**S11/L1**

**Remediation e Mitigazione**

**Identificazione della Minaccia**

Il phishing è una tecnica di attacco informatico basata sull'ingegneria sociale, progettata per indurre le vittime a fornire informazioni sensibili, come credenziali di accesso, dettagli bancari o dati aziendali riservati. Gli aggressori inviano comunicazioni fraudolente, spesso sotto forma di email apparentemente legittime, che simulano la provenienza da fonti affidabili, quali banche o reparti IT aziendali. Queste email possono contenere link che reindirizzano a siti web malevoli o allegati infetti che, una volta aperti, compromettono i sistemi del destinatario.

Un attacco di phishing può avere conseguenze devastanti per un’azienda. Tra i principali rischi vi è il furto di credenziali, che consente agli aggressori di accedere a sistemi critici, la distribuzione di malware, come ransomware o spyware, e la perdita di dati sensibili, con impatti economici e reputazionali significativi.

**Analisi del Rischio**

L’impatto di un attacco di phishing su un’organizzazione può manifestarsi in diverse forme. Dal punto di vista economico, le truffe possono portare alla perdita di fondi aziendali, al blocco delle operazioni e a costi elevati per il ripristino dei sistemi compromessi. Dal punto di vista reputazionale, l’esfiltrazione di dati sensibili può causare una perdita di fiducia da parte di clienti e partner. Inoltre, la compromissione di sistemi critici può interrompere le operazioni aziendali, causando ritardi e danni alla produttività.

Le risorse più esposte includono le credenziali di accesso dei dipendenti, i dati sensibili come contratti, informazioni dei clienti e dati finanziari, oltre all’infrastruttura IT aziendale, che comprende server, sistemi di posta elettronica e applicazioni.

**Pianificazione della Remediation**

Per mitigare efficacemente una campagna di phishing, è necessario adottare un approccio strutturato. La prima fase consiste nell'identificazione e nel blocco delle email fraudolente. Questo richiede un'analisi approfondita delle email sospette, inclusi header e indirizzi IP, per individuare la fonte dell’attacco. È fondamentale configurare filtri per bloccare domini malevoli e mettere in blacklist gli IP sospetti. Parallelamente, è opportuno segnalare la minaccia agli enti competenti, come i provider di posta elettronica e i CERT (Computer Emergency Response Team).

Un altro aspetto cruciale è la comunicazione ai dipendenti. Devono essere informati tempestivamente sull’attacco in corso attraverso email interne che descrivano le caratteristiche delle email fraudolente e le misure da adottare. Inoltre, è necessario istituire un canale dedicato per la segnalazione di email sospette, favorendo una rapida risposta.

Infine, è essenziale verificare e monitorare i sistemi aziendali per individuare eventuali compromissioni. Questo include l'analisi dei log per identificare accessi non autorizzati, il reset forzato delle credenziali dei dipendenti coinvolti e l’implementazione di soluzioni di monitoraggio continuo, come sistemi IDS/IPS, per prevenire ulteriori intrusioni.

**Implementazione della Remediation**

L’implementazione pratica delle misure di remediation prevede l’adozione di tecnologie e strategie specifiche. L’utilizzo di soluzioni di sicurezza avanzate, come gateway email dotati di funzionalità di sandboxing, rappresenta un elemento chiave per rilevare e bloccare email malevole. Inoltre, la configurazione dei protocolli SPF, DKIM e DMARC garantisce che solo le email autentiche possano essere inviate dai domini aziendali, prevenendo lo spoofing.

Parallelamente, è fondamentale educare i dipendenti sui rischi del phishing. Questo può essere fatto attraverso sessioni di training dedicate e campagne informative che forniscano strumenti pratici per riconoscere email sospette. L'aggiornamento delle policy di sicurezza aziendali, con regole specifiche sull’apertura di allegati e link, aiuta a prevenire comportamenti rischiosi. Inoltre, un piano di risposta agli incidenti ben definito consente all’azienda di reagire rapidamente a futuri attacchi.

**Mitigazione dei Rischi Residuali**

Per ridurre ulteriormente il rischio residuo, è opportuno introdurre misure preventive a lungo termine. L’esecuzione regolare di test di phishing simulati consente di valutare la capacità dei dipendenti di riconoscere le email fraudolente, fornendo feedback personalizzati per migliorare la consapevolezza.

Un’altra misura essenziale è l’implementazione obbligatoria dell’autenticazione a due fattori (2FA) per l'accesso ai sistemi critici. Questo livello aggiuntivo di sicurezza rende più difficile per gli aggressori sfruttare credenziali compromesse. Infine, mantenere sistemi, software e antivirus sempre aggiornati tramite una gestione efficace delle patch riduce il numero di vulnerabilità sfruttabili.

**Conclusione**

Un approccio integrato alla gestione della minaccia di phishing, che combina tecnologie avanzate, formazione dei dipendenti e aggiornamenti regolari dei sistemi, garantisce una protezione efficace contro gli attacchi e minimizza il rischio di compromissioni future. La sicurezza informatica è un processo continuo che richiede il costante adattamento a nuove minacce.