# MITIGATION & REMEDIATION

**Traccia:** 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**

Il phishing è una forma di attacco informatico in cui gli attaccanti tentano di ottenere informazioni sensibili (come credenziali di accesso, numeri di carte di credito, o dati personali) fingendosi una fonte affidabile, solitamente tramite email o messaggi. Gli attaccanti inviano email fraudolente con l'intento di ingannare le vittime, inducendole a cliccare su link malevoli o a scaricare allegati infetti da malware. Queste email spesso imitano comunicazioni aziendali legittime, come quelle di banche, partner commerciali o servizi interni.

Se un dipendente cade vittima di un attacco di phishing, le conseguenze possono essere gravi. Gli attaccanti potrebbero ottenere l'accesso alle credenziali aziendali, compromettere account sensibili, diffondere malware all'interno della rete aziendale, o eseguire attacchi di social engineering su vasta scala. Una volta ottenute le credenziali di accesso, gli attaccanti potrebbero accedere a informazioni riservate o persino disattivare i sistemi aziendali critici.

**Analisi del Rischio**

Il phishing può avere un impatto devastante su un'azienda, portando a violazioni di dati, perdita finanziaria, compromissione dell'integrità dei sistemi IT, danni reputazionali e sanzioni legali in caso di violazione di normative sulla protezione dei dati (come il GDPR).

Le principali risorse che potrebbero essere compromesse includono:

- Credenziali di Accesso: Gli attaccanti potrebbero ottenere username e password per accedere a sistemi aziendali critici.
- Dati Sensibili: Informazioni personali dei dipendenti, dati dei clienti e informazioni finanziarie potrebbero essere esposte.
- Proprietà Intellettuale: Documenti riservati, progetti e altri asset aziendali di valore potrebbero essere trafugati.
- Sistemi IT: I sistemi aziendali potrebbero essere compromessi, con conseguenze come interruzioni operative, perdita di dati o infezione da malware.

**Pianificazione della Remediation**

Piano di Risposta all'Attacco di Phishing:

- Identificazione e Blocco delle Email Fraudolente: Utilizzo di soluzioni di sicurezza avanzate per identificare, bloccare e mettere in quarantena le email sospette prima che raggiungano i dipendenti.
- Comunicazione ai Dipendenti: Informare immediatamente tutti i dipendenti sull'attacco di phishing in corso e su come identificarlo. Inviare linee guida per evitare l'apertura di email sospette e incoraggiare la segnalazione di attività sospette al team IT.
- Verifica e Monitoraggio dei Sistemi: Effettuare una scansione completa dei sistemi IT per identificare eventuali compromissioni, monitorando i log di accesso e di attività anomale nei sistemi aziendali.

## Implementazione della Remediation

Passaggi Pratici per Mitigare la Minaccia di Phishing:

- Implementazione di Filtri Anti-Phishing: Configurare filtri di posta elettronica avanzati per bloccare email di phishing utilizzando tecnologie come SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) e DMARC (Domain-based Message Authentication, Reporting & Conformance) per proteggere i domini aziendali da impersonazioni.
- Formazione dei Dipendenti: Organizzare sessioni di formazione regolari per educare i dipendenti su come riconoscere le email di phishing, cosa fare in caso di sospetta compromissione e l'importanza di non cliccare su link o scaricare allegati da fonti non verificate.
- Aggiornamento delle Policy di Sicurezza: Aggiornare le politiche aziendali di sicurezza per includere linee guida dettagliate su come affrontare il phishing, come l'obbligo di segnalare email sospette e l'adozione di password forti.

**Mitigazione dei Rischi Residuali**

Misure di Mitigazione per Ridurre il Rischio Residuo:

- Test di Phishing Simulati: Eseguire campagne di phishing simulate periodiche per testare la reattività dei dipendenti. Questi test aiutano a identificare eventuali debolezze nella formazione e a migliorare la consapevolezza dei dipendenti.
- Implementazione di Autenticazione a Due Fattori (2FA): Abilitare l'autenticazione a due fattori per tutti gli account aziendali critici. Questo aggiunge un ulteriore livello di sicurezza, rendendo più difficile per gli attaccanti accedere ai sistemi anche se riescono a ottenere le credenziali.

- Aggiornamenti Regolari e Patch: Garantire che tutti i sistemi aziendali e software siano regolarmente aggiornati con le ultime patch di sicurezza per ridurre il rischio di sfruttamento di vulnerabilità note da parte degli attaccanti.

**Conclusione**

Il phishing rappresenta una minaccia seria per qualsiasi azienda, ma con una combinazione di formazione dei dipendenti, tecnologie di sicurezza avanzate, e politiche aziendali aggiornate, è possibile mitigare i rischi e proteggere l'azienda da potenziali compromissioni. Pianificare una risposta rapida e completa è essenziale per minimizzare l'impatto di un attacco di phishing.

*Progetto a cura di*
*Sonia Laterza*