funzionamento efficiente delle attività industriali, ma soprattutto per la sicurezza fisica delle persone, la tutela dell'ambiente e la salvaguardia economica e sociale delle imprese e delle comunità**

Le minacce informatiche rivolte ai sistemi di automazione e controllo industriale (ICS/OT) possono generare danni significativi, superando spesso quelli tipici della cybersecurity tradizionale applicata al mondo IT. Un singolo attacco può compromettere intere catene produttive, mettere a repentaglio la sicurezza delle persone, causare incidenti ambientali o generare enormi perdite economiche. Consapevoli di questa sfida, abbiamo proposto ai nostri esperti sul tema alcune domande per avere da parte loro una visione più chiara, generando così un'auspicabile maggior consapevolezza in ambito.

Il primo quesito riguarda le principali sfide che si incontrano nell'implementare misure di cybersecurity negli ambienti industriali, con l'obiettivo di capire le difficoltà pratiche, come le limitazioni dei dispositivi legacy o la resistenza al cambiamento.

**Alex Galimi**, technical partner manager di **Trend Micro Italia** (*www.trendmicro.com/it*) risponde dicendoci che l'implementazione di misure di sicurezza negli ambienti industriali è caratterizzata da una serie di sfide, molte delle quali derivano dalla connotazione particolare dei dispositivi oggetto della protezione, dalla resistenza al cambiamento dovuta alle priorità operative e dalla difficoltà di integrare tecnologie moderne in ambienti operativi esistenti. I dispositivi legacy, infatti, spesso non sono progettati per integrarsi nativamente con sistemi di protezione, rendendoli degli asset ad alto rischio proprio per il valore che possiedono all'interno delle organizzazioni. Questi dispositivi non solo mancano di patch di sicurezza aggiornate, ma spesso non consentono l'applicazione di un processo di aggiornamento continuo e regolare: per questo motivo la loro protezione va gestita in maniera differente rispetto al tradizionale dispositivo IT. La resistenza al cambiamento è un altro ostacolo significativo, poiché molte organizzazioni sono riluttanti ad aggiornare o sostituire infrastrutture che sono state operative per anni, per paura di interrompere la produzione o di incorrere in costi elevati. Inoltre, gli ambienti industriali sono ancora spesso separati dalle reti IT aziendali, il che complica ulteriormente la protezione contro le minacce informatiche. Le soluzioni di cybersecurity devono quindi affrontare la difficoltà di proteggere reti particolarmente delicate e spesso isolate, senza compromettere l'affidabilità e la continuità delle operazioni, impresa che si rivela complessa per le tecnologie progettate esclusivamente per ambienti IT.

Secondo **Rüdiger Kügler**, vp professional services di **Wibu-Systems** (*www.wibu.com/it*), oggi molti operatori di impianti e macchinari non sono pienamente consapevoli della necessità di aggiornare regolarmente i loro sistemi. In ambito industriale è ancora comune trovare computer che operano su sistemi operativi obsoleti come Windows 7 o persino Windows XP. "Un caso emblematico è emerso all'inizio del 2024, quando un fornitore della Deutsche Bahn (ferrovie nazionali tedesche) ha pubblicato un'offerta di lavoro che richiedeva competenze su Windows 3.11 per Workgroups, un sistema operativo rilasciato più di 30 anni fa. Questa situazione impone ai fornitori di soluzioni di cybersecurity

Le soluzioni di cybersecurity devono affrontare la difficoltà di proteggere reti particolarmente delicate e spesso isolate

la necessità di supportare ambienti ormai non più sostenuti ufficialmente dai produttori. Ciò comporta il mantenimento di versioni software dedicate, basate su strumenti di sviluppo datati, rendendo difficile qualsiasi aggiornamento del codice e aumentando significativamente i costi operativi".

Concorde anche **Giorgio Triolo**, chief technology officer di **Axitea** (*www.axitea.com/it*): "i sistemi di tecnologia operativa (OT) sono spesso progettati dando priorità a efficienza e affidabilità, trascurando di fatto l'aspetto della sicurezza. Molte apparecchiature industriali utilizzano sistemi operativi e software datati, spesso non aggiornati o non più supportati, cosa che li rende vulnerabili a minacce note. Inoltre, i sistemi IT e OT utilizzano spesso protocolli e standard diversi, e questo complica ulteriormente la loro interconnessione e l'implementazione di una strategia di sicurezza a tutto tondo. Infine, la crescente diffusione dell'IoT, con il conseguente incremento delle necessità di connettività, ha messo a disposizione degli attaccanti nuove potenziali vie di accesso. A queste sfide si aggiunge la difficoltà di bilanciare la sicurezza con la necessità di mantenere la continuità operativa e l'efficienza dei processi industriali".

