WHITE PAPER

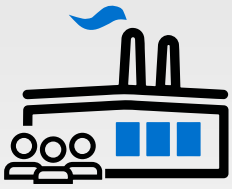
Proteggere l'Industria 4.0

Considerazioni e impatto sull'OT

Sintesi preliminare

L'iIndustria 4.0 include la modernizzazione degli ambienti basati sulla tecnologia operativa (OT) per migliorare l'efficienza dei processi aziendali e fornire più dati per il processo decisionale collegando sistemi che in precedenza erano isolati. Tuttavia, la convergenza di questi sistemi comporta ripercussioni significative in termini di sicurezza. Infatti, 9 organizzazioni su 10 hanno subito un'intrusione che ha causato danni alla produttività, ai ricavi, alla fiducia nel marchio, alla proprietà intellettuale e alla sicurezza fisica.[1] La maggioranza (70%) dei responsabili nel settore manifatturiero intervistati indica che la sicurezza informatica OT è almeno uno dei cinque principali rischi per la loro azienda.[2]

La trasformazione digitale e la crescente dipendenza dai dati è una tendenza universale. McKinsey sostiene che il COVID-19 ha accelerato il cambiamento; l'adozione digitale è cresciuta di cinque anni in sole otto settimane.[3] In molti settori, sembra che la tendenza alla trasformazione digitale non potrà che aumentare, e la produzione non fa eccezione. Anche se la minaccia posta dagli attacchi informatici è innegabile, molte organizzazioni manifatturiere stanno cercando di individuare le componenti fondamentali necessarie per affrontare i rischi di sicurezza nell'era dell'Industria 4.0.



Più dell'80% dei responsabili della produzione prevede che nel prossimo esercizio il budget dell'azienda per la sicurezza OT aumenterà.[4]

Industria 4.0 e la convergenza dell'OT e dell'IT

La trasformazione digitale della produzione è motivata dalla promessa dell'Industria 4.0, quarta rivoluzione industriale. La prima è stata la meccanizzazione, la seconda la produzione di massa e le catene di montaggio con l'avvento dell'elettricità, la terza l'adozione di computer e automazione. Ora l'Industria 4.0 migliora l'automazione con sistemi alimentati da dati e apprendimento automatico, un viaggio che ha portato alla convergenza delle reti di tecnologia operativa (OT) e tecnologia dell'informazione (IT).

Gli ambienti OT possono includere sistemi di controllo industriale (ICS) che fanno funzionare attrezzature o macchinari. Sono generalmente gestiti utilizzando controllori logici programmabili (PLC), eventualmente con sistemi SCADA che forniscono un'interfaccia utente grafica per gli ICS. Mentre l'OT controlla le apparecchiature, l'IT controlla i dati. L'IT si preoccupa garantire la riservatezza, l'integrità e la disponibilità dei sistemi e dei dati, mentre l'OT si concentra sulla sicurezza e la disponibilità delle macchine.

L'Industria 4.0 comporta l'adozione dell'automazione e dello scambio di dati nelle tecnologie e nei processi di produzione, tra cui Internet of Things (IoT) e Industrial Internet of Things (IIoT), cloud computing, cognitive computing, intelligenza artificiale e sistemi cyber-fisici (CPS). Tuttavia, l'Industria 4.0 aumenta anche le sfide che sono emerse dalla convergenza delle reti OT e IT. Con i loro team specializzati e i sistemi di controllo e le tecnologie legacy spesso senza patch, le reti OT affrontano una maggiore esposizione, diretta conseguenza della maggiore connettività. Questa connessione dei sistemi interni con risorse al di fuori del perimetro tradizionale della fabbrica ha modificato l'intero ecosistema di sicurezza dell'OT, lasciando gli esperti di IT e OT a lottare per proteggere sia l'infrastruttura aziendale che l'ambiente di produzione.

Implicazioni per la sicurezza dell'Industria 4.0

Uno degli obiettivi fondamentali dell'Industria 4.0 è quello di allineare i processi di produttivi e aziendali, in modo che la produzione funzioni di concerto con le realtà dell'azienda. Questo flusso di dati è realizzato al meglio da una rete concettuale; tuttavia, l'introduzione di fonti esterne di dati e accesso aumenta il potenziale di intrusione di hacker e campagne mirate alla perturbazione cyber-fisica. Tradizionalmente, la sicurezza industriale veniva mantenuta prevedendo la totale separazione tra rete IT e rete OT. Questo processo, noto come "air gapping", isolava le attrezzature e le tecnologie OT vulnerabili e fragili dalle reti aziendali. L'intenzione era quella di proteggerle dalla maggior parte degli attacchi esterni e dalle campagne volte a interrompere le attività.

