Un approccio di sicurezza per la protezione delle reti IT e OT convergenti

Sommario

FORTINET

Sintesi preliminare

Le reti OT (Operational Technology)*, che controllano le **apparecchiature** in infrastrutture critiche quali utenze e catene di montaggio, sono state tradizionalmente mantenute separate dalle **reti IT (Information Technology)**, che controllano i **dati** in tutte le organizzazioni. Negli ultimi anni, importanti innovazioni nel settore IT, come l'intelligenza artificiale (IA) e l'analisi dei big data, promettono miglioramenti anche per le reti OT. Di conseguenza, l'integrazione delle reti OT e IT è in rapida accelerazione, portando a un'espansione della superficie di attacco digitale ed esponendo le reti OT agli attacchi provenienti dalle reti IT. Le violazioni delle reti OT sono ora eventi comuni. Per contrastare gli attacchi e ridurre al minimo i rischi per tale reti, è necessario porre in atto cinque best practice: 1) aumentare la visibilità della rete, 2) segmentare le reti, 3) analizzare il traffico per individuare le minacce, 4) applicare regole di gestione di identità e accessi e 5) proteggere gli accessi via cavo e wireless. Queste misure consentono di stabilire solide fondamenta per migliorare la strategia di sicurezza delle reti OT.

* OT è sinonimo di **ICS (Industrial Control System, sistema di controllo industriale)**. Il termine OT è stato coniato in contrapposizione a IT, perché i protocolli, i fornitori e i casi d'uso dell'OT sono distinti. **I sistemi SCADA (Supervisory Control And Data Acquisition)** sono un elemento dell'OT. I sistemi SCADA utilizzano interfacce grafiche utente per la supervisione ad alto livello dei processi OT/ICS.

01: I motivi della convergenza tra IT e OT

Dall'apprendimento automatico (ML, Machine Learning) alla realtà aumentata (AR, Augmented Reality) all'Internet of Things (IoT), i nuovi sviluppi nell'IT stanno portando a trasformazioni dei processi e miglioramenti dei risultati in molti settori dell'economia. Generalmente ci si riferisce a questa evoluzione con il termine di trasformazione digitale (DX).

Nelle reti OT, che controllano infrastrutture critiche come condutture, reti elettriche, sistemi di trasporto e impianti di produzione, i cambiamenti sono più lenti. Gli ambienti OT sono vitali per la sicurezza pubblica e il benessere economico globale. Sono stati sviluppati decenni prima delle reti IT e sono caratterizzati da diversi fornitori e da protocolli proprietari. All'inizio non c'era motivo di collegare le reti OT e IT, soprattutto in considerazione del rischio di aumento di attacchi informatici.

Tuttavia, tre quarti delle organizzazioni OT intervistate in un recente sondaggio hanno rivelato di aver realizzato almeno connessioni di base tra IT e OT per aumentare la produttività e ridurre i costi.[1]

Le nuove tecnologie digitali negli ambienti OT sono alla base di cambiamenti abbastanza importanti da essere definiti come la Quarta Rivoluzione Industriale.[2] I sensori stanno ottimizzando le linee di produzione.[3] Gli occhiali per la realtà aumentata stanno riducendo gli errori per i magazzinieri.[4] I guadagni sono significativi: le organizzazioni che si posizionano nel quartile superiore della trasformazione digitale hanno conseguito quasi il doppio dei margini e dei profitti del quartile inferiore.[5]

I leader nella DX guadagnano 2 volte i margini e i profitti dei ritardatari.

Il problema, quando si integrano IT e OT, è costituito dall'aumento della superficie di attacco digitale, che accentua il rischio di attacchi informatici. Quasi il 90% delle organizzazioni con ambienti OT ha registrato una violazione delle loro reti OT.[6]

Quasi il 90% degli ambienti OT ha subito violazioni.

02: Best practice per la sicurezza degli ambienti OT

Come ridurre al minimo i rischi e al tempo stesso massimizzare i guadagni? Le seguenti sono cinque aree che i leader in ambito OT devono controllare per proteggersi dagli attacchi dei cybercriminali.

