White Paper

Evitare il Fermo Impianto, Tecnologie di difesa e Regolamenti a Supporto

Poche cose corrono più in fretta dell'evoluzione digitale, ed ecco perché negli ultimi anni la normativa in materia di sicurezza ha spostato in modo evidente l'attenzione sulla tecnologia. Lo scopo è proteggere la sicurezza di persone e asset produttivi dal punto di vista informatico.

Scopri di più su:

HON Srl | h-on.it | info@h-on.it
a **TÜV Rheinland** Company
Via Lepanto 23, 59100 Prato (Italia) | +39 0574 870800

TXOne Networks | txone.com
The Leader of OT Zero Trust
Taiwan | Japan | Netherlands | USA | South Europe

Parliamo di Regolamento Macchine e di Progresso Tecnologico:

Nel contesto della fabbrica digitale, la nuova fonte legislativa del Regolamento (UE) 1230/2023, che prende il posto della Direttiva Macchine 2006/42/CE, non richiede atti di recepimento, bensì atti nazionali di esecuzione, con entrata in vigore contemporanea in tutta l'UE.

Ciò significa che il tanto dibattuto Regolamento Macchine sarà immediatamente applicabile senza ulteriori transizioni con la Direttiva.

Regolamento Macchine (UE) 2023/1230

Approvato	Pubblicato	Rettificato	In vigore	Applicabile
14 giugno 2023	29 giugno 2023	04 luglio 2023	19 luglio 2023	20 gennaio 2027

Riferimenti alla cybersecurity RES 1.1.9 e RES 1.2.1

Però:

- L'atto legislativo potrebbe essere soggetto ad ulteriori modifiche prima del 20 gennaio 2027, data di applicabilità prevista, se la Commissione Europea riterrà di dover intervenire sul testo.
- È possibile, ed anzi consigliato, fare riferimento al Nuovo Regolamento Macchine prima del 2027. Secondo la attuale normativa in materia di sicurezza, il datore di lavoro è già tenuto ad adottare i più moderni strumenti che la tecnologia offre: quindi, cosa più della cybersecurity o dei sistemi di intelligenza artificiale rappresenta il progresso tecnologico?
- In ogni caso, in risposta ai requisiti del Regolamento, e per l'apposizione della marcatura CE di conformità, vale la data di messa in servizio della macchina.

Per approfondire cogli questi suggerimenti:

- Vuoi saperne di più sui RES, sulle implicazioni per costruttori, distributori e importatori, e sulla terminologia specifica del Nuovo Regolamento Macchine? Leggi questo articolo sul nostro blog.
- Il manuale **Le MACCHINE dalla direttiva al regolamento (UE) 2023/1230** è co-edito dai nostri partner dello Studio Legale Oddo Lora Gabriele. Al checkout puoi beneficiare del codice sconto **HON10**. Acquista la tua copia online.

Il Regolamento Macchine - accompagnato dalle normative che integrano il tema della cybersecurity, fra cui risaltano la Direttiva NIS 2 e il CRA (Cyber Resilience Act) – segna l'inizio di una nuova era per il mondo della produzione. Ma siamo pronti ad accettarlo?

Quello che possiamo notare è che l'automazione è figlia di una cultura tradizionalista e fedele al motto "*se funziona così, non lo cambiare*"; una cultura difficile da convertire quando mancano le figure professionali responsabili di innovazione e di cybersecurity, o quando quelle figure non hanno a disposizione gli strumenti, tecnologici o organizzativi, per affrontare il cambiamento.

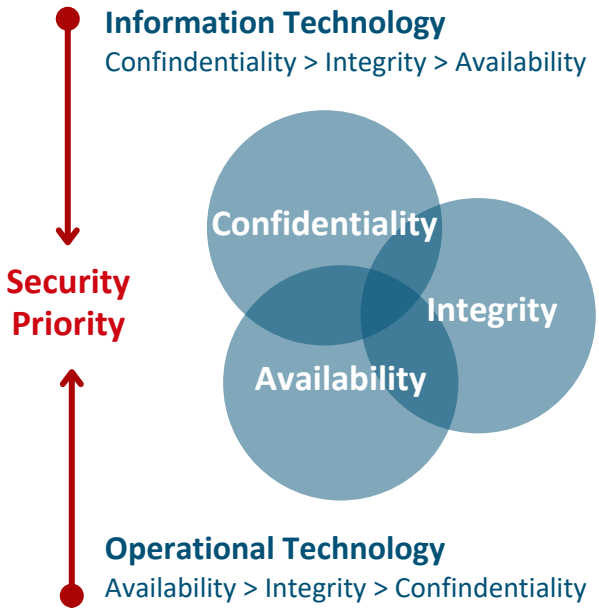
Se riconosci la tua realtà in uno scenario simile, ciò che possiamo consigliarti è di aumentare la consapevolezza del rischio al vertice aziendale.