Man mano che le aziende si trasformano, i cambiamenti nel modo in cui queste reti vengono gestite devono tenere conto e investire proporzionalmente nelle best practice di sicurezza informatica, perché sistemi come le applicazioni di produzione, i sistemi MRP (Material Requirements Planning), i PLC, l'interfaccia uomo-macchina (HMI) e altri componenti ora sono tutti interconnessi.

Quando le reti IT e OT sono collegate anche solo in misura limitata, si può riproporre un ampio spettro di vettori di attacco alla rete. Gli attacchi che prima miravano all'accesso alle reti IT possono essere utilizzati per attaccare anche obiettivi OT.

Attacchi informatici contro infrastrutture critiche possono causare danni gravi, che vanno ben oltre i titoli sensazionalistici in prima pagina. Un crash del sistema industriale nel settore manifatturiero può letteralmente bloccare la produzione per ore, rovinare materiali sensibili a metà del processo con perdite di milioni di dollari ed esporre le organizzazioni a potenziali sanzioni per mancata conformità. Questa nuova serie di vettori di attacco che prendono di mira l'OT può avere un impatto notevole sui processi cyber-fisici di cui i cittadini si fidano, ed è importante comprendere l'impatto collaterale di un attacco. Impedire la fornitura di risorse, paralizzare sistemi di difesa nazionali e persino arrecare danno a civili innocenti sono solo alcune delle potenziali conseguenze di un attacco.

Secondo i dati raccolti, ora quasi tre quarti delle organizzazioni hanno almeno di connessioni di base tra IT e OT.[5]

Rischi per la sicurezza dell'OT

L'OT è particolarmente vulnerabile sia alle minacce avanzate che a quelle legacy perché i sistemi distribuiti spesso hanno dai 20 ai 30 anni. I sistemi sono a rischio perché gli ICS spesso usano comunicazioni non autenticate o non crittografate. Le attrezzature installate ha inoltre un lungo ciclo di vita e sono spesso costituite da una serie di prodotti diversi provenienti da più fornitori che utilizzano diversi protocolli industriali. La sicurezza e la continuità del funzionamento sono una priorità assoluta, per cui un'azione semplice come una scansione attiva può causare il guasto del dispositivo e interrompere la produzione con gravi conseguenze.

Le componenti essenziali della sicurezza dell'Industria 4.0

Per avanzare nel mondo dell'Industria 4.0, i produttori stanno rivalutando la loro architettura esistente concentrandosi sulla riduzione della complessità e della frammentazione delle distribuzioni di sicurezza dei punti isolati e sarebbe opportuno anche che rivalutassero i loro programmi informatici per garantire che le pratiche di sicurezza si evolvano con le iniziative dell'azienda nell'ambito di una strategia unica, integrata e improntata alla sicurezza. È infatti necessario che le organizzazioni valutino a che punto sono, comprese le risorse che hanno a disposizione, per poi valutare i loro processi e studiare le alternative per migliorare l'agilità e la sicurezza. Forti di queste informazioni, possono quindi cercare soluzioni che le aiuteranno a progredire verso la maturità del sistema OT nell'ottica della sicurezza informatica.

Componente 1: valutare lo stato attuale

Gli standard di sicurezza informatica possono aiutare a orientare e guidare le organizzazioni verso lo sviluppo e l'attuazione di una strategia di sicurezza. Le organizzazioni dovrebbero lavorare partendo da standard consolidati come NIST o IEC 62443 per stabilire a che punto sono e dove dovrebbero essere in termini di sicurezza. Avvalendosi dei consigli di esperti del settore, i responsabili possono accrescere le loro conoscenze e soddisfare meglio gli obiettivi di sicurezza delle loro aziende.

Il NIST Cybersecurity Framework (CSF) fornisce un quadro per un programma di sicurezza convergente, nonché un linguaggio comune per migliorare le comunicazioni, la comprensione e la collaborazione tra IT e OT. I produttori possono impiegare il NIST CSF per aiutare a garantire che la loro transizione digitale soddisfi i loro obiettivi aziendali in termini di organizzazione, nonché a identificare e rendere operativi i cambiamenti necessari dell'infrastruttura, siano essi relativi a persone, processi o tecnologia.

Lo standard IEC 62443 offre un altro quadro comune che può essere usato per gestire e mitigare le vulnerabilità a livello di sicurezza nei sistemi di controllo dell'automazione industriale, oltre a offrire indicazioni su come scegliere prodotti in grado di migliorare efficacemente la strategia difensiva ICS di un'organizzazione, bilanciando i costi che ne derivano e la riduzione dei rischi.

