STORMSHIELD

ARTICOLO DI OPINIONE

INDUSTRIA 5.0: E LA SICUREZZA INFORMATICA CHE RUOLO GIOCA?

Khobeib Ben Boubaker
Head of Industrial Security Business Line, Stormshield

Umana, sostenibile, resiliente: mentre l'Industria 4.0 si è concentrata sul miglioramento della produttività attraverso Big Data, IoT e macchine intelligenti, l'Industria 5.0 promette di concentrarsi nuovamente sulle persone e sulla società. Dove si colloca la sicurezza informatica in questo contesto?

A dieci anni dall'introduzione ufficiale del termine «Industria 4.0», stiamo per assistere a una nuova rivoluzione: la nuova Industria 5.0 mira a **rimettere le persone al centro dei processi industriali**, ormai fin troppo digitalizzati. Ma le interazioni tra uomo e macchina implicano la necessità di adottare forti misure di sicurezza negli ambienti industriali. Dove si colloca allora la sicurezza informatica? Quali gli orizzonti? Ecco alcune riflessioni.

LE PROMESSE DELL'INDUSTRIA 5.0

La prospettiva che vedeva le macchine e le tecnologie portare alla scomparsa delle persone all'interno delle fabbriche e nel cuore dei processi industriali è una visione ormai superata per l'industria. Concentrandosi sull'aumento della produttività, l'Industria 4.0 mirava a rendere le fabbriche «intelligenti», con il controllo e la supervisione della produzione a distanza.

Ma allora, **cos'è l'Industria 5.0?** Nel mirino del nuovo paradigma dell'Industria 5.0 ci sono proprio le persone. «*La priorità assoluta è migliorare le condizioni di lavoro attraverso nuove soluzioni tecniche e macchine robotizzate ad alte prestazioni*», sottolinea **Vincent Nicaise**, responsabile dei partenariati e dell'ecosistema industriale di Stormshield. Proseguendo, fa luce su un'altra dimensione: «*ripristinare l'immagine dell'attività industriale in un contesto favorevole al tema della reindustrializzazione in Europa. Si tratta quindi anche di rendere più attrattivo un settore che soffre da diversi anni, suscitando l'interesse dei lavoratori di domani e del know-how ingegneristico.*» **Il credo dell'Industria 5.0 è portare benefici ai lavoratori, alle aziende e al pianeta**. Si tratta di «*utilizzare le nuove tecnologie per garantire la prosperità in termini di posti di lavoro e di crescita, ma anche e soprattutto rispettando i limiti di produzione del pianeta*», ribadisce **Stéphane Potier,** Head of IoT & IoT Cybersecurity di Advens. In questo senso, il nuovo paradigma industriale è l'antitesi dello spettro di una fabbrica automatizzata al 100% che distrugge i posti di lavoro. La macchina robotica non è prevista come entità autonoma e non sostituisce le competenze umane. «*Il robot è collaborativo e solleva l'operatore da compiti noiosi*», continua. La macchina, anzitutto, assisterà l'operatore nel suo compito fornendo nuove capacità funzionali attraverso l'integrazione di intelligenza artificiale, realtà aumentata, robotica e IoT. Fermamente incentrata su un approccio produttivo sostenibile che tenga conto dell'imperativo climatico, l'Industria 5.0 incorpora nuovi criteri come l'efficienza energetica delle tecnologie, la priorità alle energie rinnovabili e un orientamento all'autosufficienza. L'energia è un tema fondamentale per l'industriale 5.0, che dovrà tenere conto non solo del consumo energetico delle macchine, ma anche di quello dell'intera macchina produttiva. «*La questione delle terre rare, presenti in molti componenti e macchine industriali, sta diventando cruciale*», afferma Stéphane Potier. «*Ad esempio, i motori di oggi utilizzano molte meno terre rare e sono realizzati con materiali più facilmente reperibili.*»