Prima di tutto, il significato di "sicurezza" è mutato, e mette in comunicazione l'area manutenzione con quella della configurazione di rete.

Se vogliamo garantire la sicurezza complessiva delle attrezzature, da un lato dobbiamo applicare misure di tipo safety per proteggere la proprietà e le persone da malattie, incidenti e disastri fisici, ma dall'altro, in un ambiente macchina connesso in rete, dobbiamo contrastare eventuali intrusioni malevole attraverso misure di security.

Ma attenzione, non solo le tecnologie OT, legate all'uso dei sistemi di automazione e controllo industriale, sono assai diverse dalla tecnologie IT, ma, se non ben configurate, risultano vulnerabili alle minacce informatiche, che sono causa di:

- Fermo o malfunzionamento degli impianti
- Problemi di Business Continuity
- Ripercussioni sulla sicurezza dei dipendenti
- Pericoli per la salute pubblica o per l'ambiente
- Furto di dati relativi alla produzione
- Danni di immagine o assicurativi



Sono sempre i dati a parlare, anche se a volte preferiremmo non crederci.

TXOne Networks, leader delle tecnologie OT Native, ossia progettate su misura per le esigenze del mondo OT, pubblica periodicamente analisi specifiche sull'andamento degli attacchi nel mondo delle infrastrutture critiche, analizzando settori e tipologie di attacco.

*L'esperienza in ambito OT: la tecnologia **Stellar** di Antivirus/Antimalware e Threath Detection per gli endpoint industriali non richiede il reboot del PC in fase di installazione, e la tecnologia **Edge** di Intrusion Detection/Intrusion Protection della rete industriale è di tipo hardware-by-pass. Le tecnologie indicate in fase di installazione o di guasto non bloccano la produzione.* ***Continua a leggere queste pagine per saperne di più sulle possibilità offerte dalle tecnologie TXOne Networks.***

Se guardiamo la cronologia degli ultimi anni, i dati rivelano che:

- Il numero di attacchi informatici a danno dell'OT è più che raddoppiato di anno in anno; parliamo di ben oltre 500 attacchi nel 2023. Ti sembra sconcertante?
- Fra gli attacchi più frequenti regna l'associazione supply chain-ransomware, una tipologia fino a qualche anno fa diffusa solo per la parte IT, e responsabile del più comune danno di fermo impianto.
- I settori più colpiti sono l'energia, il sanitario e il manifatturiero.
- Il 97% degli attacchi nel mondo IT impatta le Operations (OT).
- Il 66% delle vulnerabilità in un impianto industriale deriva dal comportamento umano.
- Il 52% degli incidenti cyber è causato dal personale di manutenzione.

Fonte:

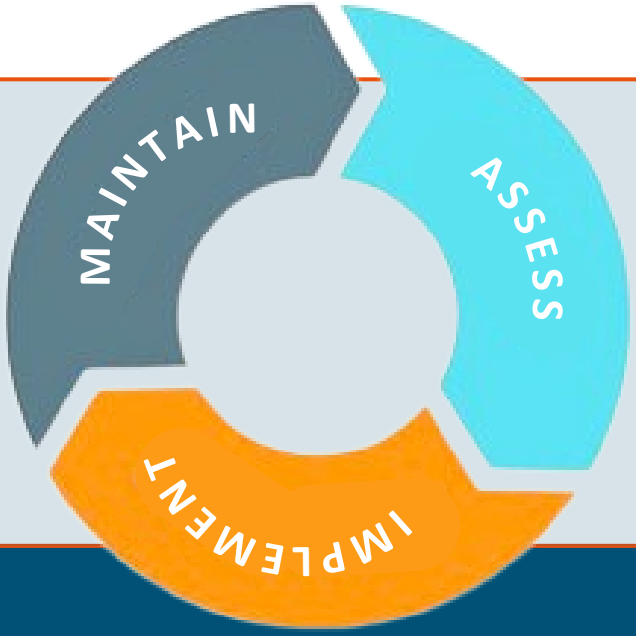
TXOne Networks' The Crisis of Convergence: OT/ICS Cybersecurity 2023

Download Report

Esistono soluzioni che intervengono sulla sicurezza senza stravolgere le infrastrutture OT.

