Mettere in sicurezza le infrastrutture informatiche critiche delle nazioni

Giugno 27, 2022
by Marco Rottigni, Technical Director Italia di SentinelOne

Le industrie fanno sempre più affidamento sulla cosiddetta Operational Technology (OT) e sui sistemi di controllo industriale (ICS) per supportare le proprie infrastrutture mission-critical, ma devono anche gestire un aumento significativo delle minacce informatiche.

Secondo la CISA (Cybersecurity & Infrastructure Security Agency), il governo russo sta esplorando ulteriori opzioni per avviare attacchi contro le infrastrutture degli altri Stati. Come accaduto già in passato, la sfida da affrontare è quella di come proteggere le risorse mission-critical fondamentali per il funzionamento dei servizi della propria nazione.

Perché gli hacker prendono di mira le infrastrutture critiche?

I motivi sono diversi, ma si possono suddividere in motivazioni finanziarie e politiche.

I cybercriminali che hanno finalità economiche cercano di colpire i servizi pubblici attraverso i ransomware, anche perché sanno che spesso gli enti pubblici si servono di hardware o software obsoleti e possono essere vulnerabili agli exploit più noti. Gli hacker sperano anche che la natura mission-critical di questi obiettivi costringa le istituzioni a pagare il riscatto per proteggere coloro che fanno affidamento sui servizi forniti.

Gli hacker con finalità politiche, invece, cercano di attaccare le infrastrutture nazionali durante i periodi di crisi o quando si verificano eventi significativi, come elezioni, emergenze sanitarie e guerre. Sono attacchi che spesso vanno oltre gli obiettivi prefissati e causano danni collaterali ad altre organizzazioni. Ad esempio, durante l'invasione dell'Ucraina da parte della Russia, i cyber criminali hanno colpito infrastrutture organizzative di importanza primaria all'interno e all'esterno della nazione. Queste azioni hanno incluso attacchi DDoS (Distributed Denial-of-Service) e la distribuzione di malware dannosi contro il governo ucraino e le imprese delle infrastrutture critiche nazionali (CNI) .

Attaccare le infrastrutture critiche per scatenare il panico significa colpire i sistemi finanziari e sanitari della nazione o le stesse reti elettriche. Gli hacker hanno mirato alle aziende importanti che assicurano servizi critici in diversi contesti, tra cui AcidRain, con il blocco ai modem KA-SAT di Viasat in Europa, gli attacchi DDoS sponsorizzati dallo Stato russo a Colonial Pipeline, l'allarme ransomware a JBS Foods e l'allarme alla a Kaseya Limited.

In che modo gli hacker sfruttano le infrastrutture critiche?

Ecco alcune metodologie utilizzate dai cyber criminali per potenziali attacchi informatici:

- **Sfruttare le vulnerabilità** – I dispositivi dell'infrastruttura non omologati e mal configurati sono ad alto rischio di violazione. Gli hacker cercano le vulnerabilità esistenti nei protocolli ICS standard e proprietari, tra cui MMS (Manufacturing Message Specification), GOOSE (Generic Object Oriented Substation Event) dello standard IEC 61850, MODBUS (supervisione e controllo), DNP3 (energia e acqua), BACNET (automazione degli edifici) e IPMI (controllo della gestione dei pannelli di base). Sanno che le misure di protezione non sono sempre attuabili e cercano di sfruttarne le debolezze.
- **Compiere attacchi denial-of-service (DOS)** – Gli hacker possono ottenere l'accesso attraverso un sistema IT compromesso, eseguire attività di ricognizione e spostarsi lateralmente verso la rete OT per avviare un attacco denial-of-service.
- **Implementare ransomware e/o wipers** – un recente report della CISA mostra l'aumento di attacchi ransomware sofisticati e ad alto impatto contro organizzazioni di infrastrutture critiche a livello globale. CISA, FBI e NSA hanno monitorato incidenti che coinvolgono ransomware contro 14 dei 16 settori delle infrastrutture critiche statunitensi, tra cui la base di difesa industriale, i servizi di emergenza e di alimentazione e l'agricoltura, le strutture governative e i settori tecnologici. Hanno inoltre osservato che diversi gruppi di ransomware hanno sviluppato un codice per bloccare le infrastrutture critiche o i processi industriali.

