Tavola rotonda

CYBER-IIOT: RETI OT A RISCHIO!

PARLIAMO DI CYBERSECURITY PER LE RETI INDUSTRIALI. PERCHÉ L'ERA DELL'INDUSTRIAL IOT NECESSITA DI UN NUOVO PARADIGMA PER LA SICUREZZA DI RETI E DATI?

***di* Ilaria De Poli, Emiliano Sisinni**

Con il termine 'cybersecurity' intendiamo l'insieme di tutte le strategie e soluzioni volte a proteggere i sistemi informatici da attacchi. La sicurezza informatica coinvolge quindi diversi fattori, ambiti e aspetti, che non si limitano a quelli tecnici, ma ne includono di organizzativi, legali e non ultimi umani.

Un attacco informatico ha di solito obiettivi economici, in quanto è generalmente finalizzato al furto di dati, sia che si tratti di un semplice dispositivo elettronico personale, sia di una rete aziendale o persino di un intero sistema eterogeneo connesso da un'infrastruttura di comunicazione su scala geografica. Nonostante una qualunque applicazione basata sull'uso delle tecnologie ICT possa oggigiorno essere destinataria di tali attacchi, il tema dell'industrial cybersecurity è, a seguito della sempre più dilagante digitalizzazione dei processi industriali, di particolare interesse e degno di attenzione. Nello specifico, con industrial cybersecurity ci si riferisce all'insieme delle soluzioni applicabili all'automazione industriale che consentono di prevenire gli attacchi informatici verso i sistemi di controllo, quali PLC, Scada e HMI. Sono proprio questi i dispositivi, la cui evoluzione ha permesso di realizzare processi produttivi sempre più efficienti ed economici, che meritano particolare attenzione. La quantità di dati scambiati ogni giorno tra i settori IT e OT ha ormai raggiunto dimensioni epocali. Un attacco informatico può facilmente coinvolgere tutti gli ambiti del mondo industriale, che si tratti di piccole e medie imprese o di grandi colossi. Gli effetti possono essere disastrosi, portando anche a un blocco immediato delle linee di produzione, con conseguenze potenzialmente molto gravi per l'azienda che li subisce.

L'Italia, Paese nel quale il settore manifatturiero è fra le principali fonti di reddito, è particolarmente a rischio. Una minaccia informatica è specialmente critica perché può essere facilmente confusa con un guasto al sistema di produzione e passare inosservata. Le piccole e medie imprese sono le più attraenti per un attacco, anche se la quantità e la rilevanza dei dati che possono essere rubati è generalmente inferiore rispetto a quelle ottenibili eludendo i sistemi informatici di grandi multinazionali. Questo perché, spesso e volentieri, le misure di sicurezza adottate dalle PMI sono inadeguate, le conseguenze di un attacco vengono sottovalutate e gli interventi si realizzano solo dopo aver subito danni tangibili e rilevanti. Non è di aiuto, inoltre, il fatto che macchinari e dispositivi siano solitamente aggiornati in periodi di tempo e con modalità differenti, per esempio con interventi di manutenzione esterna, risultando in soluzioni eterogenee e non tracciabili. Una vera e propria 'giungla', la cui affidabilità e attendibilità è di difficile gestione.

La cybersecurity è un processo complesso che coinvolge competenze anche molto diverse e che deve essere sviluppato senza mai dimenticare la potenziale entità del problema. Le persone coinvolte in questi ambiti spesso sono esperte di sicurezza OT, ma i moderni processi produttivi necessitano di conoscenze anche nel campo delle reti e sistemi embedded, solo per citarne un paio. Non di rado, i ruoli e le responsabilità di chi è coinvolto nella gestione della cybersecurity non sono chiaramente definiti e la pianificazione delle risorse, anche e soprattutto umane, è minima. Inoltre, essendoci un gran numero di attori coinvolti nella catena di approvvigionamento del processo produttivo e del ciclo di vita di un manufatto, le responsabilità a seguito di un incidente di sicurezza sono di difficile attribuzione. Oltretutto, attualmente sono applicabili solo disposizioni di responsabilità generali.

Abbiamo chiesto agli esponenti di alcune aziende di primaria importanza nel panorama dei fornitori di soluzioni di sicurezza, di dare il proprio parere in merito ad alcuni temi dove la sicurezza è critica. Ecco cosa ci hanno risposto.

Un livello di sicurezza ottimale

Il paradigma dell'Industrial IoT promuove la possibilità di accedere da remoto alle infrastrutture di comunicazione proprie dell'automazione industriale, un tempo ritenute intrinsecamente sicure proprio perché isolate. Il livello di sicurezza offerto dalle tradizionali soluzioni IT in tal caso è sufficiente? E se non lo è, che livello è richiesto?

Linda Pirovano, consulente tecnico di prevendita per reti di automazione industriale di **Siemens** in Italia (*https://new.siemens.com/it/it.html*): "Quando si parla di livello di sicurezza richiesto dalle reti di automazione, anche denominate reti OT (Operation Technology), a confronto con il livello richiesto nelle tradizionali soluzioni IT, bisogna considerare le differenze tra questi due mondi. La rete OT nasce per supportare la produzione e, in quanto tale, deve eccellere in primis per disponibilità, senza trascurare i requisiti di integrità e confidenzialità. Un ulteriore aspetto da valutare quando si parla di livello di sicurezza è legato alle caratteristiche dei sistemi industriali. Un elevato quantitativo di impianti industriali utilizza, ancora oggi, controllori progettati e commercializzati prima dell'avvento di Internet e della connessione in rete delle macchine, quando le esigenze di sicurezza informatica comuni alle reti IT non erano ancora necessarie per le reti OT. Di conseguenza, i livelli di protezione da attuare devono tenere conto di tutti questi aspetti e differenze.

Linda Pirovano di Siemens in Italia

Per la protezione delle reti di impianto, in Siemens proponiamo il concetto di 'Defense in Depth', ovvero una protezione strutturata su più livelli e con misure di difesa complementari tra di loro. Questo concetto viene spiegato in maniera strutturata nella normativa IEC62443, che è quella. di riferimento in ambito OT per la cybersecurity. In breve, la protezione viene strutturata su tre diversi livelli: le misure legate alla protezione fisica del sito produttivo, le misure tecnologiche di protezione della rete e le misure legate al rafforzamento dei sistemi informatici".

Daniela Previtali di Wibu-Systems

Daniela Previtali, global marketing director di **Wibu-Systems** (*www.wibu.com/it.html*): "La cybersicurezza è una maratona a tempo indeterminato. Chi da decenni, come Wibu-Systems, vi si dedica a tempo pieno, sa che prevenire gli attacchi o porre rimedio a minacce in essere sono azioni costanti. Una volta intrapresa la strada di totale affidamento delle nostre vite alla tecnologia, il loro incessante aggiornamento diventa parte integrante della scelta iniziale. Non esiste un traguardo che possa essere definito quale zona di comfort, né adesso, né in futuro. È ancora dibattuto quanto il quantum computing possa realmente rappresentare una minaccia agli attuali sistemi, che necessiteranno comunque di essere svecchiati. Il machine learning diventerà sempre più sofisticato e affidabile ma, nel frattempo, è suscettibile di azioni di sabotaggio, tanto nei processi su cui si fonda, quanto nei risultati che genera. Associazioni come l'**Industry IoT Consortium** (*www.iiconsortium.org*), con cui collaboriamo, continuano a sfornare linee guida anno dopo anno, frutto di una sinergia globale. I modelli da loro sviluppati rappresentano alcuni dei risultati più accreditati a livello tecnico e di business. Essi spaziano da framework dedicati all'intelligenza artificiale, alle reti, all'affidabilità dei componenti di un sistema IIoT, così come a tassonomie per la definizione di maturità di un sistema, metriche per l'analisi dei dati e princìpi alla base della sicurezza del mondo dell'Internet of Things industriale (IIoT)".

Enzo Maria Tieghi, AD e presidente di **ServiTecno** (*www.servitecno.it*): "Tutte le tradizionali soluzioni per proteggere l'azienda dal rischio cyber sono necessarie. Servono infatti a garantire la corretta postura di cybersecurity dell'organizzazione. Ricordiamoci che la sicurezza è fatta di diversi fattori, quello delle tecnologie messe in campo è solo uno dei fattori da considerare, al quale è necessario aggiungere sicuramente anche quello delle persone, che devono essere formate e costantemente aggiornate sui rischi inerenti i sistemi che utilizzano. Non dimentichiamoci però che il rischio maggiore per il mondo IT è la perdita dei dati, mentre per il mondo OT il rischio principale è la perdita di controllo sul processo controllato. E questo potrebbe portare all'interruzione della produzione o dell'erogazione del servizio, con possibili perdite di prodotto, di quote di mercato, danni di immagine e possibili impatti sull'integrità degli im-

Enzo Maria Tieghi di ServiTecno

pianti, sull'ambiente e sulla salute e sicurezza fisica delle persone. È necessario quindi prevedere, oltre alle contromisure IT, anche contromisure specifiche per la protezione di reti e sistemi di automazione e il controllo di processo, ovvero quelle destinate alla continuità operativa per il mondo OT".

Salvatore Marcis, technical director di **Trend Micro Italia** (*www.trendmicro.com*): "La sfida principale in ambito Industria 4.0, oggi, è riuscire a rendere costantemente possibile la business continuity. Gli ultimi due anni hanno dimostrato che operare in contesti anche diversi dal solito, come da remoto, è critico per il successo del business. Così come la gestione delle possibili interruzioni della produzione. E in ambito Industria 4.0 l'interconnessione delle reti di automazione con le infrastrutture IT aumenta la superficie della propria organizzazione, esposta al rischio di subire attacchi informatici. Una nostra ricerca recente, intitolata *'The State of Industrial Cybersecurity: Converging IT and OT with People, Process, and Technology'*, ha dimostrato come il 61% delle aziende manifatturiere abbia subito un attacco informatico e lotti per implementare la tecnologia necessaria a gestire in maniera efficace i rischi cyber. Inoltre, il 75% delle aziende che ha subito un attacco, ha dovuto affrontare un blocco della produzione e per il 43% questa interruzione è durata più di 4 giorni. Inoltre, secondo un'altra nostra ricerca intitolata *'How to Reduce the Risk of Phishing and* Ransomware', l'84% delle aziende ha subito un attacco di phishing o ransomware nell'ultimo anno e la metà non riesce a contrastare efficacemente queste minacce".

