FORTINET

WHITE PAPER

Protezione dei sistemi OT di fronte alla rapida evoluzione delle minacce

Cosa devono sapere I CISO sull'OT nel panorama delle minacce avanzate

Sintesi preliminare

Molte aziende che si affidano alla tecnologia operativa (OT, Operational Technology) hanno gestito questi sistemi allo stesso modo per decenni, compresa la sicurezza delle apparecchiature OT. Gran parte delle apparecchiature industriali in uso oggi è stata sviluppata in un'epoca in cui ogni azienda manteneva un "air gap" tra i sistemi OT e quelli IT. Ora, tuttavia, i sistemi OT sono collegati alle reti IT e a Internet, esponendoli a sofisticate minacce avanzate, e la loro funzionalità di sicurezza potrebbe non essere pronta a rilevarle o espugnarle. È molto probabile che i CISO temano gli attacchi ai sistemi OT, poiché possono causare molti più danni rispetto a un tipico attacco di violazione dei dati o ransomware. Oltre agli impatti finanziari e sulla reputazione, i sistemi OT compromessi possono comportare una diminuzione della produttività, danni alle risorse e rischi per la sicurezza dei dipendenti e di altri.

Il 94% degli intervistati nelle organizzazioni OT considera l'approccio alla sicurezza OT un fattore significativo o moderato nel punteggio del rischio aziendale che il CISO condivide con i dirigenti e il Consiglio di Amministrazione.[4]

Organizzazioni OT sotto la crescente minaccia di un attacco

Man mano che le organizzazioni si modernizzano e sfruttano i vantaggi in termini di efficienza delle tecnologie IIoT (Industrial Internet-of-Things), l'air gap tra IT e OT si disintegra e la superficie di attacco si espande. I sensori OT vengono sempre più integrati nelle reti IT per interfacciarsi con le tecnologie di machine learning e big data. Questa connettività crea un vantaggio competitivo per l'azienda, ma anche un maggiore rischio di intrusioni informatiche. Le crescenti opportunità di attacco sono particolarmente problematiche perché i dispositivi OT "headless" non sono stati progettati pensando alla sicurezza. Non sono in grado di eseguire il software standard di sicurezza dei client e i requisiti di uptime si traducono spesso in finestre molto ristrette per gli aggiornamenti di sicurezza. Di conseguenza, è possibile che le aziende applichino solo le patch più critiche.

Gli attacchi ai sistemi OT creano seri rischi per l'organizzazione. Non è detto che un intruso sia alla ricerca di dati da sottrarre: potrebbe invece avere l'intenzione di arrestare le apparecchiature o alterarne il funzionamento. Che l'obiettivo sia quello di arrestare una linea di produzione, aprire una valvola che dovrebbe rimanere chiusa o spegnere i monitor di processi critici, un attacco di questo tipo può creare scompiglio nell'organizzazione e presso i suoi clienti. In alternativa, un attacco di questo tipo può essere destinato invece a utilizzare le connessioni di rete IT-OT per lo spostamento laterale nei sistemi IT dell'azienda. Se le difese OT sono più facili da penetrare, una violazione riuscita potrebbe consentire all'aggressore di accedere alle informazioni a carattere personale (PII) o ai dati finanziari aziendali dei clienti.

Quasi tre quarti delle organizzazioni OT hanno subito almeno una intrusione informatica negli ultimi 12 mesi, e la metà ha subito tre o più intrusioni.[1] Inoltre, quasi tutte le organizzazioni (il 97%) che utilizzano tecnologie di supervisione, controllo e acquisizione dati (SCADA, Supervisory Control And Data Acquisition) o sistemi di controllo industriale (ICS, Industrial Control System) riconoscono le sfide di sicurezza originate dalla convergenza tra IT e OT.[2] Alcuni degli attacchi ai sistemi OT prevedono un malware riprogrammato; una volta che le soluzioni di sicurezza IT bloccano efficacemente una minaccia, gli autori del malware possono tentare di utilizzarlo contro i sistemi OT con protezioni meno sofisticate.[3] Tuttavia, una parte crescente degli attacchi ai sistemi OT è realizzata appositamente per penetrare le difese delle apparecchiature operative.