Per **Nozomi Networks** (*https://it.nozominetworks.com*) risponde **Davide Ricci**, regional sales director Italy, dicendo che ci sono tre sfide principali nella sicurezza informatica degli ambienti industriali: la mancanza di visibilità, i downtime non pianificati e l'obsolescenza delle apparecchiature. Sul primo tema la presenza di 'punti ciechi' nei dispositivi IoT e OT e il limitato accesso ai dati operativi in tempo reale ostacolano la resilienza e la gestione dei rischi. Senza una visione completa degli asset, in particolare dei dispositivi IoT e OT, negli ambienti indu-

Alex Galimi, technical partner manager di Trend Micro Italia

striali, diventa difficile valutare e mitigare le minacce. In secondo luogo, oltre agli attacchi informatici, anche errori di configurazione, procedure non conformi o picchi di utilizzo possono causare interruzioni, con impatti diretti sulla produzione e sulla redditività. E infine concorda sull'obsolescenza delle apparecchiature.

**Cristina Mariano**, country manager di **Advens** (*www.advens.fr/it*) sottolinea il fatto che le sfide che ci troviamo ad affrontare sono innanzitutto tecnologiche, legate alle necessità specifiche del mondo della produzione, in cui disponibilità e affidabilità dei sistemi sono la priorità e i fermi di produzione molto costosi. Gli impianti produttivi, progettati per durare anche diversi anni, spesso oltre i 15, non erano stati pensati per essere connessi. Per questo spesso presentano vulnerabilità che possono essere sfruttate dai cybercriminali e che rappresentano un rischio notevole per gli stessi asset industriali, ma anche per l'uomo e per l'ambiente, vista la loro stretta interazione con il mondo fisico.

Secondo **Mario Testino**, chief operating officer di **ServiTecno** (*www.servitecno.it*), la necessità di proteggere reti e sistemi di controllo nell'industria e nelle utility è ormai entrata tra i requisiti dei nuovi progetti di automazione. Il tallone d'Achille spesso sono impianti e reti esistenti che richiedono connessioni con i sistemi a livello superiore o da integrare con i nuovi sistemi in arrivo. "Ne consegue che in nuovi progetti si trovano i soldi per la cybersecurity, mentre spesso è difficile trovare oggi giustificativi all'investimento per la 'remediation' di sistemi esistenti, vecchi ma ancora in produzione ed efficienti, cresciuti nel tempo, ove il concetto di cybersecurity non era contemplato. Forse ora con gli obblighi imposti dalle normative, NIS2 oggi e a breve con i dettami del nuovo Regolamento Macchine, sarà più semplice ottenere il commitment da parte del management e la collaborazione da parte dei responsabili di produzione, manutenzione e ingegneria impianti".

Rüdiger Kügler,
vp professional services di Wibu-Systems

## Consapevolezza del rischio

Non meno importanti sono le sfide umane e organizzative: è necessario acquisire la consapevolezza che il rischio cyber abbia la stessa rilevanza, se non superiore, di un guasto meccanico o di un'anomalia di processo. In altre parole, dobbiamo accettare di cambiare i metodi di lavoro e integrare la cybersecurity nel cuore delle operazioni industriali. In secondo luogo, abbiamo voluto approfondire come la convergenza tra IT e OT abbia influenzato la strategia aziendale in temi di sicurezza informatica. Questo approfondimento ha lo scopo di esplorare come sono gestiti i rischi derivanti dalla connessione delle reti operative ai sistemi IT aziendali.

**Galimi** continua confermando che la convergenza tra IT e OT ha comportato una serie di cambiamenti significativi nella strategia di sicurezza informatica delle aziende. In passato, le reti IT e OT erano isolate, con misure di sicurezza separate per ciascun ambito, e in numerosi casi l'ambito OT veniva trascurato in termini di protezione proprio per il concetto che un ambiente isolato poteva essere protetto a prescindere. "Tuttavia, sappiamo che non è così: con l'aumento della digitalizzazione e la crescente interconnessione tra i sistemi, la sicurezza informatica deve ora coprire un perimetro molto più ampio, integrando reti aziendali e industriali. Questa convergenza ha comportato la necessità di adottare soluzioni di sicurezza che possano monitorare e proteggere sia i dispositivi IT sia quelli OT in tempo reale, di fatto consentendo di migliorare le capacità di rilevare attacchi mirati e trasversali sulle reti". Questo è possibile grazie all'unione di tecnologie come l'analisi del comportamento, l'AI e la protezione contro lo sfruttamento delle vulnerabilità.

Giorgio Triolo,
chief technology officer di Axitea

**Kügler** è convinto che la convergenza tra IT e OT sta lentamente aumentando la consapevolezza dell'importanza degli aggiornamenti di sicurezza. "Se in passato le reti di produzione erano completamente isolate, oggi, con l'avvento dell'Industria 4.0, assistiamo a una prima e prudente integrazione tra questi due mondi. La connessione viene spesso realizzata attraverso gateway dedicati, consentendo la separazione delle reti quando necessario. Questo approccio mitiga i rischi derivanti dalla connessione diretta tra le infrastrutture IT e OT, riducendo le potenziali superfici d'attacco".

