Identificazione del rischio

Traccia

Utilizzando il framework di modellizzazione delle minacce di Adam Shostack, identifica una minaccia per un'azienda di sviluppo software.

- Su cosa stiamo lavorando?
- Cosa può andare storto?
- Che cosa faremo al riguardo?
- Abbiamo fatto un buon lavoro?

Ripeti il processo, eseguendo una gap analysis per trovare i punti di miglioramento.

Su cosa stiamo lavorando?

Software per la gestione di centrali elettriche statali.

Cosa può andare storto?

Una nazione avversaria potrebbe utilizzare tecniche di Phishing per infiltrarsi nell'azienda e rubare il codice per sfruttarlo successivamente in un attacco alla supply chain.

Che cosa faremo al riguardo?

- Formazione del personale contro i tentativi di Phishing.
- Simulazione di un attacco di Phishing da parte di un red team esterno all'azienda.
- Installare un filtro Anti-Phishing nei computer aziendali.

Abbiamo fatto un buon lavoro?
Ripetere il corso di formazione anti Phishing almeno ogni sei mesi.

Simulare degli attacchi di Phishing ad intervalli casuali per valutare meglio la frequenza con cui ripetere la formazione.

Gap Analysis

Piano d'azione

Strutturare piano di formazione del personale contro il Phishing che dovrà iniziare entro due settimane. Lo scopo del piano di formazione sarà istruire i dipendenti su come riconoscere ed evitare le tecniche di Phishing più comuni. Al piano sarà assegnato un budget per assumere un esperto in materia esterno all'azienda.

Assumere un Red Team esterno per simulare una campagna di Phishing contro i dipendenti dell'azienda. La campagna dovrà partire un mese dopo la fine del corso di formazione per valutare l'efficienza di quest'ultimo.

Acquistare e installare un filtro anti Phishing su tutti i PC aziendali entro una settimana, ciò servirà come prima misura difensiva contro i tentativi di Phishing.

Tabella di Marcia

Milestone	Obiettivo Intermedio	Obiettivo Finale
Fine Prima Settimana	Acquisto e installazione filto Anti-Phishing	Filtro Anti-Phishing attivo su ogni PC
Fine Primo Mese	Strutturazione e attuamento di corso Anti-Phishing	Dipendenti formati contro il Phishing
Fine Secondo Mese	Assunzione Red Team per simulazione campagna di Phishing	Confermare che Filtro Anti-Phishing + Formazione hanno dato i risultati aspettati