Componente 2: considerare i requisiti della forza lavoro

È necessario che le aziende OT esaminino lo stato della loro forza lavoro nel suo complesso e determinino i modi per affrontare le differenze intrinseche a livello di cultura, scopo e principi tra il personale IT e OT. I produttori devono inoltre considerare le esigenze dei lavoratori a distanza. L'avvento della pandemia di COVID-19 ha imposto la rapida adozione di soluzioni globali di telelavoro, ma ha creato anche rischi notevoli. Il bisogno di mettere in sicurezza i lavoratori a distanza ha sottoposto i sistemi di sicurezza a pressioni senza precedenti, soprattutto nelle aree della migrazione al cloud e della proliferazione degli endpoint. E, dopo la pandemia, il lavoro a distanza non è destinato a scomparire.

Anche con una maggiore consapevolezza della sicurezza informatica e iniziative di formazione, il phishing continua ad essere un problema enorme e le aziende affrontano rischi considerevoli derivanti dalle minacce interne. I danni attribuibili all'attività degli insider possono essere difficili da rintracciare, poiché queste minacce sono associate a una vasta di comportamenti e motivazioni. Ed è ancora più difficile quando i dipendenti non sono in sede. I produttori devono essere in grado di gestire in modo sicuro chiunque utilizzi qualsiasi dispositivo da qualunque luogo, compresi i dipendenti in sede presso l'azienda, lo stabilimento o il magazzino, i dirigenti, i lavoratori a contratto e i lavoratori temporanei.

Il 44% delle organizzazioni non traccia e documenta il rispetto delle regolamentazioni di settore.[9]

Con il cambiamento dei ruoli, i team interfunzionali e l'aumento della collaborazione, arrivano relazioni complesse e una proprietà poco chiara. I reparti, i team e le persone che erano isolati nei giorni precedenti all'Industria 4.0 ora devono bilanciare e rispettare i reciproci valori, nonostante spesso abbiano obiettivi in competizione. CISO, CTO, architetti IT, CIO, direttori di stabilimento e analisti di rete devono considerare la necessità di lavorare intensamente e raggiungere il consenso su questioni come la riservatezza (la massima priorità per l'IT) e la disponibilità (la massima priorità per l'OT, insieme alla sicurezza fisica dei dipendenti dello stabilimento). Per una resilienza aziendale durevole, è essenziale che le organizzazioni collaborino per rafforzare la loro strategia di sicurezza aziendale.

Componente 3: condurre processi di analisi

Con la trasformazione digitale delle aziende, vengono apportati dei cambiamenti sia alle tecnologie che ai processi aziendali. L'industria 4.0 parla di come la tecnologia può automatizzare i processi che in futuro potrebbero essere svolti in meno passaggi. L'industria 4.0 utilizza ampiamente i dati per aiutare a migliorare l'efficienza in tutto un processo aziendale che può andare dalla catena di approvvigionamento all'esperienza del cliente per prendere decisioni più informate.

Tutti i processi potrebbero beneficiare di un miglioramento, dall'elaborazione degli ordini, alla produzione dei prodotti, alla fatturazione ai clienti, al rilevamento e alla risposta a una potenziale violazione della sicurezza. In ogni area, dovrebbe essere eseguita una valutazione per soppesare il guadagno di efficienza rispetto al rischio per l'azienda.

Le organizzazioni dovrebbero eseguire questo tipo di analisi disciplinata dei processi aziendali perché l'aumento della digitalizzazione significa che più dati vengono raccolti e condivisi tra sistemi e processi che prima non erano collegati. Man mano che le organizzazioni identificano aree da migliorare e digitalizzare, devono anche individuare eventuali carenze o lacune di sicurezza che logicamente emergono.

Con l'efficienza e l'ottimizzazione dell'azienda come priorità, più organizzazioni stanno incorporando i servizi cloud nell'ambito dei miglioramenti apportati ai processi. I produttori stanno rapidamente adottando più servizi basati sul cloud, come la pianificazione delle risorse di produzione (MRP) e i sistemi di pianificazione delle risorse aziendali (ERP). Questi sistemi spesso estraggono dati sia dai sistemi IT che dai sistemi OT per un processo decisionale rapido ed efficace. Garantire la protezione della sicurezza informatica per queste risorse è fondamentale, perché l'architettura può andare dal data center ai sistemi industriali e a più cloud.