**Triolo** conferma che la convergenza tra IT e OT ha radicalmente trasformato l'approccio alla sicurezza dei clienti che operano in ambito industriale e manifatturiero. "In quanto Global Security Provider, abbiamo il compito di guidarli facendo leva su una strategia unificata e integrata". Un lavoro che guida le imprese produttive verso una visione olistica del rischio che deve considerare l'intera infrastruttura come un unico ecosistema interconnesso, investendo in soluzioni di sicurezza integrate che possano monitorare e proteggere sia i sistemi IT che OT, e fornendo una visibilità completa sulla postura di sicurezza. "Una visione olistica di questo tipo richiede un adeguamento organizzativo e una revisione delle procedure di sicurezza".

**Ricci** afferma che la convergenza tra IT e OT ha esteso in modo significativo la superficie

Senza una visione completa degli asset, in particolare dei dispositivi IoT e OT, negli ambienti industriali, diventa difficile valutare e mitigare le minacce

di attacco. "Oggi assistiamo a un'integrazione sempre più forte tra OT e IT, con un ulteriore elemento aggiuntivo introdotto dai dispositivi IoT. La loro crescente diffusione ha reso più facile il controllo e il monitoraggio dei sistemi da remoto, migliorando l'accessibilità e l'efficienza, ma ha introdotto una nuova serie di criticità e vulnerabilità che devono essere tenute in considerazione. La tradizionale separazione dei sistemi OT non è più una misura di sicurezza affidabile".

**Mariano** sottolinea come il mondo OT era storicamente isolato e non collegato a Internet. E così è stato fino alla trasformazione digitale del settore, nota anche come Industria 4.0, che mira a sviluppare nuovi servizi e a migliorare l'efficienza operativa. "Si tratta di un'evoluzione che richiede l'implementazione di nuove tecnologie all'interno delle fabbriche, la raccolta e l'analisi di una grande quantità di dati di produzione, e l'integrazione di tecnologie IT negli apparati OT che diventano comunicativi. In questo contesto, la cybersecurity ricopre un ruolo essenziale e deve essere integrata in qualunque nuovo progetto industriale, oltre che nei sistemi già esistenti, con un approccio globale volto a coprire tutti i rischi".

Per **Testino** è innegabile che il driver per la cybersecurity sia sempre stato innescato dal management e più specificamente da quello dell'IT, che risulta il più esposto dal punto di vista della visibilità interna ed esterna dell'azienda. E sostiene che "anche il budget era ed è concentrato nelle mani di chi gestisce i sistemi e l'infrastruttura IT dell'azienda. Il fatto che siano sempre più connessi IT e OT ha fatto nascere l'esigenza di guardare anche alla rete di stabilimento, a cosa ci troviamo a dover connettere, e a quali dati scambiare tra sistemi IT ed OT. Nel momento in cui emergono le differenze specifiche tra reti e sistemi IT e OT, ne consegue che sono da trattare in modo differente rischi derivanti da diverse vulnerabilità e minacce. Mentre spesso metodologie e procedure di gestione dei rischi posso essere trasversali tra IT e OT, le tecnologie da utilizzare per la protezione di reti e sistemi IT e OT sono inevitabilmente differenti".

## Come proteggere i dispositivi industriali

Abbiamo chiesto successivamente quali approcci sono utilizzati per proteggere i dispositivi industriali come PLC, Scada e sensori da attacchi informatici. Ottenere insight su misure tecniche specifiche, come l'uso di firewall industriali, segmentazione della rete e autenticazione multifattoriale è di fondamentale importanza.

**Galimi** afferma che la protezione dei dispositivi industriali, come PLC, Scada e sensori, richiede un approccio altamente specializzato che va oltre la sicurezza informatica tradizionale. "In primo luogo, dobbiamo tenere in considerazione che questi asset sono essenziali per la corretta operatività aziendale. Inoltre, sono dispositivi che nella maggior parte dei casi non possono fruire di una protezione tradizionale basata su agenti software. Diventa quindi fondamentale implementare firewall industriali e soluzioni di segmentazione delle reti per separare i sistemi di controllo, riducendo così la superficie di attacco e filtrando le comunicazioni indesiderate. Inoltre, applichiamo l'intelligenza sulla protezione dalle vulnerabilità con funzionalità di virtual patching, funzionalità fondamentale per il contrasto alle intrusioni illecite, e soluzioni di sicurezza basate su hardware trasparente, che integra l'analisi delle minacce specifiche per l'industria, per proteggere i dispositivi da vulnerabilità conosciute e da minacce avanzate, garantendo la continuità con appositi filtri di bypass fisico".

**Kügler** è certo che Wibu-Systems si distingue per un approccio focalizzato sulla protezione e la licenza del software, piuttosto che sulla sicurezza della rete. "Le nostre soluzioni garantiscono la sicurezza delle applicazioni eseguite su dispositivi industriali come PLC e Scada, proteggendole dal reverse engineering, da modifiche non autorizzate e dall'uso senza una licenza valida. Questo rende più complesso per un attaccante analizzare il software in laboratorio e individuare vulnerabilità sfruttabili" soprattutto se si utilizzano ancore crittografiche, hardware e software.

