Home / Contenuti / Attrezzature e accessori / Investire in Cyber Security con uno sguardo rivolto al futuro

A+ A A-

Investire in Cyber Security con uno sguardo rivolto al futuro

dimensione font – + Stampa Email

A fine gennaio, presso il Grand Visconti Palace di Milano, si è tenuta la prima edizione di ICS Forum, mostra convegno dedicata alla sicurezza informatica in ambito industriale. Dall'incontro (che ha riscosso un grande successo di pubblico), è emersa chiara l'importanza assoluta del fattore umano come chiave di volta per una cultura diffusa nell'impresa che metta la sicurezza al centro dei processi aziendali. Durante i lavori, si è parlato anche di tecnologie in grado di rispondere in maniera efficace alle cyberminacce.

di Laura Alberelli

Marzo 2018

Lo scorso settembre, il presidente della Commissione Europea Jean-Claude Juncker ha inserito la Cyber Security tra le priorità assolute d'azione dell'organo da lui presieduto. Evidentemente, subire attacchi di hackeraggio non è più una probabilità remota ma è una minaccia concreta, soprattutto oggi dove - in piena era Industry 4.0 - qualsiasi dispositivo può trasformarsi da preziosa fonte di dati in un potenziale "pericolo", l'anello debole di una catena che consente ai cybercriminali di accedere alla rete aziendale. Quel che è certo è che il tessuto industriale - uno degli asset strategici più importanti e critici per un Paese - va sorvegliato e difeso. Se minacciato o compromesso da un attentato informatico, ingenti sarebbero infatti le conseguenze a carico dell'indotto produttivo con ripercussioni gravi anche sul Sistema Paese.
Per scongiurare scenari apocalittici, è però sufficiente adottare una strategia di protezione delle reti informatiche e dei sistemi di produzione? Siamo davvero sicuri che la minaccia più grande provenga dall'esterno e non dall'interno dell'azienda? In Italia, qual è il livello di conoscenza di queste problematiche? Quali sono le strategie difensive generalmente messe in atto e qual è il grado di

resilienza delle nostre imprese? Tante domande in cerca di risposta, e una certezza di fondo: mai come oggi, la cyber security è un tema caldo e di assoluta attualità. Per fare il punto della situazione e per aiutare imprenditori, tecnici e manager a orientarsi in questo mondo complesso e pieno di insidie, a fine gennaio Messe Frankfurt Italia ha organizzato a Milano - in collaborazione con Innovation Post - la prima edizione della mostra convegno ICS (Industrial CyberSecurity) Forum. ICS Forum ha ricevuto il patrocinio dell'Agenzia per l'Italia Digitale (AgID), dell'Associazione Italiana Professionisti della Sicurezza (A.I.PRO.S.), di ANIE Automazione, della Federazione delle Associazioni Nazionali dell'Industria Meccanica varia e affine (ANIMA), dell'Associazione Nazionale Italiana Per L'Automazione (ANIPLA), dell'Associazione Nazionale delle aziende ICT e digitali di Confcommercio – Imprese per l'Italia (Assintel), di Assolombarda Confindustria Milano Monza e Brianza, del Clusit, della Commissione Europea, di Confindustria Digitale, della Fondazione GCSEC e della Regione Lombardia. Grande affluenza di pubblico (oltre 500 partecipanti), a riprova del fatto che fare chiarezza sull'argomento è diventata una necessità impellente non più procrastinabile.

Sistemi per cyber sicurezza ma anche una pressante attività di monitoraggio

ICS Forum ha ospitato due tavole rotonde (una la mattina e una il pomeriggio) e quattro workshop che si sono alternati nell'arco della giornata. A moderare i due dibattiti sono stati rispettivamente Franco Canna (direttore di Innovation Post) e Jole Saggese (capo redattore di Class CNBC).

Ad Andrea Zapparoli Manzoni, esperto di cyber security nonché membro del comitato direttivo di Clusit (associazione italiana per la Sicurezza Informatica) è stato chiesto di illustrare con un breve video (lo specialista non era presente all'evento perché all'estero) la situazione attuale in materia di sicurezza informatica. "Mi spiace essere latore di brutte notizie, ma rispetto agli anni precedenti la situazione globale è peggiorata e in futuro la previsione è di un ulteriore aggravamento. Secondo i dati che presenteremo nel prossimo rapporto Clusit, l'aumento della criminalità informatica ha registrato un aumento a due cifre. Sfortunatamente, rispetto al passato non è solo il numero a essere cresciuto ma anche la gravità, l'intensità dell'attacco.

