Protezione del funzionamento di impianti e produzione dall’espansione della superficie di attacco

Elementi critici di un’architettura di sicurezza sofisticata

Sommario

FORTINET

Panoramica preliminare

Le operazioni degli stabilimenti e della produzione che si affidano alla tecnologia operativa (OT) si trovano sempre più spesso nel mirino degli attacchi informatici. Quasi tre quarti delle organizzazioni OT hanno subito almeno un'intrusione di malware nell'ultimo anno.[1] Nell'ambito delle azioni di contrasto a questi attacchi attraverso il miglioramento della sicurezza degli stabilimenti e della produzione, le organizzazioni che si affidano alle tecnologie OT devono valutare le soluzioni di sicurezza potenziali utilizzando diversi criteri chiave.

Innanzitutto, i responsabili operativi degli stabilimenti e della produzione devono essere sicuri che le loro tecnologie di sicurezza controllino efficacemente l'accesso alla rete, impedendo al contempo gli spostamenti laterali tra i segmenti della rete. In secondo luogo, devono cercare soluzioni di sicurezza che si integrino per abbattere le barriere tra le informazioni e ridurre il tempo richiesto al personale per la gestione della sicurezza. In terzo luogo, devono assicurarsi che ogni soluzione candidata sia specificamente progettata per supportare i protocolli e i processi utilizzati nell'ambiente delle operazioni di stabilimento e produttive.

Introduzione: le aziende manifatturiere devonomodernizzare le soluzioni di sicurezza

Anche rispetto alla velocità generale del cambiamento tecnologico, il ritmo dell'evoluzione delle imprese produttive e delle operazioni di stabilimento non ha precedenti. Molte usano sistemi SCADA (Supervisory Control and Data Acquisition) per gestire efficacemente i processi industriali. Questi sistemi raccolgono dati da sensori per poi incorporarli nei sistemi ICS (Industrial Control Systems) utilizzati per gestire i sistemi operativi dell'azienda, che tipicamente includono una complessa serie di generatori, ventilatori, robot industriali e altri dispositivi.

La capacità dei sistemi SCADA e ICS di sfruttare dati provenienti da diversi tipi di sensori si è rapidamente perfezionata. Inoltre tali sistemi sono sempre più utilizzati anche da aziende terze: il 64% delle organizzazioni OT concede ai fornitori IT terzi un accesso completo o di alto livello ai loro sistemi SCADA o ICS.[2] Come risultato di queste tendenze, molti produttori collegano ora i loro sistemi OT alla rete IT aziendale. Il collegamento dei dispositivi ICS e SCADA alle risorse IT di rete, come processori di fascia alta e supporti di archiviazione dati, facilita una gestione più efficiente dei dati degli impianti e della produzione.

Inoltre, un numero crescente di responsabili delle operazioni di stabilimento e produttive sta mettendo online i sistemi di controllo. In un recente webinar, il 35% dei partecipanti ha dichiarato che più della metà dei loro sistemi e dispositivi OT sono connessi a Internet e quasi 1 su 10 ha dichiarato che tutti i loro sistemi e dispositivi OT sono connessi a Internet.[3]

Quasi due terzi (il 64%) delle organizzazioni OT faticano a tenere il passo con il ritmo del cambiamento della tecnologia OT.[4] La sicurezza è un'area fondamentale che necessita di attenzione. Fortunatamente, la giusta combinazione di tecnologie di sicurezza può consentire ai responsabili delle operazioni di stabilimento e produttive di gestire questi rischi.

Di seguito sono riportate cinque considerazioni che i responsabili delle operazioni di stabilimento e produttive devono tenere presenti:

"Quando l'IT e l'OT operano in modo sinergico, le organizzazioni sono in grado di fornire soluzioni più efficienti e all'avanguardia."[5]

Purtroppo, solo il 55% delle organizzazioni che utilizzano sistemi SCADA e ICS adottano il controllo degli accessi basato sui ruoli per tutti i dipendenti.[6]

Implementazione di controlli efficaci sull'accesso alla rete

I dispositivi e i sistemi OT stanno diventando obiettivi sempre più attraenti per gli aggressori intenti a danneggiare le attività delle imprese, sottrarre segreti commerciali e ottenere riscatti.[7] Quasi il 60% delle organizzazioni che utilizzano SCADA e ICS ha subito una violazione di questi sistemi nell'ultimo anno, mentre solo l'11% non ha mai subito violazioni.[8] Questo è un problema enorme perché le funzionalità di sicurezza integrate nelle soluzioni ICS e SCADA sono spesso carenti.

