Industria 4.0 e i rischi per la sicurezza dei dati. 2^ parte - Il quadro normativo

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

Qual è il quadro normativo per la tutela dei dati "industriali"?
Possiamo prendere come riferimento due standard:
– ISA 99/IEC 62443
– ISO/TR 22100-4:2018

L'**ISA** *(International Society of Automation)* ha creato lo standard **IEC 62443** con l'intenzione di rendere le infrastrutture **IACS** *(Industrial Automation Control Systems)* sicure rispetto alle minacce informatiche.
Questo standard, che definisce i requisiti fondamentali per la sicurezza informatica e indica le misure da adottare mediante una valutazione del rischio informatico per proteggersi da diversi tipi di attacchi, è largamente diffuso e fortunatamente la richiesta di adeguamento sta crescendo.
Proteggere le singole apparecchiature da manipolazioni senza compromettere le funzionalità degli impianti viene esplicitato in una serie di indicazioni che sono presenti da decenni nell'informatica ma, solo recentemente, hanno preso piede nella progettazione e nell'esercizio di impianti industriali.
L'impatto della norma IEC 62443 può apparire come un aumento della complessità degli impianti industriali e del relativo costo di esercizio, ma non va sottovalutato il grande vantaggio di mitigare i rischi legati a manomissioni e danni anche accidentali.

Da parte sua, l'ISO ha pubblicato nel dicembre 2018 un rapporto tecnico (TR) che consente ai costruttori di gestire e limitare tali rischi. In questo rapporto vengono indicate importanti raccomandazioni che il costruttore del macchinario deve considerare per immettere sul mercato un macchinario sicuro anche da eventuali attacchi informatici quali, ad esempio:
– *l'utilizzo di componenti hardware e software con altissimi livelli di sicurezza e con specifiche funzionalità all'avanguardia, al fine di mitigare o ridurre al minimo la vulnerabilità degli incidenti*
– *l'integrità del software e dei dati*
– *le comunicazioni criptate*
– *gli aggiornamenti*
– *l'adozione di specifiche misure durante la progettazione della macchina come la separazione del sistema IT rilevante per la sicurezza dal sistema IT dell'intera macchina*
– *l'adozione di firewall e strumenti antivirus*
– *la riduzione della complessità del sistema IT*
– *la predisposizione di istruzioni operative (manuali d'uso e manutenzione) rivolte agli operatori, contenenti indicazioni sulle minacce e i problemi a cui l'impianto potrebbe essere esposto durante il suo utilizzo e sulle relative misure fornite dal costruttore per cercare di governarli oltre alla formazione continua degli operatori stessi*

Dal suo punto di osservazione, qual è il livello di consapevolezza nel sistema industriale italiano di questi rischi?
Purtroppo non molto alto, nonostante vi siano stati da tempo alcuni casi importanti. Ricordiamo già nel 2017 quello della **Maschio** oppure l'attacco informatico del 2019 al colosso dell'alluminio **Norsk Hydro**. In quest'ultimo caso, l'azienda è stata vittima di un attacco hacker a partire dalla sera e prolungatosi per tutta la notte. Un ransomware (che ha bloccato sistemi, con richiesta di riscatto) ha preso di mira i sistemi IT del gruppo, interessando le varie sedi nel mondo. L'attacco ha dapprima spento i server, quindi

i computer per poi arrivare fino prendere il controllo di alcune linee di estrusione. L'azienda ha dovuto chiudere alcune linee di produzione fino a dover fermare gli impianti di trasformazione dei metalli. È stato quindi necessario comandare manualmente gli impianti di estrusione, con evidenti conseguenze. Non vi è stato alcun rischio per la salute dei lavoratori, ma sicuramente si sono subite ricadute sulla produzione e sui clienti (all'apertura del mercato, il giorno dopo l'attacco, il titolo in borsa del gruppo ha perso valore).

Recenti ricerche del Politecnico di Milano *(Osservatorio di Information Security e Privacy)* riportano infatti che la conseguenza più temuta dalle organizzazioni è l'eventuale fermo parziale o totale della produzione (ma solo per il 54%), che può costituire sia l'obiettivo diretto e primario di un eventuale attacco, sia rappresentare invece una ripercussione secondaria. Tra le conseguenze più rilevanti si trova poi la safety (20%), requisito reso particolarmente critico dall'interazione sempre più diretta tra operatori e macchine (es. robotica collaborativa) o, ancora, una possibile alterazione o modifica della produzione (16%), con motivazioni riconducibili al sabotaggio. È invece considerata meno rilevante in questo ambito la possibilità di furto, perdita o divulgazione di dati confidenziali (10%), principalmente riguardanti la proprietà intellettuale.

Cosa si sta facendo ma, soprattutto, cosa si dovrebbe fare per migliorare la situazione?

Mentre un tempo tutti i dati di "officina" giravano su carta o su biglietti, oggi tutto gira sulla dorsale di fabbrica, con le macchine che dialogano con altre macchine.

È innegabile che, per affrontare bene una materia, è necessario capirne la cultura di fondo. Questo vale, per esempio, quando si tratta di sicurezza delle informazioni (orientata alla protezione di un'organizzazione), di sicurezza dei dati personali (orientata alla protezione degli interessati) o di qualità del servizio informatico (orientata alle aspettative del cliente). Ogni materia ha le sue peculiarità e queste vanno capite e apprezzate prima di farle "convergere".

"È sicuramente importante che le aziende ed il loro management prendano coscienza degli effettivi rischi, anche se gli investimenti in soluzioni di sicurezza informatica per lo Smart Manufacuring continuano a crescere, ma non al ritmo con cui si moltiplicano le minacce"

È sicuramente importante che le aziende ed il loro management prendano coscienza degli effettivi rischi, anche se gli investimenti in soluzioni di sicurezza informatica per lo Smart Manufacuring continuano a crescere, ma non al ritmo con cui si moltiplicano le minacce. Occorre aumentare la consapevolezza sugli strumenti a disposizione delle imprese e soprattutto puntare su formazione e R&S.

È quindi fondamentale che le misure di cybersecurity mantengano il passo con le novità tecnologiche, per garantire alle organizzazioni coinvolte che i possibili benefici vadano oltre i rischi. Le aziende devono occuparsi con maggior serietà dei programmi di risposta agli incidenti ICS, per evitare il rischio di gravi danni operativi, economici e reputazionali. Solo sviluppando uno specifico programma *"incident response"* e utilizzando soluzioni di cybersecurity dedicate per gestire la complessa natura degli ecosistemi industriali connessi e distribuiti, le aziende potranno tenere al sicuro i servizi, i prodotti, i clienti e il loro ambiente produttivo.