LA PROTEZIONE DELL'IT INDUSTRIALE A PARTIRE DA COMPETENZE E CULTURA

Quando la cybersecurity si unisce all'automazione

In ambito di cybersecurity, l'industria manifatturiera si trova ad affrontare varie sfide e prima fra tutte quella di reperire le competenze e le figure professionali necessarie. Tra i punti chiave per lo sviluppo del settore ci saranno gli investimenti in formazione specialistica e quelli nella sensibilizzazione e consapevolezza delle figure presenti in azienda.

Silvia Movio

Nel settore industriale, la cybersecurity si rivolge soprattutto all'automazione, concentrandosi sulla protezione di sistemi e dispositivi di controllo, come PLC, Scada e HMI

La cybersecurity non è soltanto una questione tecnologica, ma anche di processi e persone che, di pari passo, devono seguire l'evoluzione della Smart Manufacturing. Dotare le fabbriche di Intelligenza Artificiale diventa, quindi, una necessità per qualsiasi impianto industriale che voglia essere competitivo nell'industria 4.0, nell'ottica di aumentare la produttività e di offrire un prodotto e/o servizio personalizzato.

L'**Industrial Cybersecurity** è l'insieme dei mezzi applicabili all'automazione di fabbrica volti a rendere immuni da attacchi i sistemi di controllo quali PLC, Scada e HMI, fulcro dei processi produttivi moderni. Questi sistemi, se colpiti, possono portare a conseguenze disastrose. La mole di dati scambiati ogni giorno fra i reparti IT e OT è enorme ed è per questo che sono un bersaglio allettante per gli hacker.

Il contesto industriale attuale, ormai dal 2016, apre alla tematica **Security Automation**. Questa tendenza non è certamente cambiata negli ultimi anni, anzi, la moltiplicazione dei device, lo smart working ormai largamente diffuso e le conseguenti minacce di sicurezza sempre più frequenti e insidiose rendono il contenuto relativo alla sicurezza una necessità per molte imprese.

I numeri della sicurezza

Indagini recenti evidenziano che una parte consistente dei 300 miliardi di dollari di investimenti che il mercato globale della Cybersecurity farà nei prossimi 5 anni

NOTA AUTORE
S. Movio, Director di Hunters,

A FIL DI RETE
www.huntersgroup.com

verrà orientata verso misure di sicurezza automatizzate. L'obiettivo è di migliorare i tempi di rilevamento e risposta alle minacce su quattro differenti segmenti: Application Security, Endpoint Security, Data Security and Protection, Internet of Things Security. In Italia, tuttavia, la protezione delle tecnologie OT è ancora un tema sottovalutato, rendendo così i sistemi di controllo un punto debole per l'Industria 4.0 dal punto di vista informatico di contenuto tecnico, accompagnato dalla carenza di risorse specializzate.

Un percorso ancora da delineare rende la Security Automation una delle tendenze più interessanti in assoluto per le potenzialità ancora da esprimere e le criticità da risolvere. Lo dimostra il fatto che un uso pervasivo di tecniche di automazione interessa solo il 9% delle aziende, mentre un'adozione di livello medio ne accomuna il 38,3%.

Innovazione e Cybersecurity dovrebbero andare di pari passo: purtroppo ciò spesso non avviene e l'industria manifatturiera si trova ad affrontare varie sfide, prima fra tutte la mancanza di preparazione in tutto il settore che spesso si manifesta concretamente con l'assenza di un dipartimento dedicato o di professionisti IT specializzati e preposti all'attività di creazione e implementazione di un'infrastruttura di sicurezza adeguata.

Attualmente in Italia mancano circa 100mila esperti, come evidenziano le stime dell'Agenzia Nazionale per la Cybersicurezza, è evidente quindi il divario fra domanda e offerta di professionisti nel settore della Sicurezza Informatica.

Come colmare il divario?

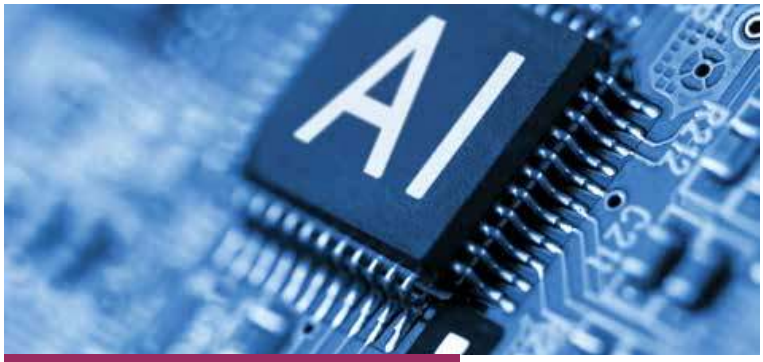
Per restituire una panoramica di mercato, **Hunters Group** ha registrato un **incremento del 14%** nel 2022 di progetti di ricerca ed head hunting, focalizzati su questo segmento professionale di specializzazione.

Si rileva un focale interesse per le seguenti figure professionali:

- ICT Security Manager,
- Data Protection Officer,
- Security Architect & Consultant.

Questi ruoli professionali sono punto di riferimento per figure professionali certificate di Middle & Top Management. Dato che l'interesse maggiore non è rivolto alle figure più junior del settore della Cybersecurity, ma ad esperti, si ricorre spesso all'head hunting.

Fondamentale sarà l'investimento culturale ed educativo nel settore ed è una responsabilità primaria di tutti i C-level aziendali, non solo di quelli dediti alla sicurezza informatica. La riduzione del divario di competenze e la creazione di una cultura dell'apprendimento



Per qualsiasi impianto produttivo, l'impiego dell'Intelligenza Artificiale diventa una necessità nell'ottica di aumentare la produttività e di offrire un prodotto o un servizio personalizzato

sui temi di sicurezza saranno fondamentali per tutti i ruoli aziendali.

Due saranno i punti chiave per lo sviluppo del settore:

- L'investimento in **formazione specialistica**, centrale anche in termini di Retention (ovvero la capacità di un'organizzazione di trattenere i propri dipendenti all'interno della propria azienda), supportando i propri collaboratori, continuando ad investire sulla loro crescita professionale, agevolando così anche la successiva interdisciplinarità e condivisione delle competenze interne;
- L'investimento nella **sensibilizzazione e consapevolezza** di tutte le figure presenti in azienda per proteggere loro stesse e i dati della propria organizzazione. ■

La mole di dati scambiati ogni giorno fra i reparti IT e OT è enorme ed è per questo che sono un bersaglio allettante per gli hacker