Salvatore Marcis di Trend Micro Italia

Stefano Corsi, amministrazione unico di **Solintec** (*www.solintec.it*): "Qualsiasi livello di sicurezza raggiunto non è un punto d'arrivo, per cui una volta arrivati lì, si possa stare tranquilli. Come un'automobile ha periodicamente necessità di manutenzione per poter durare più a lungo, così un'infrastruttura di rete deve essere sottoposta a maintenance e aggiornamenti costanti, perché la sicurezza continui a essere garantita. Pertanto, quando si costruiscono delle macchine industriali è necessario scegliere in maniera oculata la strumentazione che ha il compito di connetterle, tenendo conto di fattori che i costruttori di macchine industriali spesso non sono abituati a considerare. Per esempio, di quali servizi è corredato il dispositivo prescelto? Quante patch di aggiornamento rilascia mediamente il fornitore? Purtroppo, la continua rincorsa al prezzo per essere più competitivi e la scarsa propensione del settore a sottoscrivere canoni di 'maintenance as a service' non consentono alla sicurezza di fare passi avanti significativi all'interno delle aziende. Si spendono tanti soldi a livello IT/CED, ma poi si lasciano 'aperture' ad altri livelli. È come se, in una casa posta a pianterreno, si acquistasse una porta blindata ipersicura e cara, ma non si facesse nulla per le finestre".

Stefano Corsi di Solintec

Stéphane di Vito, product definer & security expert, Security, Software and Processors business group di **Analog Devices** (*www.analog.com*): "La sicurezza IT tradizionale è naturalmente un primo livello di difesa assolutamente necessario, in particolare per filtrare il traffico in entrata e in uscita verso le reti industriali e per rilevare attività sospette all'interno delle reti. Il problema con la sicurezza IT tradizionale è la dipendenza da dispositivi che devono essere abbastanza potenti. Antivirus, firewall o altri software di rilevamento delle intrusioni funzionano solo su processori di fascia alta o System-on-Chip. I dispositivi di rete IIoT, come attuatori, sensori, PLC o altri gateway, sono solitamente costosi, ma la loro architettura si basa su microcontrollori embedded adatti per un singolo compito, come per esempio il controllo e monitoraggio del processo. Non vi è pertanto spazio di memoria extra, né larghezza di banda della CPU per eseguire software aggiuntivi di rilevamento realtime delle intrusioni. Oltre a essere collegati a un bus di campo, i dispositivi di rete IIoT possono essere direttamente presenti su Internet attraverso un'interfaccia dedicata, quindi non sono protetti dai tradizionali dispositivi di sicurezza di rete IT. È pertanto necessario prevedere un secondo livello di difesa. I dispositivi IIoT devono essere intrinsecamente protetti. L'avvio sicuro e gli aggiornamenti sicuri del firmware, per esempio, sono fondamentali per un funzionamento affidabile, in quanto aiutano a prevenire facili modifiche sul comportamento dei dispositivi o l'inserimento di malware. Inoltre, il firmware del dispositivo IIoT deve essere ben testato prima del rilascio, per evitare qualsiasi vulnerabilità sfruttabile da remoto attraverso, per esempio, la mancanza di verifica del format dei comandi. Oltre a questo, l'uso di elementi hardware sicuri garantisce molta più protezione, in quanto questi permettono di isolare le funzioni sensibili da qualsiasi firmware compromesso o da un attacco invasivo".

Stéphane di Vito di Analog Devices

Umberto Pirovano, manager system engineering di **Palo Alto Networks** (*www.paloaltonetworks.it*): "Possiamo affermare che il paradigma dell'IIoT porta il concetto di data-driven nell'ambito dei processi produttivi aziendali. Si crea un ciclo continuo tra la rilevazione dati di varia natura (ambientali, di stato ecc.), la loro elaborazione (vicina o distante dalla fonte dei dati) e i processi decisionali o le azioni conseguenti. È evidente che a fronte dei benefici derivanti dall'automazione e dall'integrazione dei processi, si introduce un rilevante problema di sicurezza e privacy. Il punto di partenza della sicurezza è identico a quello di ogni ambito IT, ovvero la garanzia di integrità, disponibilità e riservatezza a partire dai dispositivi IIoT. Ma gli ambienti IoT e IIoT sono intrinsecamente complessi, includendo differenti tecnologie abilitanti insieme a una difformità, una distribuzione di dispositivi e infrastruttura unici. Pensiamo, per esempio, a tecnologie quali il 5G o il cloud, e cominciamo ad avere un'idea di quanto complesso possa essere il processo di adozione di sistemi IIoT dal punto di vista della compliance e della security. Vi sono poi specificità su applicazioni e protocolli di comunicazione utilizzati in ambito IIoT che devono essere considerate nella progettazione di ambienti sicuri. I processi di consumo ed elaborazione dei dati sono a loro volta distribuiti, creando flussi che tipicamente non sono più contenuti all'interno delle infra-

Umberto Pirovano di Palo Alto Networks

strutture OT e sempre più spesso neanche più in azienda. Inoltre, il rischio cibernetico entra a tutti gli effetti nel calcolo del rischio aziendale a livello di produzione in caso del settore manifatturiero. La valutazione del rischio non dovrà quindi considerare solo aspetti tecnologici, in particolare non solo legati all'ambito OT, ma anche all'interconnessione tra ambienti OT e IT. Già da queste osservazioni di base diventa evidente come il livello di protezione in ambito IIoT richieda un approccio olistico, in grado di coprire tutti gli ambiti tecnologici, i processi e l'organizzazione aziendale".

Umberto Cattaneo di Schneider Electric

Umberto Cattaneo, Eura cybersecurity consultant, Industrial Automation, di **Schneider Electric** (*www.se.com*): "Oggi è indispensabile prevedere un piano di sicurezza specifico che riguardi anche le reti che connettono le tecnologie operative. Vi sono degli standard di settore, come IEC62443, che definiscono molto chiaramente il tipo di approccio da adottare in funzione dei diversi rischi che possono essere causati da un eventuale attacco agli impianti, replicando l'approccio ben consolidato dei livelli di sicurezza fisica (SIL, Safety Integrity Level). Questo può aiutare, sulla base di un'attenta valutazione dello scenario della singola azienda, a prendere i giusti provvedimenti per ottenere protezione senza compromettere le performance. Nel mondo IT si ragiona in modo diverso, per questo è indispensabile integrare le soluzioni IT con un approccio specifico per il mondo industriale e delle infrastrutture".

Massimo Carlotti, presales team leader di **CyberArk** (*www.cyberark.com/it*): "L'air gapping è un tema che l'IT ha già affrontato, sviluppando diverse soluzioni in grado di rispondere a questo tipo di necessità, e spesso è stata considerata come la strategia migliore per tenere al sicuro anche le reti OT. Al giorno d'oggi, però, esistono diverse alternative che permettono un'integrazione sicura tra mondo IT e OT. Un esempio può essere costituito dal PAM (Privileged Access Management), che gestisce efficacemente la connessione tra l'utente e il sistema di riferimento, dimostrandosi quindi un'alternativa più efficace all'air gapping. In breve, tenendo alto il livello di sicurezza, queste soluzioni consentono la connessione remota (o addirittura esterna) ai sistemi OT, analogamente a come queste tecnologie vengono già impiegate nel mondo IT per la gestione in sicurezza di asset critici. Le reti OT possono essere quindi rese accessibili e interoperabili con delle buone misure di sicurezza. Ovviamente non esiste un approccio aureo per qualsiasi situazione, poiché ogni realtà ha bisogno di un approccio specifico. Una cosa però è chiara, qualora si volesse integrare l'OT con l'IT è ottimale affidarsi a tecnologie d'avanguardia, invece che usufruire di soluzioni legacy che potrebbero non essere in gradi di rispondere efficacemente alle nuove sfide del mondo IT".

Massimo Carlotti di CyberArk

Antonio Madoglio, senior director systems engineering, Italy & Malta, di **Fortinet** (*www.fortinet.com/it*): "Nel settore industriale tutte quelle realtà che hanno avviato il progetto di Industria 4.0 hanno deciso di rimuovere l'air-gap per mettere in comunicazione la rete OT con quella IT e avere i dati di produzione a disposizione del business. Questo processo, proprio perché guidato dalle esigenze del business, ha di solito purtroppo portato le aziende che lo hanno implementato a non considerare le segnalazioni dei vari team di security, che evidenziavano i rischi a cui si sarebbe andati incontro se non fossero stati applicati gli adeguati controlli di sicurezza. Va da sé che questo ha comportato un ampliamento dei potenziali rischi per le infrastrutture di comunicazione tipiche dell'automazione industriale e che, di conseguenza, va innalzato il livello di sicurezza correlato. È dunque bene mettere in sicurezza i punti di interconnessione tra mondo IT e OT, partendo da alcuni step che prevedono un'analisi del rischio, la scelta di un firewall, l'analisi e identificazione dei dispositivi sulla rete, per poi procedere con una segmentazione della stessa, con l'obiettivo di isolare un dispositivo sotto attacco e limitare così il rischio che ne può derivare".

Antonio Madoglio di Fortinet

Marco Bera, product manager networking di **Direl** (*www.gate-manager.it - www.direl.it*): "Le soluzioni IT per la sicurezza hanno raggiunto un ottimo livello e sono in continua evoluzione, ma privilegiano l'integrità e la confidenzialità nella triade confidenzialità-integrità-disponibilità, CIA. Invece negli impianti industriali la disponibilità, cioè il fatto che l'impianto funzioni, rappresenta una priorità. C'è pertanto un forte bisogno di soluzioni di sicurezza dedicate all'ambito industriale, che lavorino in modo armonioso e si integrino con le soluzioni IT già presenti. Non si tratta di scegliere tra soluzioni IT o OT, ma di usarle entrambe in modo corretto".

Marco Bera di Direl

Sergio Leoni, regional sales director di **Nozomi Networks** (*www.nozominetworks.com*): "I sistemi di controllo industriale (ICS) e le reti di produzione, segni distintivi delle aziende manifatturiere, non sono protetti dalle vulnerabilità quotidiane dei sistemi IT aziendali, come hanno dimostrato i famigerati esempi degli attacchi WannaCry e NotPetya del 2017. Essi colpirono molte aziende manifatturiere, tra cui Nissan, Renault e il colosso farmaceutico Merck. Le reti informatiche e di produzione sono sempre più connesse tra loro, secondo un logico trend operativo che consente a un unico team IT di gestire i sistemi di produzione in modo integrato, ma espone anche questi sistemi ad attacchi difficili da anticipare. Pensiamo, per esempio, al sistema di distribuzione delle acque in Florida (USA), che ha subito un attacco informatico contro il suo sistema ICS. Gli aggressori sono riusciti a penetrare nel sistema e ad alterare i livelli di sostanze chimiche con l'obiettivo di rendere l'acqua non potabile. Fortunatamente, questa intrusione è stata rapidamente rilevata dai team interni e risolta senza danni alla popolazione".

Sergio Leoni di Nozomi Networks

Wireless e sicurezza

Il paradigma dell'IIoT propende per una sempre maggiore inclusione di soluzioni di comunicazione wireless, che sono relativamente meno affidabili della controparte cablata e richiedono particolari accorgimenti in fase di installazione. Cosa comporta il loro uso dal punto di vista della sicurezza informatica?

Marcis: "L'utilizzo di sistemi di comunicazione wireless introduce la necessità di proteggere non solo lo scambio di informazioni su quella tipologia di rete, ma anche i metodi di autenticazione. Diviene necessario, quindi, avere un approccio dinamico e sicuro, in grado di verificare in maniera continuativa, sia l'autenticazione dei device, sia la loro postura, utilizzando un paradigma di protezione Zero Trust Access. Ulteriore scenario evolutivo è l'utilizzo di reti 5G private per mettere in comunicazione tutte le componenti di produzione, controllo e gestione".

