Come progettare la sicurezza per gli ambienti di rete OT

Prevenire, rilevare e gestire correttamente le minacce avanzate

Sommario

Panoramica preliminare 3

Introduzione 4

L'automazione del rilevamento e della risposta alle minacce migliora la disponibilità del sistema 5

Una threat intelligence specifica per OT identifica minacce uniche 7

Tecnologie ingannevoli consentono il rilevamento delle minacce avanzate 9

La segmentazione della rete isola e contiene le minacce 11

Conclusioni 13

Panoramica preliminare

Sofisticati attacchi informatici stanno mettendo a repentaglio i sistemi ICS (Industrial Control System) e SCADA (Supervisory Control and Data Acquisition). Poiché le reti OT (Operational Technology) stanno convergendo con l'IT (Information Technology), la superficie di attacco ampliata apre la porta agli autori di minacce informatiche avanzate rivolte contro questi sistemi critici. I sistemi ICS e SCADA su reti OT possiedono requisiti operativi unici che possono renderli più difficili da proteggere rispetto ai loro omologhi IT. Per questo, le reti OT richiedono approcci e soluzioni di sicurezza concepiti appositamente per loro.

L'uso di pratiche di sicurezza automatizzate e tecnologie ingannevoli può contribuire a rilevare minacce avanzate all'interno delle reti OT. Le soluzioni di sicurezza a livello di rete identificano e controllano la diffusione degli attacchi informatici provocati da hacker su una rete OT. Un elemento chiave di questa strategia è una threat intelligence specifica per OT, che supporta l'identificazione rapida e la risposta alle minacce rivolte contro più siti OT o alle minacce globali per il settore.

Il 64% dei responsabili delle decisioni riguardanti le reti OT afferma che gli attacchi informatici sofisticati rappresentano una delle massime sfide.[1]

Introduzione

I sistemi OT si trovano ad affrontare nuove minacce informatiche. In passato, le reti OT erano fisicamente isolate dai sistemi IT con un “air gap”. Tuttavia, sulla scorta dell’innovazione digitale, molte organizzazioni stanno eliminando o riducendo al minimo la dipendenza dagli air gap. Di conseguenza, le reti OT e IT sono più spesso collegate e i cybercriminali sfruttano la rete IT come trampolino di lancio per accedere alla rete OT.

I sistemi OT sono spesso beni di lunga durata, integrando componenti che in alcuni casi hanno cicli di vita sul campo di 20 anni o più. Non è raro che questi dispositivi ospitino molte vulnerabilità facilmente sfruttabili che sono state scoperte nel corso degli anni divenendo oggetto di minaccia. Ora, nuove minacce stanno emergendo nell’ecosistema criminale, e il web oscuro consente nuovi e sofisticati attacchi multiformi diretti specificamente contro gli operatori OT.

Visti i requisiti unici di disponibilità delle infrastrutture OT, è necessario che le soluzioni di sicurezza siano attentamente studiate per garantire un impatto minimo sulle operazioni. Inoltre, le reti OT devono raggiungere e mantenere la compliance alle specifiche linee guida normative, come quelle create dal National Institute of Standards and Technology (NIST), la direttiva della Commissione europea sulla sicurezza delle reti e dei sistemi informativi (la cosiddetta direttiva NIS) e la North American Electric Reliability Corporation (NERC).

L’automazione del rilevamento e della risposta alle minacce, una threat intelligence specifica per OT, le tecnologie ingannevoli e la segmentazione della rete sono i quattro elementi essenziali di un solido approccio alla sicurezza delle reti OT per affrontare il panorama delle minacce avanzate.

Quasi tre quarti delle organizzazioni OT hanno connessioni tra la rete IT e la rete OT.[2]

L’automazione del rilevamento e della risposta alle minacce migliora la disponibilità del sistema

Gli autori di minacce avanzate hanno le risorse e la sofisticazione necessarie per progettare attacchi che sfuggono ai tradizionali meccanismi di rilevamento. Le organizzazioni hanno bisogno una profonda visibilità della rete e conoscenza del contesto per distinguere tra minacce reali e falsi rilevamenti e, dunque, procedere all’attribuzione riconoscendo il comportamento dell’attacco e identificando l’autore della minaccia.

Il raggiungimento del livello richiesto di visibilità e conoscenza del contesto per una rapida risposta agli incidenti richiede automazione. La raccolta, l’aggregazione e l’analisi automatizzata dei dati di sicurezza contribuiscono a individuare le minacce reali (evitando un numero spropositato di falsi rilevamenti) e fornisce il quadro necessario per rispondere alle minacce e correggerle in maniera precisa.