Evoluzione nel panorama delle minacce avanzate

Gli attacchi OT mirati sono concepiti per colpire i punti più deboli delle reti OT, che sono generalmente le parti più piccole e semplici dell'infrastruttura. I ponti e i convertitori seriali sono un obiettivo comune.[5] Industroyer, un attacco malware che ha fatto crollare la rete elettrica ucraina nel 2016, ha attaccato i relè di protezione.

L'attacco era su più fronti, ma è iniziato sfruttando una nota vulnerabilità nei relè delle sottostazioni digitali prodotte da Siemens.[6] Il malware ha utilizzato questa vulnerabilità per accedere alla rete di dispositivi OT che supportano la rete elettrica di Kiev. Ha creato due access point alla rete di backdoor, poi distribuiti simultaneamente a tutti gli interruttori e i relè di protezione che poteva raggiungere, così come alle workstation Windows che utilizzavano il software ABB MicroSCADA per controllare tali dispositivi.

L'attacco è stato regolato da un timer. Quando è arrivata l'ora stabilita, ha eseguito un attacco DDoS (Distributed Denial-of-Service) su ogni relè di protezione della rete che utilizzava uno dei quattro protocolli di comunicazione.[7] Contemporaneamente, ha eliminato tutti i file relativi a MicroSCADA dai dischi rigidi delle workstation. Il risultato immediato di questo sofisticato attacco è stata la mancanza di risposta dei relè in tutta la rete, che ha causato un blackout nell'intera città di Kiev. Il danno non si è fermato qui. Anni dopo, Industroyer ha continuato ad attaccare i dispositivi OT in tutto il mondo.[8]

Sebbene Industroyer sia un esempio precoce, la tendenza all'aumento degli attacchi specifici di OT non si è arrestata. Oggi l'85% di tutte le minacce OT mira a uno dei tre protocolli di controllo OT.[9] Uno è OPC Classic, sviluppato tra gli anni '90 e 2000. I sistemi che utilizzano questo protocollo sono obiettivi appetibili per gli aggressori perché sono molto diffusi; si tratta del protocollo OT più utilizzato. Il secondo è BACnet, che risale al 1987 ed è utilizzato da molti sistemi di riscaldamento, ventilazione e condizionamento dell'aria (HVAC, Heating, Ventilation, and Air Conditioning), compresi quelli realizzati da Johnson Controls and Carrier. Nel 2018, le tre principali minacce in termini di numero di dispositivi che le utilizzano erano tutte sul protocollo BACnet.[10] La terza è Modbus, un protocollo di comunicazione OT sviluppato nel 1979. Quattro decenni fa, gli sviluppatori si aspettavano che i sistemi fossero sempre di tipo air gap. Un'altra sfida per i responsabili della sicurezza OT è che Modbus presenta numerose iterazioni, create da un una vasta serie di fornitori. Il monitoraggio delle vulnerabilità note di Modbus richiede molto tempo.[11]

Un'altra sfida per i responsabili della sicurezza dei sistemi OT è che gli attacchi mirati sono spesso progettati per concentrarsi su sistemi che sono sotto carico di picco, ovvero il momento in cui gli attacchi possono causare il maggior numero di danni o creare la massima pressione sull'organizzazione presa di mira per soddisfare le richieste dell'aggressore. Ad esempio, gli attacchi ai sistemi HVAC e alle reti elettriche in Nord America hanno un picco nei mesi estivi.[12]

"Il malware complesso come Industroyer gode di lunga vita, anche dopo la distribuzione di rilevazioni e firme".[13]

"Gli aggressori sono passati dalla diffusione di malware con l'intento di causare il caos in più sistemi, all'acquisizione di conoscenze dettagliate sui sistemi di controllo industriale per colpire industrie, paesi e aziende specifiche".[17] - Mark Carrigan, Chief Operating Officer, PAS Global