Madoglio: "L'utilizzo di soluzioni di comunicazione wireless comporta nuovi rischi per le aziende. Basti pensare al fatto che, se le minacce riescono a raggiungere le linee di produzione, è possibile che l'operatività si possa fermare e che magari possano passare giorni prima di risolvere una criticità, con chiare conseguenze in termini di business continuity. Sicuramente vi sono delle accortezze specifiche di cui tenere conto nei diversi casi specifici. Si può affermare che visibilità, controllo e protezione siano alla base della sicurezza in ambito industriale suggerita dal framework del Purdue Model (IEC62443). Questi sono anche i fattori fondanti della 'vision' di Fortinet per la OT/IIoT security e del suo approccio olistico".

Cattaneo: "Oggi il wireless è diffuso nei sistemi industriali principalmente per quanto riguarda la connettività sul campo nell'impianto. In questo ambito i problemi possono nascere dall'uso di protocolli di trasmissione non abbastanza sicuri, quindi la prima attenzione da avere è quella di scegliere soluzioni che garantiscano la cifratura e l'autenticazione degli utenti (persone o componenti IoT che siano) che si connettono e ricevono. In ottica evolutiva, possiamo pensare all'adozione di architetture in linea con l'approccio 'zero trust' che si sta diffondendo in ambito IT, che prevede una sicurezza applicata in modo puntuale, anche sui collegamenti remoti, da portare nel mondo IIoT".

U. Pirovano: "Anche nel caso dei sistemi di trasporto, l'ambito Ilot richiede una grande varietà di tecnologie. Accanto al 'classico' wi-fi con gli standard 802.11, troviamo anche trasporto su reti licenziate (LTE/5G, NB-IoT), moduli RF, ma anche protocolli di comunicazione tra componenti, per esempio Zigbee, Z-Wave, Bluetooth e simili. Spesso in ambiti complessi e distribuiti sono impiegati più protocolli differenti. L'implicazione base è l'aumento della cosiddetta superficie di attacco, ovvero l'introduzione di nuovi potenziali canali per vettori di attacco di varia natura, per esempio: Denial of Service, tramite oscuramento o saturazione dei canali di comunicazione. La saturazione in alcuni casi può avvenire esaurendo le risorse di alcuni processi relativi alla trasmissione, non solo di tipo volumetrico sul traffico; furto di dati e informazioni, derivanti dall'intercettazione delle comunicazioni; accesso alla rete alla ricerca di canali che consentono movimenti laterali interni.

È complesso riassumere in poche righe cosa occorre fare per rendere sicuri questi canali di comunicazione, anche perché molto dipende dalla tecnologia utilizzata. Un approccio vincente, in questo caso, implica: analisi della sicurezza su ciascuno dei layer della pila ISO/OSI; meccanismi di autenticazione implementati e a quale livello; impiego estensivo della cifratura forte; verifica continua tramite professionisti dei penetration test".

Previtali: "Nonostante la compulsiva spinta verso la digitalizzazione e la messa in comunicazione in remoto di dispositivi, impianti e intere smart grid, constatiamo la presenza massiva di unità disconnesse da qualsiasi rete. Infrastrutture critiche e impianti fuori confine e in territori presieduti da diversi orientamenti geopolitici

Un attacco informatico può facilmente coinvolgere tutti gli ambiti del mondo industriale, che si tratti di piccole e medie imprese o di grandi colossi

resteranno molto probabilmente disconnessi, una mossa conservativa e condivisibile. Da tempo l'hacking è di fatto entrato in uno stadio di sofisticazione tale, per cui agenzie nazionali ad hoc sono chiamate in prima persona a difendere il Paese da una guerra cibernetica. Il Computer Security Incident Response Team (Csirt Italia) della nostra stessa Agenzia per la Cybersicurezza Nazionale rilascia allerte su imminenti pericoli, bollettini su vulnerabilità rilevate e campagne di sensibilizzazione, che aiuteranno sempre più aziende pubbliche e private a prendere dimestichezza con la materia e mettere in pista misure predittive, preventive e proattive. Dalla nostra prospettiva, abbiamo puntato su soluzioni di sicurezza ibride, in grado di soddisfare tanto chi ha sposato l'IIoT, quanto chi invece non è ancora pronto a questo passo o non intende compierlo. Modularità e interoperabilità consentono di utilizzare gli stessi strumenti software di protezione e gli stessi elementi di sicurezza hardware, software o cloud, costruendo architetture eterogenee e personalizzate fin nei minimi dettagli. I componenti hardware possono inoltre essere incapsulati all'interno del dispositivo da proteggere, oppure spostati manualmente da un'unità all'altra per maggiore mobilità".

Leoni: "Le tecnologie IIoT sono emerse insieme all'IoT di taglio più consumer. Sono costruite su piattaforme e protocolli comuni e presentano una serie simile di punti deboli della sicurezza. Ciò che le rende più facili da gestire e meno co-

Fonte: Pixabay_TheDigitalArtist

stose da sviluppare è anche ciò che le rende vulnerabili, perché i cybercriminali, consapevoli che i sistemi di controllo della produzione sono sempre più spesso costruiti su tecnologie comuni, possono ora operare in modo più semplice e con meno personalizzazioni. Come per l'IoT, anche l'intero settore che sta dietro l'IIoT ha sottovalutato la necessità di sicurezza e molti sistemi hardware di prima e seconda generazione presentano vulnerabilità nella configurazione e nella progettazione del software. Una volta che questi sistemi vengono implementati, non è facile rimediare, soprattutto quando l'arresto di sensori e dispositivi porta a problemi in produzione. Rimediare a questa vulnerabilità delle apparecchiature richiede, per la maggior parte delle aziende, un livello di visibilità estremamente difficile da raggiungere.

A lungo termine, per affrontare la sfida della cybersecurity sono necessarie soluzioni di difesa che possano operare in modo unificato attraverso un unico sistema di gestione. Piuttosto che tornare indietro e isolare le reti industriali, ha più senso integrarle in modo sicuro. Le aziende devono avere accesso a un inventario accurato dei loro sistemi, essere in grado di monitorare il loro stato in tempo reale e avere un modo per definire la manutenzione, compresa l'applicazione delle patch, in modo complesso. Prima ancora di acquistare qualsiasi apparecchiatura è imperativo verificarne la sicurezza e la capacità di affrontare i punti deboli. È inoltre necessario integrare l'intelligence sulle minacce, dal maggior numero possibile di fonti, per ottenere informazioni dettagliate sugli attacchi, siano essi previsti o rilevati in incidenti reali".

Di Vito: "Le comunicazioni wireless rappresentano effettivamente una riduzione dei costi, dato che i cavi possono essere costosi da implementare. È anche vero che le reti di comunicazione wireless rendono più facile la vita dell'aggressore. Con il wireless, gli attacchi di tipo 'drive-by' diventano possibili. Non serve più entrare fisicamente nei locali e intercettare i cavi. Questi attacchi ravvicinati sono possibili perché le tecnologie wireless a volte presentano una serie di vulnerabilità. Per esempio, i protocolli wi-fi WPS, LoRa, Zigbee hanno debolezze note. Questi protocolli non sono necessariamente insicuri, ma c'è un rischio considerevole nel configurare male le loro opzioni di sicurezza e anche qualche rischio quando si assegnano le chiavi di sicurezza ai vari nodi della rete. Come best practice necessaria, le opzioni non sicure devono essere disabilitate e tutte le chiavi e le password coinvolte nella messa in sicurezza della rete devono essere cambiate, poiché i dispositivi sono spesso dotati di chiavi o password predefinite dal produttore, e ben protette, in modo che non si perdano. Inoltre, va notato che le apparecchiature IT di fascia alta spesso dispongono di radio wireless più recenti e possono essere aggiornate facilmente. Al contrario, i nodi IoT industriali specifici sono dispositivi embedded limitati, che possono non essere così flessibili in termini di configurazione, e i loro protocolli radio possono essere obsoleti, nonché non aggiornabili. Quindi, questi dispositivi rimangono vulnerabili e, dato che di solito hanno un ciclo di vita lungo, rappresentano una grande preoccupazione. In ogni caso, il Denial of Service è una debolezza comune dei protocolli radio, poiché è più facile provocare un'interferenza a un collegamento radio che a una comunicazione cablata e portare il caos in un impianto industriale. Questa minaccia è estremamente difficile da contrastare, nonostante il fatto che le opzioni di sicurezza siano state configurate correttamente".

Bera: "L'uso di soluzioni wireless, sebbene molto comode per eliminare o limitare il cablaggio, aumenta la superfice di attacco del sistema di automazione industriale (Iacs). Essendo poi l'etere un mezzo intrinsecamente condiviso, l'uso della tecnologia wireless rende possibile 'sniffare' il traffico anche se criptato e permette di realizzare un serie aggiuntiva di attacchi senza dover accedere fisicamente, per esempio, al quadro elettrico. È sufficiente essere nelle vicinanze e percepire il segnale wireless. Inoltre, l'uso della tecnologia wireless consente di effettuare attacchi mediante 'rouge access point', per indurre gli operatori a collegarsi a un access point 'malevolo'".

Tieghi: "Non sono completamente d'accordo sull'affermazione che le comunicazioni cablate siano in genere più affidabili di quelle wireless. Entrambe possono avere gravi vulnerabilità ed entrambe, se necessario, oggi, possono essere rese molto affidabili e resilienti. Tutto dipende dai criteri di hardening da adottare in seguito a un'accurata valutazione dei rischi. Certo una grave minaccia può essere insita all'utilizzo di componenti 'low cost' e di provenienza non nota, che ormai siamo abituati a trovare in oggetti IoT connessi, non espressamente ingegnerizzati e fabbricati per utilizzo in ambienti industriali o nelle infrastrutture critiche. Anche l'utilizzo di affidabili provider di connettività sicura e di cloud certificati secondo criteri ed elevati SLA condivisi, come per esempio Cloud Control Matrix e CSA Star di Cloud Security Alliance, o secondo standard IoT/IIoT come quelli pubblicati da Nist, possono rendere accettabile il livello di security per applicazioni in ambito industriale o utility".

Norme e standard: a che punto siamo?

Il successo delle comunicazioni industriali deriva anche dalla disponibilità di standard e normative internazionali che hanno permesso l'interoperabilità tra

Fonte: Pixabay_Elchinator

Vi sono prodotti specifici che, con l'ausilio di apposite applicazioni che utilizzano machine learning e AI, identificano le anomalie e aiutano i responsabili a prevenire eventuali incidenti

prodotti di diversi costruttori. Qual è la situazione della normativa relativamente alla sicurezza industriale? Quali le eventuali carenze?