1. Individuare e classificare le risorse e stabilirne la priorità in base al valore

Il miglioramento della strategia di sicurezza inizia dalla visibilità: non si può proteggere ciò che non si vede. La mancanza di visibilità è una lacuna di sicurezza critica in molte organizzazioni: l'82% ammette di non essere in grado di identificare tutti i dispositivi collegati alla propria rete.[7]

I team addetti alla sicurezza necessitano di un inventario aggiornato dei dispositivi e delle applicazioni in esecuzione nella rete.
Un problema è che per molte reti OT non è possibile eseguire una scansione attiva con i metodi utilizzati per le reti IT, perché potrebbero interferire con le prestazioni della rete o danneggiare elementi OT come i PLC.[8]

Per i team di sicurezza è consigliabile contattare un fornitore o un partner tecnologico che esegua una valutazione delle minacce.

Questa valutazione a volte utilizza un sistema come un firewall NGFW, in grado di riconoscere i protocolli applicativi OT e di osservare passivamente il traffico di rete, compreso il traffico criptato.
Il sistema utilizza le informazioni raccolte per profilare e classificare i dispositivi presenti in rete in base alle loro caratteristiche e al loro comportamento. Il risultato è un report che:

- Fornisce un inventario dei dispositivi connessi
- Indica le applicazioni ad alto rischio
- Rileva e identifica gli exploit più frequenti delle vulnerabilità delle applicazioni
- Valuta il rischio connesso a ogni risorsa
- Individua indizi di malware, botnet e dispositivi che potrebbero essere compromessi
- Categorizza le applicazioni e analizza il loro utilizzo della rete

Queste informazioni forniscono una base solida per definire le priorità dei rischi e un piano di sicurezza ottimizzato.

L’82%

delle aziende non è in grado di identificare tutti i dispositivi presenti nelle proprie reti.

Offriamo una valutazione gratuita delle minacce per mappare l’intera rete.

2. Segmentare la rete

La segmentazione della rete è uno degli approcci architetturali più efficaci per la protezione degli ambienti OT.[9]

L'idea è quella di suddividere la rete in una serie di segmenti funzionali o "zone" (che possono includere sottozone o microsegmenti) e rendere ogni zona accessibile solo da dispositivi, applicazioni e utenti autorizzati. Un firewall definisce e applica le zone e definisce inoltre le condotte, ossia canali che consentono ai dati e alle applicazioni essenziali di passare da una zona all'altra.

- **Il firewall limita gli spostamenti degli aggressori all'interno della rete.**
- **Controlli rigorosi limitano l'accesso a ogni zona.**

L'architettura a zone e condotte riduce notevolmente il rischio di intrusione, limitando la possibilità degli aggressori di spostarsi in direzione "est-ovest" o laterale. Gli utenti o i dispositivi autorizzati per una specifica attività in una determinata zona possono operare solo all'interno di tale zona.

La segmentazione è una best practice fondamentale per la protezione degli ambienti OT, come descritta negli standard di sicurezza ISA/IEC-62443 (precedentemente ISA-99).[10] Tali standard sono stati definiti dalla International Society of Automation (ISA) come ISA-99 e successivamente rinumerati 62443 per allinearli agli standard corrispondenti della Commissione Elettrotecnica Internazionale (IEC, International Electrotechnical Commission).

Gli standard ISA/IEC-62443 forniscono indicazioni pratiche su come segmentare le reti OT. A ogni zona è assegnato un livello di sicurezza da 0 a 4, dove 0 rappresenta il livello di sicurezza minimo e 4 il massimo. Rigorosi controlli limitano l'accesso a ogni zona e condotta in base all'identità autenticata dell'utente o del dispositivo.