**Triolo** conferma che per proteggere i dispositivi industriali "adottiamo un approccio multistrato che parte dalla gestione delle vulnerabilità dei sistemi OT, identificando il rischio di un attacco e prevedendo sistemi di monitoraggio continuo per rilevare attività sospette e rispondere rapidamente agli incidenti. Una volta implementati questi sistemi, è necessario poi identificare le corrette procedure di accesso, limitandolo al solo personale autorizzato, e provvedere all'aggiornamento regolare dei sistemi OT con le patch di sicurezza più recenti". Certo poi si devono implementare anche misure di sicurezza avanzate, come la segmentazione della rete, l'autenticazione multifattore, e soluzioni di rilevamento delle intrusioni specifiche per l'OT.


La protezione dei dispositivi industriali, come PLC, Scada e sensori, richiede un approccio altamente specializzato che va oltre la sicurezza informatica tradizionale

Secondo **Ricci** sono diversi gli aspetti fondamentali da considerare per proteggere in modo adeguato i dispositivi industriali. "L'inventario completo degli asset è essenziale, così come identificare tutti i dispositivi, firmware, configurazioni hardware, vulnerabilità e criticità operative per avere una base solida di sicurezza. È essenziale il rafforzamento del sistema attraverso misure specifiche, come corretta gestione della configurazione, realizzazione di architetture di rete sicure e adozione di protocolli sicuri. Rilevante anche il monitoraggio delle minacce e il rilevamento delle anomalie in tempo reale per una risposta immediata, oltre all'implementazione di un playbook di risposta agli incidenti e di un Deep Packet Inspection (DPI)".

"Come sempre in tema di sicurezza, dobbiamo partire dai rischi, integrando le attività critiche dell'organizzazione e tenendo conto delle vulnerabilità e delle caratteristiche tecnologiche dei dispositivi da proteggere. In generale, il nostro approccio si basa su una combinazione tra prevenzione e rilevamento/risposta, in cui vengono incorporate soluzioni di sicurezza dedicate agli ambienti OT, come ad esempio le sonde di sicurezza di rete" ha affermato **Mariano**.

"Come ServiTecno, abbiamo iniziato a parlare di microsegmentazione e segregazione di asset sulle reti di fabbrica oltre 20 anni fa" sottolinea **Testino** "quanto lo standard ISA99 era ancora in evoluzione e non era ancora pubblicato nei diversi capitoli della norma IEC62443. Oggi si parla anche di Zero-Trust per il mondo OT, spesso poco praticabile proprio per vincoli dovuti a componenti e dispositivi datati presenti sulle reti di fabbrica. Un buon disegno dell'infrastruttura della rete di fabbrica è propedeutico, e quindi una revisione critica è necessaria prima di procedere a mettere sonde, firewall e diodi in giro: spesso il ridisegno rende necessaria la sostituzione di switch e poi lo studio di regole e connessioni che rendano equilibrati e congrui i livelli di security richiesti dalle isole di automazione, per proteggere adeguatamente sensori in rete, PLC, PC, Scada, server Historian e MES. Non dimentichiamo il crescente utilizzo anche in fabbrica di applicazioni in cloud che costringono a un ridisegno dell'infrastruttura, con utilizzo di egde e firewall, con regole specifiche per le connessioni verso il web. Proprio per queste connessioni utilizziamo tecnologie specifiche di tunelling e data-HUB, per consentire trasmissioni di dati su 'canali protetti' per favorire l'integrazione IT/OT sicura".

## Continuità operativa

Inoltre, abbiamo domandato quali best practice si possono consigliare per garantire la continuità operativa in caso di attacco informatico facendo emergere soluzioni di disaster recovery, piani di backup e procedure per il ripristino rapido.

**Galimi:** "garantire la continuità operativa in caso di attacco informatico richiede una solida preparazione e un piano di risposta ben definito. Le best practice più comuni includono l'adozione di strategie di backup e la creazione di piani di disaster recovery che consentano un rapido ripristino delle operazioni. Oltre a questo, è fondamentale implementare soluzioni di monitoraggio continuo e analisi delle minacce, per rilevare tempestivamente gli attacchi, permettere agli analisti di contenere velocemente un eventuale intrusione e rispondere in modo rapido ed efficace. La segmentazione delle reti è un altro elemento cruciale per limitare la diffusione di attacchi all'interno dell'infrastruttura industriale. Infine, è essenziale predisporre tecnologie che garantiscano continuità operativa anche in caso di incidente, grazie all'implementazione di interfacce di comunicazioni dotate di filtri bypass altamente affidabili".

Quando si parla di best practice **Kügler** conferma che la prevenzione degli attacchi informatici è ovviamente la priorità, ma disporre di un piano d'emergenza dettagliato è essenziale per gestire al meglio una possibile compromissione. In situazioni di crisi, seguire una procedura ben strutturata è fondamentale per minimizzare l'impatto operativo. "Le

Davide Ricci,
regional sales director Italy di Nozomi Networks

strategie possono variare dalla ridondanza dei sistemi alla creazione di piani di backup e ripristino affidabili. Un elemento cruciale è la figura del responsabile della gestione dell'emergenza, il quale deve garantire un coordinamento efficace, mantenendo la calma, impartendo istruzioni chiare e supervisionando l'intero processo. La comunicazione tempestiva ed efficace, spesso trascurata, rappresenta un fattore determinante per il successo delle operazioni di ripristino".