Costruttori ed end-user possono raggiungere un livello maturo in termini di cybersecurity OT sviluppando processi, procedure e governance, in base ai principali standard di riferimento. Ciò, come abbiamo detto, va a beneficio della sicurezza complessiva delle attrezzature, e, a livello europeo, facciamo capo ai già citati Regolamento Macchine, Direttiva NIS 2 e Cyber Resilience Act.

Tuttavia, se ci spostiamo sul piano globale, lo standard cardine per la protezione dell'automazione è IEC 62243, norma che detta la totalità delle best practices oggi rilevanti per la cybersecurity OT.



IEC 62443 LIFECYCLE

La norma stabilisce i requisiti tecnici ed organizzativi per costruttori, integratori di sistema, e utilizzatori finali, con lo scopo di tutelare la sicurezza delle infrastrutture messe in servizio. Se non ne hai mai sentito parlare, o se vuoi ricordare cosa indica lo standard IEC 62443, leggi qui.

Soluzioni consulenziali per i costruttori di attrezzature | OT Cybersecurity Risk Assessment

H-ON a TÜV Rheinland Company

L'applicazione degli standard IEC 62443, guida massima per la progettazione delle attrezzature, passa attraverso l'analisi del rischio macroscopico (i.e. *analisi di alto livello*), con la precisazione di un secondo passaggio di analisi (i.e. *analisi di dettaglio*), che fornisce la base per la redazione delle specifiche di cybersecurity dell'impianto finale.

Seguire le direttive IEC 62443, e implementare soluzioni tecnologiche avanzate, significa immettere sul mercato attrezzature con una notevole posizione di vantaggio in termini di innovazione.

Per applicare lo standard IEC 62443:

Contattaci

Contattaci per una consulenza
h-on.it | +39 0574 870 800

Scopri di più sui prodotti
txone.com/contact/

Il processo di Cybersecurity Risk Assessment per i costruttori di attrezzature

Analisi dei Rischi di Alto Livello + **Analisi dei Rischi di Dettaglio**

Specifiche per la protezione degli asset critici installati nell'impianto finale

Security Lifecycle IEC 62443

- **Definizione di Zone & Conduit**
- **Analisi dei Requisiti richiesti dal cliente**
- **Procedure di Test**
- **Procedure Operative**
- **Conformità degli artefatti**

Presupposto per la Certificazione IEC 62443 della soluzione di automazione

Soluzioni consulenziali per le aziende finali | OT Cybersecurity GAP Analysis

H-ON a TÜV Rheinland Company

L'audit iniziale del livello di cybersecurity di un'infrastruttura OT è l'input attraverso il quale possiamo darvi evidenza di quali interventi, quali risorse e quanto tempo potrebbero servirvi per raggiungere lo stato di cybersecurity ottimale per la vostra realtà.

Pianificheremo ogni intervento, compresa l'implementazione delle soluzioni tecnologiche per l'OT, con la dovuta accortezza, organizzazione e trasparenza.

Per impostare una GAP Analysis:

Contattaci

- **Definizione delle aree di analisi**
- **Identificazione delle criticità OT**
- **Definizione del Piano di Miglioramento**
- **Stima degli interventi necessari**

Presupposto per l'implementazione delle contromisure (tecnologie e governance)