U. Pirovano: "Per migliorare le operazioni sicure e proteggere gli ambienti OT le organizzazioni devono adottare un framework di sicurezza informatica progettato ad hoc, come la serie di standard ISA/IEC 62443, che fornisce un quadro flessibile per affrontare e mitigare le vulnerabilità di sicurezza presenti e future nei sistemi di controllo e automazione industriale. Poiché possono essere applicati a tutti i settori industriali chiave e alle infrastrutture critiche, gli standard ISA/IEC 62443 sono componenti integranti del framework di sicurezza informatica del Nist e dell'Enisa. Allo stesso tempo, il modello Zero Trust ha acquisito lo status di mainstream per la protezione delle reti IT. Simile al concetto del principio del 'less route' (percorso minimo) all'interno di OT, Zero Trust è un approccio alla sicurezza informatica ampiamente accettato, che può essere prontamente applicato agli ambienti OT per aiutare a soddisfare i requisiti tecnici e architetturali di ISA/IEC62443. Meglio ancora, l'utilizzo della metodologia Zero Trust semplificherà l'implementazione della serie di standard IEC62443 per ambienti OT, consentendo alle organizzazioni di migliorare la sicurezza dei loro sistemi OT critici utilizzando un approccio iterativo che segue queste cinque fasi: definizione della superficie da proteggere; mappatura dei flussi di dati; progettazione di una rete Zero Trust a zone; creazione di policy Zero Trust; monitoraggio e mantenimento.

Una delle principali problematiche rimane l'assenza di un framework di cybersecurity che includa DevSecOps. Il cloud e le applicazioni sviluppate secondo metodologia DevOps stanno diventando lo standard anche in ambito OT, con un'adozione rapida spinta da esigenze di business. Allo stesso tempo, un framework Nist o uno standard ISO su questo argomento sono tuttora inesistenti o incompleti".

Madoglio: "Se si parla di normative, lo standard internazionale IEC62443-4-2 resta un punto di riferimento. La sua applicazione, infatti, protegge efficacemente i sistemi di controllo industriale dalle minacce informatiche, consentendo alle aziende di evitare di incorrere in problematiche come il blocco delle linee di produzione e la conseguente perdita dei ricavi. Allo stato delle cose, quello che si evidenzia è purtroppo ancora un diffuso scetticismo da parte delle aziende riguardo la prevenzione dei rischi correlati all'ambito informatico. Per questo motivo Fortinet ha lanciato il programma 'The Fortinet Fabric-Ready Technology Alliance Partner Program' con lo scopo di condividere le funzionalità della propria tecnologia con partner tecnologici interessati ad arricchire la propria soluzione, o a integrare la propria attraverso connettori o API. In questo programma

molti dei produttori di soluzioni specifiche per il mondo industriale stanno collaborando con Fortinet per integrare le soluzioni di security all'interno delle loro proposte tecnologiche, facendo comprendere il valore aggiunto di una componente di security al personale che opera all'interno del mondo industriale".

Di Vito: "L'isolamento di solito è decisivo nella sicurezza. Quando una rete è segmentata, un attacco eseguito con successo su un segmento di rete può non essere in grado di propagarsi all'intera rete. Ma la standardizzazione dei protocolli di comunicazione porta alla generalizzazione delle interconnessioni tra componenti e sottosistemi, il che è ottimo dal punto di vista dell'automazione industriale, ma crea ancora più potenziali vulnerabilità. Lo standard IEC62443 sta diventando 'de facto' un framework per la sicurezza informatica nelle applicazioni industriali. È esplicitamente menzionato nella proposta di un quadro normativo comune sulla cybersecurity in Europa, che potrebbe essere applicato nei prossimi anni dalla legge europea sulla cybersecurity del 2019. Questo atto sulla cybersicurezza imporrà criteri di sicurezza più o meno rigorose sui prodotti ICT, cioè quelli che elaborano e/o trasmettono informazioni, come i sensori, le apparecchiature di prova, i PLC e, di fatto, tutti i dispositivi IIoT. Con ciò, sarà obbligatorio un certo livello di valutazione e certificazione da parte di terzi. Pur essendo estremamente utile, poiché la certificazione permette un certo grado di fiducia, in quanto una terza parte valuta in modo indipendente la sicurezza dell'attrezzatura, è un falso senso di fiducia. La valutazione della sicurezza del prodotto si basa su una serie di ipotesi a loro volta basate su un'analisi dei rischi e può non coprire tutte le minacce realmente presenti sul campo. Inoltre, la maggior parte dei prodotti non sono intrinsecamente sicuri Devono quindi essere configurati bene per funzionare in modo sicuro, quindi sono necessarie anche policy operative ed esseri umani che devono applicare le procedure".

Tieghi: "Solo negli ultimi anni siamo entrati nel merito della sicurezza da adottare nelle comunicazioni industriali, ma standard e normative iniziano solo ora a essere valutati e adottati. Conosciamo le attività dei gruppi di lavoro IEC e ISA, con i primi documenti discussi e pubblicati. ISA99 ha dato un notevole contributo con il suo standard ISA99 divenuto IEC62443, declinato in molte sezioni, definendo modelli organizzativi, architetture e strutture per reti di fabbrica sicure. Vorrei anche ricordare qui il lavoro fatto dal comitato ISA100 Wireless, che ha generato la norma IEC62734. È uno standard internazionale di comunicazione per rete wireless industriali progettato per soddisfare le esigenze delle industrie di processo. Mediante rete IPv6 nativa e architettura a oggetti, ISA100 Wireless estende l'IIoT al wireless. Gli utilizzatori possono selezionare dispositivi ISA100 Wireless Compliant da diversi fornitori, con garanzie di interoperabilità. Consente inoltre ai progettisti di creare, modificare, ottimizzare e scalare rapidamente reti wireless aperte, interoperabili e affidabili per le loro applicazioni più critiche. ISA100 Wireless è attualmente l'unico protocollo industriale IPv6, 6LowPAN progettato per l'automazione industriale".

Bera: "La normativa IEC62443, nelle sue varie declinazioni (system integrator, product supplier, asset owner), sembra rappresentare una linea di riferimento universalmente accettata e applicabile a un numero significativamente vasto di settori, ma richiede per poter essere efficace che ognuno dei tre attori in gioco svolga la propria parte e in modo coordinato. Mi aspetto che un crescente numero di produttori cerchi di certificare il processo di sviluppo secondo la norma IEC62443-4-1 (Security Development LifeCycle) e poi, come secondo step, valuti il Security Level (SL) del dispositivo secondo IEC62443-4-2. Richieste per prodotti con un SL minimo potrebbero diventare comuni nei prossimi anni".

Cattaneo: "Lo standard IEC62443, che rappresenta la risposta 'europea' allo standard ISA99 americano, riprende i concetti fondamentali già assimilati per la sicurezza fisica con il tema dei Safety Level e li porta anche nel contesto della sicurezza informatica. Il suo valore è fondamentale, perché nasce come standard specifico industriale e quindi tiene conto delle caratteristiche dei sistemi che integrano tecnologie operative e digitali. Il principale problema, in questo momento, è che nel nostro Paese la conoscenza approfondita dello standard e di ciò che prevede non è ancora molto diffusa, per cui in molte realtà si richiamano e usano standard tipici della sicurezza IT, che sicuramente aiutano a proteggere i dati a livello di sistemi aziendali, in generale, ma non dettagliano protezioni specifiche per i sistemi di produzione".

Marcis: "L'attuale standard per le reti fieldbus IEC61784/61158 ha efficacemente permesso di trovare un modello generalmente comune per far dialogare apparati industriali differenti ed eterogenei, anche con missioni differenti. Il panorama delle normative vigenti copre gli aspetti di sicurezza sul lavoro in relazione alla tutela delle persone e dei sistemi in esercizio, con l'obiettivo di proteggere la salute degli operatori. Come per la sicurezza informatica, esistono normative per la protezione delle informazioni e delle identità di chi utilizza un determinato servizio. Queste normative, in ambito OT, dovrebbero estendere la protezione anche sull'esenzione dei comandi da parte dell'infrastruttura OT, oltre che mirare solo alla protezione della persona fisica".

Leoni: "Linee guida, indicazioni e normative a livello dei singoli stati, in combinazione con una certa 'autogestione' a livello di settore, aiuteranno a stabilire e applicare una base standard per la cybersecurity delle infrastrutture critiche. Standard e best practice (come ISA e Nist) riceveranno maggiore attenzione. Nel 2022 l'approccio Zero Trust ricoprirà un ruolo maggiormente strategico nella cybersecurity OT, mentre le organizzazioni faranno evolvere i loro paradigmi di sicurezza per affrontare una nuova realtà fatta di architetture distribuite e IoT. Le politiche Zero Trust inizieranno a imporre restrizioni sui dispositivi e i PLC insicuri 'by design', come sensori e controller IoT. Come minimo, i fornitori di cybersecurity OT dovranno affrontare la visibilità e l'aderenza alle politiche di Zero Trust su tutti i loro dispositivi OT e IoT, con l'effetto di creare un modello di riferimento in continua evoluzione verso una cybersecurity sempre più estesa oltre che mirata".

La componente umana

Quanto impatta il fattore umano, ovvero quanto sono importanti gli atteggiamenti e le competenze degli operatori (dandone per scontata la formazione)?

Previtali: "Il fattore umano conta in ogni ambito della vita. Sono le persone dotate di un alto senso di responsabilità, di una spiccata capacità di osservazione e instancabili nel loro percorso educativo, che di norma prendono l'iniziativa, si documentano, suggeriscono migliorie, al di là della formazione aziendale e dei modelli di qualità di riferimento. Assistiamo anche a una complementarietà della forza lavoro, in virtù della quale i nuovi laureati sono proiettati verso la trasformazione digitale e possono trasmettere informazioni fresche a chi, uscito da scuola da molto, ha però acquisito una competenza diretta dei mercati e delle dinamiche. Insieme questi due attori possono sostenersi e procedere speditamente, arricchendosi l'un l'altro. Negli ultimi due anni tutti hanno preso dimestichezza con i sistemi digitali, abbracciato il lavoro dalla propria dimora, limitato le trasferte e si sono concentrati sulle occasioni di accrescimento praticamente illimitate che il mondo virtuale può offrire. Da parte delle aziende, va comunque favorito l'aggiornamento delle competenze su larga scala, con scambi multi-disciplinari, spesso coadiuvati da associazioni di settore, progetti di ricerca, collaborazioni tra il mondo accademico e quello industriale".

Marcis: "La sicurezza dell'Industria 4.0 è un percorso che deve tenere in considerazione diversi snodi cruciali. Per proteggersi al meglio è bene agire simultaneamente da un punto di vista sia culturale, sia tecnico. Prendendo in

considerazione quest'ultimo, è necessario introdurre specifiche soluzioni dedicate proprio alle parti produttive e integrate con l'intera strategia di security. Passando al punto di vista culturale e umano, invece, i responsabili della security degli impianti di produzione e gli addetti ai lavori devono essere consapevoli dei nuovi rischi e di come questi riguardino le proprietà intellettuali, gli asset strategici, la reputazione dell'organizzazione in caso di furto di dati, ma anche la possibilità di danni fisici a cose o persone, sia all'interno degli impianti sia all'esterno".

