Industrial Cybersecurity: scenari di rischio ed esigenze di difesa



Il settore industriale è sicuramente fra i più interessati dalla trasformazione digitale.

L'assioma *Industry 4.0*, reso possibile dall'evoluzione delle tecnologie legate alla gestione di sistemi complessi e in Italia già destinatario dell'omonimo piano nazionale d'intervento, oggi apre il passo all'ancor più dinamico *Industry 5.0*.

Su questo settore in espansione si concentrano, inevitabilmente, anche mire e ambizioni del crimine informatico; tendenza tanto più preoccupante se si considera come nel settore industriale rientrino *asset* altamente critici in ottica di sicurezza nazionale.

Standard internazionali di sicurezza

Proprio in ragione della sua elevata criticità, il settore industriale è da tempo oggetto di prescrizioni e linee guida che stabiliscono – ai vari livelli internazionali, comunitari o statali – regole condivise a garanzia della sicurezza fisica dei prodotti. Negli anni recenti sempre più fonti in materia includono standard o divieti mirati anche alla tutela di informazioni e dati coinvolti, di volta in volta concentrandosi su criteri generali oppure su particolari campi di attività.

Tuttavia, la normativa fatica a tenere il passo dell'innovazione.

Infatti la crescente integrazione uomo-macchina, l'automazione

di numerosi processi e servizi, l'impiego dell'Intelligenza Artificiale e la generalizzata interconnessione tra dispositivi fisici e digitali non hanno solo reso più vulnerabili i contesti preesistenti. Hanno anche portato al proliferare di nuovi ecosistemi ibridi che esigono una protezione su molteplici fronti: fra questi il paradigma IoT (qui inteso come IIoT o *Industrial Internet of Things*, destinatario di specifiche e insidiose categorie di minacce) o lo *Smart Manufacturing,* dove guadagnano assoluta centralità la *Operation Technology Security* e gli *Industrial Control Systems* (ICS).

Fronti di vulnerabilità e tipologie di minacce

Come per ogni altro contesto, anche nel mondo produttivo e manifatturiero la digitalizzazione degli ultimi decenni ha portato a una massiccia espansione delle superfici d'attacco.

Lo confermano le statistiche di settore, concordi nell'evidenziare un significativo e progressivo aumento delle minacce informatiche rivolte alle industrie. Nel 2022 il settore è salito al terzo posto fra i più frequentemente colpiti da un *cyberattack*, con 68 incidenti di sicurezza segnalati solo nel primo semestre dell'anno.

Oltre alla persistente prevalenza dei *ransomware* (che oggi frequentemente scelgono come obiettivi singoli "anelli" delle articolate *supply chain* sottostanti a ogni produzione o servizio complesso), a preoccupare sono anche gli attacchi di tipo *Hijacking* volti a sabotare singole componenti dei macchinari o ad assumerne il controllo da remoto; insieme alla rilevante ascesa del *cyber espionage* finalizzato al furto di informazioni o codice di proprietà industriale.

Prospettive future per la cyber-resilienza industriale

Simili rischi rendono evidente la necessità, per le aziende, di pianificare adeguate strategie di *Risk Assessment* e adottare strumenti che sappiano proteggere sistemi e dati senza compromettere la continuità operativa, garantendo monitoraggio e aggiornamento ininterrotti dei relativi ambienti (fisici o digitali) senza trascurare la possibilità di eventuali *Insider Threat*.

Ma è anche evidente come a tale scopo le buone pratiche di sicurezza informatica e la *compliance* alle normative, per quanto fondamentali, non bastino.

La continua innovazione dei processi deve procedere in parallelo a una altrettanto rapida evoluzione dei meccanismi di difesa; obiettivo possibile soltanto promuovendo strette collaborazioni fra organizzazioni del settore industriale, istituzioni ed enti di ricerca che facciano della cybersecurity un reale fattore abilitante per lo sviluppo di prodotti e servizi intrinsecamente sicuri.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/industrial-cybersecurity-scenari-di-rischio-ed-esigenze-di-difesa/