Building blocks

SICUREZZA ATTIVA E PASSIVA

COMBINARE IL MONITORAGGIO PASSIVO E QUELLO ATTIVO NEGLI AMBIENTI OT E IOT PERMETTE DI OTTENERE UNA MIGLIORE CYBER RESILIENZA

Gabriele Webber

Fonte: foto Shutterstock

Il monitoraggio attivo compensa alcuni dei limiti del monitoraggio passivo rendendo le reti in ambienti OT e IoT più sicure

Storicamente, per i sensori di sicurezza che monitorano le reti OT e i sistemi ICS nelle infrastrutture critiche, l'unico approccio consentito all'utente finale è stato quello passivo. Per ridurre al minimo i rischi, le condizioni delle reti OT impongono che tali dispositivi non possano essere coinvolti attivamente nel monitoraggio.

Il monitoraggio passivo in tempo reale fornisce visibilità su queste reti senza interferire con il traffico, né interrompere le operazioni. Sapere cosa viene comunicato, quando e come, è utile ai fini dell'inventario degli asset, della gestione delle vulnerabilità, della visibilità operativa e della difesa dagli attacchi informatici. Tuttavia, in un contesto di minacce informatiche in continua evoluzione, il solo monitoraggio passivo potrebbe non essere sufficiente.

Con un approccio più completo al monitoraggio, che comprenda anche altre tecniche, è possibile proteggere più efficacemente i propri sistemi OT e IoT.

File di progetto e integrazioni

A estensione del monitoraggio passivo, i file di configurazione di progetto del sistema, se disponibili, possono essere importati per arricchire l'inventario degli asset. Il file è un'istantanea di informazioni statiche legate a un sistema specifico. Naturalmente ci sono delle limitazioni: non sono sempre disponibili, poiché alcuni fornitori non condividono queste informazioni, e se le informazioni sono aggiornate, i file devono essere reimportati.

Gli ambienti OT e ICS contengono anche una moltitudine di tecnologie di fornitori esterni. Le integrazioni sono necessarie per consolidare le informazioni sugli asset di fornitori terzi con le informazioni esistenti per mantenere aggiornato l'inventario degli asset. Il problema dell'inserimento di dati esterni è che si basa su tecnologie di terze parti, che potrebbero non essere sempre disponibili; inoltre, le diverse fonti potrebbero avere livelli di accuratezza differenti.

Il vantaggio del monitoraggio passivo è che fornisce informazioni continue della rete basandosi sulla comunicazione esistente; il monitoraggio passivo, però, presenta delle limitazioni che possono influire sull'inventario accurato delle risorse, sulla valutazione delle vulnerabilità e sulla visibilità dei dispositivi non comunicanti. Per questi motivi, il monitoraggio attivo compensa alcuni dei limiti del monitoraggio passivo.

Monitoraggio attivo

L'introduzione del monitoraggio attivo negli ambienti OT e IoT richiede un cambiamento culturale. La scansione pura comporta un aumento del throughput e un cattivo utilizzo dei cicli della CPU degli end-point, con possibili ripercussioni su prestazioni e stabilità di rete. Alcune soluzioni affrontano il problema adottando il monitoraggio attivo tramite query e il monitoraggio attivo tramite sensore su end-point.

1. Monitoraggio attivo tramite query e sensore su end-point

A differenza della scansione classica, il monitoraggio attivo tramite query mira a interrogare i dispositivi in base alla conoscenza delle loro capacità di protocollo, sfruttando messaggi e istruzioni speciali, che sono noti, per restituire informazioni utili, minimizzando il throughput e senza influire sulla stabilità del dispositivo. Questa è una buona opzione per i dispositivi embedded, dove le soluzioni basate su agenti, storicamente, non potevano essere ospitate.

Il monitoraggio attivo tramite query è adatto quando sono in uso dispositivi embedded OT/IoT e quando sono in uso soluzioni IT e non è possibile utilizzare un sensore end-point.

Con il monitoraggio attivo tramite query si ottengono i seguenti vantaggi:

- massima visibilità sui dispositivi embedded;
- maggiore visibilità sui dispositivi Windows/Linux/macOS;
- miglioramento della valutazione delle vulnerabilità.

Il fornitore, il nome del prodotto e la versione del firmware di una telecamera a circuito chiuso, per esempio, non sono disponibili con il monitoraggio passivo. Recuperando attivamente queste informazioni, si calcolano le vulnerabilità.

2. Monitoraggio attivo tramite sensore su end-point

In questo caso, la presenza del sensore aumenta la visibilità dall'interno dell'end-point stesso, combinando i rilevamenti di rete, come il monitoraggio del traffico, e l'estrazione di informazioni dell'asset. Questo sensore aggiunge funzionalità che non sarebbero possibili se non da installati sulla macchina obiettivo. Il monitoraggio di massa della rete offerto da un monitoraggio passivo viene integrato da un monitoraggio locale, che trasforma le macchine obiettivo in sensori, compresa la possibilità di eseguire il monitoraggio attivo tramite query attive, di cui abbiamo parlato prima, dall'end-point stesso.

Con il monitoraggio attivo tramite sensore end-point si ottengono i seguenti vantaggi:

- rilevamenti unici basati sull'host, che garantiscono la massima visibilità sui dispositivi Windows/Linux/macOS;
- miglioramento della valutazione delle vulnerabilità;
- visibilità locale completa grazie al monitoraggio del traffico direttamente dal sensore su end-point, senza affidarsi a switch o tap;
- visibilità completa per gli asset che non comunicano in rete tramite raccolta dati offline;
- tutti i vantaggi del 'monitoraggio attivo tramite query' da posizione privilegiata, in quanto eseguite dall'end-point.

Nozomi Networks - https://it.nozominetworks.com