Corsi: "Si calcola che il 50% delle minacce arrivi dall'interno della rete proprio a causa di errori, disattenzioni o scarse competenze del personale operatore. Di qui l'esigenza di creare non solo un'infrastruttura sicura rispetto a ciò che può venire dall'esterno, ma soprattutto un sistema in grado di riconoscere all'interno della rete i comandi impartiti in maniera errata. Esistono già speciali firewall che hanno la capacità di 'sniffare' i protocolli di comunicazione industriali e di autorizzare o meno certi comandi in funzione della sensatezza degli stessi. Sono tuttavia dispositivi costosi, che rendono la macchina o l'impianto meno competitivo e non c'è a oggi una cultura diffusa sul loro utilizzo…".

Di Vito: "Il fattore umano fa purtroppo parte del panorama della sicurezza, poiché la sicurezza si basa in parte sulle policy operative. Il personale deve avere competenze sufficienti per configurare correttamente la sicurezza dei dispositivi connessi, quando vengono distribuiti, e anche per mantenere intatto il livello di sicurezza degli stessi. E, ancora prima, ci deve essere una buona logica nel collegare i dispositivi sensibili, quelli coinvolti in alcune automazioni industriali critiche, a Internet. Pertanto, i tecnici e gli ingegneri incaricati della progettazione e dell'implementazione dei sistemi industriali devono essere ben formati anche sulla gestione il rischio. L'atteggiamento poi è davvero fondamentale per una sicurezza di successo. Al di là delle best practice applicate dalle figure che implementano i sistemi industriali, è necessario applicare l'enforcement. L'applicazione della sicurezza consiste nello spiegare ai dipendenti cosa si può e cosa non si può fare, senza rivelare il modo per disattivare la sicurezza. I dipendenti devono anche essere istruiti in modo che sappiano come operano gli attaccanti. La maggior parte delle violazioni alla sicurezza avviene attraverso il social engineering, per esempio attraverso una semplice telefonata 'fake' con cui l'attaccante chiede la password di amministrazione a un dipendente. Infine, la minaccia interna è anch'essa legata al fattore umano. Per le infrastrutture veramente cruciali tutto il personale deve essere degno di fiducia, quindi devono essere eseguiti controlli di background. Una pratica invadente ma purtroppo molto efficace. Inoltre, l'accesso fisico ai dispositivi sensibili deve essere controllato, come in un datacenter, e la condivisione delle informazioni deve essere attentamente considerata, per cui, per esempio, la password di amministrazione del PLC non deve essere scritta su un post-it…".

Madoglio: "Il fattore umano è sempre fondamentale, indipendentemente dall'ambito e dalle soluzioni tecnologiche adottate. In tale ottica gli atteggiamenti e le competenze degli operatori sono estremamente importanti, in quanto ciascuno di essi costituisce, di fatto, un primo baluardo di difesa dei sistemi aziendali. Ciascun lavoratore dovrebbe essere consapevole delle minacce, dei rischi e dei comportamenti a rischio che potrebbero mettere a repentaglio anche il più sofisticato sistema di sicurezza. Tale consapevolezza può essere raggiunta soltanto tramite un'adeguata formazione. In aggiunta, esistono sistemi automatici che, se resi disponibili agli sviluppatori software, possono essere di ausilio nel controllo del codice, al fine di identificare falle di sicurezza già in fase di scrittura e progettazione delle applicazioni".

Tieghi: "Tutti gli esperti di security ci ricordano che l'anello debole è sempre l'uomo. Davanti allo schermo di un sistema di automazione e controllo ci sono sempre operatori che hanno come compito quello di gestire l'impianto per mandare avanti la produzione o l'erogazione del servizio secondo specifiche definite. Meglio quindi siano sensibilizzati al tema security, formati per poter gestire al meglio eventuali incidenti, che possono compromettere la continuità operativa. Ovvio che se le applicazioni che utilizzano quotidianamente sono state progettate e sviluppate secondo i crismi del 'security by design', molte delle possibili minacce saranno già 'disattivate' e loro potranno concentrarsi maggiormente sull'operatività dell'impianto. In questa direzione ci possono aiutare anche prodotti specifici che, con l'ausilio di apposite applicazioni che utilizzano machine learning e AI, identificano le anomalie e aiutano i responsabili a prevenire eventuali incidenti".

Carlotti: "L'attenzione, la vigilanza e la cautela degli operatori sono fondamentali. Nonostante l'architettura e la strategia di difesa possano essere ottimali, il fattore umano rischia sempre di essere l'anello debole. In questo senso, gli attacchi si sono fatti sempre più pericolosi e mirati, in grado di sfruttare qualsiasi disattenzione dell'utente. Può essere sufficiente una piccola incertezza, anche di un operatore non critico, per mettere in pericolo l'intera infrastruttura. Naturalmente il livello di attenzione deve aumentare in base all'importanza del ruolo ricoperto all'interno dell'azienda. Si suppone poi che siano attive delle misure di sicurezza adeguate a sopperire anche all'errore umano e in grado di ridurre al minimo i disservizi e le conseguenze di un attacco informatico. Qualora la vittima fosse però uno sviluppatore, un sysadmin o il responsabile di un'infrastruttura OT e le credenziali non fossero gestite in sicurezza, il danno potrebbe essere più profondo e propagarsi velocemente all'intera infrastruttura, come accade in caso di attacco alla supply chain. L'attenzione degli utenti, quindi, è un elemento fondamentale perché, nonostante tutti gli investimenti in cybersecurity, il rischio non potrà mai essere nullo.

Nel nostro settore è necessaria una conoscenza approfondita delle dinamiche e dei processi per soddisfare i particolari requisiti di sicurezza informatica dei sistemi di controllo industriale e delle reti OT. Queste ultime sono complesse in quanto utilizzano protocolli e sistemi spesso unici e proprietari, che presentano una serie di vulnerabilità in ambienti mission-critical e legacy. Sulla spinta dell'automazione e della trasformazione digitale, oltre che dell'adozione diffusa delle tecnologie IoT, gli ambienti di pura tecnologia operativa non esistono più. Al contrario, questi stessi ambienti includono molte macchine IT e sensori IoT distribuiti, che rafforzano la visibilità e il controllo del sistema. Produzione intelligente, edifici intelligenti, città intelligenti, reti intelligenti, assistenza sanitaria intelligente: tutti questi settori verticali stanno sfruttando le piattaforme IoT e l'integrazione IT per rispondere alle esigenze del mercato in modo migliore e più rapidamente, nonché per ridurre i costi. In qualità di difensori e ingegneri che devono mantenere i sistemi in esecuzione in modo sicuro e protetto, è importante capire in che modo l'adozione dell'IoT influisca sulla visibilità e sulla sicurezza dei sistemi OT. Non solo, molti progetti di sicurezza si verificano dopo un attacco, quando il cliente si rende conto di non avere visibilità sufficiente sulle proprie reti per rilevare il comportamento dannoso prima di una violazione. In genere, visibilità e rilevamento vengono considerati necessari, ma il budget per queste iniziative viene spesso visto come si trattasse di un'assicurazione, con il risultato di essere considerato solo a posteriori. Sono fondamentali alcuni passaggi, molto prescrittivi, che i fornitori devono intraprendere prima che sia troppo tardi. Deve essere posta maggiore enfasi sulla sicurezza informatica, o attacchi come quelli che abbiamo visto al Colonial Pipeline e all'Oldsmar Water Plant saranno solo l'inizio. Finanziamenti, supporto e linee guida chiare svolgeranno un ruolo importante nel garantire che le nostre infrastrutture critiche siano resilienti e sicure".

Fonte: Pixabay_arthur_bowers

Va fatto uno sforzo importante nella formazione e sensibilizzazione, per portare i concetti di cyber education e cyber hygiene a essere parte del normale bagaglio culturale di ciascun operatore

Cattaneo: "Il fattore umano è determinante. Come si forma alla sicurezza fisica e si verifica l'adesione dei dipendenti ai comportamenti richiesti, così si deve fare per il tema della cybersecurity nel contesto industriale. Si deve creare consapevolezza dei rischi insiti nelle azioni che si compiono, insegnare a distinguere le operazioni a maggior rischio e a evitare di 'aprire le porte' alle minacce agendo in modo improprio. È importante condurre verifiche periodiche e casuali sulle persone, oltre che sui sistemi. Come questi ultimi vengono mantenuti costantemente aggiornati, anche le persone devono essere costantemente allineate alle esigenze di sicurezza informatica aziendali per costituire un'importante linea di difesa".

Bera: "Il fattore umano è determinante e spesso rappresenta l'anello debole delle soluzioni di sicurezza. È fondamentale creare una sempre maggiore 'cybersecurity awareness' e accrescere la cultura relativa alla sicurezza. Altrimenti tutte le misure messe in campo saranno percepite come degli ostacoli al proprio lavoro e gli operatori saranno i primi che cercheranno di aggirarle o di limitarne l'efficacia anche in modo inconsapevole. È necessario investire risorse in formazione sui temi legati alla cybersecurity".

U. Pirovano: "Ci sono due aspetti principali da considerare: da un lato, la cybersecurity è un argomento estremamente specialistico e contemporaneamente multi-disciplinare; dall'altro, l'insieme di complessità e criticità dell'ambito OT in cui risiede l'IIoT. Stiamo assistendo a uno shortage di competenze a livello globale, con una ricerca di professionisti qualificati che possano affrontare i temi sempre più complessi della cybersecurity, mentre la data driven economy richiede di affrontare i temi cyber come fattore abilitante dell'adozione rapida del modello. Diversi studi mostrano che più del 95% degli attacchi rilevati fanno leva su errori umani, quali configurazioni errate, implementazioni incomplete, comportamenti a rischio, patch non applicate ecc. In ciascuno di questi aspetti va fatto uno sforzo importante nella formazione e sensibilizzazione, per portare i concetti di cyber education e cyber hygiene a essere parte del normale bagaglio culturale di ciascuno di noi.

Anche nelle fasi della gestione di un sistema OT informatizzato, il fattore umano è fondamentale, ma è ancora più importante che sia l'infrastruttura di cybersecurity a monitorare l'adozione di metodi di protezione e prevenire configurazioni sbagliate o interruzioni di servizio. Con 5 milioni di nuovi dispositivi IoT connessi ogni ora e una stima di 1,5 miliardi di attacchi nel 2021, è evidente che un approccio puramente reattivo in tutte le fasi della cybersecurity, dal design all'implementazione e fino alla gestione, non sia da considerare. I migliori sistemi di cybersecurity devono implementare nativamente sistemi di telemetria sofisticati (Aiops), in grado di monitorare in realtime l'adozione delle best practice, suggerendo automaticamente modifiche opportune per sfruttare appieno le capacità di protezione. Devono inoltre poter monitorare in modo continuo e predittivo lo stato di corretto funzionamento del sistema, in modo da scongiurare interruzioni di servizio indesiderate. Questi sistemi, assieme a tecnologie capaci di identificare attacchi mai visti prima (ML e deep learning inline nei sistemi cyber), analisi comportamentali avanzate e un approccio architetturale Zero Trust, rappresentano un deciso passo in avanti nella capacità di protezione e prevenzione di attacchi ai sistemi OT".