Le minacce in continua evoluzione sono sempre più difficili da rilevare

Nessun fornitore di sistemi SCADA o ICS è immune da questi rischi. Uno studio condotto da Fortinet nel 2019 sulle minacce OT ha rilevato che, sebbene i dispositivi Advantech, Schneider Electric, Moxa e Siemens siano stati attaccati con maggiore frequenza, ognuno dei 70 fornitori valutati ha subito periodicamente attacchi.[14] Inoltre, lo studio ha dimostrato che il numero e la frequenza degli attacchi sono in aumento per quasi tutti i fornitori di SCADA e ICS.

Questi attacchi sono sempre più mirati. Si concentrano su un risultato desiderato specifico presso un'unica organizzazione, per poi adottare un approccio su più fronti per raggiungere tale obiettivo. Industroyer ne è un esempio. L'attacco è stato eseguito nel corso di mesi, con una data d'inizio specifica. Si ritiene infatti che la Russia abbia perpetrato Industroyer con lo scopo di creare disagi a Kiev a sostegno dell'invasione russa dell'Ucraina, in un momento ben determinato. Inoltre, l'attacco ha comportato diversi passaggi discreti: ingresso nella rete OT attraverso i relè Siemens, creazione di due access point backdoor separati, distribuzione nei dispositivi OT e workstation nell'ambito dell'intera rete, quindi attivazione.

Anche gli attacchi ai sistemi OT stanno diventando sempre più evasivi. In questo caso, il malware spesso include funzionalità specificamente progettate per eludere le soluzioni antivirus o di rilevamento delle minacce. Il malware può essere in grado di rilevare quando è in esecuzione in un ambiente sandbox, può riuscire a disabilitare gli strumenti di sicurezza nelle macchine infette e può utilizzare i dati indesiderati per rendere più difficile il disassemblaggio.[15] Sempre più minacce malware che mirano ai sistemi OT impiegano la crittografia per evitare il rilevamento, e i ricercatori della sicurezza hanno scoperto tattiche di evasione estremamente sofisticate come la capacità del ransomware Ryuk di distruggere la propria chiave di crittografia ed eliminare le copie shadow dai sistemi infetti.[16]

Gli attacchi ai sistemi Triconex passano inosservati per mesi

L'attacco TRITON, noto anche come TRISIS, ha come obiettivo i controller SIS (Safety Instrumented System) Triconex sviluppati da Schneider Electric. Il primo exploit noto di TRITON ha attaccato un impianto petrolchimico in Arabia Saudita. Il malware ha ottenuto l'accesso alla rete IT dell'azienda attraverso mezzi sconosciuti ma sospettati di essere un attacco di phishing.[18] Una volta all'interno del perimetro IT, gli aggressori si sono spostati lateralmente nel lato OT dell'organizzazione. Sebbene nell'impianto fosse stata distribuita

un'architettura a "zona demilitarizzata" (DMZ, Demilitarized Zone) in cui le reti IT e OT erano separate da un firewall, gli aggressori hanno avviato sessioni RDP (Remote Desktop Protocol) verso le workstation di ingegneria dell'impianto dalla rete IT.[19]

Il primo incidente noto di un attacco a un reparto di ingegneria OT[20], TRITON/TRISIS sembra essersi concentrato sulla ricognizione della rete. Gli aggressori non hanno sottratto dati, non hanno acquisito screenshot e non hanno registrato i tasti digitati dagli utenti.[21] Hanno invece raccolto le credenziali degli utenti tramite malware che ha creato backdoor sia nella rete IT che in quella OT e le hanno poi utilizzate per accedere alle workstation dell'ingegneria SIS. Il malware ha anche rinominato i propri file in modo che assomigliassero ai file di Microsoft Update e ha utilizzato sia le webshell che i tunnel SSH (Secure SHell).[22]