Parlando di imprese manifatturiere, la più grande minaccia che intravedo nel mondo IoT e Industria 4.0 è la sproporzione tra i vantaggi immediati dell'impiego di tecnologie e processi destinati a garantire la cyber sicurezza e la consapevolezza che queste stesse soluzioni si dimostrano estremamente fragili e attaccabili. Per rafforzare la barriera difensiva, è necessario affiancare un'azione di monitoraggio stringente, continuo, professionale e avanzato che deve coinvolgere tutti gli eventi che avvengono in rete. Al tempo stesso, è altresì importante tenere costantemente monitorati tutti i dispositivi e i macchinari utilizzati in azienda. Questo è l'unico modo di cui disponiamo per intercettare i segnali di allarme provenienti da un attacco in corso, gli unici che consentiranno all'azienda di mettere in atto le opportune procedure di difesa e di recovery. Per ottenere un certo tipo di risultato, l'azienda deve però investire in soluzioni performanti e di qualità, prediligendo solo quei produttori di tecnologia sicura e testata. Ciò vuol dire che non bisogna più considerare la sicurezza informatica come un costo, ma va vissuta come un investimento che a medio/lungo termine può garantire la sostenibilità del nuovo modello produttivo di Industry 4.0. Senza sicurezza, la filosofia produttiva propria dell'IoT rappresenterebbe uno dei più grandi rischi che la nostra società abbia mai corso".

Secondo Fabio Sammartino di Kaspersky (fornitore di soluzioni per una protezione premium contro virus e attacchi cybernetici e per la salvaguardia di tutti i dispositivi), la situazione non è però così drammatica come può sembrare. "Secondo una ricerca pubblicata da Shodan (motore di ricerca dedicato ai devices collegati al Web), nel 2017 in Italia sono stati hackerati circa 157 PLC connessi a Internet. Il dato in sé non è certo positivo, ma è anche vero che nella stessa ricerca è stato evidenziato che esistono altrettanti indirizzi IP che utilizzano lo stesso protocollo di protezione e che fanno riferimento a degli honeypot, meglio conosciuti come "trappole informatiche". Questo vuol dire che, al di là di tutto, c'è chi si sta comunque dando da fare per sviluppare sistemi dedicati alla cyber security".

Una convergenza sempre più stretta tra mondo IT e OT

Durante l'evento organizzato da Messe Frankfurt Italia molti addetti ai lavori hanno notato una convergenza sempre più stretta tra il mondo dell'Information Technology (IT) e quello dell'Operation Technology (OT). A detta di Antonio Madoglio di Fortinet (fornitore di soluzioni di cybersecurity ad alte prestazioni) "trasportare le esperienze maturate nel mondo IT al mondo OT non è poi così difficile. Ovviamente esistono differenze sostanziali di cui bisogna tenere conto. I protocolli utilizzati per il mondo IT sono diversi da quelli OT. Inoltre, il mondo OT si differenzia da quello IT per le caratteristiche ambientali. Alcuni dispositivi devono infatti poter gestire determinate sollecitazioni meccaniche o elettromagnetiche tipiche del mondo OT ma inesistenti nel mondo IT. Chi lavora con entrambi, sa che esistono punti di convergenza ma anche di divergenza che caratterizzano da sempre i due mondi e che vanno salvaguardati".

In termini di cyber security, quali sono i principali rischi legati al mondo OT? A dare una risposta è Dario Amoruso di KPMG (gruppo specializzato in Information Risk Management). "Se all'interno di una infrastruttura – IT od OT - si adottano una serie di misure tecnologiche in grado di bloccare l'attacco informatico, l'hacker farà più fatica a raggiungere il perimetro tecnologico che porta ai dispositivi di campo (dunque alla rete OT) o alla rete IT. Più difficile sarà invece difendersi dagli attacchi derivanti dal fattore umano (si pensi, ad esempio, alle operazioni di "fishing"). In questo caso, l'hacker attacca la vittima (la persona fisica) la cui reazione innescherà un meccanismo che gli permetterà di colpire il target mirato. Gli attacchi di social engineering sono tra i più numerosi e pericolosi. Per cercare di contrastare la minaccia del "fattore umano", la nostra azienda (così come fanno altre società che si occupano di risk management) realizza corsi di awareness in modo da garantire un certo grado consapevolezza e conoscenza. Poiché le tecniche di "fishing" stanno diventando drammaticamente sempre più sofisticate, oggi la formazione deve essere sempre più mirata e soprattutto smart".

