REMEDIATION E MITIGAZIONE DI MINACCIA DI PHISHING

1. Identificazione della Minaccia

Cos'è il phishing e come funziona?

Il phishing può essere definita come una truffa informatica in cui un attaccante invia email fraudolente per ingannare le persone e far loro compiere azioni dannose, come:

- **Cliccare su link pericolosi** che portano a siti falsi simili a quelli reali.
- **Inserire credenziali aziendali** in un modulo fasullo.
- **Scaricare allegati infetti** che contengono virus o ransomware.

Esempio pratico

Un dipendente riceve un'email apparentemente inviata dall'ufficio IT con oggetto:
"Aggiornamento obbligatorio della password".
Il messaggio contiene un link a un sito che sembra identico al portale aziendale, ma in realtà è un clone. Se il dipendente inserisce le sue credenziali, queste finiscono direttamente nelle mani degli attaccanti.

Come può compromettere la sicurezza aziendale?

- **Accesso non autorizzato ai sistemi aziendali**, permettendo a malintenzionati di rubare dati o sabotare i servizi.
- **Furto di informazioni finanziarie**, causando perdite economiche.
- **Danneggiamento della reputazione aziendale**, riducendo la fiducia di clienti e partner.

2. Analisi del Rischio

Quali sono i possibili impatti sull'azienda?

Se l'attacco ha successo, l'azienda potrebbe affrontare:

- **Perdita di dati sensibili** (es. informazioni su clienti e dipendenti).
- **Sanzioni legali all'Azienda**, se vengono compromessi dati protetti da GDPR.

Quali risorse sono a rischio?

- **Credenziali di accesso** a email, sistemi gestionali e servizi cloud.
- **Dati finanziari**, come per esempio codici IBAN e numeri di carte di credito aziendali.
- **Informazioni sui clienti**, che potrebbero essere vendute nel dark web.

3. Pianificazione della Remediation

Una volta individuata la minaccia, è essenziale agire rapidamente con un piano ben strutturato.

Passaggi per rispondere all'attacco

1. Identificazione e blocco delle email fraudolente

- **Configurare filtri anti-phishing** sui server di posta per rilevare email sospette.
- **Bloccare i domini e gli indirizzi email** identificati come malevoli.

2. Comunicazione ai dipendenti

- Inviare un'email interna con l'avviso: **"Attenzione: nuova campagna di phishing in corso"**.
- Educare i dipendenti con esempi reali, mostrando screenshot delle email pericolose.
- Chiarire **cosa fare** in caso di email sospette: non cliccare, non rispondere e segnalarle subito al team IT.

3. Verifica e monitoraggio dei sistemi

- **Controllare i log di accesso** per individuare eventuali intrusioni.
- **Analizzare i dispositivi aziendali** per verificare la presenza di malware.
- **Forzare il reset delle password** per gli account compromessi.

4. Attuazione della Remediation

Ora è il momento di mettere in pratica il piano di sicurezza per prevenire futuri attacchi.

1. Potenziare la sicurezza delle email

- **Abilitare l'autenticazione SPF (**Sender Policy Framework) **, DKIM (DomainKeys Identified Mail) e DMARC (**Domain-based Message Authentication, Reporting, and Conformance**)**, per impedire agli hacker di inviare email falsificate a nome dell'azienda.
- **Utilizzare software anti-phishing**, come Microsoft Defender o Google Workspace Security.

2. Formazione dei dipendenti

- **Organizzare corsi di formazione** con esempi pratici di phishing.
- **Fare simulazioni di phishing**, inviando email fasulle controllate per vedere quanti dipendenti cadono nel tranello.

3. Aggiornamento delle policy aziendali

- **Implementare regole più rigide** per il riconoscimento delle email sospette.
- **Stabilire una procedura chiara** per verificare richieste sensibili, come bonifici o reset di password.

5. Mitigazione dei Rischi Residuali

Anche con misure di sicurezza avanzate, il rischio di attacchi futuri non scompare del tutto. Ecco alcune strategie per ridurlo ulteriormente:

- **Test di phishing simulati ogni 3-6 mesi**, per valutare la preparazione dei dipendenti.
- **Implementazione dell'autenticazione a due fattori (2FA)** su tutti gli account critici.
- **Monitoraggio continuo con strumenti SIEM**, per rilevare accessi sospetti e attività anomale.

Conclusione

Contrastare un attacco di phishing richiede un approccio combinato di **Tecnologia** (filtri email, 2FA, monitoraggio dei sistemi), **Formazione** (sensibilizzazione e test pratici per i dipendenti) e **Procedure chiare** (policy aziendali e protocolli di verifica).