Le minacce da affrontare

Quali sono le minacce più comuni/probabili e come ci si può difendere?

Marcis: "Attraverso le indagini dei nostri laboratori abbiamo scoperto delle vulnerabilità nei protocolli IoT industriali, nelle interfacce uomo macchina degli impianti idroelettrici, nei radio controlli dei cantieri che pilotano gru e macchinari e nei robot delle catene di produzione. Recentemente, abbiamo indagato anche su come alcune caratteristiche dei linguaggi di programmazione per la robotica industriale possano portare a programmi di automazione vulnerabili

Fonte: Pixabay_geralt

L'accesso fisico ai dispositivi sensibili deve essere controllato e la condivisione delle informazioni deve essere attentamente considerata, per cui, per esempio, la password di amministrazione del PLC non deve essere scritta su un post-it...

e permettere a un aggressore di creare nuove tipologie di malware. Per proteggere i processi industriali si deve pensare a una strategia di security che metta in sicurezza l'intera organizzazione, non solo alcune parti. L'infrastruttura va protetta a tutti i livelli, a partire dagli end-point (PC, tablet, ma anche macchinari), passando per reti, server ecc. È bene comunque non limitarsi a implementare solo soluzioni specifiche per proteggere gli impianti OT, bensì occorrono soluzioni di più ampio respiro, che abilitino una strategia completa, per rilevare attacchi mirati e movimenti sulla rete in tempo reale, avvalendosi anche di capacità di machine learning e custom sandboxing".

L. Pirovano: "La minaccia più comune è rappresentata dall'introduzione di malware nei sistemi per via di hardware esterno, come chiavette USB infette, o tramite l'esposizione dei controllori a Internet. I malware possono essere introdotti anche a seguito di azioni di phishing condotte verso il personale. Un chiaro esempio è la ricezione di email contenenti link che portano al download di virus. Scaricando il malware sui dispositivi utilizzati per lo svolgimento delle attività quotidiane, come il PC di ingegneria, queste apparecchiature vengono infettate e l'attacco viene diffuso alla rete alla quale sono connesse. Tra gli attacchi tipici realizzati tramite malware figurano il DoS (Denial of Service), in cui la rete viene resa indisponibile per mezzo di un elevato invio di dati; l'IP spoofing, in cui pacchetti di dati vengono inseriti in rete con un falso indirizzo sorgente; o ancora l'attacco 'Man in the middle', in cui il traffico di rete viene intercettato con conseguente furto di informazioni, laddove i protocolli utilizzati non usino crittografia. Prima di qualsiasi meccanismo tecnico di difesa è fondamentale che il personale che opera sull'impianto abbia consapevolezza dei rischi e delle policy di sicurezza. Le misure tecnologiche non bastano a prevenire attacchi causati da un uso non idoneo dei dispositivi. Gli attacchi citati in precedenza si possono prevenire grazie all'utilizzo di antivirus o strumenti di whitelisting, che impediscono l'introduzione di potenziali minacce. Un altro aspetto importante è lo studio di un'architettura di rete che favorisca la segmentazione e la riduzione dei domini di broadcast, in modo da confinare il dilagare di un potenziale attacco a una sola porzione della rete di automazione. Non da ultimo, si raccomanda sempre il rafforzamento dei sistemi, con continui aggiornamenti e installazioni di patch per la risoluzione di vulnerabilità, nonché l'utilizzo di protocolli sicuri, dotati di opportuni meccanismi di crittografia e autenticazione, per la trasmissione dei dati in rete".

Previtali: "L'Industria 4.0 è potuta diventare parte dell'agenda mondiale in virtù di costi computazionali ed energetici appetibili, che si dava per scontato potessero permanere internazionali in un'ottica globalista. In questo momento storico, tuttavia, l'intero concetto su cui si basa viene messo totalmente in discussione da costi energetici che stanno divenendo insostenibili, attacchi cibernetici massivi, a cui le aziende non sono preparate, e dissesti generalizzati delle catene di approvvigionamento. Nel momento in cui le premesse stesse vengono a mancare, non è da escludere che l'industria faccia retromarcia per garantire la sua stessa sopravvivenza e si concentri su altri aspetti ancora da ottimizzare, quali un'armonizzazione delle condizioni riservate alla forza lavoro, un'attenzione alla produzione a corto raggio e il rispetto per l'ambiente. Le lezioni sin qui imparate consentiranno in ogni caso al software di avere un peso preponderante, atto a ottimizzare processi produttivi e logistici e creare modelli di vendita rispondenti alle richieste del mercato. Se la crisi dovesse invece placarsi a breve, l'Industria 4.0 è pronta al 'grande balzo' e a uscire una volta per tutte dai modelli teorici e dalle prototipazioni per un'applicazione a 360°. In tal caso, il ruolo dell'individuo nel mondo del lavoro cambierà drasticamente, la sovranità digitale di ciascun individuo sarà sottoposta a revisione e la privacy assumerà una nuova dimensione".

Cattaneo: "Negli ultimi tempi le minacce più comuni che hanno colpito le aziende del settore industriale sono state principalmente ransomware, ovvero malware che 'mettono sotto chiave' i dati aziendali impedendo il funzionamento dei sistemi. I ransomware si infiltrano nei sistemi sfruttando delle falle di sicurezza native, ma possono anche essere il risultato di azioni di phishing o social engineering, sfruttando i punti deboli degli scenari industriali, delle persone e delle infrastrutture. Sono scenari in cui storicamente il tema delle minacce informatiche è emerso più tardi e in cui si scontano dei ritardi culturali e tecnologici. Ritardi che vanno colmati molto rapidamente, laddove presenti, perché oggi con l'avanzata dell'IIoT il perimetro dei sistemi si è estremamente allargato e così anche i potenziali veicoli d'attacco. E, proprio per i recenti fatti internazionali, dobbiamo aspettarci attacchi provenienti da organizzazioni che non hanno più finalità legate al solo riscatto economico, ma che cercano di creare danni concreti alle infrastrutture dei Paesi".

Tieghi: "Vorrei qui riportare alcuni dati che troviamo nell'ultima 'Sans 2021 Survey OT/ICS Cybersecurity': la più alta preoccupazione per oltre il 54% dei CIO/Ciso è il ransomware, senza dimenticare le altre 'classiche' minacce provenienti dall'interno, accidentali come intenzionali. Se dovessimo menzionare le tre o quattro prime cose da fare per difendersi, direi: programmi di security awareness/training per tutti coloro che sono coinvolti in produzione; segmentazione della rete e segregazione degli asset critici secondo quanto indicato nella IEC62443; monitoraggio della rete per avere 'early warning' di eventuali problemi; infine, soprattutto, riguardo al tema ransomware, avere sempre i back up in salvo e tenerli aggiornati, di tutti i dispositivi connessi in rete PC, PLC, switch, firewall ecc.".

Madoglio: "L'ultimo 'FortiGuard Labs Global Threat Landscape Report' ha evidenziato un incremento nell'automazione e nella velocità degli attacchi, mettendo in luce l'esistenza di strategie di cybercrime più avanzate, più distruttive e imprevedibili. In aggiunta, la superficie attaccabile in espansione è un punto focale che i cybercriminali stanno cercando di sfruttare. Ci sono diversi metodi per contrastare i continui mutamenti dei vettori di attacco. Per esempio, è particolarmente efficace l'utilizzo di sistemi che integrano funzionalità di intelligenza artificiale, in quanto sono quelli maggiormente in grado di adattarsi alle evoluzioni dei metodi di attacco, andando a identificare un nuovo threat in base al metodo utilizzato e non alla classica comparazione con definizioni statiche contenute nelle molteplici signature disponibili".

Leoni: "Dato che il governo degli Stati Uniti sta stringendo la sua morsa attorno alle organizzazioni responsabili del ransomware, nel 2022 sarà più probabile assistere a una maggiore concentrazione dei cyberattacchi verso gli Stati europei. Questo perché i cybercriminali si sposteranno su obiettivi più facilmente attaccabili e in Paesi dove è meno presente la minaccia di ritorsione da parte dei governi. Con tensioni crescenti a livello globale, il 2022 sarà un anno record per gli attacchi condotti da Stati sovrani sia per numero che per gravità. La Russia continuerà a giocare un ruolo importante contro gli Stati Uniti, l'Ucraina e altre nazioni. Ci aspettiamo anche che gli attacchi cinesi crescano in volume e aggressività con l'aumento delle ostilità per i divieti tecnologici, le pressioni finanziarie e i boicottaggi diplomatici legati alle Olimpiadi invernali. E se le tensioni aumentano in Medio Oriente, la probabilità che un attacco simile a Stuxnet disabiliti o danneggi gravemente il programma di armi nucleari dell'Iran rimane molto alta. Infrastrutture e settori critici come sanità, trasporti e produzione alimentare sono sempre più visti come obiettivi altamente vulnerabili e lucrativi, in base alla loro capacità di interrompere servizi essenziali. Tra luglio e dicembre 2021 sono state segnalate più di 651 vulnerabilità con un aumento del 21% rispetto ai sei mesi precedenti, e quelle legate alla supply chain continuano a rappresentare la più grande opportunità di creare rapidamente danni su una vasta gamma di prodotti, fornitori di servizi o utenti".

Di Vito: "I dispositivi IIoT sono concretamente esposti a molte minacce. Ovviamente gli attacchi remoti attraverso le reti sono i più probabili, in quanto hanno più impatto, sono più 'comodi' per gli attaccanti che non si espongono personalmente, e possono anche passare inosservati più facilmente, almeno per un po'. I vettori di attacco tradizionali sono gli aggiornamenti del firmware, dove gli aggressori inseriscono il firmware modificato ai dispositivi IIoT che possono raggiungere via Internet, o corrompono il server di distribuzione degli aggiornamenti firmware via etere. Il firmware può anche essere corrotto all'interno della supply chain, quando i dispositivi vengono prodotti. Un altro attacco massicciamente utilizzato consiste nello sfruttamento delle debolezze del protocollo di comunicazione, portando all'esecuzione del codice arbitrario nei dispositivi IIoT. In entrambi i casi l'attacco mira a prendere il controllo del dispositivo per vari scopi. La corruzione del firmware è già stata osservata in attacchi mirati agli impianti industriali, come nel caso del vecchio ma ancora famoso malware Stuxnet, che falsava i valori dei sensori riportati a un PLC, il quale inviava comandi errati agli attuatori, portando a danni fisici. Anche l'impersonificazione dei dispositivi IIoT è efficace. Richiede il furto delle chiavi di autenticazione, che può essere fatto attraverso un attacco intrusivo preliminare su un dispositivo reale. Una volta che la chiave è stata presa, gli attaccanti possono collegare i dispositivi compromessi nelle reti industriali esistenti. L'estrazione della chiave è in teoria più difficile da realizzare e richiede l'accesso fisico ad almeno un dispositivo, ma se la gestione delle chiavi di rete non è ben progettata, il furto di una singola chiave può compromettere l'intera rete, nel caso i dispositivi condividano la stessa chiave di autenticazione. Le misure cruciali per prevenire questi attacchi sono: l'avvio sicuro, gli aggiornamenti sicuri del firmware, l'uso di elementi sicuri, cioè IC sicuri dedicati, per la memorizzazione delle chiavi, e l'esecuzione di algoritmi crittografici per rendere estremamente difficile la maggior parte degli attacchi remoti e intrusivi".