È consigliabile che i team di sicurezza scelgano un firewall con processori di sicurezza appositamente progettati per accelerare parti specifiche delle funzioni di elaborazione dei pacchetti e di scansione dei contenuti, rispetto alle CPU generiche presenti in molti firewall. I processori di sicurezza dedicati consentono la crittografia e l'ispezione dei contenuti ad alta velocità, senza compromettere le prestazioni della rete. Questo è un aspetto importante per evitare che le zone e le condotte si trasformino in colli di bottiglia.

3. Analizzare il traffico per individuare minacce e vulnerabilità

Dopo che i firewall NGFW hanno suddiviso una rete OT in segmenti e condotte, è importante analizzare il traffico di rete per individuare minacce note e sconosciute.

Il firewall NGFW integrato dai team di sicurezza deve essere in grado di ispezionare il traffico applicativo crittografato. Deve inoltre essere dotato di un servizio di live-feed che fornisca aggiornamenti sui più comuni protocolli OT e sulle vulnerabilità delle applicazioni OT. Un servizio di questo tipo consente all'NGFW di ispezionare il traffico delle applicazioni OT e di individuare gli exploit. Il firewall viene aggiornato da avvisi di intelligence globale in tempo reale, in modo che possa identificare anche minacce nuove e sofisticate. Quando è integrato con una soluzione di sicurezza per endpoint compatibile, l'NGFW è in grado di monitorare gli endpoint alla ricerca di indicatori di compromissione (IOC) acquisiti da diverse fonti in tutto il mondo.

Il firewall può anche apprendere dal traffico su una rete, definendo aspettative su ciò che è normale o anomalo negli scambi tra i sistemi IT e OT. Può mettere elementi in quarantena, bloccarli o inviare avvisi quando rileva attività anomale o IOC. Le funzionalità di intelligenza artificiale, integrate negli NGFW e fornite come parte di un sistema di intelligence delle minacce in grado di evolvere autonomamente, sviluppano signature per individuare le minacce zero-day prima ancora che vengano create.

Per semplificare la ricerca delle minacce e il reporting di conformità, i team di sicurezza dovrebbero aggiungere un SIEM (Security Information and Event Manager), in grado di correlare i dati provenienti da soluzioni di sicurezza specializzate e registri dei dispositivi tra le reti IT e OT. L'approccio ottimale è rappresentato dall'integrazione di un SIEM in grado di mappare in tempo reale la topologia della rete, monitorando e registrando gli eventi di sicurezza. Tale approccio consente di correlare informazioni provenienti da diverse soluzioni per fornirne il contesto, ridurre al minimo i tempi di risposta e semplificare il reporting.

- **Un punteggio di valutazione quantifica le prestazioni di sicurezza.**
- **Un feed globale in tempo reale fornisce aggiornamenti sulle vulnerabilità delle applicazioni.**

Per quantificare le prestazioni di sicurezza e consentire il confronto dei livelli di sicurezza di un'organizzazione rispetto a organizzazioni simili del settore è necessario ottenere un punteggio di valutazione della sicurezza, fornito come parte di un pacchetto di feed di Threat Intelligence. Tale punteggio è molto utile per elaborare i report di conformità e rispondere alle domande dei dirigenti senior sull'efficacia della sicurezza.

45%

delle aziende non monitora gli account con accesso di alto livello.

4. Controllare la gestione di identità e accessi

La sottrazione di credenziali è un elemento di molti attacchi alle reti OT, tra cui tre dei quattro descritti in precedenza. Lo spear phishing, utilizzato per accedere alle credenziali, è una componente fondamentale di tali attacchi. Di fatto, due terzi del malware installato nel panorama delle minacce viene trasmesso tramite email.[11] Un primo livello di difesa nel controllo degli exploit relativi alla gestione di identità e accessi (IAM) deve essere quindi costituito da un gateway email sicuro, con prevenzione basata sulle signature e sulla reputazione.

Il 45% delle organizzazioni OT non utilizza il controllo degli accessi basato sui ruoli.