Molti sistemi OT attualmente in uso sono stati progettati decenni fa, quando le aziende mantenevano un "air gap" tra le loro reti IT e i loro ambienti OT, compresi i sistemi di stabilimento e produzione. Gli attacchi informatici non erano nemmeno presi in considerazione nello sviluppo di tali dispositivi. Di conseguenza, molti sistemi OT mancano di funzionalità moderne che li renderebbero più sicuri con il venir meno della separazione dai sistemi IT.

Come prima linea di difesa, per impedire ai cybercriminali di attaccare i sistemi SCADA, ICS e di altre operazioni di stabilimento e produttive, è necessario conoscere tutto ciò che è connesso o che tenta di connettersi alla rete aziendale. A questo proposito, è fondamentale il controllo degli accessi alla rete (NAC). Dal momento che molti sistemi OT sono headless e non possono quindi accettare patch e aggiornamenti, gli approcci tradizionali alla sicurezza degli endpoint sono inadeguati.

I responsabili delle operazioni di stabilimento e produttive devono inoltre adottare il controllo degli accessi basato sui ruoli per garantire che gli utenti possano accedere solo ai dispositivi e alle applicazioni a cui sono autorizzati ad accedere. L'attendibilità deve essere costantemente monitorata e verificata da un motore di attendibilità integrato nella più ampia piattaforma di sicurezza. L'adozione di un approccio all'accesso alla rete basato sui privilegi minimi (parte del modello di sicurezza degli accessi "zero-trust") aiuta a prevenire l'accesso non autorizzato ai sistemi OT.

Le ricerche mostrano che è importante garantire un accesso sicuro degli utenti alle reti IT e OT. A questo scopo si può utilizzare una rete privata virtuale privata (VPN) che utilizza l'autenticazione a più fattori per garantire la protezione degli utenti quando accedono a determinate aree della rete aziendale.

“[I sistemi] ICS non sono progettati per garantire la resilienza contro attacchi concertati... I sistemi e i componenti ICS sono stati progettati senza tenere preventivamente conto delle minacce informatiche e, pertanto, la messa in sicurezza di questi sistemi sarà un’area crescente della ricerca sulla guerra informatica e ingegneristica.”[9]

Riduzione al minimo della superficie di attacco

Il recente incremento della connettività tra sistemi OT e IT crea rischi in entrambe le direzioni. Gli attacchi messi a segno sui sistemi IT possono consentire ai criminali di accedere ai dati e alle applicazioni OT, mettendo potenzialmente a rischio le apparecchiature e i processi delle operazioni di stabilimento e produttive. Un attacco a un sistema ICS o SCADA è in grado di alterare i movimenti delle apparecchiature, con possibili danni alle apparecchiature o lesioni ai lavoratori.[10] Nei casi più estremi, il malware che attacca le operazioni di stabilimento e produttive potrebbe mettere a rischio vite umane.

Allo stesso tempo, i sistemi ICS, SCADA e altri sistemi OT compromessi da hacker possono aprire backdoor per l'accesso alle risorse di rete. Alcuni sistemi operativi delle apparecchiature delle operazioni di stabilimento e produttive non supportano il software standard per la sicurezza dei client e non consentono l'applicazione di patch per correggere le falle di sicurezza. Anche per i sistemi delle operazioni di stabilimento e produttive che supportano il software di sicurezza, l'applicazione di patch delle vulnerabilità è di solito difficile perché i sistemi OT devono funzionare ininterrottamente; non possono essere messi offline per gli aggiornamenti di sicurezza.

Per questi motivi, i sistemi delle operazioni di stabilimento e produttive sono spesso più vulnerabili rispetto ai tipici server, sistemi di storage o endpoint dei sistemi IT. Con la sempre maggiore efficacia delle soluzioni di sicurezza nel bloccare il malware, alcuni aggressori rivolgono l'attenzione ai sistemi delle operazioni di stabilimento e produttive come canale alternativo e più semplice per accedere alle reti aziendali.