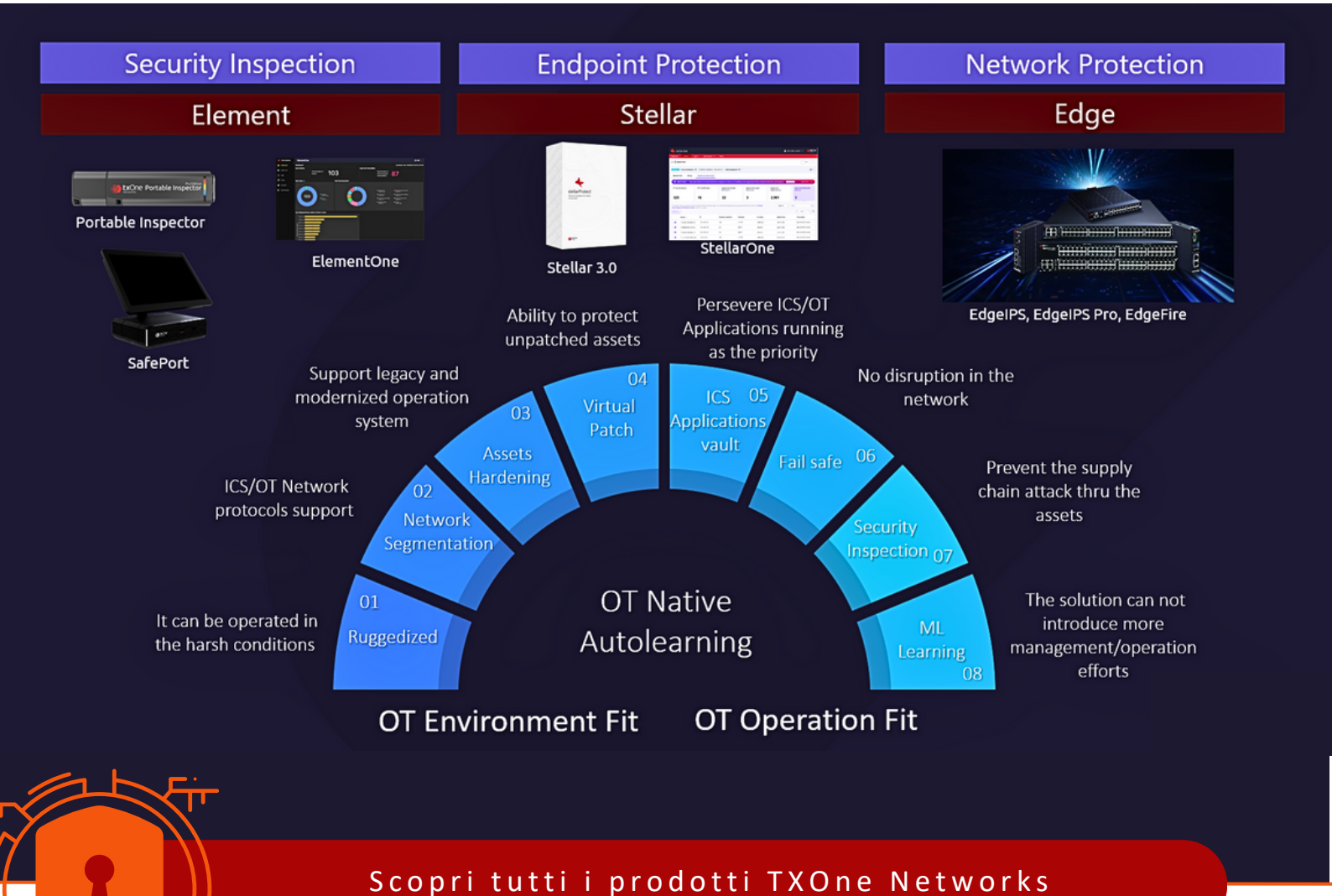
Contattaci per una consulenza
h-on.it | +39 0574 870 800

Scopri di più sui prodotti
txone.com/contact/

Soluzioni tecnologiche per l'ambiente OT | Strategia OT Zero Trust

TXOne Networks

L'implementazione delle soluzioni tecnologiche è un passaggio pratico e strategicamente rilevante per la cybersecurity. La logica OT Zero Trust aiuta a raggiungere i risultati di protezione desiderati sia da chi costruisce che da chi impiega sistemi di automazione, in quanto logica basata sul concetto secondo cui l'accesso ai sistemi debba essere consentito solo agli autorizzati.
Tutte le tecnologie offerte da TXOne Networks hanno tale aspetto comune e fondamentale: sono *on premise* e *adattative*, ossia apprendono il comportamento dell'OT e lo traducono in regole e policy circa i privilegi di accesso, senza il bisogno di interrompere mai la continuità operativa. Esempi dei prodotti più referenziati sono Portable Inspector per la visibilità sull'asset inventory, Stellar 3.0 per la protezione degli endpoint, e la serie Edge per la totale protezione della rete.



