Cos’è la OT Security e come si relaziona con la sicurezza IT

La sicurezza OT (Operational Technology) si occupa solitamente della protezione dei sistemi Industriali: sistemi di controllo distribuito (DCS, Distributed Control System), sistemi di controllo industriale (ICS, Industrial Control System), reti di controllo supervisione e acquisizione dati (SCADA, Supervisory Control And Data Acquisition), controllo dei processi (PLC, Programmable Logic Controller), l’internet delle cose industriale (IIoT, Industrial Internet of Things), automazione degli edifici (BAS, Building Automation System), così come dei sistemi PACS (Physical Access Control Systems).

L’OT security è un campo relativamente nuovo nella sicurezza informatica in grado di avere ripercussioni sul mondo fisico ed impattare sia sulla security che sulla safety a 360° poiché coinvolge persone, tecnologie e processi in quelle che vengono definite infrastrutture critiche.

Fonte: www.cisa.gov

Cos’è la sicurezza OT?

L’OT Security deve garantire il controllo in *real time,* l’adattabilità, la disponibilità e la continuità di funzionamento, la confidenzialità e l’integrità dei dati. Deve essere in grado di sostenere e proteggere le reti di automazione utilizzate per controllare i processi fisici, come i servizi di emergenza, impianti di produzione farmaceutici, chimici, i trasporti, la distribuzione di energia, acqua, petrolio e gas, da attacchi informatici. Un problema di sicurezza in questo contesto di infrastrutture critiche

determinerebbe gravi danni sospendendo quelli che sono definiti servizi essenziali e causando perdite economiche, come ad esempio in caso di fermo della produzione, e perfino conseguenze peggiori come la manomissione di un impianto idrico o la perdita di vite umane.

I dispositivi che compongono l'infrastruttura OT non sono stati progettati per sostenere la connettività che la trasformazione digitale impone e i costi di aggiornamento che l'industria si trova a dover affrontare sono molto elevati poiché i sistemi OT sono stati progettati per durare oltre 30 anni e quindi con tecnologia *legacy,* perciò il rinnovamento di tutti i macchinari risulta spesso una spesa molto alta a cui è difficile fare fronte.

Ma visti i casi di cronaca, che hanno determinato l'interruzione di servizi primari come quelli energetici, l'investimento nella OT cybersecurity negli ultimi anni è diventato sempre più ingente ed impellente. Gruppi di cyber criminali si stanno sempre più specializzando nell'attaccare le infrastrutture critiche, incentivati anche da forti finanziamenti statali come nel caso dello *state-sponsored hacking*. Ciò avviene perché questo tipo di crimine è in grado di condizionare la geopolitica come si vede anche nel conflitto russo-ucraino garantendo agli autori del crimine l'anonimato vista la difficile attribuzione del cyber attacco.

Come ridurre il rischio informatico negli ambienti OT

Per ridurre il rischio cyber, l'OT Security manager deve applicare una strategia che prevede:

- controllo accessi e gestione privilegi attraverso la predisposizione di Intrusion Detection System (IDS)
- segmentazione della rete
- soluzioni di antivirus e utilizzo di sistemi di Endpoint Detection and Response (EDR)

- monitoraggio della rete
- analisi dei log
- vulnerability assessment
- penetration testing
- stabilire corrette policy di sicurezza
- programmi di valutazione/audit
- approccio zero trust

Convergenza tra IT e OT

La convergenza tra IT e OT nasce con la trasformazione digitale che determina la necessità dei sistemi industriali ad essere sempre più connessi generando così maggiori vulnerabilità e nuovi rischi per la sicurezza ma anche maggiore sostenibilità, facilità di gestione, flessibilità, competitività nel settore industriale.

L'affermarsi della OT cybersecurity avviene per garantire una risposta all'esigenza di monitorare e controllare l'infrastruttura OT da remoto che ha generato nell'ultimo decennio un impressionante aumento del numero di attacchi informatici indirizzato alle infrastrutture critiche dovuto sia al collegamento a reti IP che al numero sempre più crescente di endpoint. Ciò rende sempre più difficile per le organizzazioni di identificare tutti i dispositivi connessi alla rete e la loro relativa messa in sicurezza generando così un quantitativo di vulnerabilità mai visto prima, alimentando il rischio di cyber attacchi grazie all'avanzare dei sistemi IoT, al cloud computing e ai tool di hacking che diventano di giorno in giorno sempre più sofisticati e facilmente reperibili.

L'Industrial IoT (IIoT) sfida l'Operational Technology

L'Industrial Internet of Things (IIoT) è stato un fattore determinante nel causare la non sicurezza delle infrastrutture

OT progettate inizialmente esclusivamente per connessioni interne.

L’IIoT è una rete di oggetti fisici che trasmettono dati. Si tratta in genere di una serie di dispositivi industriali, macchine, sensori, attuatori o controller connessi a internet o ad una intranet per consentire il monitoraggio e il funzionamento da remoto, con lo scopo di migliorare l’efficienza, ridurre i costi e aumentare la redditività.

Differenza tra OT Security e IT Security

La sicurezza IT e OT sono campi diversi con obiettivi diversi.

L’IT Security ha come requisito base la confidenzialità, integrità e disponibilità dei dati mentre la sicurezza OT si concentra su una tecnologia che non è stata progettata per essere connessa alla rete e le comunicazioni avvengono tipicamente machine-to-machine. Per tale motivo i volumi di traffico negli ambienti industriali sono generalmente inferiori a quelli degli ambienti IT e ciò determina un vantaggio in quanto è più facile monitorare rete e traffico identificando velocemente le anomalie, segno di un eventuale attacco. Ciò viene incontro a quello che è il requisito base della OT security, la disponibilità, le risorse devono essere ininterrottamente accessibili al fine di garantire la continuità operativa.

A cura della Redazione

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/cose-la-ot-security-e-come-si-relaziona-con-la-sicurezza-it/