Una best practice che consiglia **Triolo** è "la creazione e la manutenzione di un Incident Response Plan dettagliato, che definisca ruoli, responsabilità e procedure da seguire in caso di incidente. Inoltre, è essenziale il monitoraggio continuo dei sistemi per rilevare e rispondere tempestivamente a potenziali minacce, abbinato a una gestione proattiva delle vulnerabilità. Avvalersi di un Managed Security Service Provider che offra servizi di IoT & OT Security può aiutare a implementare le misure e le pratiche migliori per le esigenze di ciascuna azienda. Infine, per garantire la continuità operativa in caso di attacco informatico è fondamentale stabilire procedure di backup e recovery, in modo da poter di ripristinare rapidamente i sistemi e i dati compromessi, minimizzando i tempi di inattività e le perdite economiche".

Anche secondo **Ricci** è sempre una buona idea rivedere annualmente il piano di continuità aziendale, verificando che, in caso di attacco informatico andato a buon fine, siano stati predisposti adeguati schemi di backup e politiche di ripristino. "Inoltre, raccomandiamo vivamente la definizione di playbook di risposta agli incidenti, che includono intrinsecamente elementi di business continuity e disaster recovery. Anche l'attenzione a una risposta rapida e al ripristino presuppone che i piani di backup siano componenti fondamentali di una strategia completa".

**Mariano** afferma che "è necessario prepararsi e non pensare che gli attacchi accadano solo agli altri. È necessario condurre regolarmente esercitazioni di crisi, con scenari personalizzati sul proprio specifico settore". L'importante è seguire le procedure di gestione della crisi precedentemente definite: identificare l'origine del problema, isolare le apparecchiature compromesse, definire le modalità degradate. "Nel caso del cyber, è necessario comprendere le specificità di una crisi. Il movente malevolo non è sempre il primo fattore di incidente che viene in mente, perché siamo più abituati a gestire guasti e malfunzionamenti. E nel caso dell'OT, alcune risposte classiche del mondo IT non funzionano esattamente allo stesso modo. Un esempio è quello del backup: quante aziende hanno un backup di tutti i programmi PLC? Hanno le competenze per implementarli se i PLC sono stati danneggiati? L'età degli apparati e la loro specificità possono rendere questa fase particolarmente complessa e dispendiosa in termini di tempo".

Anche secondo **Testino,** per affrontare le sfide della continuità operativa in infrastrutture critiche, è cruciale adottare tecnologie avanzate per il backup non solo dei dati, ma anche degli applicativi di processo. "Questo significa implementare soluzioni che consentano di eseguire snapshot istantanei dei sistemi critici, garantendo la ripartenza rapida dei processi essenziali in caso di interruzione. Tecnologie come la virtualizzazione del sistema, che permettono di creare e ripristinare ambienti di lavoro virtuali in pochi minuti, sono particolarmente efficaci in questo contesto. Inoltre, strumenti di gestione del parco installato e monitoraggio delle variazioni possono rivelarsi cruciali. Tali strumenti aiutano a tenere traccia delle configurazioni e delle modifiche e a identificare e risolvere anomalie o potenziali violazioni prima che possano compromettere la sicurezza o la continuità operativa. Rispondere alle direttive di NIS2 richiede un approccio integrato che comprenda la protezione dell'intera supply chain, compresi macchinari e impianti industriali, per garantire la resilienza e la sicurezza delle operazioni anche in scenari critici e regolamentati".

## Limitare i rischi

I temi riguardanti il personale ricoprono un'importanza cruciale per limitare i rischi cyber, e per questo abbiamo chiesto in che misura le aziende coinvolgono il personale operativo nella strategia di cybersecurity e quale tipo di formazione sia necessaria. Approfondire, infatti, come è promossa la cultura della sicurezza tra gli operatori di impianti e tecnici fornisce la misura della prontezza nei confronti di questo tema così importante.

Secondo **Galimi** "Il coinvolgimento del personale operativo è fondamentale per una strategia di cybersecurity efficace, poiché spesso sono gli operatori a interagire direttamente con i dispositivi e i sistemi vulnerabili. La formazione deve essere continua e incentrata su scenari reali, come la gestione delle minacce informatiche in ambito industriale. Inoltre, è importante educare il personale sull'importanza delle pratiche quotidiane, come l'autenticazione sicura, il controllo degli accessi, l'utilizzo di dispositivi rimovibili e il riconoscimento dei segnali di attacchi informatici. La formazione deve essere mirata a creare una mentalità di 'security by design' tra gli operatori, affinché diventino un alleato degli analisti contro gli attacchi".

