Industria 4.0 e i rischi per la sicurezza dei dati.
1^ parte - Il punto della situazione

intervista a Ugo Gecchelin – Ingegnere, Innovation Manager, UNI/UNINFO CT 519 e CT526, e Stefano Ferrari – ingegnere, Innovation Manager and Security Consultant

Industria 4.0 e protezione dei dati, un fronte forse messo in secondo piano sul piano mediatico dalla tutela dei dati personali ma di essenziale rilevanza per l'economia e la sicurezza dell'intero Sistema Paese. Possiamo fare il punto sui rischi derivanti dalla Trasformazione Digitale dei processi industriali?

Le aziende che entrano nella logica del Piano Industria (e Impresa) 4.0 ed ora nel nuovo "Piano Transizione 4.0" acquisiscono dati dagli impianti, dalle macchine, dalla strumentazione di controllo, dai sensori, dai dispositivi IoT e li elaborano con software dedicati quali MES, ERP, sistemi di gestione e di controllo e altro, li analizzano con strumenti sempre più affinati e li archiviano. I dati sono in quantità sempre maggiore: non a caso si parla di Big Data e sempre più spesso vengono utilizzate soluzioni in Cloud.

Più passa il tempo e più le aziende diventano strettamente dipendenti da questi dati e, di conseguenza, devono essere sempre più attente al rischio della loro perdita. Non si ragiona più solamente in termini di "sicurezza IT" *(Information Technology)*, ma si deve considerare la "sicurezza OT" *(Operational Technology)*, cioè *"l'insieme di hardware e software che rileva o causa cambiamenti attraverso il monitoraggio o il controllo diretto di dispositivi fisici, processi ed eventi di un'impresa"* (https://www.gartner.com).

I termine **sicurezza OT** è ormai comunemente usato per elencare un vasto insieme di strumenti, inclusi quelli **ICS** *(Industrial Control Systems)* e **SCADA** *(Supervisory Control And Data Acquisition)*.

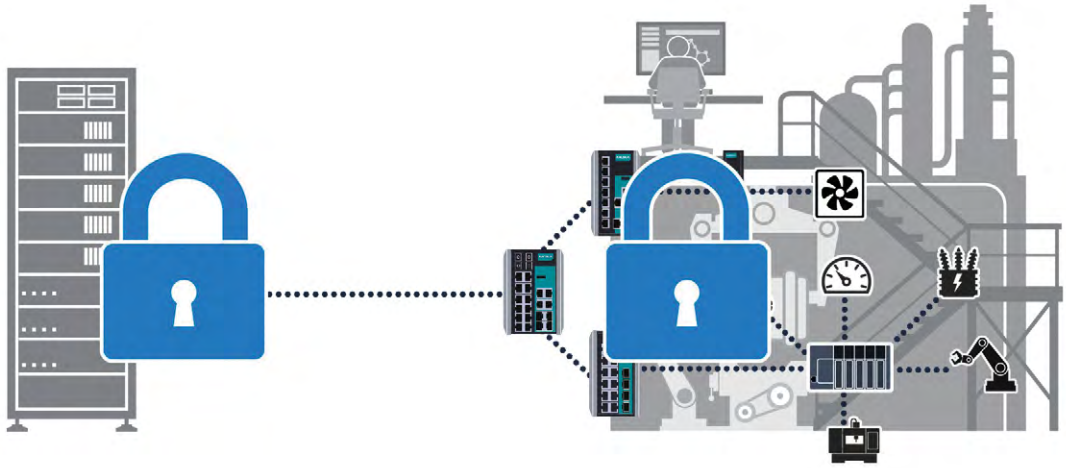
La sicurezza OT si concentra sulla difesa della **sicurezza fisica** *(security)*, dell'**affidabilità** *(reliability)* e della **produttività** *(productivity)*, parametri evidentemente diversi da quelli della sicurezza informatica.

Quando si tratta di sistemi OT è necessario considerare anche elementi come:

- *comportamento del sistema in caso di assenza di alimentazione*
- *comportamento del sistema in fase di avvio o riavvio e in fase di spegnimento*
- *separazione completa dei sistemi di sicurezza fisica dagli altri sistemi*
- *presenza sulla rete di dispositivi obsoleti e non più mantenuti dal produttore*
- *condivisione dei macchinari tra più operatori*
- *necessità di accesso in situazioni di emergenza*
- *protezione dai fattori ambientali (polvere, calore, ecc.)*

> ***"Il punto di arrivo deve essere l'integrazione della sicurezza IT/OT, senza la quale oggi un'impresa può davvero rischiare tantissimo in termini di continuità della propria attività"***

Il punto di arrivo deve essere l'integrazione della sicurezza IT/OT, senza la quale oggi un'impresa può davvero



rischiare tantissimo in termini di continuità della propria attività. Questo processo di convergenza tra il mondo IT e quello OT è sempre più necessario per affrontare e implementare la trasformazione digitale: l'avvento del paradigma di **Industria 4.0** e la sempre maggiore diffusione dell'**IoT** *(Internet of Things)* anche in campo industriale presuppongono da un lato l'interconnessione di sistemi e dispositivi di produzione originariamente non progettati per essere connessi; dall'altro, l'integrazione in rete di sensori e macchinari che generano e scambiano enormi moli di dati in tempo reale.

