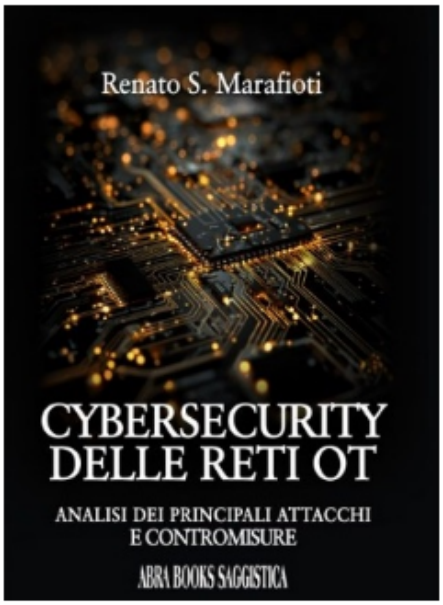
OT security, quando la fabbrica diventa vulnerabile

Di **Giuseppe Mariggiò** - 16 Dicembre 2025

La sicurezza delle reti OT si gioca prima nei reparti produttivi e poi nelle architetture digitali. Renato S. Marafioti smantella il trade-off categorico tra sicurezza e continuità operativa



SE l'OT è nel mirino degli attacchi cyber che hanno funestato il 2025, uno degli aspetti meno considerati resta la cultura della sicurezza informatica in produzione, dove l'imperativo è produrre senza mai fermare gli impianti. Un imperativo che spesso costituisce anche il tallone d'Achille legato a doppio filo al fattore legacy dei sistemi industriali.

Renato S. Marafioti, presidente dell'Associazione Culturale Format E.T.S di Reggio Calabria, arriva al cuore del problema nel suo libro dal titolo *"Cybersecurity delle reti OT – Analisi dei principali attacchi e contromisure"*, attualmente disponibile solo in versione e-book (*Abra Books*, 2025 – Saggistica). E affronta il tema della sicurezza OT dal punto di vista del change management: «La cybersecurity industriale non è solo una sfida tecnologica, ma soprattutto culturale e manageriale».

Formatore di lungo corso, Marafioti ha dedicato la sua vita alla preparazione e riqualificazione delle risorse umane partendo da una regione, la Calabria, che sta puntando moltissimo sullo sviluppo e le certificazioni delle competenze per la crescita del territorio. Con la progressiva convergenza tra IT e OT, la fabbrica connessa abbatte i domini classici. Marafioti parte proprio da questa frattura: l'IT storicamente centrato sui dati, l'OT focalizzato sui processi, sulla disponibilità e sulla sicurezza fisica. Una dicotomia che si è sedimentata nelle organizzazioni industriali e che rappresenta uno dei principali ostacoli alla costruzione di una strategia di sicurezza integrata.

Il punto di forza del volume è l'attenzione al fattore umano. Se è vero che le reti OT sono sempre più nel mirino degli attacchi cyber, è altrettanto vero che molti incidenti vanno a segno per errori operativi, configurazioni errate, accessi remoti non protetti e una conoscenza incompleta degli asset presenti in rete.

Leggi anche: Rilasciato il nuovo Ransomware Report di Semperis: attacchi ransomware implacabili

In numerosi impianti produttivi – come evidenzia l'autore – non si sa nemmeno quanti dispositivi siano effettivamente collegati. In questo scenario, firewall mal configurati e una segmentazione di rete insufficiente diventano porte spalancate per i malware industriali.

I dati di contesto rafforzano l'urgenza del tema. La quasi totalità degli incidenti cyber che colpiscono l'IT ha ricadute anche sull'OT, e circa un terzo delle aziende industriali ha già subito attacchi che hanno generato interruzioni operative e impatti diretti sul business.

Il Rapporto CLUSIT 2025, colloca l'Italia tra i Paesi più colpiti a livello globale, con oltre il 10% degli attacchi mondiali. Un dato che rispecchia la struttura del nostro tessuto produttivo: una forte presenza di PMI manifatturiere, spesso dipendenti da tecnologie operative avanzate ma non sempre adeguatamente protette.

Marafioti affronta con chiarezza le principali vulnerabilità delle infrastrutture critiche e propone una rassegna ordinata di best practice: dalla gestione degli accessi alla segmentazione delle reti, dal monitoraggio continuo all'adozione di tecnologie di difesa specifiche per l'ambiente OT, smantellando il trade-off categorico tra sicurezza e continuità operativa. Oggi sappiamo che un incidente cyber interrompe la produzione, un ransomware OT può fermare un impianto per giorni e la mancanza di sicurezza è una minaccia diretta alla continuità. «La non-sicurezza è il vero rischio operativo» – spiega Marafioti.

Il libro si distingue per il taglio pragmatico e formativo, coerente con il profilo dell'autore, da anni impegnato nella formazione in ambito ICT. Non è un manuale iper-specialistico per addetti ai lavori, né un testo divulgativo generico: si colloca in una zona intermedia, utile a manager industriali, responsabili di stabilimento, professionisti della sicurezza e decisori chiamati a governare la convergenza tra IT e OT.