Gli aggressori hanno avuto accesso al sistema DCS (Distributed Control System) dell'impianto, ma sembra che si siano concentrati esclusivamente sui controller SIS.[23] Infine, la loro sofisticazione non è servita a nulla; i sei sistemi SIS Triconex infettati si sono spenti in quella che sembra essere stata un'attivazione accidentale del malware prima del programma pianificato dagli aggressori.[24] Sono entrati in uno stato di "sicurezza non riuscita" e il disastro è stato evitato.[25]

L'attacco rivela tuttavia il grado in cui un codificatore impegnato può sviluppare un attacco multisfaccettato che utilizza metodi estremamente sofisticati (ad es. cambiando i nomi dei file, sviluppando e distribuendo tunnel SSH, creando più backdoor per l'accesso alla rete) per aggirare le misure di sicurezza standard. In realtà, il malware era talmente sfuggente che il primo tentativo degli aggressori (un primo tentativo di arresto due mesi prima di un singolo sistema Triconex SIS presso lo stesso impianto) non è stato rilevato. Schneider Electric ha estratto i file di registro dal dispositivo, ha eseguito una diagnostica sui dati raccolti e ha identificato il problema come un problema meccanico.[26]

Gli exploit sconosciuti e zero-day vengono spesso ignorati

Il malware noto può essere difficile da rilevare se la sua sofisticazione raggiunge quella dell'attacco TRITON/TRISIS. In effetti, TRITON/TRISIS ha compromesso una seconda vittima in Medio Oriente nell'aprile 2019[28] e il gruppo che si pensava fosse dietro TRITON/TRISIS avrebbe attaccato diversi obiettivi nordamericani del settore petrolifero e del gas all'inizio del 2019.[29]

Tuttavia, il noto malware di successo non è l'unico rischio per i sistemi OT. Nuovi attacchi avanzati emergono continuamente. Un esempio è LockerGoga, uno schema ransomware che ha temporaneamente interrotto la produzione negli stabilimenti di alluminio Norsk Hydro in tutto il mondo nel marzo 2019. La principale innovazione di questo attacco è stata la distribuzione del malware senza utilizzare il traffico di rete, il DNS (Domain Name System) o i server Command&Control.[30] Al contrario, ha diffuso il malware utilizzando i servizi Active Directory della rete.[31] Il giorno dopo aver rilevato LockerGoga per la prima volta presso Norsk Hydro, solo 17 dei 67 prodotti antivirus più importanti lo hanno riconosciuto come una minaccia.[32]

"Sulla carta, l'impianto era dotato di un'architettura sicura. Ma abbiamo identificato un'infrastruttura DMZ configurata erroneamente che ha consentito agli aggressori di compromettere la DMZ e di controllare la rete".[27] - Julian Gutmanis, Principal Threat Analyst, Dragos Inc.

"Il panorama delle minacce dovrebbe essere preso sul serio da qualsiasi organizzazione con sistemi ICS/SCADA collegati. I consulenti stanno pensando in modo strategico, estraendo il maggior valore possibile da ogni nuova minaccia che sviluppano sfruttando sistemi non protetti e vulnerabilità".[33]

Le violazioni dei sistemi OT causano ingenti perdite con strascichi nel tempo

L'impatto commerciale delle violazioni dei sistemi OT può essere grave. Alcuni, come LockerGoga, sono progettati per arrestare i sistemi OT con l'obiettivo di ricevere un riscatto. Tuttavia, molti sono progettati per spegnere o danneggiare le apparecchiature industriali.[34] L'arresto imprevisto di una linea di produzione danneggia ovviamente la capacità dell'azienda di raggiungere gli obiettivi di produzione, probabilmente per un periodo di tempo prolungato.