Scopri tutti i prodotti TXOne Networks

HON Srl | h-on.it | info@h-on.it

a **TÜV Rheinland** Company

Via Lepanto 23, 59100 Prato (Italia) | +39 0574 870800

TXOne Networks | txone.com

The Leader of OT Zero Trust

Taiwan | Japan | Netherlands | USA | South Europe

Appendice - Le FAQ sulla Cybersecurity OT

Fa parte della nostra missione di consulenti suggerirvi le soluzioni tecnologiche più valide a soddisfare ogni vostra esigenza aziendale. Dalla collaborazione con TXOne Networks sono nati numerosi e preziosi spunti, che abbiamo raccolto in più occasioni.
Per proseguire l'analisi iniziata in questo white paper, te ne presentiamo una. Dal confronto fra i nostri responsabili tecnici e le aziende che da anni rinnovano la loro fiducia verso i nostri consigli, qui puoi scorrere una serie di domande e curiosità emerse nel corso del seminario di febbraio 2024.

Non perdere le notifiche sui prossimi eventi: Segui i nostri canali social.

Come si riesce a far convivere e gestire safety e security in un ambiente industriale con un parco macchine datato?

Una componente importante è evitare la compromissione di un sistema, per cui le soluzioni di tipo adattativo possono agevolare la configurazione di applicazioni che non possono essere manomesse.
Il controllo dell'integrità in termini di cybersecurity protegge anche la safety. La logica può essere implementata su macchine nuove tanto quanto su sistemi terzi o datati, ad esempio attraverso l'installazione di un agent che svolge le funzioni di messa in security della macchina.
A livello di organizzazione, safety e security sono solitamente gestite con reparti e logiche diversi, ma nonostante questo, oggi i due binari viaggiano in parallelo quando si parla di messa in sicurezza delle attrezzature: il revamping delle macchine dal punto di vista safety è l'occasione per prendere in considerazione l'aggiornamento delle procedure di cybersecurity. Quindi, pur essendo due comparti separati, è indubbia la convergenza, in quanto le possibili minacce di security possono impattare sulle funzioni safety.

In breve, quali sono le prossime normative che entreranno in vigore e che avranno impatti operativi e non solo formali?

Le novità normative non si esauriscono con il Regolamento Macchine, bensì è necessario maturare conoscenza di una ampia gamma di standard in ingresso nel mondo della produzione, fra cui: Regolamento PSTI, rivolto al mercato UK dei dispositivi wireless, in vigore a partire da aprile 2024, Direttiva NIS 2 in arrivo a ottobre 2024, che tratta in particolare la governance delle organizzazioni all'interno dei settori critici, Direttiva RED per i costruttori di apparecchiature radio, ed effettiva in Europa da agosto 2025. A queste si aggiungono le normative per il mercato automotive che abbracciano specifici requisiti di cybersecurity. Questi regolamenti talvolta si sovrappongono e sono fra loro correlati; in ciò la consulenza (i.e. *GAP Analysis*) può aiutarvi a razionalizzare quali sono gli standard ai quali conformare i propri sistemi, e quali aggiornamenti futuri andranno a sommarsi ai requisiti già adottati.

Quali sono i dettagli sulle tendenze relative agli attacchi informatici nel mondo OT?

Il 97% degli attacchi al mondo OT deriva da attacchi che si propagano dall'IT, e sono quindi dovuti alla mancata protezione della convergenza fra ambito OT e IT (oltre alla bassa protezione dei sistemi OT). Anche il fattore umano può essere un vettore significativo; in questo senso si nota che la maggior parte degli attacchi accade nei periodi di manutenzione. Sempre meno sono gli attacchi ransomware caratterizzati da lunghi periodi di incubazione, in quanto oggi tali malware riescono a propagarsi nel giro di pochi secondi. Consulta il report di TXOne Networks per saperne di più.

Come si possono affrontare le criticità legate a budget e competenze per poter proteggere i propri impianti?

Ciò che può aiutare a capire come gestire le criticità è comprendere che la strategia giusta non è attendere gli obblighi legislativi, o che un attacco ci colpisca, ma assumere competenze - interne o esterne -, per quantificare il rischio informatico sugli impianti.
Se vogliamo, il vero costo da quantificare è quello di ripristino della produzione in caso di attacco, più elevato rispetto all'investimento nella prevenzione. Questo perché, facendo un parallelo col mondo assicurativo, quando si è bersaglio di attacchi informatici, è necessario fare i conti con le perdite dovute al furto dei dati e ai danni di immagine e reputazionali.
Insomma, potremmo siglare che l'organizzazione e la prevenzione costano meno della riparazione.
La GAP Analysis, assessment sul livello di rischio, si conferma una utile indicazione di quali saranno gli investimenti necessari, in termini di risorse economiche ed umane, per contenere gli incidenti informatici.