I responsabili delle operazioni di stabilimento e produttive devono distribuire firewall NGFW sia sul perimetro della rete che tra i suoi segmenti interni. Le verifiche di attendibilità dei firewall NGFW devono essere dinamiche, con l'aggiornamento continuo del set di signature utilizzato per verificare l'identità degli utenti, per ispezionare e controllare le applicazioni e per bloccare gli attacchi rilevati. Inoltre i firewall NGFW devono adattarsi a diversi fattori di forma, per ottimizzare le spese per le apparecchiature se i firewall vengono distribuiti per proteggere segmenti di dimensioni diverse con diversi volumi di traffico. Un'altra considerazione chiave è la necessità di ispezionare la crittografia SSL/TLS (Secure Sockets Layer/Trasport Layer Security) senza influire sulle prestazioni dei firewall NGFW.

"Un attacco informatico che prende di mira con successo un sistema OT o anche dispositivi collegati, come valvole, manometri o interruttori, potrebbe avere conseguenze fisiche devastanti per infrastrutture e servizi critici, per l'ambiente e persino per la vita umana."[11]

Eliminazione delle barriere per una sicurezza più efficace

La maggior parte delle imprese produttive e delle operazioni di stabilimento utilizza soluzioni di sicurezza di più fornitori. Queste imprese selezionano l'opzione migliore per la sicurezza di ogni dispositivo ma, in questo modo, creano una sicurezza a compartimenti stagni, con diverse conseguenze negative. Una di queste è che i diversi elementi della sicurezza potrebbero non scambiarsi informazioni sulle minacce rilevate. Se una soluzione in un'area della rete rileva o impedisce un tentativo di attacco, il malware può comunque portare a termine l'attacco in un'altra area. Il problema si aggrava quando la sicurezza OT non si integra con la protezione di email, endpoint, switch, punti di accesso wireless o firewall NGFW.

Le organizzazioni OT devono cercare soluzioni di sicurezza strettamente integrate, che condividano informazioni sulle minacce rilevate e sulla loro risposta a tali minacce. L'integrazione può anche consentire al personale di monitorare meglio il rilevamento e la risposta alle minacce in tutti i sistemi OT e IT dell'organizzazione, per una maggiore visibilità di tutta la strategia di sicurezza della rete.

IL 56%

delle organizzazioni OT ha subito una violazione della sicurezza nell'ultimo anno.[12]

Miglioramento di visibilità e automazione

Per il 45% delle organizzazioni OT, la carenza di personale specializzato nei settori dell'IT e della sicurezza informatica è un problema rilevante,[13] che può compromettere la capacità di un'azienda di adottare tecnologie e pratiche di sicurezza sofisticate. I team addetti alle operazioni di stabilimento e produttive devono implementare soluzioni che automatizzino le attività manuali, per snellire i flussi di lavoro a carico di un personale già ridotto al minimo.

Quando valutano soluzioni per la sicurezza, i responsabili delle operazioni di stabilimento e produttive devono cercare prodotti che non solo si integrino con la restante architettura di sicurezza, ma che automatizzino anche il rilevamento e la risposta alle minacce in ambiente sia OT che IT. La combinazione di automazione e orchestrazione può ridurre da alcuni giorni a pochi minuti il tempo necessario per rispondere a una minaccia alla rete. Può anche ridurre significativamente il tempo richiesto al personale per gestire l'infrastruttura, perché il personale non deve dedicare tempo prezioso all'esecuzione di report sulle varie soluzioni di sicurezza e alla successiva compilazione manuale delle informazioni.

Infine, un'infrastruttura di sicurezza integrata e automatizzata può semplificare i controlli e il reporting normativo, riducendo ulteriormente il carico di lavoro manuale sullo scarso personale addetto alla sicurezza.

Per il 45% delle organizzazioni OT, la carenza di personale specializzato è un problema rilevante.[14]

Verifica della compatibilità OT delle soluzioni di sicurezza

In parte a causa della separazione che un tempo esisteva tra i sistemi ICS e SCADA e le reti IT, molte soluzioni di sicurezza IT non supportano determinati protocolli OT. Tuttavia, le imprese produttive e delle operazioni di stabilimento che collegano i sistemi OT alle loro reti IT devono assicurarsi che gli elementi chiave della loro infrastruttura di sicurezza supportino tali sistemi.