L’automazione può anche consentire una risposta più rapida a una minaccia identificata. Creando playbook delle minacce che codificano le risposte a quelle più comuni, un’organizzazione può automatizzare parti del processo di rilevamento e correzione. Ciò contribuisce a supportare le esigenze di alta disponibilità dei sistemi OT poiché, nel momento in cui un analista ha identificato una minaccia attiva, alcune o tutte le fasi di ripristino possono essere eseguite istantaneamente, riducendo al minimo l’impatto della minaccia sulle operazioni.

La maggiore conoscenza del contesto e l’automazione della risposta agli incidenti contribuiscono a garantire la sicurezza e la disponibilità dei sistemi OT. Le risposte mirate, che identificano le minacce e le correggono a livello di processo, riducono al minimo l’impatto della risposta agli incidenti sulla disponibilità del sistema.

Il 78% delle organizzazioni ha solo una visibilità parzialmente centralizzata dei propri ambienti OT.[3]

L’automazione aumenta la disponibilità del sistema consentendo una risposta rapida e mirata alle minacce informatiche.

Una threat intelligence specifica per OT identifica minacce uniche

I sistemi OT sono obiettivi preziosi. Gli avversari sono disposti a investire il tempo e le risorse necessarie per identificare e sfruttare le vulnerabilità di questi sistemi. Gli autori delle minacce informatiche eseguono normalmente attività di ricognizione contro sistemi specifici per OT e sfruttano il fatto che i sistemi OT utilizzano protocolli di rete personalizzati, spesso non compresi dalle soluzioni di sicurezza informatica progettate per le reti IT, per nascondere le loro attività.

La gestione delle minacce informatiche sulle reti OT richiede un livello simile di conoscenze specifiche degli ambienti OT e molti anni di esperienza nella protezione di tali ambienti. La sicurezza delle reti OT si fonda sull'accesso a una threat intelligence specifica per OT. Poiché le organizzazioni OT integrano apparecchiature prodotte da una rosa selezionata di vendor, la visibilità delle vulnerabilità all'interno dei prodotti di questi fornitori è fondamentale per la sicurezza. Ciò permette ai vendor di OT di irrobustire i sistemi per evitare che vengano sfruttati e distribuire patch virtuali per proteggere efficacemente quelli vulnerabili durante i lunghi intervalli tra le finestre di manutenzione.

Le organizzazioni hanno anche bisogno di poter condividere threat intelligence all'interno e all'esterno dell'organizzazione e sfruttare la threat intelligence di terzi. Ciò consente l'identificazione e la risposta rapida alle vaste campagne di attacco specifiche per OT che utilizzano l'intelligenza artificiale (AI) e l'apprendimento automatico (ML).

L'85% delle minacce OT è diretto contro le macchine che utilizzano i protocolli OPC Classic, BACnet e Modbus.[4]

Le soluzioni di sicurezza informatica per sistemi OT richiedono la conoscenza delle minacce e dei protocolli specifici per OT.

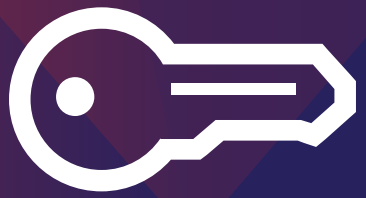
Tecnologie ingannevoli consentono il rilevamento delle minacce avanzate

Gli autori di minacce avanzate spesso sferrano attacchi "bassi e lenti" che sfuggono alle tradizionali difese della rete, attraverso un aggressore presente nella rete di un'organizzazione senza essere rilevato.

L'uso di tecnologie ingannevoli può contribuire a smascherare queste minacce evasive. Queste "trappole" possono essere configurate in modo da assomigliare a sistemi OT realistici, aumentando la probabilità che l'autore di una minaccia o il suo malware decida di interagire.

Se ciò accade, è sintomo della presenza di una minaccia all'interno della rete ombra, poiché nessuna operazione legittima utilizzerebbe questi sistemi. Inoltre, esaminando i dettagli delle operazioni dell'aggressore nel sistema, è possibile estrarre preziose informazioni sulle minacce riguardanti i suoi strumenti, le sue tecniche e le sue capacità. Questa threat intelligence alimenta una capacità di rilevamento e correzione più efficiente di tali minacce in altri sistemi all'interno della rete OT e può consentire all'organizzazione di identificare gli attacchi zero-day che i sistemi di rilevamento tradizionali basati su signature non sarebbero in grado di identificare.