Il fattore resilienza è fondamentale anche per l'Industria 5.0, che sta prendendo atto di un contesto macroeconomico e geopolitico che dimostra ogni giorno la necessità di sapersi adattare agli shock. Secondo **Marc Bagur**, responsabile del settore Human-Machine Performance di Airudit, ciò rappresenta un'enorme opportunità strategica per i produttori. «*Chi sceglie di dare priorità ai valori umani piuttosto che alla tecnologia, adotta un approccio globale e un modello organizzativo più performante nel lungo periodo.*» Non è più una corsa alla digitalizzazione dell'ambiente industriale a tutti i costi,

bensì la realizzazione di una «*solidità sistemica che sia socialmente, umanamente ed ecologicamente accettabile*». E sottolinea che questa esigenza «*coincide perfettamente con quella delle nuove generazioni di ingegneri e lavoratori per i quali l'allineamento ai valori ecologici, il tema delle risorse energetiche e la stabilità sociale sono oggi questioni cruciali*».

Tuttavia, poiché i livelli di maturità dei vari sistemi industriali variano, rimane difficile valutare con precisione quando questo nuovo paradigma sarà effettivamente operativo. E l'Industria 4.0 è ancora relativamente nuova...

INDUSTRIA 4.0 VS INDUSTRIA 5.0: SOSTITUZIONE O COMPLEMENTARIETÀ?

L'Industria 5.0 non è solo l'ennesima iterazione nella marcia forzata verso il progresso. **Questo nuovo paradigma va visto come un complemento a quello dell'Industria 4.0 e mira a collocare il tema dell'innovazione tecnologica in un quadro specifico, incentrato sul trittico «persone-sostenibilità-resilienza»**. A tal fine, l'Industria 5.0 attinge all'efficacia delle tecnologie dell'Industria 4.0, ad esempio per risolvere problemi legati al criterio della sostenibilità. «*Per ridurre il consumo energetico di una macchina, sia essa nuova o vecchia, dobbiamo prima essere in grado di misurarne il consumo. L'Industria 4.0 ci fornisce gli strumenti per farlo, grazie a sensori, contatori e sistemi IoT*», sottolinea Stéphane Potier. «*Inoltre, possiamo cercare di ottimizzare il funzionamento di una macchina che consuma troppa energia. Da un lato con la manutenzione predittiva per influenzare la durata di vita della macchina, dall'altro con l'intelligenza artificiale per ottimizzarne i consumi*». Nel suo rapporto «*Industry 5.0 - Towards a sustainable, human-centric and resilient European industry*», la Commissione europea illustra questo approccio complementare. **Occorre anche rispondere alle debolezze dell'Industria 4.0, che finora si è sviluppata a troppa distanza dalle tematiche sociali**. L'obiettivo è formare industriali capaci non solo di essere produttivi ed efficienti, ma anche di ispirare fiducia con valori che riflettono i tempi e le sfide poste dalle nuove generazioni.

Con questi orientamenti strategici, **come possiamo preparare l'industria di domani?** La fabbrica 4.0 di oggi è in gran parte digitale, con i Big Data per la gestione dei dati, l'IoT per le misurazioni precise, il 5G per il collegamento in rete dei siti industriali e l'edge computing per l'implementazione di una maggiore capacità di calcolo sulla macchina… Ma deve anche tenere conto di un contesto macroeconomico e geopolitico particolarmente complesso, caratterizzato dall'aumento dei prezzi dell'energia e dall'urgenza delle questioni ambientali. **Preparare una risposta industriale alle sfide della nostra civiltà richiede quindi di indirizzare gli investimenti giusti nei posti giusti, ma anche di rivedere i processi in ogni fase della catena produttiva**. Secondo Vincent Nicaise, la modernizzazione degli impianti industriali richiede sia «*nuove conoscenze legate a protocolli e processi tecnicamente innovativi, sia nuove competenze per i lavoratori, gli attori chiave della catena produttiva*». L'introduzione di un nuovo livello informativo da parte dell'Industria 5.0 dà origine a nuove esigenze, che hanno un impatto diretto sul tema della formazione del personale. «*Possiamo scegliere di creare nuove posizioni, come il referente locale responsabile dell'applicazione dei nuovi protocolli di sicurezza alle*

macchine nelle fabbriche sparse per il mondo, oppure possiamo scegliere di aumentare le competenze degli operatori esistenti», spiega.