Ad esempio, alcune soluzioni di sandboxing non sono compatibili con alcuni sistemi operativi OT. Le tecnologie di sandboxing identificano le minacce sconosciute e zero-day eseguendo test sui pacchetti potenzialmente infetti da malware prima che vengano immessi nella rete. Tuttavia, se non possono eseguire un particolare protocollo OT, non potranno completare questa funzione per i sistemi che utilizzano tale protocollo. I responsabili delle operazioni di stabilimento e produttive devono assicurarsi che le loro soluzioni di sandboxing siano state progettate per supportare gli specifici dispositivi OT che devono proteggere, ad esempio un controllore logico programmabile (PLC) Siemens o un'unità terminale remota (RTU) Schneider.

Lo stesso tipo di due diligence, per garantire la compatibilità, è necessario per ogni componente di sicurezza della rete.

Le soluzioni di sicurezza che proteggono una rete OT devono supportare tutti i protocolli specifici in uso tra SCADA, ICS, RTU, PLC e altre tecnologie operative dell'organizzazione.

Conclusione: L'architettura giusta garantisce la sicurezza degli ambienti OT e IT

I responsabili delle operazioni di stabilimento e produttive mettono a rischio le loro organizzazioni se non hanno le soluzioni di sicurezza giuste. Con la caduta del muro tra OT e IT e la proliferazione di sistemi e dispositivi OT, le sfide (e i rischi) sono senza precedenti. Le soluzioni di sicurezza tradizionali, semplicemente, non possono proteggere questa superficie di attacco ampliata.

In risposta, i responsabili delle operazioni di stabilimento e produttive devono modernizzare la loro architettura di sicurezza, che dovrà utilizzare controlli di accesso alla rete completi, impedire spostamenti laterali non autorizzati attraverso la rete, offrire visibilità trasparente e controlli centralizzati ed essere totalmente compatibile con gli ambienti OT.

L'"air gap" si è dissolto, aggravando il rischio comportato dall'ampliamento della superficie di attacco per le operazioni di stabilimento e per i produttori. I responsabili delle operazioni di stabilimento e produttive non possono più rimandare la gestione della sicurezza dei loro ambienti OT di fronte all'evoluzione delle minacce.

[1] "Report sullo stato dell'Operational Technology e della Cybersecurity", Fortinet, 15 marzo 2019.

[2] "Studi indipendenti individuano notevoli rischi per la sicurezza dei sistemi SCADA/ICS", Fortinet, 28 giugno 2019.

[3] "Webinar: Securing the Future of Industrial Control Systems", Fortinet, consultato il 9 settembre 2019.

[4] "Report sullo stato dell'Operational Technology e della Cybersecurity", Fortinet, 15 marzo 2019.

[5] "Causes and Consequences of IT and OT Network Convergence", Fortinet, 25 luglio 2019.

[6] "Studi indipendenti individuano notevoli rischi per la sicurezza dei sistemi SCADA/ICS", Fortinet, 28 giugno 2019.

[7] Joe Weiss, "Industrial control systems: The holy grail of cyberwar", The Christian Science Monitor, 24 marzo 2017.

[8] "Studi indipendenti individuano notevoli rischi per la sicurezza dei sistemi SCADA/ICS", Fortinet, 28 giugno 2019.

[9] Joe Weiss, "Industrial control systems: The holy grail of cyberwar", The Christian Science Monitor, 24 marzo 2017.

[10] John Maddison, "Resolving the Challenges of IT-OT Convergence", CSO, 21 giugno 2018.

[11] Ibid.

[12] "Studi indipendenti individuano notevoli rischi per la sicurezza dei sistemi SCADA/ICS", Fortinet, 28 giugno 2019.

[13] "Report sullo stato dell'Operational Technology e della Cybersecurity", Fortinet, 15 marzo 2019.

[14] Ibid.

www.fortinet.com

443523-0-0-IT

aprile 27, 2020 4:06 PM

eb-protecting-plant-manufacturing-operations