Smart manufacturing e cybersecurity

Author : Francesco Maldera

Date : 10 Giugno 2019

Il contesto di riferimento

La parola **sicurezza** corrisponde, nella lingua inglese, a due termini che esprimono significati molto diversi: *safety* e *security*. Il primo corrisponde a quello che - in italiano - è espresso dalla parola **salubrità**, connessa alle azioni per ridurre il rischio per il benessere fisico e psicologico delle persone. Il secondo si riferisce, invece, alle azioni che intendono **prevenire o ridurre danni** al patrimonio delle persone, delle organizzazioni e della società in generale.

Questi concetti, pur rimanendo distinti, sono stati oggetto di un approfondimento dell'Agenzia dell'Unione Europea per la Sicurezza delle Reti e delle Informazioni (ENISA)[1] nel documento *"Good Practices for Security of Internet of Things in the context of Smart Manufacturing"*[2] orientato a focalizzare l'attenzione sulla *security for safety* nelle aziende manifatturiere moderne.

L'impegno dell'ENISA è partito dalla considerazione che negli apparati produttivi delle aziende manifatturiere operano molti **attuatori** che agiscono sul mondo reale e, potenzialmente, sulle persone. Tradizionalmente, questi elementi sono stati dotati di meccanismi di prevenzione finalizzati a ridurre la probabilità che la loro azione possa incidere sulla salute (*safety*) delle persone; si pensi, per esempio, a un braccio di verniciatura di una fabbrica automobilistica: il suo angolo d'azione è configurato a monte affinché non sconfini in un'area dove possono essere presenti gli operai.

Tuttavia, nell'industria 4.0 e, in particolare, nella cosiddetta Industrial Internet of Things (IIOT) gli oggetti che compongono la **fabbrica** hanno una caratteristica in più: sono connessi attraverso protocolli aperti (appunto quelli del **mondo Internet**) diversamente da quelli tradizionali che comunicavano, spesso in maniera molto elementare, attraverso protocolli proprietari. Questo, certamente, li rende flessibili perché sono raggiungibili, configurabili e impiegabili **"quando serve"**e **"da dove serve"**; d'altra parte, la connessione attraverso protocolli ben noti aggiunge una vulnerabilità cui è necessario far fronte affinché siano ridotte le probabilità che una minaccia possa sfruttarla per fare danni (a persone e a cose).

ENISA, nell'affrontare questo problema, ha ritenuto di indicare le prossime sfide connesse a questo tema e di fornire alcune raccomandazioni per i soggetti interessati. Il documento, molto snello, pubblicato il 20 maggio 2019 con il titolo *"Industry 4.0 - Cybersecurity Challenges and Recommendations"*[3], riepiloga le azioni che dovrebbero caratterizzare il mondo della Smart Manufacturing con riguardo alle tre componenti essenziali delle realtà produttive moderne: le persone, l'organizzazione e la tecnologia.

Le persone

La prima sfida riguardante le persone è la necessità di stimolare e allineare la competenza e la consapevolezza tra la sicurezza operativa (OT) e la sicurezza informatica (IT). La maggior parte delle persone che lavorano negli ambienti manifatturieri sono abituate a maneggiare la strumentazione pensando soprattutto a evitare comportamenti che possano comprometterne l'operatività immediata, trascurando che esistono aspetti IT che possono causare danni molto più gravi. Per esempio, per l'accesso al pannello di configurazione di un robot, utilizzare una password facile da ricordare e messa in comune tra tutti gli operatori ha il vantaggio di garantire, in modo semplice, la continuità di governo e funzionamento; ma, al tempo stesso, potrebbe costituire un elemento di debolezza che aumenta il rischio per l'intero sistema produttivo e per la stessa sicurezza delle persone (ancora, *safety*).

L'ENISA, quindi, raccomanda di curare questo aspetto promuovendo una **conoscenza trasversale** tra sicurezza OT e sicurezza IT, sia attraverso interventi formativi specifici per gli operatori già impiegati in azienda sia attraverso la diffusione della sicurezza IT nei curricula accademici rivolti agli studenti.

La seconda sfida riguarda le persone che, in azienda, ricoprono incarichi di alta responsabilità. In molti casi, il top management ha scarsa sensibilità verso la sicurezza IT: la considera un costo aggiuntivo sia per gli investimenti necessari sia perché credono che i meccanismi di sicurezza informatica rallentino i ritmi produttivi. Molte aziende manifatturiere, per esempio, si sono affidate a soluzioni *cloud* pubbliche per i loro impianti facendo prevalere l'immediata riduzione dei costi e non tenendo conto dei rischi che sono connessi a questo tipo di tecnologia.

