Gestione di una Campagna di Phishing Mirata contro un'Azienda

1. Identificazione della Minaccia

Cos'è il phishing e come funziona:

Il phishing è una tecnica di attacco informatico in cui i criminali informatici inviano email fraudolente che sembrano provenire da fonti affidabili. L'obiettivo è indurre le vittime a:
- Divulgare informazioni sensibili, come credenziali di accesso o dati personali.
- Scaricare allegati o cliccare su link che installano malware sui dispositivi.

Impatto sulla sicurezza aziendale:

Un attacco di phishing può compromettere la sicurezza aziendale in vari modi:
- Accesso non autorizzato: Gli attaccanti possono ottenere credenziali per accedere a sistemi critici.
- Perdita di dati: Informazioni sensibili aziendali possono essere esfiltrate.
- Interruzione delle operazioni: Malware, come ransomware, può bloccare l'accesso ai sistemi aziendali.
- Danni alla reputazione: La divulgazione di dati dei clienti o partner può minare la fiducia nell'azienda.

2. Analisi del Rischio

Impatto potenziale sulla compagnia:

- Operativo: Interruzioni nei processi aziendali critici.
- Finanziario: Costi per il ripristino dei sistemi e possibili multe.
- Legale: Implicazioni legate alla non conformità al GDPR o altre normative.
- Reputazionale: Perdita di fiducia da parte dei clienti e dei partner.

Risorse a rischio:

- Credenziali di accesso: Potrebbero essere usate per accedere a sistemi sensibili.
- Dati sensibili: Informazioni su clienti, fornitori o piani strategici.
- Infrastruttura IT: Sistemi critici potrebbero essere compromessi o danneggiati.
- Finanze aziendali: Attacchi mirati potrebbero portare a frodi finanziarie.

3. Pianificazione della Remediation

Piano per rispondere all'attacco di phishing:

1. Identificazione e blocco delle email fraudolente:
   - Implementare filtri avanzati anti-phishing per l'email aziendale.
   - Analizzare i log email per identificare i mittenti fraudolenti e bloccarli.
2. Comunicazione ai dipendenti:
   - Inviare un avviso immediato ai dipendenti informandoli della campagna di phishing.

- Fornire istruzioni su come riconoscere e segnalare email sospette.
3. Verifica e monitoraggio:
   - Controllare i sistemi per individuare segni di compromissione.
   - Monitorare le attività insolite sui sistemi e sugli account aziendali.

4. Implementazione della Remediation

Passaggi pratici:

1. Filtri anti-phishing e soluzioni di sicurezza:
   - Configurare soluzioni di sicurezza per le email con protezioni contro phishing, spoofing e malware.
   - Abilitare strumenti di verifica dell'identità del mittente, come SPF, DKIM e DMARC.
2. Formazione dei dipendenti:
   - Organizzare workshop o corsi di formazione online per insegnare ai dipendenti come identificare email di phishing.
   - Simulare attacchi di phishing per testare la reattività dei dipendenti.
3. Aggiornamento delle policy aziendali:
   - Aggiornare le policy di sicurezza per includere procedure chiare sulla gestione di email sospette.
   - Implementare restrizioni sui download di file da fonti sconosciute.

5. Mitigazione dei Rischi Residuali

Misure per ridurre il rischio residuo:

1. Test di phishing simulati:
   - Condurre regolarmente campagne simulate per verificare la prontezza dei dipendenti.
   - Analizzare i risultati per identificare le aree di miglioramento.
2. Autenticazione a due fattori (2FA):
   - Implementare il 2FA per tutti gli account aziendali critici.
   - Utilizzare metodi di autenticazione robusti, come app di autenticazione o chiavi hardware.
3. Aggiornamenti e patching
   - Eseguire regolarmente patch di sicurezza sui sistemi operativi, software e applicazioni aziendali.
   - Assicurarsi che i dispositivi endpoint siano protetti da antivirus aggiornati.
4. Backup regolari:
   - Configurare backup automatici e frequenti dei dati aziendali.
   - Verificare la possibilità di ripristinare i dati senza interruzioni.