**Triolo** conferma che una strategia di cybersecurity efficace non può prescindere dal coinvolgimento del personale operativo. "È fondamentale formare lo staff sui rischi informatici e sulle best practice di sicurezza OT, nonché sulle tecniche di riconoscimento delle minacce anche attraverso test pratici che permettano di verificare e migliorare la capacità del personale di riconoscere e rispondere alle minacce. La formazione deve considerare anche la consapevolezza delle conseguenze di un attacco, come l'interruzione delle attività produttive, i danni alla reputazione e i rischi per l'incolumità fisica. Questo permette di creare una cultura della sicurezza diffusa, in cui tutti sono consapevoli dei rischi e sanno come comportarsi per prevenirli e mitigarli".

**Ricci** sottolinea che esiste ancora un divario di competenze tra i professionisti della sicu-

rezza informatica e le sfide specifiche degli ambienti OT che deve essere colmato: "con l'escalation e la proliferazione degli attacchi, l'attuale divario nelle conoscenze tecniche del personale addetto alla sicurezza informatica si sta ampliando e mette le organizzazioni in una posizione precaria nella lotta contro le minacce e gli attacchi. La formazione del personale addetto alla sicurezza informatica sui sistemi e sulle sfide specifiche dell'OT è fondamentale".

Secondo **Mariano** bisogna agire su due fronti: sensibilizzazione e definizione della governance. "Per la sensibilizzazione, sono necessari approcci educativi e dinamici, adattati alla quotidianità dei team che operano nelle fabbriche e nelle entità industriali. Per la definizione della governance, è fondamentale stabilire referenti e responsabili della cybersecurity all'interno delle squadre operative. Il tema della sicurezza è trasversale e non può essere gestito esclusivamente dai team IT".

Per **Testino,** il coinvolgimento attivo del personale operativo nella strategia di cybersecurity è essenziale per promuovere una cultura della sicurezza robusta. "Investire nella formazione del personale e nell'adozione di tecnologie avanzate per il backup e il ripristino rapido sono pilastri fondamentali per garantire la continuità operativa e la sicurezza delle infrastrutture critiche in un contesto sempre più regolamentato e vulnerabile agli attacchi informatici".

## Qualche esperienza

Abbiamo poi chiesto di illustrare esperienze specifiche riguardanti attacchi informatici nell'ambito industriale e come siano state gestite, con l'obiettivo di favorire la condivisione di esperienze pratiche e lezioni apprese durante incidenti reali.

Trend Micro ha avuto esperienza diretta nella gestione di attacchi informatici in aziende industriali, tra cui ransomware e attacchi mirati alle reti OT. **Galimi** ci dice che in una situazione specifica, un attacco mirato a un impianto di produzione ha portato a un'interruzione delle operazioni, di fatto obbligando l'azienda all'interruzione delle attività. "In risposta, abbiamo supportato l'azienda cliente nell'attuazione di un piano di incident response che includeva il blocco immediato delle connessioni sospette, l'isolamento delle macchine infette e il ripristino dei sistemi. In quel caso si è rivelata fondamentale la presenza di un SOC attivo in modalità 24x7 che ha permesso di rilevare la minaccia immediatamente e far partire lo stato di allerta. La sfida maggiore da affrontare è stata quindi quella di bloccare i flussi di comunicazione malevoli garantendo la ripresa operativa veloce e sicura. La lezione appresa è stata che una preparazione adeguata, combinata a un'ottima conoscenza della propria rete e flussi di comunicazione da parte del cliente, può ridurre significativamente il rischio di danni maggiori".

Cristina Mariano,
country manager di Advens

**Triolo** racconta che, nonostante il progressivo impegno delle aziende con ambienti OT nel creare ecosistemi resilienti dal punto di vista della cybersecurity, il coinvolgimento di strutture Security Operations Center (SOC) per la gestione di interruzioni operative rimane una necessità frequente. "Un caso esemplare è stato un attacco informatico, verificatosi nel 2024, in un'azienda del settore metallurgico. Nonostante l'implementazione di molteplici layer di sicurezza, sia l'ambiente produttivo OT sia l'infrastruttura amministrativa sono stati colpiti da un ransomware, causando un fermo produttivo di cinque giorni. L'incident response, condotta attraverso un approccio combinato di tecnologie e procedure, ha avuto come obiettivo primario l'identificazione della root cause, con un'analisi approfondita che ha incluso l'esame dettagliato dei log di infrastruttura, un assessment dell'Active Directory (AD), la revisione della segmentazione di rete e l'analisi delle vulnerabilità infrastrutturali e applicative in base agli standard più aggiornati. L'indagine ha evidenziato lo sfruttamento di una vulnerabilità a livello server, che era in comunicazione diretta con i sistemi di produzione, consentendo la criptazione dei dischi e il blocco di diverse macchine Scada e PLC. Un attacco che ha impattato in modo significativo anche asset legacy, compromettendo la stabilità operativa dell'impianto. Per mitigare i rischi futuri, è stato necessario un ridisegno dell'infrastruttura di rete, focalizzandosi sul monitoraggio dei flussi di comunicazione OT, la valutazione della superficie di attacco esposta, l'implementazione di misure di hardening e remediation per ridurre il rischio e sanare le vulnerabilità individuate. Grazie a queste misure, l'azienda ha potuto ripristinare la piena operatività, rafforzando al contempo la propria cyber resilience per prevenire attacchi futuri".