I tempi di attività dei sistemi OT possono comportare una perdita immediata di profitti, che può arrivare fino a centinaia di migliaia o addirittura milioni di dollari in pochi minuti, a seconda dell'azienda. Ad esempio, il ransomware NotPetya nel 2017 è costato al colosso farmaceutico Merck quasi un miliardo di dollari dopo aver interrotto la produzione.[35] Al colosso delle spedizioni Maersk, NotPetya ha causato un calo del 20% del volume, con una perdita di 300 milioni di dollari.[36] Molte aziende erano ancora in affanno dopo l'attacco sferrato da NotPetya un anno dopo. [37]

In un attacco OT, anche il danno ambientale è una possibilità reale. Sebbene non sia accaduto, l'attacco TRITON/TRISIS avrebbe potuto causare il rilascio nell'atmosfera di gas di acido solfidrico tossici.[38] Un tale disastro ambientale comporterebbe probabilmente costi di risanamento e sanzioni normative, e potrebbe avere anche un grave impatto sulla reputazione dell'azienda.

Inoltre, quando le apparecchiature OT vengono arrestate inaspettatamente, si crea un rischio di lesioni o addirittura di morte per i dipendenti che le utilizzano. In ambienti medici, questi rischi si estendono ai pazienti, la cui salute potrebbe essere compromessa se una macchina come un ventilatore si fermasse senza preavviso. I team di sicurezza delle strutture ospedaliere temono sempre di più i potenziali attacchi che potrebbero causare l'interruzione delle attività cliniche.[39]

Le ricerche sugli attacchi informatici presso le organizzazioni OT rivelano tutti questi effetti. Più di un intervistato su quattro (43%) in un recente studio di Fortinet ha dichiarato che le interruzioni di servizio che hanno subito hanno avuto un impatto sulla produttività, mentre il 36% ha dichiarato che le interruzioni hanno avuto un impatto sui profitti, il 23% ha dichiarato che hanno messo a rischio la sicurezza fisica, il 30% ha dichiarato che hanno causato un forte danno d'immagine e il 28% ha dichiarato che l'attacco OT ha causato la perdita di dati business-critical.[40]

Il ransomware NotPetya ha causato quasi un miliardo di dollari di danni a Merck e 300 milioni di dollari a Maersk.[41,42]

Conclusione: ponderare i rischi

I costi di un attacco OT sono troppo elevati per essere ignorati. I CISO nei settori che si affidano a sistemi di produzione operativi e industriali, come la produzione, i servizi pubblici e i trasporti, faticano sempre più a garantire che il lato operativo della loro rete sia adeguatamente protetto. Tuttavia, gli approcci tradizionali alla sicurezza OT non riescono a tenere il passo con il tasso di evoluzione delle minacce avanzate.

Considerando la potenziale gravità delle conseguenze di una violazione, i CISO dovrebbero porsi diverse domande:

- Mi fido della capacità dei nostri fornitori di rilevare gli attacchi a tutti i nostri sistemi OT business-critical?
- La nostra organizzazione è in grado di identificare le minacce sconosciute e zero-day?
- Abbiamo implementato i processi giusti per attenuare i rischi scoperti?
- I nostri sistemi includono tecnologie di risposta agli incidenti che possono contrastare le minacce alla sicurezza avanzate che utilizzano l'offuscamento?
- Quali sono i potenziali impatti di una violazione? Se devo creare un business case per migliorare la sicurezza OT, quali sono i rischi più critici da affrontare?

Il CISO che può rispondere con fiducia a queste domande è più preparato a proteggere i sistemi OT che sono fondamentali per le operazioni dell'organizzazione.

[1] "State of Operational Technology and Cybersecurity Report", Fortinet, 15 marzo 2019.

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

[3] "Report Fortinet: Tendenze nella sicurezza delle tecnologie operative 2019. Un aggiornamento sul panorama delle minacce per i sistemi ICS e SCADA", Fortinet, 16 maggio 2019.

[4] "State of Operational Technology and Cybersecurity Report", Fortinet, 15 marzo 2019.

[5] "Report Fortinet: Tendenze nella sicurezza delle tecnologie operative 2019. Un aggiornamento sul panorama delle minacce per i sistemi ICS e SCADA", Fortinet, 16 maggio 2019.

[6] Charlie Osborne, "Industroyer: An in-depth look at the culprit behind Ukraine's power grid blackout", ZDNet, 30 aprile 2018.

[7] Ibid.