Componente 4: aggiornare la tecnologia

Per supportare l'Industria 4.0, le organizzazioni devono garantire che la loro sicurezza OT e IT sia pronta anche per gli attacchi più sofisticati. Una soluzione di sicurezza informatica completa deve essere in grado di coprire l'intera superficie di attacco, condividere la threat intelligence tra i prodotti di sicurezza e automatizzare le risposte alle minacce. La protezione di un ambiente Industria 4.0 convergente comprende cinque best practice.

1. **Ottenere la visibilità della rete identificando e classificando le risorse e stabilendone la priorità**

   Mantenere un inventario aggiornato degli ambienti e delle risorse IT e OT di un'organizzazione facilita la pianificazione e la consapevolezza della sicurezza di base. Le organizzazioni non possono proteggere nessuna parte della loro infrastruttura che non possono vedere, quindi hanno bisogno di un inventario aggiornato dei dispositivi e delle applicazioni in esecuzione nelle loro reti. Questi dispositivi e applicazioni dovrebbero essere identificati e profilati in base alle loro caratteristiche e al loro comportamento.

2. Segmentare la rete

La segmentazione è uno dei concetti architettonici più efficaci per proteggere gli ambienti di rete. La mancanza o l'inadeguatezza della segmentazione IT/OT può sicuramente consentire uno sfruttamento più ampio quando una vulnerabilità viene rivelata su una rete OT. Con una corretta segmentazione della rete, la rete è compartimentata in una serie di segmenti funzionali o zone che possono includere sottozone o microsegmenti. Ogni zona è accessibile solo da dispositivi, applicazioni e utenti preautorizzati. Un firewall di prossima generazione (NGFW) definisce e fa rispettare le zone di controllo. Il firewall NGFW definisce anche i conduit, ossia canali che consentono a dati e applicazioni essenziali di passare in modo sicuro da una zona all'altra.

Questo modello architettonico di zone e conduit riduce notevolmente il rischio di contaminazione e sfruttamento di un'ampia infrastruttura limitando l'impatto potenziale di una violazione poiché riduce la capacità di un aggressore di muoversi in direzione orizzontale (est-ovest) o verticale (nord-sud) all'interno della rete OT. Gli utenti o i dispositivi autorizzati per una specifica attività in una determinata zona possono solo operare all'interno di quella zona. Il modello delle zone e dei conduit deve essere dinamico, non statico, con un controllo capillare dell'accesso che monitora continuamente i livelli di fiducia e adatta di conseguenza le policy di sicurezza.

Il 54% delle persone con incarichi di responsabilità che possono svolti essenzialmente anche a distanza afferma di voler lavorare da casa per tutto o per la maggior parte del tempo anche quando la pandemia sarà superata.[10]

3. Analizzare il traffico

I firewall servono per dividere una rete in zone, segmenti e conduit, ma è altrettanto importante analizzare il traffico di rete per rilevare le minacce note e sconosciute. Le organizzazioni OT possono ottenere una protezione aggiuntiva contro le vulnerabilità per applicazioni e dispositivi dai principali produttori ICS. Poiché molti dispositivi OT funzionano senza patch, la capacità di identificare e neutralizzare gli exploit e proteggerli con "patch virtuali" è preziosa. Il traffico di rete dovrebbe essere presentato nel contesto degli eventi di rete. Anziché incrociare manualmente i dati, è possibile utilizzare un motore intelligente di identificazione di infrastrutture e applicazioni in grado di individuare e rappresentare graficamente la topologia dell'infrastruttura fisica e virtuale, dei sistemi on-premises e dei cloud pubblici e privati con l'impiego di credenziali e senza alcuna precedente conoscenza dei dispositivi o delle applicazioni.

4. Controllare l'accesso

Dispositivi, utenti e applicazioni devono essere autenticati prima di accedere all'ambiente OT o a qualsiasi risorsa segmentata. L'autenticazione sicura è fondamentale. Molte delle violazioni della sicurezza OT più dannose sono state causate da account utente e password compromessi e aggravate dall'assegnazione di livelli di accesso inappropriati agli utenti.

I produttori hanno bisogno di soluzioni che possano al tempo stesso convalidare chi e cosa si sta connettendo alla rete e limitarne l'accesso solo alle risorse essenziali. Impiegando soluzioni di controllo, si possono applicare policy e intraprendere azioni appropriate in base alle necessità, senza interrompere l'attività dei sistemi critici o spegnerli. L'autenticazione a più fattori (MFA) e la capacità di limitare l'accesso alla rete a utenti e dispositivi autenticati sono capacità importanti. Le soluzioni di controllo dell'accesso alla rete dovrebbero coprire ogni parte dell'infrastruttura, compresi perimetro, 5G, IIoT e cloud ibrido e pubblico.

