Ufficio stampa H-ON (*)

# Non c'è sicurezza industriale senza sicurezza informatica

**Senza la Security non è più possibile garantire la "sicurezza" della produzione, degli operatori e delle attrezzature industriali. Lo hai sentito dire spesso, soprattutto in questo ultimo anno. Ma che significa davvero?**

(*) Società del gruppo TÜV Rheinland operativa in oltre 10 settori industriali, con progetti di consulenza e certificazione estesi su tutta la filiera industriale: dalla conformità del componente fino alla certificazione di intere linee di produzione. **https://h-on.it/it/azienda/**


Partiamo col chiarire i due termini, Safety e Security, che nel linguaggio comune spesso si sovrappongono al punto da essere considerati sinonimi. È importante capire che tra le due fattispecie esiste una sottile quanto importantissima differenza. Quando si parla di garantire la Safety si vuole intendere l'insieme delle misure adottate per proteggere la proprietà e le persone da malattie, incidenti e disastri causati dall'ambiente. La Security, invece, include il contrastare azioni, spontanee o deliberate, che hanno l'intenzione di nuocere. Esempio primo tra tutti: un attacco cyber è una conseguenza inesorabile di una falla dei sistemi di security.

## In ambito industriale

In ambito industriale esistono numerose norme e testi normativi che obbligano a determinate azioni di tutela verso le aziende, i luoghi aperti al pubblico, le amministrazioni e tutti i siti in cui esiste un potenziale rischio per lavoratori e utenti. La Security, però, a differenza della Safety, non è standardizzata.

Il vero problema è che, nell'ambito dell'OT (Operational Technology), cioè quella tecnologia operativa utilizzata per controllare i dispositivi industriali, vi è ancora un'ideologia non sufficientemente al passo con la digitalizzazione, che ha evoluto i sistemi senza però evolverne anche le misure di sicurezza. La percezione delle minacce cyber non è ancora chiara e delineata in ambito Operational quanto in quello IT, cioè nella tecnologia delle infrastrutture.

## I rischi dell'OT digitale

Ma quali sono i veri rischi che si corrono in caso di cyber attack? Nel contesto OT l'impatto di un attacco può avere conseguenze devastanti, primi fra tutti il fermo o il malfunzionamento di un impianto, ma anche conseguenti ripercussioni su chi lavora su quegli stessi impianti.

Senza considerare il pericolo per la sicurezza dei dipendenti o di salute pubblica e danni all'ambiente: si pensi al caso di un'azienda farmaceutica che, se vittima di attacco, può subire alterazioni dei principi attivi dei propri prodotti. Si possono poi subire gravi danni di immagine e perdita di fiducia dovuta alla cattiva pubblicità data dalla diffusa consapevolezza che un'azienda non sia stata pronta a contrastare un attacco o rapida a ripristinare un problema. Ultimo ma non per importanza, il furto di informazioni sensibili legate alla qualità dei prodotti o alla proprietà intellettuale.

Leggi l'articolo integrale

## Smart Manufacturing e Industria 4.0

Fino a qualche tempo fa l'OT viveva disconnesso da internet: l'hardware era tendenzialmente proprietario e la tecnologia era eseguita su sistemi oramai datati. Con l'evoluzione digitale delle tecnologie OT, arriviamo al paradigma dello Smart Manufacturing e dell'Industria 4.0, dove di base la produzione è collegata tramite sistemi ERP e si registra un costante flusso di dati che permette di realizzare, per esempio, azioni di manutenzione predittiva, ma che allo stesso tempo espone i dispositivi OT ai nuovi rischi legati alla cyber security. Nelle fabbriche odierne, spesso ci troviamo quindi di fronte a tecnologie di ultima generazione, ma non opportunamente configurate e, di conseguenza, vulnerabili a possibili attacchi cyber. La rinnovata attenzione verso la tecnologia è quindi essenziale per prevenire i possibili effetti che questa potrebbe avere sulla sicurezza dei prodotti. Ma non solo.

**In ambito OT (tecnologia operativa per controllare i dispositivi industriali) i sistemi sono passati al digitale senza evolvere anche le misure di sicurezza. Risultato: in ambito Operational la percezione delle minacce cyber non è ancora delineata quanto in quello IT (tecnologia delle infrastrutture)**

## Cyber Security nel Regolamento Macchine

Piano piano la Cyber Security OT sta entrando anche nel campo del Nuovo Regolamento Macchine, assumendo un peso importante, con la possibilità che la sicurezza informatica industriale diventi un requisito cogente. È quindi sempre più vicina l'obbligatorietà di valutare i rischi di attacco informatico per garantire la sicurezza degli utilizzatori finali delle attrezzature, in modo da evitare incidenti causati da atti deliberati, che sempre più spesso mettono alla prova molti comparti industriali. Come rivela la più recente documentazione presente sul sito della Comunità Europea, proprio l'attenzione del Nuovo Regolamento Macchine si concentra anche sui rischi derivanti da azioni malevoli a danni della security che hanno un impatto sulla sicurezza (safety) e sull'affidabilità delle macchine.