FLASH NEWS

Una partnership al servizio dei clienti

Al fine di acquisire un vantaggio competitivo rispetto ai concorrenti, molti operatori nella lavorazione delle lamiere si mostrano interessati ad ampliare la propria offerta produttiva con operazioni di taglio tubi....

Sicurezza del network, delle tecnologie e delle persone

Dopo aver riportato le opinioni di società che in maniera diretta o indiretta si occupano di cyber security, pubblichiamo le testimonianze di alcune aziende del comparto della meccanica intervenute a ICS Forum, che adottano al loro interno protocolli per la sicurezza informatica.

"Nel corso degli anni, Siemens è una delle aziende che ha investito maggiormente in Cyber Security", ha spiegato Roberto Zuffrada durante il suo intervento in rappresentanza della società. "È necessario investire in sicurezza, non solo in sicurezza del network, ma anche in sicurezza degli apparati e in sicurezza delle persone che lavorano in azienda. Solo così si può andare verso il modello di Industry 4.0, dove la connessione tra uomini, network e device sarà totale. In cammino verso la Smart Factory è però solo all'inizio. Per raggiungere il risultato, c'è ancora tanto da fare".

In termini di Cyber Security, Siemens supporta i propri clienti attraverso la strategia di Defense in Depth - un concetto multistrato per gli utilizzatori industriali che garantisce una protezione degli impianti, delle reti e dell'integrità del sistema - secondo le norme ISA 99 ed IEC 62443 (gli standard più importanti per la sicurezza nel settore dell'automazione industriale).

Defense in Depth dimostra l'importanza di attuare una segmentazione delle reti, realizzando celle di protezione, con prodotti dedicati alla sicurezza di rete (firewall e router industriali). Altrettanto fondamentale sono la tracciabilità e la possibilità di verificare gli accessi sia in termini di edificio/fabbrica sia in termini di sistema, reti e macchine.

Parte dell'approccio Siemens alla sicurezza industriale è anche l'ampio portfolio di controllori e sistemi HMI con funzioni integrate di Security Integrated per la protezione su accesso multi-level, know-how e protezione dalla copia. Da segnalare anche i sistemi PC-based con funzioni di Security implementabili attraverso whitelistening Firewall, antivirus software e Security updates del sistema operativo, le soluzioni di motion control e drives con funzioni di sicurezza integrata e un DCS per la Process Automation in grado di salvaguardare la produttività del processo industriale, secondo l'Industrial Security Concept, basato sulle raccomandazioni di ISA 99 / IEC 62443.

È necessario un cambio di approccio anche da un punto di vista culturale

Proprio come Zuffrada, anche Roberto Motta di Rockwell Automation pensa che il modello di Industry 4.0 sia ancora lontano dall'essere concretizzato. "Fatta eccezione per alcuni casi, siamo molto distanti dal raggiungimento di un reale modello di interconnessione. Per andare in quella direzione, è necessario che le aziende modifichino il loro approccio, anche da un punto di vista culturale". Per rispondere alle richieste delle aziende che richiedono infrastrutture di informazione e di sicurezza, Rockwell Automation propone i Connected Services. Essi comprendono numerosi servizi quali la valutazione dell'infrastruttura di rete industriale esistente, la progettazione, l'implementazione, e il supporto e monitoraggio remoti di sistemi di rete integrati.

L'offerta Connected Services parte dalla creazione di un'infrastruttura di rete di informazione industriale sicura. I servizi di rete e cybersecurity di Rockwell Automation includono la valutazione delle esigenze, la progettazione, il supporto, la formazione IT/OT, il monitoraggio remoto, il rilevamento e la risoluzione delle minacce, l'implementazione "chiavi in mano", le soluzioni di rete pre-ingegnerizzate, il monitoraggio e la gestione della rete. Questi servizi possono accelerare l'integrazione di nuove apparecchiature e sistemi, migliorare notevolmente la sicurezza e ridurre i fermo macchina con l'accesso alle risorse tecniche.