Come proteggere i sistemi ICS con piani d'azione suggeriti ad hoc

Alcune indicazioni che aiutano a proteggere le risorse OT nel mondo interconnesso di oggi:

- Condurre regolarmente valutazioni di sicurezza dei sistemi OT (ICS/SCADA).
- Identificare le reti OT e IT e implementare la loro segmentazione tra le reti IT e OT. La segmentazione della rete limita la capacità degli avversari di puntare alla rete OT quando la rete IT è compromessa.
- Identificare le risorse nella rete OT ed eliminare le possibili vulnerabilità attraverso la serie completa di vettori di attacco.
- Identificare, rilevare e indagare sulle attività sospette che coinvolgono gli endpoint e indicano movimenti laterali all'interno delle reti IT e OT. Implementare soluzioni basate sugli endpoint, come Singularity Identity, per rilevare le connessioni laterali.
- Proteggere le credenziali. Gli attori di minacce APT sponsorizzati dallo Stato russo hanno dimostrato la loro capacità di persistere utilizzando credenziali compromesse.
- Implementare procedure di backup dei dati sia sulle reti IT che su quelle OT, testandole regolarmente per garantire che queste siano separate dalle connessioni ed analizzando con attenzione ogni dispositivo, cosa fa e a cosa si connette.

Come SentinelOne Identity può essere di supporto?

SentinelOne è leader nella tecnologia deception e offre soluzioni innovative di sicurezza ICS per proteggere le infrastrutture critiche. Cinque delle maggiori organizzazioni ICS/SCADA della classifica Fortune 10 hanno già implementato le soluzioni complete di SentinelOne. Anche il PNNL (Pacific Northwest National Laboratory), un laboratorio nazionale del DoE, ha convalidato le soluzioni di sicurezza che proteggono le infrastrutture critiche nazionali.

La soluzione Singularity™ Hologram offre capacità di deception che coprono le reti IT e OT aziendali tradizionali. La piattaforma di deception offre una difesa adattiva della cybersecurity utilizzando l'apprendimento automatico per creare strategie di deception che proteggono la superficie di attacco in evoluzione. La piattaforma supporta un ampio sottoinsieme di protocolli ICS e consente ai clienti di creare emulazioni di vari PLC, nodi SCADA, apparecchiature mediche e altro ancora. Gli hacker che sfruttano le vulnerabilità dei sistemi di interfaccia uomo-macchina (HMI) sono vettori di attacco comuni. I clienti possono distribuire sistemi HMI esca utilizzando golden images.

La soluzione di sicurezza ICS offre funzionalità di deception complete che coprono le reti IT e OT aziendali tradizionali. La piattaforma produce esche ingannevoli nelle reti SCADA, ICS, IoT, Point of Sale e Medical Device, identificando i lateral movement degli hacker e le attività di ricognizione mirate ai sistemi critici per la produzione. Inoltre, le soluzioni Singularity™ Identity distribuiscono credenziali ingannevoli in grado di rilevare e segnalare i criminali informatici che si muovono attraverso servizi remoti e sfruttano l'infrastruttura ICS.

Conclusioni

Le infrastrutture critiche sono fondamentali per la sicurezza e la salute pubblica, ma questi servizi vengono spesso gestiti da organizzazioni con budget ridotti che utilizzano hardware e software obsoleti. Per garantire la sicurezza degli asset mission-critical, le aziende devono mettere in atto solidi piani d'azione che includano controlli autonomi della sicurezza degli endpoint, in grado di ridurre la necessità di un SOC di grandi dimensioni, pur monitorando costantemente la rete ICS, di dover continuamente ricercare attività sospette e dannose.

Per ulteriori informazioni consultare http://it.sentinelone.com.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Sicurezza di Active Directory | Che cos'è e cosa occorre sapere
- Da SentinelOne alcuni suggerimenti per proteggere l'Active Directory