Cyber security e Industria 4.0

Date : 15 febbraio 2017

Sempre più nel mondo manifatturiero si stanno affermando i concetti di Industrial Internet ed Industria 4.0. I due termini non sono sinonimi: di “Industrial Internet” ha iniziato a parlare nel 2012 Marco Annunziata, Chief Economist ed Executive Director of Global Market Insight di General Electric, indicandola come il luogo in cui avviene la convergenza tra l’industria e le possibilità fornite dai sistemi di gestire “big data”, fare analisi, raccogliere informazioni da tutti gli ulteriori sensori che è possibile connettere ed integrare, grazie proprio alla connettività messa a disposizione da Internet.

Il termine Industria 4.0 (in realtà Industrie 4.0, in tedesco) è stato invece usato in Germania dal 2011 come espressione per definire nuovi scenari per le “smart factory” nei quali modelli organizzativi innovativi e modulari sono coadiuvati da una estesa digitalizzazione a supporto ed integrazione delle attività umane e di quelle automatizzate per aumentare la catena del valore, anche all’esterno del perimetro della fabbrica.

Quando internet scende in fabbrica

Siamo abituati a sentir parlare di IT, Information Technology. Ma quando si parla di industria la parola chiave è OT, Operational Technology, che rappresenta l’insieme di tutti i “sistemi intelligenti” che gestiscono informazioni dell’impianto.

Pensare di affrontare la questione della security dei sistemi industriali con lo stesso approccio finora impiegato nelle soluzioni “business” sarebbe un errore. Se in ambito IT i principi base della Cyber security definiscono un dato sicuro quando sono rispettati i criteri RID (Riservatezza, Integrità, Disponibilità), in ambiente OT l’ordine di questi tre fattori va letto al contrario: le caratteristiche irrinunciabili sono infatti “Disponibilità” ed “Integrità”, mentre la Riservatezza è quasi un parametro accessorio. Un sistema infatti deve essere innanzitutto essere “Always On” e dunque, a seconda dell’utilizzo più o meno critico, la disponibilità del sistema deve prevedere anche la Fault Tolerance. Questo significa avere sistemi ridondati a caldo (almeno 2 attivi in parallelo) e tempi di ripartenza ridoti al minimo.

L’Integrità del dato, invece, si può ottenere solo adottando soluzioni software pensate e sviluppate per garantire affidabilità nella catena di gestione del dato (dal sensore allo schermo

del computer), una completa tracciabilità degli accessi e una precisa registrazione (eventualmente anche con sistemi di doppia firma elettronica o similari) in caso di variazioni o correzione di dati o valori (anche con un log ed Audit Trail)

Una logica conseguenza di questi principi è che in ambito industriale vanno utilizzate soluzioni espressamente pensate per questo scopo. Il mercato propone oggi dispositivi intelligenti con funzioni IPS/IDS, Firewall, Antimalware e soprattutto dotate di avanzate funzioni di filtraggio, application/protocol/datapackage White-Listing ed Anomaly detection: le uniche tecniche che si sono dimostrate veramente efficaci nel contrastare problemi di security su reti e sistemi di controllo e telecontrollo in molti settori industriali.

Si è infatti dimostrato inefficace il semplice utilizzo di Firewall pensati per le applicazioni web ed IT tradizionali, in quanto non è agevole definire regole per le connessioni ed il filtraggio dei dati che possano essere valide anche per il mondo dell'OT (Operation Technology): porte, protocolli e regole sono infatti diverse e tipiche dei dispositivi collegati alla rete di impianto e dei sistemi di controllo e telecontrollo. Come diverse sono le competenze richieste per capire e quindi proteggere in modo adeguato le applicazioni OT in reti di automazione, controllo e telecontrollo dai rischi informatici nell'industria e nelle Infrastrutture Critiche.

Ransomware anche per l'industria

Il ransomware è stata una delle minacce informatiche più diffuse nel 2016. Il pensiero comune è che le vittime siano solo consumatori inesperti, facile preda delle mille trappole di cui è popolata la rete. La realtà è ben diversa: Cryptolocker e le sue mille varianti hanno letteralmente funestato anche le aziende.

È capitato, per esempio, lo scorso mese di gennaio ad un'impresa del settore alimentare, che si è vista bloccare l'applicazione di supervisione e monitoraggio dei macchinari di un impianto di produzione. Che cosa era successo?

La rete di stabilimento era "piatta", con scarsa segmentazione e senza segregazione degli asset critici (PC/Server di fabbrica). Sulla stessa rete erano collegati anche i PC per la posta ed altri applicativi, con accesso a internet. E così è bastato che un impiegato dell'amministrazione aprisse un allegato denominato "fattura" per scatenare la violenza del ransomware (una delle molteplici e sempre più raffinate versioni di Cryptolocker), che ha criptato i file di tutti i dischi dei PC con risorse condivise.

Tra questi dischi c'era anche quello del server SCADA (il software per la supervisione delle macchine), che era collegato alla rete office al fine di poter produrre e scaricare reportistica sull'andamento dell'impianto.

Il server SCADA, che lavora con routine contenute nella RAM, ha continuato a funzionare, ma su questo computer non era più possibile cambiare schermate: in altre parole, il sistema era praticamente bloccato. È stato così necessario provvedere allo spegnimento dei sistemi per la bonifica dei computer. Siccome l'ultimo back-up degli applicativi e della configurazione

installata era “datata” una parte delle ultime variazioni applicative è andata persa. Sono risultati inutilizzabili anche i file delle licenze dei software installati e sono andati persi gli ultimi dati storici e gli allarmi raccolti dopo l’ultimo back-up.