5. Proteggere l'accesso cablato e wireless

Storicamente, le infrastrutture di rete OT erano meno dipendenti dalla connettività wireless nelle attività produttive. Tuttavia, sempre più organizzazioni OT stanno distribuendo sensori e altri dispositivi IIoT nei loro ambienti OT e si connettono utilizzando la tecnologia wireless. L'espansione della portata e della frequenza di queste connessioni aumenta proporzionalmente la superficie di attacco digitale. Gli access point wireless e gli switch di rete sono bersagli accattivanti per gli attacchi informatici. Sia gli access point che gli switch hanno bisogno di essere protetti nel contesto della progettazione dell'intera infrastruttura, affidando la gestione della sicurezza a un'interfaccia centrale, anziché essere protetti da soluzioni di sicurezza puntuali aggiunte in un secondo momento e gestite da più interfacce. La gestione

centralizzata della sicurezza non solo riduce il rischio e rende più facile l'applicazione delle policy, ma migliora anche la visibilità e ottimizza i tempi di intervento per i team responsabili della gestione operativa e della sicurezza.

Componente 5: aggiungere intelligence e reporting utili per l'azione

Oltre all'adozione delle best practice in materia di sicurezza informatica, lo sviluppo di una strategia di sicurezza completa per l'Industria 4.0 dovrebbe includere la condivisione integrata e automatizzata della threat intelligence e il reporting della compliance. Ai CISO occorre un approccio proattivo alla soluzione di sicurezza per l'OT che copra e possa comunicare automaticamente la presenza di qualsiasi minaccia industriale identificata all'ecosistema OT. L'intelligence utile per l'azione dovrebbe essere distribuita per difendere in modo proattivo gli ambienti OT attraverso ogni elemento della sicurezza, dal data center e dal campus principale fino al perimetro della rete.

Gran parte (78%) delle organizzazioni ha solo una visibilità centralizzata parziale dei propri ambienti OT.[11]

La strada verso l'Industria 4.0

Per ottenere il massimo dall'odierno modello aziendale digitale in espansione e creare valore nell'era dell'Industria 4.0, i produttori devono affrontare la questione critica della sicurezza OT e, quando supportano l'Industria 4.0 e modernizzano il loro ambiente OT, è fondamentale che analizzino e strutturino una strategia di trasformazione con un approccio incentrato sulla sicurezza. Partendo dall'analisi del loro stato attuale, delle loro risorse e delle loro iniziative per migliorare i processi aziendali, possono poi introdurvi miglioramenti a livello di tecnologia e sicurezza che li aiuteranno a raggiungere i loro obiettivi.

Creando un ambiente che garantisca visibilità, controllo e monitoraggio continuo, i produttori riusciranno a proteggere le nuove reti IT e OT convergenti che supportano le loro iniziative Industria 4.0. Adottando misure per garantire che la loro strategia rimanga agile, riusciranno man mano ad adattarsi ai cambiamenti dell'attività, dell'industria e della tecnologia.

[1] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, 30 giugno 2020.

[2] David Beckoff, et al., "Securing Critical Operational Technology in Manufacturing: Managing Cyber Risk, Readiness, and Resilience," Manufacturers Alliance for Productivity and Innovation, 2020.

[3] Aamer Baig, et al., "The COVID-19 recovery will be digital: A plan for the first 90 days," McKinsey Digital, 14 maggio 2020.

[4] David Beckoff, et al., "Securing Critical Operational Technology in Manufacturing: Managing Cyber Risk, Readiness, and Resilience," Manufacturers Alliance for Productivity and Innovation, 2020.

[5] "Independent Study Pinpoints Significant SCADA/ICS Security Risks," Fortinet, 28 giugno 2019.

[6] "Microsoft Digital Defense Report," Microsoft, settembre 2020.

[7] David Beckoff, et al., "Securing Critical Operational Technology in Manufacturing: Managing Cyber Risk, Readiness, and Resilience," Manufacturers Alliance for Productivity and Innovation, 2020.

[8] Ibid.

[9] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, 30 giugno 2020.

[10] Kim Parker, et al., "How the Coronavirus Outbreak Has—and Hasn't—Changed the Way Americans Work," Pew Research Center, 9 dicembre 2020.

[11] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, 30 giugno 2020.

FORTINET

www.fortinet.com

settembre 14, 2021 2:45 PM

wp-FA-ot-considerations-and-impact_A4_4282021-IT

989802-0-1-IT