La sicurezza OT beneficia anche della distribuzione di sandbox in grado di emulare sistemi specifici per OT. La strumentazione automatizzata e l'apprendimento automatico permettono di rilevare minacce sconosciute in base al rilevamento di comportamenti anomali o sospetti quando vengono eseguiti in questi ambienti emulati.



“Un’esca, per essere efficace, deve essere credibile. Non deve essere tanto sorvegliata da non poter essere violata, né tanto vulnerabile da non poter essere creduta. Se gli aggressori riconoscono un’esca, possono evitarla; un’esca deve quindi sembrare, presentarsi e comportarsi come il resto della rete.” [5]

La segmentazione della rete isola e contiene le minacce

Gli ambienti OT hanno esigenze di disponibilità estremamente elevate che incidono sulla sicurezza informatica OT. A causa dei requisiti di operatività e delle ridotte finestre di manutenzione, molti dispositivi utilizzano sistemi operativi e software a fine vita. Spesso, l'hardware più obsoleto non dispone delle risorse per far funzionare i sistemi antivirus tradizionali. Infine, in caso di incidente, può non essere possibile disattivare i sistemi colpiti per le necessarie azioni correttive.

Per tutti questi fattori, spesso la sicurezza OT viene assicurata a livello di rete anziché a livello di endpoint. Attraverso l'uso della segmentazione della rete e dei patch virtuali, è possibile ridurre il rischio rappresentato da dispositivi senza patch e vulnerabili. Invece di applicare aggiornamenti al dispositivo, incidendo sulla disponibilità del sistema, i patch virtuali assicurano che il traffico che tenta di sfruttare una vulnerabilità nota venga bloccato prima che raggiunga il dispositivo vulnerabile.

La segmentazione della rete può anche contribuire a ridurre l'impatto di una violazione della sicurezza informatica limitando lo spostamento laterale di un avversario attraverso la rete. La segmentazione assicura che tutte le comunicazioni tra i dispositivi siano analizzate alla ricerca di contenuti dannosi o anomali e che l'autenticazione forte degli utenti e i controlli di accesso siano applicati in tutta la rete.

È più probabile (51%) che le organizzazioni OT di alto livello utilizzino la segmentazione della rete rispetto alle organizzazioni di basso livello.[6]

La segmentazione della rete è necessaria per prevenire lo spostamento laterale delle minacce avanzate attraverso le reti OT.

Conclusioni

Le reti OT sono sempre più spesso bersaglio di minacce informatiche avanzate. Questi aggressori hanno familiarità con i sistemi OT e sviluppano malware personalizzati progettati per sfruttare le vulnerabilità dei sistemi comunemente utilizzati negli ambienti OT.

I responsabili della gestione operativa della rete devono rendersi conto che la superficie di attacco si sta ampliando e valutare l'opportunità di introdurre l'automazione della sicurezza, tecnologie ingannevoli, una threat intelligence specifica per OT e la segmentazione della rete per combattere le minacce avanzate.

Ecco alcune domande che i responsabili della gestione operativa di una rete dovrebbero porsi:

- Disponiamo di flussi di lavoro automatizzati di risposta agli incidenti e gestione degli eventi per mitigare le intrusioni riuscite prima che si propaghino e incidano sulle nostre operazioni?
- La nostra infrastruttura di sicurezza è integrata in modo che la threat intelligence possa essere condivisa in tempo reale tra tutti gli elementi di sicurezza?
- Disponiamo di capacità avanzate di rilevamento di minacce e violazioni, come sandboxing ed esche?
- Sono state adottate misure per ridurre la finestra di attacco e bloccare l'accesso alle risorse di rete dopo l'intrusione?

[1] "Caught in the Crosshairs: Are Utilities Keeping Up with the Industrial Cyber Threat?" Siemens and Ponemon Institute, 2019.

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

[3] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, 30 giugno 2020.

[4] "Fortinet 2019 Operational Technology Security Trends Report," Fortinet, 8 maggio 2019.

[5] Kevin Townsend, "How Deception Technology Can Defend Networks and Disrupt Attackers," SecurityWeek, 5 giugno 2019.

[6] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, 30 giugno 2020.

www.fortinet.com

726519-0-0-IT

novembre 19, 2020 12:13 PM

eb-how-to-design-security-for-ot-network-environments_IT