Un'altra vulnerabilità comune del controllo degli accessi è rivelata dalle risposte degli intervistati nel sondaggio sull'OT, il 45% dei quali non provvede alla gestione delle identità privilegiate per gli amministratori, una gestione che consente alle organizzazioni di monitorare gli account di alto livello negli ambienti IT.[12] Tale carenza aumenta il rischio di danni causati dalla sottrazione di credenziali amministrative, un bersaglio ambito da molti aggressori.

Un altro 45% delle organizzazioni OT non utilizza il controllo degli accessi basato sui ruoli per i dipendenti, aumentando così il rischio di minacce interne,[13] anche se la maggior parte delle organizzazioni dichiara di avere in programma di adottare queste tecnologie.[14]
I team addetti alla sicurezza dovrebbero scegliere una soluzione IAM che:

- Applichi l'accesso basato sui ruoli per ogni utente, limitando l'accesso, attraverso l'integrazione con il firewall, solo alle risorse e al microsegmento di rete appropriati
- Convalidi le identità con l'autenticazione a più fattori, che combina un dato noto all'utente, come nome utente e password, con un oggetto in suo possesso, come un telefono, un certificato laptop o una chiave di sicurezza fisica, oppure con una sua caratteristica fisica, come un'impronta digitale o altri dati biometrici
- Abiliti il Single Sign-On (SSO), che consente risparmi di tempo grazie all'applicazione della sicurezza basata sull'identità utente aziendale, senza necessità di schermate di accesso aggiuntive
- Autentichi i dispositivi collegati alla rete osservandone le caratteristiche e il comportamento e rilevando la necessità di aggiornamenti software per correggere le vulnerabilità tramite patch
- Limiti l'accesso ai soli dispositivi autenticati, bloccando tutte le altre porte

5. Proteggere gli accessi via cavo e wireless

In un ambiente OT, due obiettivi attraenti per gli attacchi informatici sono gli switch di rete e gli access point wireless (AP). Entrambi devono essere dotati di sicurezza fin dalla progettazione, amministrata da un'unica interfaccia centralizzata, invece di essere protetti da soluzioni di sicurezza specializzate aggiuntive gestite da più interfacce.

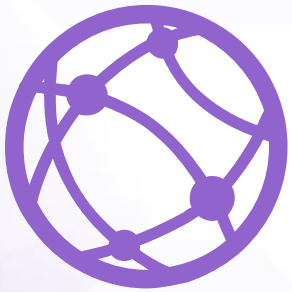
Una gestione della sicurezza centralizzata non solo riduce i rischi, ma migliora anche la visibilità e riduce al minimo i tempi amministrativi per i team operativi e di sicurezza.

In molte aziende del settore OT cresce l'esposizione a potenziali attacchi attraverso AP cablati e wireless. In un sondaggio, ogni azienda intervistata disponeva di tecnologie wireless o IoT, che potevano includere connessioni a reti OT.[15] Erano collegate in media 4,7 tecnologie IoT, le prime due rappresentate da localizzazione GPS e sensori di sicurezza.[16]

L'esposizione al rischio può essere ridotta al minimo scegliendo un firewall incluso in una piattaforma di sicurezza olistica. Tale piattaforma consente agli amministratori di applicare a livello centrale policy di sicurezza granulari ad AP wireless e switch integrati e di controllare VLAN personalizzate per diversi gruppi di dipendenti e apparecchiature. Questo tipo di firewall consente inoltre di centralizzare il provisioning e la gestione dei più diffusi AP wireless e switch legacy di fornitori terzi.

La gestione centralizzata della sicurezza dei punti di accesso riduce i rischi.

Un'altra caratteristica distinta da considerare in firewall, switch e AP wireless è la robustezza del fattore di forma, che ne consenta l'installazione nelle condizioni estreme dei siti tipici degli ambienti OT, come reti elettriche, oleodotti o altri sistemi distribuiti. I dispositivi devono essere progettati per funzionare nei luoghi più caldi e freddi della terra. Devono supportare policy di sicurezza create centralmente sul perimetro più esterno della rete, dove è probabile che gli aggressori attacchino perché si attendono livelli di sicurezza più bassi. Un guasto delle apparecchiature sul perimetro della rete non è solo un fastidio, ma può comportare tempi di inattività critici e costosi e la necessità di una distribuzione in tempi rapidi per risolvere il guasto.