L'ENISA ritiene che l'avvio di specifiche campagne di incentivazione all'investimento in cybersecurity da parte degli organismi governativi possano convincere molti top manager a pianificare interventi in questo ambito.

L'organizzazione

Dal punto di vista dell'organizzazione dell'intero sistema Industry 4.0, l'ENISA vede uno specifico problema nella scarsa attenzione degli operatori a identificare le responsabilità, contrattuali e di altro tipo, nel corretto funzionamento della strumentazione, anche rispetto ad eventuali minacce IT. Nello *smart manufacturing*, infatti, ogni elemento è frutto della cooperazione di molti attori: chi produce le componenti hardware, chi le assembla, chi realizza il software, chi lo vende, chi fa manutenzione, ecc. Ma quali di questi è responsabile per **eventuali vulnerabilità** che dovessero essere sfruttate da una minaccia?

L’appello dell’ENISA, per questa sfida, è ai soggetti governativi, nazionali ed internazionali: occorre stabilire un quadro normativo che indichi chiaramente quali sono le responsabilità di ciascun **attore** in caso di eventi sfavorevoli che possano incidere sulle persone o sul patrimonio dell’azienda utilizzatrice dei dispositivi *smart*.

ENISA prende atto, inoltre, che esistono standard di sicurezza IT molto frammentati nel mondo dell’industria 4.0. È necessario un impegno internazionale per uniformare i **comportamenti** che sono attesi dalla strumentazione intelligente con riguardo alla loro capacità di reazione a tentativi di attacchi informatici o a situazioni di possibili alert.

La tecnologia

In realtà, la standardizzazione appare come una questione **di confine** tra gli aspetti organizzativi e gli aspetti tecnologici. E lo riconosce anche l’ENISA che, tra le sfide tecnologiche, inserisce quella della necessità di rendere interoperabili le singole componenti dei sistemi industriali *smart*. È noto, infatti, che per garantire la sicurezza di un sistema non basta che sia ridotto al minimo il rischio per ciascun componente, ma è necessario che ciascun componente possa validamente interagire con gli altri per evitare il propagarsi della minaccia.

Anche in questo caso, è raccomandabile che siano definiti appositi criteri e protocolli di interoperabilità, anche attraverso la classica impostazione **a livelli** che incapsuli adeguatamente i comportamenti dei sistemi *legacy* operanti nelle realtà manifatturiere.

Un reale problema di natura strettamente tecnologica, invece, risiede nei limiti - economici e costruttivi - che alcune componenti devono avere: dimensione, peso, costi di manutenzione, ecc. Questi limiti incidono indubitabilmente sulla possibilità di integrare funzionalità di sicurezza IT evolute e anche sulla possibilità di rimuovere vulnerabilità che vengono alla luce nel tempo. È chiaro che, in questo caso, non ci sono raccomandazioni valide per tutte le fattispecie applicative e, quindi, ENISA indica, per ogni operatore economico, la strada di un approccio sistematico all’analisi del rischio e alla conseguente valutazione costi?benefici per comprendere quale assetto tecnologico convenga adottare a supporto del proprio modello di business.

Quali soggetti responsabilizzare

ENISA, nel fornire le raccomandazioni per ciascuna delle sfide esplorate, individua i soggetti che hanno l’onere di applicarle, così come sintetizzati nella tabella sottostante.

Soggetto interessato Raccomandazione	**Esperti di industria 4.0**	**Operatori economici di Industria 4.0**	**Organi regolatori**	**Comunità di stan dardizzazione**	**Centri d e svilup**
Promozione della consapevolezza trasversale *OT/IT security*	SI	SI	–	–	SI

Incentivazione degli investimenti in sicurezza IT	–	SI	SI	–	–
Definizione delle responsabilità tra gli attori di Industry 4.0	–	SI	SI	–	–
Armonizzare gli standard di Industry 4.0	–	–	SI	SI	–
Stabilire le basi di interoperabilità con criteri di sicurezza	SI	SI	SI	SI	SI
Bilanciare i limiti fisici delle componenti *smart* con le vulnerabilità conseguenti	SI	SI	–	–	–

Questo ci dice che, per lo *smart manfacturing*, occorre uno **sforzo globale**: difficile e complesso ma, almeno nel medio periodo, non impossibile.

Note

[1] https://www.enisa.europa.eu/.

[2] https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot/at_download/fullReport.

[3] https://www.enisa.europa.eu/publications/industry-4-0-cybersecurity-challenges-and-recommendations.

Articolo a cura di **Francesco Maldera**