LE NOSTRE SOLUZIONI

IoT & OT Protection

Rileva la superficie di attacco ed esegue una valutazione dei rischi includendo tutti gli asset esposti in rete.

Assicurare la sicurezza di una azienda significa capire quanti e quali sono i dispositivi connessi in rete. A parte i classici dispositivi end point, server, le applicazioni cloud esistono anche dispositivi OT e IoT connessi in rete: telecamere, tornelli di accesso, sensori. Per le realtà industriali, i macchinari connessi alla catena di produzione, nell'Health care le macchine elettro medicali per la diagnostica o per la rianimazione. Questi in un mondo interconnesso alla rete sono tutti punti di accesso per un attaccante. Diventa prioritario capire quale è la reale superfice di attacco. Un sistema di assett management è uno strumento fondamentale per il monitoraggio di tutti i dispositivi IoT e i sistemi OT presenti nell'infrastruttura. Molto spesso si possono identificare oggetti connessi di cui si ignorava la presenza si possono monitorare e tracciarne il comportamento. Le Piattaforme di sicurezza agiscono in maniera predittiva: rilevano i comportamenti non standard degli apparati, riconducono alcune attività a potenziali rischi, mettono in isolamento i dispositivi e li scollegano dalla rete. Sono soluzioni dotate di funzionalità di intelligenza artificiale e autoapprendimento in grado di rilevare le minacce e di eseguire azioni di remediation. I dati rilevati da queste piattaforme vengono integrati ai sistemi di sicurezza aziendali esistenti, come i sistemi SIEM, estendendo ai concetti di sicurezza IT anche agli ambienti IoT e OT.

Come funzionano queste piattaforme?

Sono on cloud e Agent less.

Eseguono il monitoraggio continuo degli assett aziendali.

Rilevano le vulnerabilità e bloccano gli attacchi su tutti i dispositivi connessi in rete.

Perché l'IoT Security è importante

Per gestire in modo efficiente la sicurezza di una azienda o di una organizzazione i sistemi di controllo fisico e logico devono essere unificati. In un mondo interconnesso alterare il funzionamento di un sistema IT può significare causare malfunzionamenti a sistemi di controllo accessi, ai sistemi industriali di produzione, alla logistica e al supply chain. In un contesto di infrastrutture critiche significa agire sui sistemi di distribuzione dell'energia, bloccare i sistemi bancari e i servizi della pubblica amministrazione. La porta di accesso attraverso la quale innescare azioni malevole di sabotaggio è qualsiasi dispositivo interconnesso. Il perimetro di sistemi e di infrastrutture da monitorare sono in continuo aumento ed evoluzione. Le piattaforme software per il monitoraggio degli assett e i processi attraverso i quali si ha accesso ai sistemi produttivi e alla gestione del business devono essere governate quindi da un unico sistema di sicurezza.

Per informazioni: sales@redfrogsecurity.it