Una piattaforma di sicurezza olistica può consentire di applicare policy di sicurezza a livello globale.

Conclusione: limitazione proattiva del rischio nelle reti OT

Per rimanere competitive, le organizzazioni collegano gli ambienti OT alle loro reti IT. Nella maggior parte dei casi, la convergenza IT e OT è pianificata e riveste un'importanza strategica nell'organizzazione. Potrebbe anche esistere un'integrazione non pianificata o addirittura non nota. Ad esempio, il progetto SHINE (SHodan INtelligence Extraction), che effettua una scansione globale pluriennale di Internet, ha identificato 2 milioni di dispositivi OT collegati (comprese infrastrutture che supportano dispositivi di controllo OT, come i controllori HVAC e i convertitori seriali).[17]

Mentre l'integrazione tra IT e OT sta diventando un'iniziativa strategica, causa anche un aumento della probabilità di violazioni degli ambienti OT. L'esperienza suggerisce che una violazione della sicurezza informatica non è una questione di "se" ma di "quando". Anche se non è possibile bloccare il 100% delle violazioni, è possibile limitarle attraverso la segmentazione della rete, rilevarle più rapidamente attraverso l'analisi del traffico e ridurne la frequenza attraverso la gestione di identità e accessi e il controllo degli accessi via cavo e wireless. Seguire queste best practice può ridurre notevolmente i costi e i tempi di inattività potenziali nel caso in cui un aggressore riesca a penetrare in una rete OT.

[1] "Studi indipendenti individuano notevoli rischi per la sicurezza dei sistemi SCADA/ICS", Fortinet, 7 maggio 2018.

[2] Le prime tre rivoluzioni industriali sono state 1) il passaggio dalla forza muscolare alla forza vapore nel XVIII secolo, 2) il passaggio dal vapore alle linee di assemblaggio elettriche nel XX secolo, 3) l'ascesa dell'automazione all'inizio del XXI secolo. Bernard Marr, "What is Industry 4.0? Here's A Super Easy Explanation For Anyone," Forbes, 2 settembre 2018.

[3] Bernard Marr, "What is Industry 4.0? Here's A Super Easy Explanation For Anyone," Forbes, 2 settembre 2018.

[4] Cornelius Baur and Dominik Wee, "Manufacturing's next act," McKinsey, giugno 2015.

[5] Robert Bock, et al., "What the Companies on the Right Side of the Digital Business Divide Have in Common," Harvard Business Review, 31 gennaio 2017.

[6] "Studi indipendenti individuano notevoli rischi per la sicurezza dei sistemi SCADA/ICS", Fortinet, 7 maggio 2018.

[7] Jeff Goldman, "IoT Security Fail: 82 Percent of Companies Can't Identify All Network-Connected Devices," eSecurity Planet, 8 novembre 2017

[8] Kyle Coffey, et al., "Vulnerability Analysis of Network Scanning on SCADA Systems," Hindawi, 13 marzo 2018.

[9] Keith Stouffer, et al., "Guide to Industrial Control Systems (ICS) Security," NIST, maggio 2015.

[10] "ISA Standards: Numerical Order," International Society of Automation, consultato il 3 gennaio 2018.

[11] David Finger, "Provide Customers with Advanced Threat Defense Against Email-Based Attacks," Fortinet, 26 aprile 2018.

[12] "Studi indipendenti individuano notevoli rischi per la sicurezza dei sistemi SCADA/ICS", Fortinet, 7 maggio 2018.

[13] Ibid.

[14] Ibid.

[15] Ibid.

[16] Ibid.

[17] Taylor Armerding, "Critical infrastructure: Off the web, out of danger?" CIO, 22 marzo 1017.

www.fortinet.com

358609 -0-0-IT

luglio 10, 2019 10:06 AM

eb-converged-it-and-ot_it_IT