Aspisec

RED TEAM PER IL SETTORE DELLE UTILITY ENERGETICHE

Le aziende di utility energetiche, come quelle elettriche o del gas, rappresentano una parte critica dell'infrastruttura nazionale.

Un'interruzione o un compromesso dei loro sistemi non solo può causare danni economici, ma può anche mettere a rischio la sicurezza e il benessere dei cittadini.

La sicurezza di queste infrastrutture è quindi di primaria importanza.

Aspisec

Overview

SCENARIO

Una delle principali società di fornitura elettrica, “ElectroPower Co.”, vuole assicurarsi le sue reti di distribuzione, sistemi di controllo, applicazioni ed infrastrutture IT siano a prova di intrusioni. Per avere una visione realistica delle potenziali minacce, decide di avvalersi di un’operazione di red teaming.

Workflow

STEPS

01/ **SCOPING**
In collaborazione con “ElectroPower Co.”, Aspisec definisce gli obiettivi dell’operazione, delineando le aree chiave da testare e stabilendo i limiti d’intervento.

02/ **RECONNAISSANCE**
Il team di Aspisec esegue una fase di raccolta informazioni, studiando i sistemi di distribuzione, i protocolli di comunicazione e le applicazioni software in uso.

03/ **SIMULAZIONE DI ATTACCO**
Il red team di Aspisec lancia una serie di attacchi mirati, cercando di compromettere i sistemi di controllo, bypassare i firewall e accedere ai pannelli di gestione della rete.

04/ **EVASIONE E MOVIMENTO LATERALE**
Dopo aver guadagnato un punto d’appoggio, il team tenta di muoversi all’interno della rete, cercando di accedere ad altri sistemi e sottraendo informazioni critiche, simulando le azioni di un vero attaccante.

05/ **REPORT**
Al termine dell’operazione, Aspisec fornisce un rapporto dettagliato, elencando le vulnerabilità scoperte, i successi dell’attacco e le raccomandazioni per migliorare la sicurezza.

Aspisec

Overview

COME POSSIAMO AIUTARTI

01/ **ESPERIENZA NEL SETTORE**

Aspisec ha specialisti con una profonda conoscenza dei sistemi SCADA e delle infrastrutture critiche, garantendo un'analisi pertinente e approfondita.

02/ **TATTICHE AVANZATE**

Aspisec simula attacchi basati su tecniche avanzate e minacce emergenti specifiche per il settore energetico.

03/ **COLLABORAZIONE CONTINUA**

Oltre a svelare vulnerabilità, Aspisec lavora a stretto contatto con "ElectroPower Co." per sviluppare piani di mitigazione e strategie di difesa.

04/ **FORMAZIONE MIRATA**

Basandosi sui risultati, Aspisec offre sessioni di formazione per il personale di "ElectroPower Co.", focalizzandosi sulle aree di debolezza rilevate.

Con l'approccio red team di Aspisec, "ElectroPower Co." ottiene una visione chiara e realistica delle sue vulnerabilità, consentendo all'azienda di fortificare le sue difese e garantire un servizio continuo e sicuro ai suoi clienti.

L'esempio di use case fornito rappresenta solo una delle molte applicazioni possibili. Aspisec ha una consolidata esperienza in vari settori, tra cui Energy, Oil & Gas, Telco, Transport, Banking, Health, Insurance, Industry, Gov e Space.

Contattaci per una consultazione gratuita ad info@aspisec.com

Rome
Piazzale Flaminio 19,
00196, Italy