ICS, OT e SCADA Security: a rischio le infrastrutture critiche



Il 2021 è stato un anno da dimenticare per la sicurezza della tecnologia operativa (OT) e dei sistemi di controllo industriale (ICS). Infatti, un numero crescente di minacce informatiche ha preso di mira proprio le infrastrutture critiche di organizzazioni di tutto il mondo, il numero di vulnerabilità scoperte nei sistemi OT nel 2021 è più che raddoppiato rispetto all'anno precedente.

Il **ransomware** è diventato il vettore numero uno per attacchi ai danni dell'industria; il settore manifatturiero è quello maggiormente preso di mira con oltre il 60% di cyber attacchi.

L'importanza della protezione nei sistemi cyber fisici (Cyber-Physical System, CPS)

Le industrie di tutto il mondo si affidano alla **tecnologia operativa (OT)**, ai **sistemi di controllo industriale (ICS)** e a quelli **controllo di supervisione e acquisizione dati (SCADA)** rendendo la protezione dal rischio cyber un tassello fondamentale e imprescindibile a garanzia della sicurezza delle infrastrutture critiche.

I sistemi di controllo industriale sono un sottoinsieme importante all'interno del settore OT: reti elettriche, trasporti, monitoraggio e distribuzione dell'acqua, petrolio e gas e sistemi di comunicazione si affidano tutte a sistemi ICS/SCADA per fornire servizi essenziali. Se questi ambienti vengono esposti a vulnerabilità, possono aprire la strada a eventi anche gravi.

La comunità industriale ha discusso per anni dell'importanza della sicurezza informatica degli ambienti OT. Gli attacchi del 2021 sottolineano gli esiti potenzialmente devastanti che una violazione della sicurezza delle infrastrutture OT potrebbe avere sulle comunità e l'economia di un paese.

Lo dimostrano i tre attacchi gravi avvenuti negli Stati Uniti: un attacco ransomware contro la **Colonial Pipeline Co**., che ha provocato l'interruzione di fornitura di gas in tutto il sud-est, un attacco a **JBS Foods** e a un impianto di **trattamento delle acque a Oldsmar**, in Florida.

Due tipologie di ransomware, **Conti** e **Lockbit 2.0**, hanno causato il 50% degli attacchi ransomware ai danni dell'industria nel 2021.

Nel dettaglio, gli attacchi informatici hanno colpito per il 65% il settore produttivo, seguito dal Food & Beverage al secondo posto e al terzo dai Trasporti. Analizzando invece i sotto settori manifatturieri emerge che tra i preferiti delle cyber gang ci sono i produttori di componenti in metallo, il settore automotive e quello tecnologico.

La trasformazione digitale dei settori industriali e la maggiore connettività tra IT e OT hanno rappresentato due fattori chiave nell'aumento della vulnerabilità. In molti casi, i confini deboli tra OT e IT e le interazioni tra questi ambienti, insieme all'aumento degli accessi da remoto dovuti anche alla pandemia, hanno aumentato il rischio complessivo.

A prendere di mira il settore ICS/OT sono stati gruppi hacker come:

- **KOSTOVITE**, che nel marzo 2021 ha compromesso una rete di fornitura di servizi energetici e manutenzione, sfruttando una vulnerabilità zero-day nella popolare soluzione di accesso da remoto Ivanti Connect Secure;
- **PETROVITE**, che ha preso di mira le operazioni minerarie ed energetiche in Kazakistan;

- **ERYTHRITE**, un gruppo attivo almeno da maggio 2020 che si rivolge principalmente alle organizzazioni di Stati Uniti e Canada con campagne malware in corso. Dragos ha riscontrato una compromissione per mano di ERYTHRITE nel comparto OT di un'azienda Fortune 500 e nelle reti IT di una grande azienda elettrica, di aziende di Food & Beverage, di case automobilistiche, di fornitori di servizi IT e di diverse società attive nei settori del petrolio e del gas naturale.

Tra i cyber criminali annoverati dai ricercatori di Dragos, società che si occupa di proteggere le infrastrutture critiche, ci sono anche STIBNITE, TALONITE, KAMACITE, VANADINITE.

Il futuro della sicurezza negli ambienti ICS e OT

Nella maggior parte dei casi, la vulnerabilità dei sistemi ICS/OT è riconducibile a fattori come:

- visibilità della rete OT limitata o assente. Una scarsa o mancata visibilità dell'ambiente ICS impedisce una identificazione tempestiva delle minacce;
- falle nei sistemi di sicurezza: problemi con la segmentazione della rete di protezione;
- credenziali di accesso intercambiabili fra ambienti IT e OT.

La pressione sugli ambienti OT/ICS non è destinata ad allentarsi, per questo motivo ogni comparto industriale deve esercitarsi con scenari di emergenza che coinvolgano la presenza di ransomware all'interno dei loro ambienti operativi e a non abbassare la guardia.

A cura della Redazione

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/ics-ot-e-scada-sec

urity-a-rischio-le-infrastrutture-critiche/