Secondo **Mariano**, Advens dispone di un team di risposta agli incidenti (Csirt) all'interno del suo Cert, che si è trovato a gestire diversi attacchi in ambienti OT per i loro clienti. "Ad esempio, abbiamo implementato servizi di rilevamento degli incidenti (SOC) per infrastrutture industriali all'interno degli stadi di Parigi durante le Olimpiadi del

2024. I nostri team sono composti da professionisti esperti in grado di aiutare i clienti ad affrontare gli attacchi e a gestire le crisi, sia dal punto di vista tecnico che organizzativo. L'aspetto più importante è integrare il personale operativo nel sistema di gestione delle crisi. La qualificazione di un incidente in un ambiente industriale richiede una conoscenza approfondita di questi ambienti, dei suoi potenziali impatti e delle soluzioni disponibili per affrontarlo, tra riavvio, piano di backup, dispositivi sostitutivi ecc. Questo aspetto è cruciale per ridurre i tempi di elaborazione e quindi accelerare il ritorno alla normalità".

"Il maggior numero di incidenti industriali che abbiamo analizzato risultavano essere la diretta conseguenza di grandi di criticità nella postura di sicurezza informatica" sostiene **Testino**. "Tra le cause primarie la mancanza di segmentazione di rete e la diffusa obsolescenza dei sistemi operativi e degli apparati hardware. Ovviamente se la richiesta di supporto avviene quando il danno si è già verificato possiamo solo cercare di ripristinare i sistemi produttivi nel tempo minore possibile. Ben diversa è la situazione se le aziende ci chiedono attività di assessment e di progettazione per la messa in sicurezza dei sistemi produttivi. In questo caso si può attingere a una 'tavolozza' molto ampia di soluzioni, che possono andare dalla creazione di specifiche zone di sicurezza di livello elevato alla visibilità e notifica tempestiva degli eventi di sicurezza OT".

## Standard e normative

Anche l'approfondimento sugli standard e le normative è importante per comprendere come garantire la conformità in materia di sicurezza informatica negli impianti industriali. "Trend Micro aderisce a una serie di standard e normative internazionali per garantire la conformità e la sicurezza delle proprie tecnologie volte all'impiego in impianti industriali, tra cui ad esempio le direttive del Nist per la protezione delle infrastrutture critiche e gli standard ISO/IEC 27001 per la gestione della sicurezza delle informazioni. La compliance a queste normative ci consente di garantire che le soluzioni di sicurezza siano allineate con le migliori pratiche e con i requisiti legali specifici di ciascun mercato. Inoltre, collaboriamo con le organizzazioni governative e industriali per rimanere aggiornati sui cambiamenti normativi e per garantire che le nostre soluzioni siano sempre conformi alle leggi locali, che possono variare in base alla regione e al settore" conferma **Galimi.**

**Kügler** ci dice che essendo "fornitori di componenti software impiegati nei dispositivi e nei sistemi di controllo industriale, la conformità agli standard di sicurezza è per noi una priorità. Poiché le nostre soluzioni vengono utilizzate in molteplici settori, non possiamo aderire a tutti gli standard specifici di ogni industria. Tuttavia, abbiamo sviluppato un rigoroso standard interno per lo sviluppo di software sicuro, documentato nell'ambito delle certificazioni ISO 9001 e ISO 27001. Tra le pratiche adottate rientrano l'uso di guide per la codifica sicura, revisioni periodiche del codice, analisi automatizzata del codice sorgente e rigorosi controlli di accesso. Queste misure ci permettono di garantire un livello di sicurezza elevato nelle soluzioni che offriamo ai nostri clienti".

"Oltre agli standard e framework di riferimento generali per la cybersecurity, come ISO 27001 e Nist Cybersecurity Framework, seguiamo attentamente le evoluzioni normative specifiche per il settore industriale" afferma **Triolo**. "In particolare, stiamo supportando i nostri clienti nell'adeguamento al nuovo Regolamento Macchine (EU) 2023/1230, che introduce requisiti stringenti in materia di cybersecurity per le macchine industriali. Questo regolamento impone ai produttori di valutare e mitigare i rischi di cybersecurity fin dalla fase di progettazione delle macchine, garantendo che siano protette da manipolazioni dannose che potrebbero comprometterne la sicurezza. Il nostro

Mario Testino,
chief operating officer di ServiTecno

La crescente diffusione dell'IoT con il conseguente incremento delle necessità di connettività, ha messo a disposizione degli attaccanti nuove potenziali vie di accesso

La cybersecurity in ambito OT rappresenta un buon modo per sviluppare nuove competenze per gli operatori, le cui posizioni potrebbero evolvere con i progetti di automazione

approccio include la valutazione della conformità al Regolamento Macchine, l'implementazione di misure di sicurezza adeguate e la verifica periodica dell'efficacia di tali misure".