Qual è l'importanza di una visione strategica in ambito OT security?

Il paradigma OT Zero Trust implica un approccio alla sicurezza che rende inapplicabili/inefficaci - e talvolta dannose - le soluzioni IT trasferite al mondo OT, perché incapaci di rilevare anomalie legate ai sistemi di controllo industriale. È sempre preferibile avere una visione strategica come OT Zero trust per la protezione di un impianto industriale da incidenti cyber, evitando di implementare tecnologie puntuali senza uno scenario di cybersecurity di riferimento.
Ad esempio, nel mondo OT è fondamentale garantire la disponibilità degli asset produttivi, o meglio le priorità sono: l'affidabilità dell'asset industriale, la disponibilità e l'integrità dell'asset, e la confidenzialità del dato di produzione. Lo spunto è quindi quello di adottare un approccio adattativo e di *autolearning*, senza mai interrompere la produzione.
Ciò rappresenta una possibilità a disposizione anche dei costruttori di macchine, in quanto finalmente oggi esistono tecnologie (*OT Native*) che nascono appositamente per soddisfare le esigenze di OT cybersecurity, e che possono essere implementate sulla singola macchina, o sulla rete industriale, senza doverne modificare caratteristiche e funzionalità; soluzioni che per altro sono conformi alle direttive di prodotto, compreso il Regolamento Macchine e la Direttiva NIS2.

La protezione da attacchi cyber si attua solo con soluzioni tecniche o ha impatto anche sulla governance?

La cybersecurity impatta sia a livello tecnico che di governance, ossia a livello dell'organizzazione dietro al processo di costruzione della macchina. La governance è lo strumento attraverso cui le aziende possono innescare il cambiamento culturale, adattandosi all'evoluzione dei rischi, non più solo legati, ad esempio, allo schiacciamento, ma anche alle intrusioni esterne. Questa è la chiave attraverso cui dare impulso a una più ampia percezione del rischio nell'operatività dei lavoratori.
La formazione tecnica è l'approccio di base per acquisire competenze sui concetti di governance e di business continuity, per sviluppare professionalità che si occupano di cybersecurity, per far maturare la consapevolezza del top management circa i rischi di sicurezza informatica, e per mettere in atto processi migliorativi per la protezione degli asset.

Come si intersecano il comportamento del personale di automazione con la cybersecurity?

Essi si intersecano quando la resistenza al cambiamento incontra l'abitudine delle persone di svolgere operativamente determinate funzioni. Per questo, di fronte a un'ipotetica minaccia informatica, è fondamentale sviluppare procedure condivise fra reparto ingegneria e reparto cybersecurity, sensibilizzando ciascun operatore verso i rischi e le misure di mitigazione. Un esempio è la gestione dell'accesso remoto, pratica oggi diffusa, ma al contempo rischiosa se non opportunamente processata.
In sostanza, la cybersecurity deve essere parte integrante di ogni organizzazione, ed accompagnare tutte le altre funzioni migliorandone gli output. Solo così può essere vista come un *alleato* e non come un *nemico interno* da parte delle diverse funzioni aziendali.
Le organizzazioni industriali devono addestrare il personale di Automation nel produrre con un occhio alla cybersecurity, ma questo esige un cambiamento culturale che può richiedere anni. Infine, la formazione non può evitare l'errore umano; dunque, è necessario proteggere la produzione in conformità con, ad esempio, la Direttiva NIS 2, e con l'uso delle tecnologie di OT Endpoint Security e di OT Network Security.

Come è possibile gestire le richieste di cybersecurity presenti nei capitolati dei clienti se ancora non esiste uno standard cogente?

Il consiglio è standardizzare le architetture a prescindere dalla presenza degli obblighi normativi. Per esempio, la norma volontaria a cui potersi conformare è la IEC 62443, che può essere utilizzata come ragionevole requisito contrattuale. In questo senso, il fornitore che ha già adottato i requisiti di cybersecurity avrà maggiori chance di soddisfare la domanda all'interno del suo mercato di riferimento.

HON Srl | h-on.it | info@h-on.it
a **TÜV Rheinland** Company
Via Lepanto 23, 59100 Prato (Italia) | +39 0574 870800

TXOne Networks | txone.com
The Leader of OT Zero Trust
Taiwan | Japan | Netherlands | USA | South Europe