U. Pirovano: "Le minacce relative al mondo IIoT sono in forte crescita. Clusit (Associazione italiana per la sicurezza informatica - www.clusit.it) ha registrato l'aumento più significativo, dal 7% del totale nel 2020 al 18% nel 2021, con un incremento netto del 156%. È importante considerare il peso che questi problemi di cybersecurity potrebbero avere sul business delle aziende del settore. Per anni, l'impatto è stato minimo. La manifattura e gli altri settori non avevano bisogno di collegare i propri sistemi di controllo industriale (ICS) a Internet. Era sufficiente assicurarsi che i processi fisici che quegli ICS stavano supervisionando fossero disponibili, motivo per cui sono stati tenuti offline e lontani dalle minacce che stavano iniziando a prendere forma. Ora, la maggior parte delle aziende ha una presenza digitale, desidera dati in tempo reale in modo da poter monitorare lo stato dei propri processi fisici. Questo le aiuta a eseguire la manutenzione preventiva sulle apparecchiature e a ridurre al minimo i tempi di fermo. Per fare ciò vengono riuniti gli ambienti OT, di cui gli ICS rappresentano una tipologia, e IT. I produttori si stanno rivolgendo all'IIoT come mezzo per utilizzare il lato IT dei dispositivi al fine di ottenere informazioni cruciali sul modo in cui funziona il loro OT. La minaccia più spesso rilevata nel mondo IIoT è di gran lunga il ransomware, associato spesso a campagne mirate di phishing, che danno il via all'attacco. Riguardo al ransomware, si registra un continuo aumento del riscatto richiesto (e molto spesso pagato). La difesa da tali minacce va condotta su due fronti. Il primo è la cyber education degli utenti, per evitare di essere vittime delle campagne di phishing; il secondo è la disponibilità di strumenti avanzati e integrati di sicurezza per rilevare e bloccare il ransomware, basati su AI, che fermino le minacce sconosciute prima che possano causare danni. Fondamentale è adottare un approccio olistico al problema, con soluzioni integrate in grado di avere visibilità su tutta l'infrastruttura, reti ed end-point, e sul comportamento degli utenti, per implementare il paradigma Zero Trust".

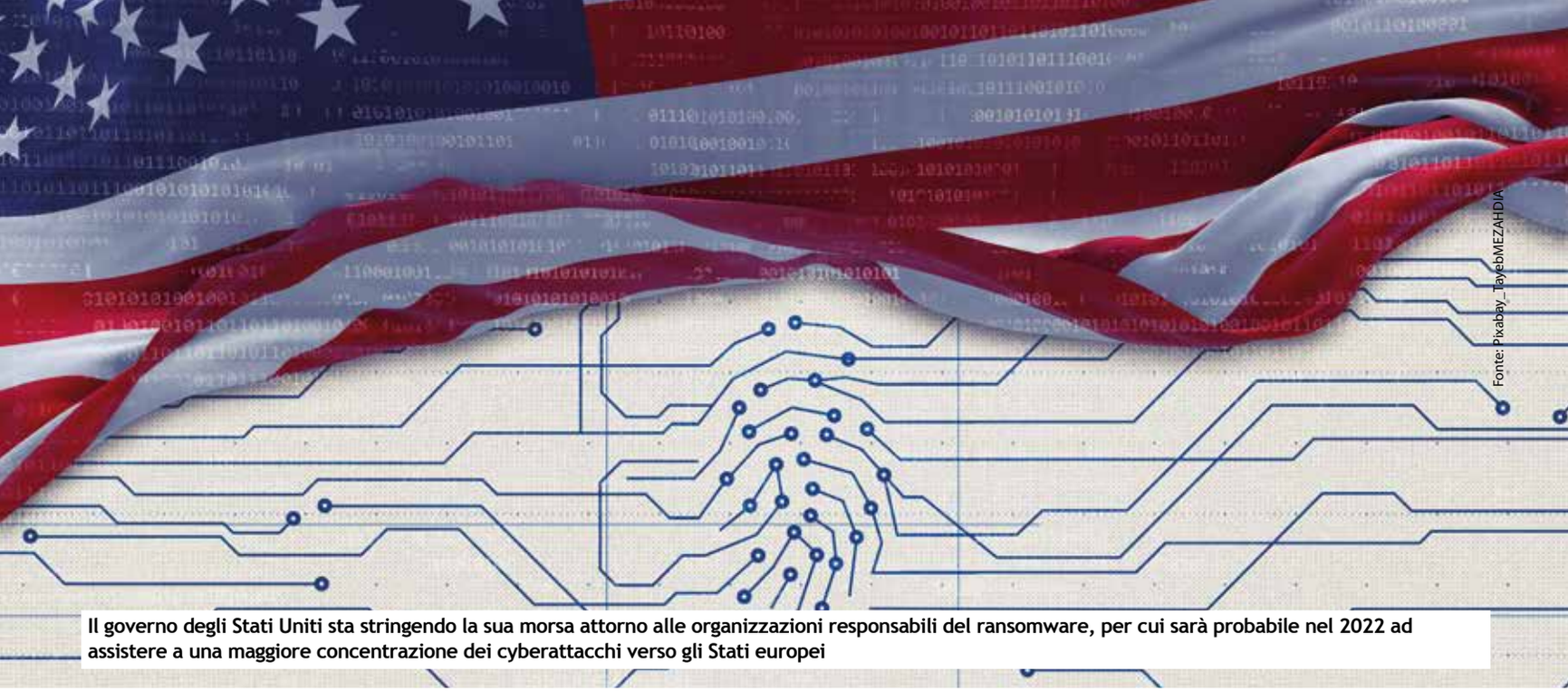
Carlotti: "Gli attacchi di phishing e spear phishing sono sicuramente quelli più comuni e, purtroppo, efficaci. Si tratta infatti di un tipo di minaccia che presenta un ritorno economico più facile e immediato, perché questi attacchi diventano sempre più sofisticati e spesso le vittime, che non sono esperti IT ma dipendenti (a volte) non adeguatamente formati, hanno una maggiore possibilità di cadere nella trappola semplicemente cliccando su un link o aprendo un allegato pericoloso. Un'area ancora spesso sottovalutata è quella dei dispositivi mobile. Il loro utilizzo sempre più massiccio, anche in ambienti aziendali, li ha resi un obiettivo più appetibile e concreto per i cyber criminali, soprattutto perché spesso non sono protetti come gli strumenti più tradizionali. I responsabili OT che stanno iniziando ad 'aprire' le proprie infrastrutture per lavorare anche in smartworking, spesso sottovalutano il rischio proveniente dall'utilizzo di dispositivi mobili personali, come tablet o smartphone, che, se non adeguatamente protetti, potrebbero diventare il punto debole dell'intera infrastruttura. Alla base di tutto ci deve essere la cautela. È necessario aprire un canale di comunicazione solo quando rappresenta un vantaggio reale per il business e, soprattutto, è assolutamente sicuro. Infine, gli attacchi ransomware continuano a essere una delle minacce più comuni e pericolose per le aziende".

Bera: "Le minacce possono essere di vario tipo, ma il rischio maggiore è che venga impattata la disponibilità (availability) degli impianti industriali, con perdite significative di denaro e di immagine per l'azienda che subisce l'attacco. Si va dagli attacchi Denial of Service (DoS e Ddos) ai ransomware, che possono bloccare in tutto o in parte l'impianto con successiva richiesta di riscatto perché riparta, fino a malware che possono far funzionare l'impianto in modo anomalo, con forti implicazioni anche sulla sicurezza fisica. Ci si può difendere considerando la sicurezza una priorità, fin dal progetto di un sistema di automazione (Iacs) per il produttore e per l'asset owner, considerando la sicurezza globale dell'impianto, per esempio attraverso security assestment e penetration test. Va ricordato inoltre che la sicurezza non è una attività 'one shot', ma un processo continuo nel tempo che richiede sorveglianza e azioni continue".

Conseguenze da non sottovalutare

Che cosa rischia chi sottovaluta il problema della sicurezza informatica nel contesto delle reti per l'automazione industriale?