È poi necessario considerare che i sistemi OT, come i cosiddetti ICS, hanno spesso un ciclo di vita molto lungo, a differenza di quelli IT, e si tratta nella maggior parte dei casi di sistemi proprietari, in cui sono stati progressivamente integrati sviluppi IT. Inoltre, sui sistemi industriali sono sempre più frequentemente installati strumenti di amministrazione remota *(Remote Access Tool)* che permettono a terzi di accedere da un computer remoto attraverso internet o attraverso un network locale, per svolgere poi determinate attività di manutenzione o gestione del sistema senza doversi recare di persona sull'impianto.

Tutti gli elementi menzionati contribuiscono, dal punto di vista della security, ad aumentare i rischi, ampliando enormemente la superficie di attacco e creando un panorama complesso e intricato, in cui le minacce indirizzate alle infrastrutture critiche e ai sistemi ICS e SCADA sono in continua crescita.

"le possibili ripercussioni di un attacco in ambito industriale possono avere un impatto diretto sulla produzione o addirittura sulla safety umana e/o ambientale"

Il mondo OT, che fino a pochi anni fa era isolato e inaccessibile, è ora esposto a rischi per i quali non era preparato, che mettono a repentaglio la sicurezza dell'intera supply chain. La sicurezza in ambito industriale acquisisce una rilevanza ancora maggiore considerando che riguarda sistemi in grado di operare direttamente sul mondo "fisico": le possibili ripercussioni di un attacco possono avere un impatto diretto sulla produzione o addirittura sulla safety umana e/o ambientale.

Tutto ciò con le minacce che continuano a moltiplicarsi e a evolversi, ampliando in modo esponenziale i fronti che le aziende devono presidiare. Di certo i rischi sono incomprimibili, spesso inevitabili, e si ha la sensazione che possano causare danni sempre più consistenti al conto economico e alla reputazione delle imprese che non riusciranno ad adottare adeguate contromisure.

Semplici esempi come l'aumento delle forze che può sprigionare un macchinario fino a raggiungere livelli pericolosi oppure l'abbassamento della temperatura di cottura fino a provocare contaminazioni alimentari evidenziano come gli attacchi informatici possano danneggiare il sistema industriale e generare rischi personali.

Sul piano pratico, quali convergenze si possono verificare per la sicurezza dei dati "industriali" con quella dei dati "personali"?

Il concetto di "dato personale" non si ferma ai soli nome e cognome, ma coinvolge un universo di informazioni scaturenti dalle nuove tecnologie digitali, come:

– *biometria: dati legati al fisico come impronte e riconoscimento facciale*
– *geolocalizzazione: non solo mezzi ma anche persone, dispositivi e prodotti*

– *cloud computing: archiviazione e condivisione di dati di ogni genere sulla nuvola*
– *videosorveglianza: dati che coincidono con le immagini*
– *Internet of Things: la connessione di oggetti rende disponibili moltissime informazioni*

Si pensi anche al Digital Marketing: le organizzazioni hanno aumentato velocemente la possibilità di rilevare i dati, le preferenze dei clienti e le tendenze dei mercati. Contemporaneamente, questo grande vantaggio concorrenziale espone le aziende maggiormente alle minacce cibernetiche. La conseguenza naturale è che i dati sensibili e la reputazione online dell'azienda debbano essere protetti mediante nuove strategie per fornire informazioni, best practice e linee guida mirate per evitare i rischi e reagire tempestivamente alle minacce cibernetiche

Con l'aumento dell'utilizzo dell'intelligenza artificiale, delle app mobili, dei social e di una grande quantità di informazioni contenenti dati sensibili gestiti attraverso ambienti Cloud o soluzioni ibride, la vulnerabilità ad attacchi interni e/o esterni è cambiata. Fino all'arrivo di questi strumenti, i dati e le infrastrutture critiche erano stati relativamente protetti dagli hacker perché posizionati in ambienti sicuri all'interno dell'IT tradizionale.

Con l'arrivo di tutti questi nuovi strumenti originato dalla *Digital Transformation* di aziende e servizi, la situazione si è capovolta. Lo stesso vale per l'ambito dell'applicazione dei temi Industria 4.0 dove è prevista una convergenza estesa tra i sistemi che governano dispositivi, impianti e infrastrutture critiche industriali e i sistemi dell'IT tradizionale.

Il problema maggiore nella gestione della sicurezza in ambito industriale è che cambia l'oggetto della protezione. Non si tratta infatti solo di proteggere un dato ma delle funzioni, dei processi fisici, e, ad oggi, non esistono ancora metodologie standard né un quadro concettuale coerente ed unificato per trattare questo argomento.