In sintesi, il danno è difficilmente calcolabile, tra tempo di fermo macchina, costi diretti per consulenti e componenti da sostituire, costi indiretti dovuti alla mancata produzione, alla cancellazione dei lotti, all’impossibilità di produrre e alla lesa reputazione.

Lessons learned? La base di ogni sistema “sicuro” (anche se nessuna architettura può ritenersi al sicuro al 100%) sono le policy: non si può certo dare la colpa solo all’impiegato dell’amministrazione che ha aperto l’allegato. Bisogna essere pronti e avere sempre un piano B: sapere, insomma, come ripartire in fretta e senza perdere dati.

Proteggersi dai cyber-rischi

L’incidente o il danno – lo abbiamo visto – possono essere dietro l’angolo: una recente analisi di SANS (SANS 2016 State of ICS Security Survey) sullo stato della security dei sistemi di controllo industriale (ICS, Industrial Control Systems) indica che il 42% delle minacce ai sistemi arrivano dall’interno delle organizzazioni. In questa cifra rientrano quelle intenzionali – i sabotaggi – che rappresentano oltre il 10% del totale; quelle non volute (errori degli operatori dovuti a scarsa competenza oppure a sistemi di interfacciamento non chiari), che pesano per oltre il 15%; o ancora i problemi derivanti da malfunzionamenti o da non accurata integrazione IT/OT (circa il 10%).

Quale che sia la causa, è evidente che con il diffondersi dell’IoT (che in ambito industriale diventa IIoT, Industrial Internet of Things) ogni dispositivo, sensore, server, client di visualizzazione o periferica è un potenziale punto di accesso. Soprattutto nelle architetture non presidiate (tipiche delle vaste Reti di Distribuzione) non si può rischiare che un “single point of failure”, l’anello debole della catena, comprometta la sicurezza dell’intero sistema: è bene perciò segmentare la rete, creare compartimenti stagni entro i quali isolare l’attacco o il problema. Un primo passo potrebbe quindi essere quello di “proteggere” l’impianto e l’infrastruttura sistemistica esistente mediante l’utilizzo di dispositivi da considerare come presidi di security secondo il modello proposto proprio dallo standard ISA99/IEC62443 per segmentare la rete in “Zone” e segregare asset critici (RTU/PLC e server) concedendo la connessione solo attraverso “Conduit” logici controllati e filtrati.

Un modo adeguato e migliore di procedere sarebbe adottare i dettami previsti dal modello della “security by design”: progettando cioè il sistema, l’impianto e l’infrastruttura tenendo presenti le questioni rilevanti per la cyber security, mettendo al primo passo proprio una attenta analisi e valutazione del rischio: questo consente di concentrare gli sforzi nei punti in cui si riterranno le contromisure e gli interventi più efficaci ed urgenti. E soprattutto rivisitare periodicamente le scelte fatte per verificare se le contromisure adottate siano ancora adeguate ai rischi correnti.

Di grande aiuto poi risultano tecnologie come la virtualizzazione, il cloud, i Virtual desktop e i thin client che hanno mostrato come lavorare su credenziali e controllo accessi, sul traffico dati

in entrata e in uscita, sulla possibilità di eseguire backup temporizzati e ravvicinati sia strada assai più sicura di quella di creare un “perimetro invalicabile” come si tendeva a fare negli anni addietro.

A proposito del Cloud, vale la pena evidenziare che gli stessi fattori che costituiscono una “preoccupazione” per gli utenti in ambito business sono paradossalmente i punti di forza delle soluzioni in Cloud dell’industrial internet: eliminare o comunque ridurre all’osso la parte fisica di un’architettura di sistema contribuisce infatti a rimuovere l’errore umano dalle possibili modalità di attacco: chiavette infette o una navigazione non controllata difficilmente potranno ancora essere l’origine di una problematica di security. Attualmente molte attività per definire modelli e strategie per mettere in sicurezza le applicazioni in Cloud sono in fase di studio da parte di diversi attori e dobbiamo sicuramente menzionare documenti e standard rilasciati da CSA (Cloud Security Alliance).

Inoltre la possibilità di creare un elevato numero di immagini dei server online (prima era impossibile per non dire ingestibile: sarebbe stato necessario un numero di computer improponibile ed una sala server immensa) permette di programmare i backup del sistema anche a distanza molto ravvicinata, permettendo di recuperare dati e rimettere in piedi il sistema in tempi rapidissimi, anche con un occhio alla “resilienza”.

Le architetture con l’utilizzo di macchine virtuali aumentano la disponibilità e le prestazioni in caso di Disaster Recovery: una macchina sempre attiva o “dormiente” si riavvierà comunque più in fretta di un server tradizionale.

Oggi sul mercato sono disponibili anche tool software per rendere “Fault Tolerant” applicazioni HMI/SCADA con un livello di costi ed impegno tecnico assolutamente abbordabile anche per applicazioni di piccole e medie dimensioni con l’obbiettivo di renderle “always-on” fino anche al 99,9999% del tempo.

A cura di: **Enzo Maria Tieghi**