L'occasione giusta per mettere finalmente la sicurezza informatica al centro dell'industria?

DOVE SI COLLOCA LA CYBERSICUREZZA NELL'INDUSTRIA 5.0?

Nel corso della FIC 2022, la questione della cybersicurezza negli ambienti industriali era sulla bocca di tutti. **Perché la fabbrica connessa sta moltiplicando la superficie di attacco e quindi i problemi di sicurezza.** In effetti, a causa della combinazione di un numero sempre maggiore di macchine robotizzate, della crescente interconnessione, dell'integrazione dell'IoT, della realtà aumentata e delle nuove interfacce uomo-macchina, il numero di potenziali falle di sicurezza nei sistemi sta aumentando.

Un rapporto di Claroty indica che solo nel 2021 sono stati attaccati 82 produttori industriali. Nello stesso anno, il numero di vulnerabilità rilevate è aumentato drasticamente, passando da 637 a 787. Tanti i punti di accesso critici... Spesso citato come esempio, il sistema operativo obsoleto in esecuzione sulle apparecchiature di fabbrica è uno dei fattori di vulnerabilità più frequenti in termini di sicurezza informatica industriale. Il famoso Windows XP è ancora un sistema essenziale per alcuni ambienti industriali e richiede strumenti speciali di cybersecurity per ridurre il rischio. Questo perché le conseguenze di un attacco informatico in un ambiente operativo hanno un impatto decuplicato, dal blocco completo delle linee di produzione alla messa in pericolo dei lavoratori, per non parlare del forte impatto reputazionale per l'azienda interessata. Senza contare il rischio ambientale, a cui l'Industria 5.0 è particolarmente sensibile.

La domanda è quindi: **quali soluzioni di sicurezza informatica utilizzare per proteggere gli ambienti industriali di domani?** Per affrontare la sfida della sicurezza industriale 5.0, sono al vaglio due scenari. Il primo prevede un «revamping», in cui la catena di produzione viene aggiornata incorporando il tema della sicurezza informatica nelle apparecchiature. In questo primo scenario, l'installazione di «*componenti di tipo firewall è un buon modo per segmentare i flussi e analizzare i protocolli*», afferma Vincent Nicaise, così come «*una protezione più severa dele postazioni di lavoro, con un'attenta gestione delle porte USB, delle reti Wi-Fi e degli accessi*». La scelta di soluzioni di cybersecurity sovrane è una garanzia di trasparenza ed evita qualsiasi rischio di sfruttamento dei dati per scopi dannosi. L'obiettivo è disporre di un codice sovrano controllato che mitighi i rischi di compromissione e di attacco da parte di organismi estranei. È l'unico modo per garantire una difesa in profondità senza anelli deboli. Il secondo scenario dell'Industria 5.0 riguarda le apparecchiature più recenti, che incorporano la sicurezza informatica come caratteristica nativa. Ma perché ciò avvenga, l'aspetto umano e la natura collaborativa saranno fondamentali; più ancora della sensibilizzazione, è necessario instaurare una vera e propria collaborazione tra i team di tutti i nuovi progetti. Da un lato, le esigenze di sicurezza dei team informatici e, dall'altro, i vincoli operativi dei team IT. Dobbiamo lavorare insieme per confrontare i punti di vista e raggiungere compromessi che soddisfino sia i vincoli informatici che quelli dell'IoT.

A patto che i produttori siano davvero pronti per questa Industria 5.0 cybersicura.

