Il Sole 24 ORE RAPPORTI24/IMPRESA

Settimanale

Data 15-05-2018
Pagina 17+19
Foglio 1

Sicurezza informatica / 2

Contro i rischi spazio alla ricerca

di **Alberto Calvo**
e **Marco De Bellis**

La prima ondata di investimenti innescata dal piano Industria 4.0 (ora Impresa 4.0) è stata indirizzata, essenzialmente, a costruire l'architettura digitale primaria dei processi manifatturieri, con l'installazione di reti di sensori collegati tra loro e la predisposizione di sistemi per la raccolta e l'elaborazione di grandi volumi di dati di produzione. In questa fase si è prestata tuttavia ancora poca attenzione all'"intelligenza" necessaria per estrarre valore dai dati a beneficio dell'efficacia e dell'efficienza dei processi, mentre si registra una quasi totale assenza di sensibilità e consapevolezza sulle implicazioni di sicurezza informatica derivanti dalla svolta hi-tech.

Continua ▸ pagina 19

STRUMENTI
È importante avviare programmi di ricerca applicata per sfruttare la convergenza di tecnologie innovative per il miglioramento della security in ambito Industria 4.0: si pensi, ad esempio, alla blockchain

Sicurezza informatica

Contro i rischi spazio alla ricerca

di **Alberto Calvo**
e **Marco De Bellis**

▸ Continua da pagina 17

Le reti di comunicazione tra i sensori, gli stessi oggetti intelligenti e le piattaforme di acquisizione ed elaborazione dati costituiscono un ampliamento importante della "superficie di contatto" dei sistemi Ict che oggi può essere oggetto di ampi attacchi informatici. Sensori e oggetti intelligenti, infatti, essendo connessi tra loro e interagendo con l'uomo, comportano lo scambio di informazioni spesso sensibili, che possono essere illegalmente acquisite attraverso operazioni di hacking, un fenomeno in forte crescita. I dati sensibili possono riguardare alcune competenze cruciali all'interno dei processi di produzione o addirittura sono segreti industriali e, come tali, rappresentano un asset che qualsiasi organizzazione dovrebbe tutelare con adeguate misure di sicurezza.

La possibilità di inserirsi illecitamente nei sistemi di comunicazione dell'Industrial Internet of Things può poi esporre le organizzazioni a rischi ancora superiori rispetto al furto di know-how: si pensi alla possibilità di effettuare operazioni di sabotaggio per interrompere interi cicli di produzione e danneggiare sistemi concorrenti, Paesi stranieri etc.

Peraltro i rischi di blocchi produttivi non sono soltanto correlati a possibili operazioni illecite, ma dipendono altresì dalla maggiore complessità tecnologica intrinseca dell'Industria 4.0. È quindi evidente che le indubbie opportunità determinate dalla "quarta rivoluzione industriale" debbano essere colte considerandone, a più livelli, anche i profili di rischio.

Dal punto di vista normativo-regolamentare in alcuni Paesi sono in fase di definizione linee-guida specifiche nell'ambito delle aree di rischio: ad esempio l'"Internet of Things Cybersecurity Improvement Act del 2017" è stato varato dal Senato Americano per disciplinare i profili di sicurezza dei device prodotti per il Governo. È quindi auspicabile che vengano adottate misure, possibilmente con copertura internazionale, che concorrano a definire e imporre standard di sicurezza che debbano essere rispettati dai produttori di smart device, da chi progetta reti di comunicazione IIoT e sviluppa progetti d'integrazione.

È importante allo stesso modo che vengano avviati programmi di ricerca applicata per sfruttare la convergenza di tecnologie innovative per il miglioramento della security in ambito Industria 4.0: si pensi, ad esempio, alla blockchain (nota come sistema per la gestione delle transazioni di criptovalute), che può rappresentare uno strumento estremamente efficace per "certificare" le comunicazioni tra oggetti intelligenti e per prevenire duplicazioni illecite di dati. Abbiamo già alcuni esempi virtuosi, e significativi, d'impiego congiunto di queste tecnologie per l'incremento dell'efficacia e dell'efficienza dei processi di supply chain. Uno di questi è Maersk, player mondiale della logistica: ha digitalizzato il processo di gestione e tracking delle spedizioni dei container consentendo a tutti gli attori coinvolti (clienti, trasportatori marittimi, dogane, autorità portuali ecc.) di avere visibilità, in tempo reale, di tutti gli eventi della supply chain in modo sicuro e in ragione dei privilegi di ciascuno. Un altro caso è quello di Toyota, che ha sviluppato un programma basato su IoT e blockchain per ottimizzare e rendere più sicuro il processo di gestione dei componenti per la costruzione di un'auto, provenienti da differenti nazioni e fabbriche, attraverso passaggi intermedi intrinsecamente critici.

Sono casi al cui successo hanno contribuito in modo decisivo la disponibilità di competenze distintive. Infatti la complessità dei sistemi Ict sui cui si basa l'Industria 4.0, compresi quelli relativi alla gestione della sicurezza, determina la necessità di avere a disposizione dell'intero ecosistema specifiche figure professionali, delle quali in Italia si registra attualmente una carenza rilevante (si calcola un deficit di 500mila-1milione di unità entro il 2029). È fondamentale quindi che il sistema industriale possa investire in modo consistente nella formazione di questi profili nuovi, accelerandone il percorso di maturazione, facendo affidamento su adeguati strumenti contrattuali per il loro inserimento nelle aziende e favorendone la mobilità internazionale: oggi i centri di competenza più interessanti in questo ambito si trovano in Germania, Corea, Giappone e Cina.

Questo impegno è in verità un fatto strategico, perché la nostra storia e la nostra cultura industriale devono passare necessariamente attraverso questa evoluzione per poter continuare a tramandare tutta la loro ricchezza.

Alberto Calvo è partner Value Partners Management Consulting; Marco De Bellis è partner Exage