L. Pirovano: "Una violazione della rete IT di un'azienda può avere ripercussioni negative sulle operazioni aziendali quotidiane. Esempi di questo sono il furto informatico di proprietà intellettuale, di informazioni sui clienti o la disabilitazione del sito web dell'azienda rivolto al pubblico. Nel caso di una violazione della rete di automazione industriale, le conseguenze possono essere invece di gravità superiore. La rete OT è l'infrastruttura attraverso la quale fluiscono tutte le informazioni e i segnali gestiti dai controllori per lo sviluppo delle logiche di produzione. È evidente, quindi, che un attacco su questa rete si può riflettere in un'interruzione parziale o totale della produzione, con conseguente danno economico. Avere l'impianto fermo e improduttivo non è l'unica preoccupazione che scaturisce quando si verifica una tale violazione. Dal momento che sulla rete OT operano macchinari adibiti alla realizzazione di prodotti finiti, o alla gestione dei processi, un attacco a tale rete può portare al danneggiamento permanente dei macchinari, con conseguente perdita delle risorse fisiche dell'azienda.
Inoltre, molto spesso, i macchinari presenti in impianto sono complessi e pericolosi, se non opportunamente controllati. Una minaccia informatica atta a causarne un malfunzionamento può persino procurare lesioni o anche la morte agli operatori che utilizzano questi asset. In aggiunta, un attacco informatico può interessare la modifica dei parametri di processo o di lavorazione delle materie prime, con conseguente realizzazione di prodotti con difetti di produzione e, pertanto, danni al consumatore finale. Oltre ai rischi descritti vi è il pericolo di spionaggio e furto di know-how legato all'ingegnerizzazione della macchina e alla gestione del processo produttivo".
Marcis: "Si rischiano ingenti danni materiali, economici e reputazionali. Per fortuna sempre più aziende capiscono l'importanza della protezione e si attivano per mettere al sicuro le proprie infrastrutture e preservare così la continuità del business. Eventuali attacchi potrebbero causare anche danni fisici ai lavoratori che utilizzano i macchinari, o alle persone che vivono nei dintorni di impianti critici, oltre a permettere ai cybercriminali di effettuare ricatti bloccando o minacciando di bloccare la produzione, allo scopo di ottenere denaro".
Leoni: "Il concetto di Industria 4.0, che si basa sul principio dell'integrazione tra fisico e digitale come base di una quarta rivoluzione industriale, non integra la straordinaria ondata di attacchi informatici che le aziende del settore hanno subito negli ultimi anni. Tuttavia, il futuro dell'Industria 4.0 alla luce delle minacce informatiche rappresenta un notevole rischio, la cui entità è difficile da anticipare, valutare e mitigare. Di fronte a questa minaccia, le aziende manifatturiere di tutto il mondo e la loro catena di approvvigionamento devono agire rapidamente e investire massicciamente in nuove tecnologie per proteggere al meglio le attività. Mentre si continueranno a vedere richieste di riscatto multimilionarie, cresceranno al contempo gli attacchi di dimensioni più ridotte, che utilizzeranno tattiche di estorsione multiple come vettore di attacco principale. Difatti, gli attaccanti stanno cercando modalità per aumentare la probabilità di pagamento, pur rimanendo lontani dai riflettori. Ci aspettiamo quindi di vedere violazioni di obiettivi ICS più piccoli, compresi quelli dell'industria alimentare, che hanno tipicamente a disposizione budget minori per la sicurezza, ma che si troveranno ad affrontare gli stessi attacchi delle installazioni ICS più strutturate. Man mano che i cybercriminali continueranno a eseguire le loro strategie, le vittime modificheranno le loro risposte. Vedremo governi e imprese private intraprendere un numero maggiore di azioni offensive, mentre più organizzazioni combatteranno simultaneamente. Le forze dell'ordine rafforzeranno la loro spinta nel recupero di bitcoin e aumenteranno le taglie per le informazioni che porteranno all'arresto dei criminali informatici. Sul lato privato, con ogni probabilità vedremo più organizzazioni che affronteranno direttamente la situazione, assumendo cyberdetective e white hat hacker per trovare e contrastare i cybercriminali".
Di Vito: "L'automazione industriale porta a delegare i processi industriali alle macchine. Le macchine sono molto efficienti quando si tratta di ottimizzare l'esecuzione dei processi, ma occorre stare attenti quando sono responsabili di processi potenzialmente dannosi. I danni causati dall'interruzione di un processo industriale possono variare da un semplice arresto delle operazioni a danni su larga scala. L'arresto di una fabbrica può non causare alcun danno al di là delle perdite finanziarie. L'interruzione del funzionamento di un oleodotto avrà invece una vasta portata causando caos in una città o in un'intera regione. Danneggiare un impianto nucleare sarebbe ancora più pericoloso.
Diventa ovvio che la sicurezza informatica deve essere considerata dal primo giorno. Implementare la sicurezza come un ripensamento è più dispendioso, poiché potrebbero essere stati utilizzati dispositivi hardware inadeguati e impossibili da proteggere. Inoltre, l'integrazione di nuovi dispositivi di sicurezza per riparare le falle può 'disturbare' il livello OT della rete e causare interruzioni. Ultimo ma non meno importante, i requisiti di conformità alla cybersecurity possono evolvere e diventare più severi nel tempo. Questo renderebbe le implementazioni esistenti insicure e obsolete dal punto di vista della sicurezza informatica e causerebbe problemi legali. In conclusione, l'applicazione di linee guida riconosciute come IEC62443, Nist SP800-XXX e l'uso di dispositivi IIoT sicuri sono un must e questo deve essere considerato fin dall'inizio".
Tieghi: "Il rischio va valutato caso per caso, azienda per azienda, impianto per impianto. Come abbiamo detto, il rischio è quello di perdere il controllo del processo controllato. Si può fermare la produzione o l'erogazione di un servizio essenziale. In alcuni casi estremi potrebbero esserci ripercussioni sull'ambiente e anche danni alle persone. Da anni consigliamo che il rischio cyber in fabbrica inizi a essere considerato anche nelle riunioni dei Consigli di Amministrazione".
Previtali: "Di cybersicurezza si è parlato per decenni a vario titolo, non senza creare allarmismi atti a commercializzare soluzioni. Allo stato attuale delle cose, la cybersicurezza non è più un'opzione rimandabile a quando si verifica un eventuale attacco, ma una necessità immediata, una volta intrapresa la migrazione verso il digitale. Le aziende hanno due strade percorribili: creare un dipartimento interno che sovrintenda a questi punti controversi con cognizione di causa e massima sollecitudine, oppure affidarsi a terze parti, il che implica il doversi documentare a priori per scegliere a chi rivolgersi. Poiché l'Italia consta di una costellazione di piccole e medie realtà imprenditoriali, che difficilmente potranno disporre delle risorse atte ad abbracciare la prima ipotesi, si auspica che vengano creati percorsi educativi paralleli a quelli universitari, dalla cui formazione risultino chiare le competenze, anche a chi non ha dimestichezza con il settore, con completa trasparenza e uniformità dei titoli e delle qualifiche. Per chi intraprendesse la digitalizzazione dei processi senza un occhio attento alla sicurezza informatica dell'intera architettura, e non soltanto delle reti, partendo dalla protezione della proprietà intellettuale digitale in tutte le sue forme (firmware, software e dati), i rischi consistono in fermi macchina o interruzione dell'intera attività aziendale, screditamento pubblico, azioni legali di clienti e/o fornitori. In definitiva, un impattante calo degli introiti, che difficilmente il nostro tessuto imprenditoriale può sostenere. Quest'ultimo, tuttavia, è anche la nostra forza. Così come in ambito finanziario la diversificazione è fondamentale, l'economia italiana ha sempre puntato sulla flessibilità che le viene da realtà agili, da organigrammi snelli e da decisioni rapide".
Carlotti: "L'infrastruttura industriale è tipicamente un sistema fortemente legato a soluzioni di sicurezza tradizionali, perciò esposta costantemente a nuovi attacchi. I rischi purtroppo sono enormi e legati ai diversi obiettivi dell'attaccante, che si tratti del semplice ritorno economico, o della volontà di interrompere le attività di un'azienda, magari per giorni. Pensiamo per esempio al settore ferroviario, dove un attacco ai sistemi potrebbe avere conseguenze realmente


Fonte: Pixabay_TayebMEZAHDIA

Il governo degli Stati Uniti sta stringendo la sua morsa attorno alle organizzazioni responsabili del ransomware, per cui sarà probabile nel 2022 ad assistere a una maggiore concentrazione dei cyberattacchi verso gli Stati europei

disastrose, con i cybercriminali in grado di gestire o modificare uno scambio o un semaforo ferroviario senza che i sistemi di controllo, per esempio, anch'essi compromessi dagli attaccanti, siano in grado di rilevarlo in tempo. L'impatto potrebbe essere catastrofico. Per questo è fondamentale che la consapevolezza sulla sicurezza diventi una reale priorità in ogni azienda, indipendentemente dal settore di appartenenza e dal grado di digitalizzazione".

Bera: "I rischi sono altissimi sia a livello economico, sia di immagine. Le infrastrutture critiche come centrali elettriche, impianti chimici, acquedotti, sono sicuramente obiettivi primari. In generale, qualunque sistema di automazione industriale collegato a Internet è un obiettivo potenziale".

Madoglio: "I rischi possono essere molteplici: dall'indisponibilità dei dati di produzione e di business, al blocco totale di una linea di produzione. Per questo motivo è strategico non sottovalutare il problema e mettere in opera strategie e soluzioni efficaci per contrastarlo. Così come le minacce si evolvono, anche i metodi di difesa si devono adeguare alla stessa velocità. È quindi indispensabile avere dei processi aziendali che tengano sotto controllo il livello di rischio della rete OT e ne propongano un continuo aggiornamento, per evitare di rimanere scoperti di fronte a nuove tipologie di minacce informatiche".

U. Pirovano: "Per qualsiasi organizzazione, la rete e gli elementi a essa interconnessi sono ormai elementi chiave, direttamente legati al business, e veicolano informazioni di vitale importanza. Le reti per l'automazione industriale sono addirittura più critiche, dato che hanno lo scopo di gestire e supervisionare direttamente il processo industriale. Sottovalutare il problema della sicurezza in questo contesto espone l'azienda a un rischio altissimo. Questo era stato, fino a poco tempo fa, il motivo principale per cui le reti OT erano state tenute disconnesse da Internet, ma ora che questo non è più possibile, bisogna tenere conto di molteplici rischi, tra cui: furto di dati, che possono includere proprietà intellettuali, informazioni strategiche; furto del controllo dei dispositivi appartenenti all'impianto industriale, con diversi possibili effetti quali blocco dell'operatività dell'impianto, con conseguente perdita economica e danni alle infrastrutture e agli elementi dell'impianto. Potenzialmente, danni al personale, come possibile effetto collaterale dei danni ai dispositivi. Uno dei maggiori rischi è legato al ransomware, ovvero la crittografia di dati fondamentali per l'organizzazione con richiesta di riscatto o pubblicazione di dati rubati all'organizzazione, per lederne l'immagine e fare pressione per ottenere il pagamento del riscatto. I dati pubblicati possono essere, per esempio, proprietà intellettuali o informazioni relative alla clientela. A questi si aggiungono i danni di immagine, effetto 'collaterale' dei rischi prima elencati, ma con ripercussioni molto importanti sul business. Sono solo alcuni esempi che sottolineano l'importanza della cybersecurity in ambito OT".

Cattaneo: "Ci sono principalmente tre livelli di rischio: economico-finanziario, ambientale e per le persone. Ai rischi finanziari legati a fermi macchina e blocchi della produzione, che possono costare anche centinaia di migliaia di euro al giorno, si sommano i danni economici indiretti, per esempio dovuti a ritardi nelle consegne, sprechi di materia prima, danneggiamento del prodotto finito ecc. In vari settori industriali vi è anche un rischio ambientale elevato, legato all'utilizzo di materiali pericolosi o di emissioni potenzialmente nocive che vanno gestite. In tutti i casi, poi, possono essere a rischio le persone. La sicurezza fisica può essere impattata nell'immediato da un attacco che interessi i sistemi operativi, che rende per esempio inefficaci o meno controllate le misure di protezione. Persone, macchinari, sistemi sono strettamente interconnessi e non è più ammissibile affrontare il tema della sicurezza informatica con poca attenzione".

Un compito 'a tempo pieno'

Volendo concludere, è evidente come la sempre maggior connessione dei sistemi industriali abbia aumentato le opportunità di un attacco contro la proprietà intellettuale, rendendo necessario un cambio di mentalità nella gestione delle minacce, attività che deve diventare un compito a tempo pieno. In particolare, gli operatori del settore dell'automazione industriale devono:

- adottare una mentalità di sicurezza basata sul rischio (legando la criticità aziendale alle strategie di difesa);
- predisporre un inventario accurato e aggiornato delle risorse OT in tempo reale;
- combinare le strategie di difesa di IT e OT per controbattere su tutte le possibili superfici di attacco;
- identificare e aggiornare i sistemi obsoleti, vulnerabili e scarsamente protetti;
- vigilare per individuare potenziali nuove minacce, ordinandole in base al rischio connesso;
- garantire che i fornitori di tecnologia e i produttori di apparecchiature connesse si impegnino a eseguire regolarmente patch e audit di sicurezza e software.
- Diviene pertanto necessario anche in un contesto industriale attivare servizi di intelligence sulle minacce e sistemi di allerta precoce per scoprire attacchi pianificati. Prevenire le violazioni e intraprendere azioni immediate per proteggere le risorse aziendali digitali e l'infrastruttura fisica sarà sempre più un compito a tempo pieno, che non ci si potrà permettere di trascurare.