L'importanza di testare in anteprima le patch di security

Per Alessandro Galmuzzi di Schneider Electric è fondamentale aiutare i propri propri clienti a intraprendere un percorso di trasformazione digitale quanto più sostenibile. "In termini di infrastrutture, da sempre l'imperativo assoluto è quello di riuscire a garantire la continuità di servizio e di esercizio. Per eliminare il rischio legato al continuo aggiornamento delle patch di security, Schneider ha scelto ad esempio di testare in anteprima l'affidabilità delle nuove versioni rilasciate dalle principali software house con cui l'azienda collabora. Solo una volta superati i test, le patch vengono validate e rilasciate agli end-users che potranno così introdurle nel proprio sistema di sicurezza senza il rischio di falle o disservizi". In ambito di cybersecurity, Schneider Electric propone EcoStruxure. Si tratta di una piattaforma ad architettura aperta, basata su standard e abilitata dall'Industrial Internet of Things. Tutte le soluzioni specifiche, i componenti, i software e i servizi che la compongono sono nativamente concepiti in ottica cybersecurity, assicurandone la compliance con le più stringenti direttive di settore. In aggiunta, i servizi di difesa di Schneider Electric sono flessibili e adattabili alle caratteristiche di ogni infrastruttura e impianto anche già esistenti, tanto da consentirne l'applicazione nel rispetto degli standard di riferimento, su sistemi OT e IT propri e di altri brand oltre che di varie generazioni tecnologiche.

Anche ABB, nella persona di Massimo Scanu, ha sottolineato l'importanza di testate in primis le patch di sicurezza prima di condividerle con gli end-users. "Ci siamo accorti che il timeframe tra il rilascio di una nuova patch e il rilascio di un nuovo virus è diventato sempre più stretto. Solo un aggiornamento veloce e continuo del sistema consente all'azienda di proteggersi da questo tipo di minacce. In quest'ottica, ABB (grazie alla partnership con Microsoft®) riceve in anteprima le patch in modo da poterle testare prima sui propri sistemi. Una volta certificate dal nostro reparto di ricerca e sviluppo, le patch vengono caricate sul nostro portale dove i clienti iscritti possono scaricare in completa sicurezza tutti gli aggiornamenti".

Il Security-by-Design è il modello più indicato in un ambiente di processo

Secondo Enzo Maria Tieghi, CEO di ServiTecno oltre che Presidente dello Steering Committee di ICS Forum "nei prossimi anni l'Operational Technology (OT) dovrà dimostrarsi all'altezza di una duplice sfida: mettere finalmente in sicurezza il "Plant Floor" e farlo in un momento in cui la spinta di Industria 4.0 sta di fatto eliminando perimetri fisici e limiti di connettività.

Il concetto di Security-by-Design è l'unico applicabile in un ambiente di processo, dove la complessità degli impianti è cresciuta a volte attraversando un arco temporale di venti o trenta anni, che hanno dato vita a "macchine" più inclini al risultato finale che alle performance e all'interazione con altri sistemi. È necessario "cucire la security" direttamente sugli impianti e sui loro Sistemi di

Controllo e Supervisione".

Elevare il livello di sicurezza delle comunicazioni tra gli strumenti di controllo e le infrastrutture tecnologiche correlate è un obiettivo chiave anche per ESA Automation. Per la tutela dei volumi di dati che circolano sulla rete aziendale e su piattaforme Cloud, l'impegno di ESA Automation si concretizza nel suo servizio di manutenzione remota Everyware. Sviluppato per garantire la massima sicurezza grazie all'implementazione di soluzioni come la double authentication, a valutarne l'efficacia è stata la società KPMG, che ha rivelato la sua affidabilità con una buona mitigazione dei rischi informatici.

L'interesse che ruota intorno alla tematica della cyber security non si esaurisce qui ma, al contrario, è destinato a crescere. Non a caso, sarà protagonista anche della seconda edizione del Forum, in programma nel 2019. Nel frattempo, di sicurezza informatica si parlerà anche a SPS Italia (evento espositivo organizzato da Messe Frankfurt e in programma a maggio di quest'anno a Parma), dove nel nuovo padiglione Digital District (DD) i dibattiti tra IT e OT verteranno sui processi di digitalizzazione per la nuova manifattura italiana, che vedrà il coinvolgimento dei principali player del mondo Digital, Software e Cyber Security.