Building blocks

LA CYBERSICUREZZA NEGLI AMBIENTI OT

CINQUE STRATEGIE CONSIGLIATE DEGLI ESPERTI DI PAESSLER PER MONITORARE NEL MIGLIORE DEI MODI LE RETI OT (OPERATIONAL TECHNOLOGY) E ATTUARE PIANI DI CYBERSECURITY EFFICACI

Chiara Ornigotti

Con la convergenza IT-OT molte reti OT oggi sono integrate con sistemi e reti esterne per cui è fondamentale adottare strategie di cybersicurezza complete

Non c 'è dubbio che l'ambiente OT - Operational Technology più sicuro sia una rete isolata, che non necessariamente richiede particolari misure di sicurezza. Tuttavia, con la convergenza di IT e OT molte reti OT oggi devono essere integrate con sistemi e reti esterne e per queste reti OT è fondamentale adottare strategie di cybersicurezza complete. Come nell'IT, il monitoraggio di infrastrutture, dispositivi e sistemi costituisce una parte vitale di tali strategie.
Paessler, azienda specializzata nel monitoraggio di rete, ha individuato cinque ragioni fondamentali per cui il monitoraggio dovrebbe essere parte di una strategia di sicurezza. Vediamole.

Monitoraggio dei certificati

Nell'IT il monitoraggio dei certificati fa parte di ogni buon piano di cybersicurezza e così dovrebbe essere anche nell'OT. Gli standard industriali come OPC UA impiegano la crittografia X.509 basata su certificato e tali certificati devono essere mantenuti aggiornati. Il monitoraggio può essere usato per garantire che i certificati siano sempre validi, così da prevenire downtime o buchi nella sicurezza causati da certificati scaduti.
Lo svantaggio nell'uso dei certificati è che vengono aumentate la complessità e il lavoro amministrativo, pertanto in ambienti non criptati potrebbe essere più comodo usare altri approcci.

Individuazione delle anomalie

Per 'anomalia' in una rete si intende qualunque deviazione dalla norma, per esempio picchi inspiegabili nel consumo di banda, traffico inusuale, nuove connessioni impreviste alla rete. Un'anomalia non sempre è segno di attacco, ma potrebbe esserne un indicatore. La capacità di riconoscere un'anomalia implica che vi sia uno stato basale, ovvero la 'norma'. Il monitoraggio in questo caso ha due funzioni: primo, può essere usato per identificare lo stato di 'normalità' su un certo periodo di tempo; secondo, può servire per cercare le deviazioni dalla norma. Con il monitoraggio possiamo definire allerte e notifiche che vengono lanciate quando sono superate determinate soglie, segnalando qualunque tipo di attività sospetta sulla rete.

Difesa in profondità

Per proteggere le reti OT sono richiesti diversi livelli di difesa specializzati. Questo concetto, noto come 'difesa in profondità', opera sulla base che, se si hanno molteplici livelli di sicurezza, il cuore della rete è più sicuro. Nell'OT un livello è generalmente rappresentato dai firewall industriali. Un'altra possibilità è la segmentazione della rete, in cui la rete OT o è separata dalla rete IT per mezzo di una zona demilitarizzata (segmentazione verticale), o in cui la stessa rete OT è separata in diverse zone (segmentazione orizzontale). Il monitoraggio può essere particolarmente utile nella difesa in profondità sorvegliando i firewall industriali, le interfacce tra i segmenti ed elementi come le porte aperte.

Deep Packet Inspection (DPI)

Si tratta di un meccanismo in cui il contenuto dei pacchetti dati viene esaminato in tutte le sue componenti, dall'intestazione al payload, per identificare il protocollo e le funzioni associate a quel pacchetto dati. I dati vengono quindi verificati rispetto a un insieme di regole per accertarsi che non siano anomali. Ciò permette di applicare regole più complesse e dettagliate di quelle che possono essere gestite da un firewall.
La DPI costituisce la base di due particolari strategie di cybersicurezza per l'OT: Industrial Intrusion Prevention Systems (IPS) e Industrial Intrusion Detection Systems (IDS). In un ambiente OT, sia IPS che IDS sono dispositivi o sistemi che operano all'interno di una rete e hanno lo scopo di prevenire o lanciare una notifica quando vengono scoperti dati anomali, in funzione del sistema in uso. Il monitoraggio può essere usato insieme con soluzioni IPS e IDS per fornire un'immagine completa di quanto sta accadendo nella rete OT.

Allarmi e notifiche

In caso di attacco, la tempestività della reazione è della massima importanza. Oltre che individuare un cyberattacco, è importante avvisare il team che deve provvedere alla reazione. Gli allarmi vengono avviati quando si superano certe soglie o quando sono rispettati determinati criteri e le notifiche vengono inviate direttamente ai team responsabili.

Monitoraggio dell'IT industriale con Prtg

Il software di monitoraggio Prtg di Paessler può essere parte di una buona strategia di cybersicurezza. Oltre al monitoraggio dei vari elementi dell'IT e dell'OT, può monitorare le attività anomale nelle reti industriali. Inoltre, può lavorare con molte popolari soluzioni di sicurezza, come Rhebo e Moxa, per costituire un tassello vitale di uno scenario, quello della cybersecurity, in continua evoluzione.
Paessler ritiene che il monitoraggio abbia un ruolo fondamentale nel ridurre il consumo di risorse. Il monitoraggio dei dati aiuta i clienti a risparmiare risorse ottimizzando le infrastrutture IT, OT e IoT per ridurre il consumo di energia e le emissioni per il bene del nostro futuro e del nostro ambiente.

Paessler - www.paessler.it