S11L1 Luca Calvigioni

Remediation e Mitigation di minacce di Phishing

Scenario:
Immagina di essere un amministratore di sicurezza per una media azienda che ha scoperto una campagna di phishing mirata contro i propri dipendenti. Gli attaccanti inviano email fraudolente che sembrano provenire da fonti affidabili, inducendo i dipendenti a divulgare informazioni sensibili o a scaricare malware.

Identificazione della minaccia:

- **Cos'è il phishing?**
  Il phishing è una tecnica di ingegneria sociale in cui gli aggressori inviano email fraudolente che sembrano provenire da fonti affidabili per indurre le vittime a compiere azioni dannose, come fornire credenziali, numeri di carte di credito o altri dati sensibili.

- **Come funziona un attacco phishing?**
  Gli attaccanti creano email che imitano comunicazioni legittime, includendo link o allegati dannosi. Quando la vittima clicca, può fornire informazioni o installare software malevolo senza accorgersene.
  In un ambiente aziendale un attacco di phishing può compromettere la sicurezza di un'azienda sfruttando la fiducia e la disattenzione dei dipendenti per ottenere accesso a informazioni sensibili o a sistemi critici come nas o server.

Analisi del rischio:

Impatto potenziale sull'azienda
Un attacco di phishing può avere conseguenze profonde e devastanti per un'azienda, sia dal punto di vista economico che operativo. Tra i principali impatti troviamo:

- **Perdita Finanziaria**

Gli attaccanti potrebbero indurre trasferimenti fraudolenti di denaro, appropriandosi di fondi aziendali.

- **Danni Reputazionali**

Una violazione dei dati aziendali può minare la fiducia di clienti e partner.

- **Costi Operativi e di Recupero**

Gli attacchi di phishing spesso comportano downtime interrompendo le attività aziendali critiche che di conseguenza portano ad una perdita di denaro.

Pianificazione della Remediation

La pianificazione della remediation è un processo essenziale per rispondere a un attacco di phishing in modo tempestivo ed efficace. Comprende una serie di azioni che mirano a identificare, bloccare e mitigare i rischi associati alla minaccia.

- **Identificazione:**

È cruciale analizzare le email fraudolente ricevute dai dipendenti per comprendere la tecnica di phishing utilizzata e anche analizzando i log dei server email per tracciare l'origine delle email.
Sfruttare servizi di threat intelligence per rilevare domini utilizzati nelle campagne di phishing.

- **Blocco:**

Configurare regole nei sistemi di posta elettronica per filtrare e bloccare automaticamente email con contenuti, mittenti o URL sospetti, filtri anti-spam.

- **Comunicazione:**

Inviare immediatamente un avviso interno a tutti i dipendenti, spiegando la natura dell'attacco in corso e fornendo indicazioni su come evitare ulteriori compromissioni.
Assicurarsi che i dipendenti conoscano le procedure per segnalare email sospette e ricevano linee guida per evitare interazioni con i messaggi fraudolenti.

Implementazione della Remediation

L'implementazione della remediation è il momento in cui le misure pianificate vengono messe in pratica per neutralizzare la minaccia di phishing e prevenire futuri attacchi. Una strategia ben eseguita coinvolge strumenti tecnologici, formazione del personale e aggiornamento delle policy aziendali.

- **Strumenti tecnologici**

I filtri anti-phishing rappresentano la prima linea di difesa contro le email fraudolente. La loro corretta implementazione garantisce un blocco efficace delle minacce prima che raggiungano i dipendenti.
Configurare un sistema che ispeziona ogni link contenuto in un'email e lo confronta con una blacklist di domini malevoli. Qualora il dominio fosse sospetto, l'email viene bloccata o segnalata.

- **Formazione dipendenti**

Il comportamento umano è spesso il fattore più debole nella catena di sicurezza. Una formazione mirata può trasformare i dipendenti da bersagli vulnerabili a una risorsa attiva nella lotta contro il phishing.
Testare periodicamente i dipendenti con campagne simulate di phishing per valutare la loro prontezza. Questi test servono anche a identificare aree dove è necessaria ulteriore formazione.

- **Aggiornamento Policy**

Le policy aziendali devono evolvere per rispondere alle minacce emergenti e creare un ambiente di lavoro sicuro.
Redigere una policy che obbliga l'uso di strumenti di password manager per creare e gestire credenziali complesse, riducendo così la possibilità di riutilizzo o compromissione.

Mitigazione dei Rischi Residuali

Dopo aver implementato le misure di remediation, è essenziale pianificare azioni di mitigazione dei rischi residui per prevenire futuri attacchi e rafforzare la sicurezza aziendale a lungo termine. Questo processo si concentra sul miglioramento continuo delle difese e sulla riduzione della probabilità e dell'impatto di attacchi futuri.

- **Test phishing simulati**

I test di phishing simulati sono strumenti essenziali per valutare l'efficacia delle misure adottate e per sensibilizzare i dipendenti. Questi test migliorano la consapevolezza dei dipendenti e rafforzano la cultura della sicurezza aziendale.

- **Implementazione della MFA (Multi Factor Authentication)**

Il MFA aggiunge un ulteriore livello di protezione che richiede non solo la password, ma più fattori di autenticazione combinati insieme, come un codice generato da un'app, un SMS o un token hardware.
Il MFA aumenta significativamente la resilienza dell'azienda contro attacchi basati sul furto di credenziali.

- **Aggiornamenti Regolari**

Gli aggiornamenti regolari dei sistemi sono essenziali per chiudere le vulnerabilità sfruttabili dagli attaccanti.

Conclusione

Queste misure di mitigazione non solo rafforzano le difese aziendali, ma forniscono un approccio proattivo alla sicurezza. Eseguire test periodici, adottare il 2FA e mantenere aggiornati i sistemi sono strategie complementari che aiutano a minimizzare i rischi residui, rendendo l'azienda un bersaglio meno vulnerabile per i futuri attacchi.