L'INDUSTRIA DI DOMANI E LA MATURITÀ INFORMATICA: I PRODUTTORI SONO PRONTI?

Secondo uno studio di Wavestone dell'aprile 2023, la maturità informatica delle grandi organizzazioni in Francia rimane bassa: solo il 49% degli intervistati ha dichiarato di averla raggiunta. La media è simile per **il settore industriale, con solo il 49,4% degli intervistati che si dichiara maturo in termini di cybersecurity**. Anche se il settore industriale è in crescita di 4,6 punti rispetto allo scorso anno, la sicurezza dei sistemi industriali è una delle questioni ancora aperte che le grandi aziende faticano ad affrontare (al pari della gestione delle terze parti e della sicurezza nel cloud).

Per forzare queste aziende ad adottare i necessari standard di cybersicurezza, saranno presto applicate leggi e regolamenti europei, come la direttiva NIS2 per la gestione dei subappaltatori in ambienti sensibili e il Cyber Resilience Act per il rafforzamento dei prodotti digitali connessi. Per Vincent Nicaise, questi testi legislativi aiuteranno i professionisti ad adottare una serie di misure di sicurezza concrete: «*non appena il Cyber Resilience Act sarà attuato a livello europeo, i produttori saranno obbligati, ad esempio, a incorporare caratteristiche di sicurezza nelle loro apparecchiature*». Allo stesso tempo, anche gli standard come MITRE ATT&CK e NIST possono contribuire ad aumentare la maturità dei produttori in materia di cybersecurity. Qualunque sia il mezzo utilizzato, una diagnosi tecnica approfondita e seria dovrebbe consentire ai produttori di aumentare rapidamente la loro resilienza di fronte agli attacchi, in vista dell'Industria 5.0.

«Una persona consapevole vale due. E questo, a mio avviso, è un concetto che rientra pienamente nei principi dell'Industria 5.0, che sancisce la collaborazione tra uomo e macchina.»

Stéphane Potier, Head of IoT & IoT Cybersecurity di Advens

In termini operativi, questa capacità si può tradurre nella segmentazione delle reti e degli ambienti di produzione, nell'uso della crittografia per lo scambio di dati sensibili, nell'implementazione di sistemi di autenticazione forti o nel monitoraggio continuo delle infrastrutture sensibili. **Diventa quindi fondamentale sensibilizzare e formare il personale su come rilevare gli attacchi informatici**. «*Gli operatori conoscono le loro macchine e sono perfettamente consapevoli delle normali reazioni dei loro strumenti*», ribadisce Stéphane Potier. «*Sensibilizzarli sul tema della sicurezza informatica, spiegando i diversi tipi di attacco e le potenziali conseguenze per il loro ambiente di lavoro aiuta a tenerli all'erta. L'operatore sarà quindi in grado di rilevare molto rapidamente una situazione anomala e di segnalarla al proprio CISO*». Tuttavia, la sensibilizzazione in ambiente OT non è così sistematica come nell'ambiente IT. «*Contrariamente al pensiero comune sulla cybersecurity, secondo cui la principale vulnerabilità si trova tra la sedia e la tastiera, io penso invece che sia la soluzione a trovarsi tra la sedia e la tastiera*», osserva. E continua: «*Una persona consapevole vale due. E questo, a mio avviso, è un concetto che rientra pienamente nei principi dell'Industria 5.0, che sancisce la collaborazione tra uomo e macchina.*»

Per essere efficace, l'Industria 5.0 dovrà quindi combinare i suoi principi cardine - persone, sostenibilità e resilienza - con una maggiore consapevolezza della sicurezza informatica, unita all'integrazione di dispositivi robusti nel cuore dei suoi sistemi. In altre parole, la cybersecurity dovrà essere parte integrante di questo nuovo paradigma industriale per tutte le aziende che desiderano accelerare in questa direzione.