[8] "Report Fortinet: Tendenze nella sicurezza delle tecnologie operative 2019. Un aggiornamento sul panorama delle minacce per i sistemi ICS e SCADA", Fortinet, 16 maggio 2019.

[9] Ibid.

[10] Ibid.

[11] Ibid.

[12] Ibid.

[13] Ibid.

[14] Ibid.

[15] "Threat Landscape Report Q2 2019", Fortinet, secondo trimestre 2019.

[16] Ibid.

[17] Robert Lemos, "TRITON Attacks Underscore Need for Better Defenses", Dark Reading, 15 aprile 2019.

[18] Thomas Roccia, "Triton Malware Spearheads Latest Generation of Attacks on Industrial Systems" McAfee, 8 novembre 2018.

[19] Kelly Jackson Higgins, "Triton/Trisis Attack Was More Widespread Than Publicly Known", Dark Reading, 16 gennaio 2019.

[20] Ibid.

[21] Charlie Osborne, "Triton hackers return with new, covert industrial attack" ZDNet, 10 aprile 2019.

[22] Ibid.

[23] Ibid.

[24] Kelly Jackson Higgins, "Triton/Trisis Attack Was More Widespread Than Publicly Known", Dark Reading, 16 gennaio 2019.

[25] Charlie Osborne, "Triton hackers return with new, covert industrial attack" ZDNet, 10 aprile 2019.

[26] Kelly Jackson Higgins, "Triton/Trisis Attack Was More Widespread Than Publicly Known", Dark Reading, 16 gennaio 2019.

[27] Ibid.

[28] "Report Fortinet: Tendenze nella sicurezza delle tecnologie operative 2019. Un aggiornamento sul panorama delle minacce per i sistemi ICS e SCADA", Fortinet, 16 maggio 2019.

[29] "Threat Landscape Report Q2 2019", Fortinet, secondo trimestre 2019.

[30] Dan Goodin, "'Severe' ransomware attack cripples big aluminum producer", Ars Technica, 19 marzo 2019.

[31] Mathew J. Schwartz, "Hydro Hit by LockerGoga Ransomware via Active Directory", BankInfoSecurity, 20 marzo 2019.

[32] Dan Goodin, "'Severe' ransomware attack cripples big aluminum producer", Ars Technica, 19 marzo 2019.

[33] "Report Fortinet: Tendenze nella sicurezza delle tecnologie operative 2019. Un aggiornamento sul panorama delle minacce per i sistemi ICS e SCADA", Fortinet, 16 maggio 2019.

[34] Robert Lemos, "TRITON Attacks Underscore Need for Better Defenses", Dark Reading, 15 aprile 2019.

[35] "Report Fortinet: Tendenze nella sicurezza delle tecnologie operative 2019. Un aggiornamento sul panorama delle minacce per i sistemi ICS e SCADA", Fortinet, 16 maggio 2019.

[36] Iain Thomson, "NotPetya ransomware attack cost us $300m", The Register, 16 agosto 2017.

[37] Kim S. Nash, et al., "One Year After NotPetya Cyberattack, Firms Wrestle With Recovery Costs", The Wall Street Journal, 27 giugno 2018.

[38] Kelly Jackson Higgins, "Triton/Trisis Attack Was More Widespread Than Publicly Known", Dark Reading, 16 gennaio 2019.

[39] Mark Klimek, "Hospitals face rising risk of sophisticated cyberattacks", Healthcare Finance, 17 settembre 2019.

[40] "State of Operational Technology and Cybersecurity Report", Fortinet, 15 marzo 2019.

[41] "Report Fortinet: Tendenze nella sicurezza delle tecnologie operative 2019. Un aggiornamento sul panorama delle minacce per i sistemi ICS e SCADA", Fortinet, 16 maggio 2019.

[42] Iain Thomson, "NotPetya ransomware attack cost us $300m", The Register, 16 agosto 2017.

FORTINET®

www.fortinet.com

settembre 22, 2020 8:59 AM

370120-0-1-IT