Secondo **Ricci** sono diversi i framework e gli standard comunemente utilizzati per la cybersecurity industriale, tra i quali spiccano Nist, IEC 62443 e ISO 27001. "Ad esempio, Nist supporta la gestione del rischio di cybersecurity fornendo un approccio strutturato all'identificazione, alla protezione, al rilevamento, alla risposta e al recupero dalle minacce informatiche. Chi vuole valutare la propria maturità informatica, può utilizzare standard consolidati come ARC Cybersecurity Maturity Model, che fa inoltre riferimento alla conformità alle normative come obiettivo strategico per le organizzazioni".

**Mariano** conferma che la cybersecurity e le attività industriali sono ambiti regolati da numerosi standard e normative. "Non ci manca nulla… e a volte ne abbiamo persino troppe. Uno degli standard di riferimento è l'IEC 62443, particolarmente adatta a questo contesto. Dal punto di vista regolatorio, la direttiva NIS2 avrà un impatto molto significativo, così come il Cyber Resilience Act e la Direttiva Macchine".

"I due pilastri sono sempre IEC 27001 per realizzare un sistema di gestione della cybersecurity adeguato (utile è anche il Nist SP 800-53 Rev.5) e IEC 62443, che permette di focalizzarsi sugli apparati e sistemi Iacs" sottolinea **Testino**.

## Quale futuro per la cybersecurity industriale?

Infine, abbiamo posto una domanda sull'evoluzione del panorama della cybersecurity industriale nei prossimi anni e quali nuove tecnologie o approcci diventeranno essenziali.

**Galimi** conferma infine che il panorama della cybersecurity industriale è destinato a evolversi rapidamente nei prossimi anni, con l'aumento delle minacce informatiche e la crescente digitalizzazione delle operazioni industriali. "Una delle tecnologie che diventerà sempre più essenziale è l'AI usata per la rilevazione delle minacce e i gemelli digitali per monitorare e simulare attacchi. Inoltre, con l'adozione crescente dell'IoT industriale, l'implementazione di soluzioni di sicurezza integrate diventerà sempre più critica. Le aziende dovranno adottare un approccio proattivo, investendo in tecnologie di sicurezza avanzate e in formazione continua, per contrastare le minacce sempre più sofisticate e salvaguardare gli asset più a valore nelle aziende".

Secondo **Kügler** "nell'ambito della protezione e licenza del software industriale, prevediamo un ruolo sempre più centrale della sicurezza applicativa all'interno della strategia di cybersecurity globale. Osserviamo inoltre una crescente attenzione da parte dei produttori di dispositivi industriali e dei loro fornitori nei confronti della sicurezza del software. Questo trend suggerisce che, nei prossimi anni, la protezione delle applicazioni e dei dati diventerà un pilastro fondamentale della sicurezza industriale, complementando le misure di difesa tradizionali come firewall e segmentazione delle reti".

**Triolo** prevede che "il futuro della cybersecurity industriale richiederà un approccio sempre più proattivo e basato sull'intelligence. Non ci si dovrà limitare solo a proteggere i sistemi esistenti, ma anche anticipare le nuove minacce e adattare le difese. Questo richiederà una maggiore attenzione al monitoraggio continuo del traffico, all'analisi dei dati basato su AI e alla condivisione delle informazioni sulle minacce interne ed esterne con un response efficace che deve essere attivo h24x365".

**Ricci** conferma che c'è una crescente adozione di tecnologie avanzate. "Con la continua evoluzione del settore, l'offerta di prodotti dedicati è diventata più ricca e completa, includendo tecnologie avanzate come l'AI, il machine learning, il rilevamento delle anomalie e le soluzioni basate sul cloud, che diventeranno sempre più centrali nei prossimi anni".

Anche secondo **Mariano** "è necessario concentrarci sulle minacce. È fondamentale comprendere le modalità operative degli aggressori. Nel contesto OT, possiamo prevedere che l'AI generativa renderà più facile la creazione di exploit o programmi malevoli rivolti a PLC o ICS. Inoltre, gli aggressori stanno prendendo sempre più di mira il mondo industriale, in particolare i settori alimentare e manifatturiero, perché si tratta di obiettivi che, in caso di attacco, sono più disposti a pagare per ridurre tempi di inattività e perdite di fatturato. Quindi possiamo pensare che le minacce in questo campo siano destinate ad aumentare. Dal lato della difesa, le aziende struttureranno meglio i loro dipartimenti di cybersecurity OT e i SOC OT saranno sempre più diffusi (separatamente o all'interno del tradizionale SOC IT). E i grandi vendor della cybersecurity offriranno soluzioni software e hardware sempre più adatte ai vari ambienti OT da proteggere".

Secondo **Testino** "l'AI, intesa come machine learning, è già molto presente per la diagnostica delle anomalie di sicurezza e si iniziano a utilizzare i LLM (Large Language Model) per l'interrogazione intelligente dei sistemi. Ma la vera sfida futura nel mondo dell'Automazione sarà la qualità del software, la certificazione e il miglioramento (leggi riduzione) del ciclo di vita dei sistemi presenti".