1. Identificazione della Minaccia

Il phishing è una forma di attacco informatico in cui un attore malevolo tenta di ingannare gli utenti, spingendoli a divulgare informazioni sensibili, come credenziali di accesso, dati bancari o altre informazioni personali. Questo avviene solitamente attraverso email fraudolente, messaggi istantanei o pagine web falsificate che imitano fonti legittime.

Gli attacchi di phishing si basano sull'ingegneria sociale, sfruttando la fiducia dell'utente e la somiglianza visiva tra i messaggi falsi e quelli reali. Alcuni tipi comuni di phishing includono:

- **Spear Phishing**: Attacchi mirati contro singoli individui o aziende.
- **Whaling**: Attacchi diretti verso dirigenti o alte cariche aziendali.
- **Pharming**: Manipolazione di DNS o reindirizzamenti verso siti web falsificati.

Un attacco di phishing può:

- **Rubare credenziali di accesso**: Gli attori malevoli possono ottenere password per accedere a sistemi critici aziendali.
- **Installare malware**: Allegati o link malevoli possono installare ransomware, keylogger o trojan.
- **Compromettere la reputazione aziendale**: L'esposizione di dati dei clienti o interruzioni dei servizi può danneggiare l'immagine pubblica dell'azienda.
- **Causare perdite finanziarie**: Attraverso trasferimenti fraudolenti o costi associati alla riparazione del danno.

2. Analisi del Rischio

Impatto potenziale sull'azienda

L'impatto di un attacco di phishing può includere:

- **Perdita di dati sensibili**: Informazioni relative a clienti, contratti o strategie aziendali.
- **Interruzione operativa**: Sistemi critici potrebbero essere inaccessibili o compromessi.
- **Danni finanziari diretti**: Truffe o riscatto in caso di ransomware.
- **Sanzioni legali**: Se si violano regolamenti come il GDPR.

Risorse che potrebbero essere compromesse

1. **Credenziali di accesso**: Permettono agli attaccanti di accedere a sistemi interni.
2. **Dati sensibili**: Informazioni personali, finanziarie o proprietà intellettuali.
3. **Infrastruttura IT**: Server, database, applicazioni interne.
4. **Reputazione aziendale**: Fiducia di clienti e partner commerciali.

3. Pianificazione della Remediation

Piano di risposta all'attacco

1. **Identificazione e blocco delle email fraudolente**
    - Implementare filtri di sicurezza email per rilevare e bloccare messaggi sospetti.
    - Aggiornare le blacklist con gli indirizzi e i domini utilizzati dagli attaccanti.
    - Analizzare i log dei server di posta per identificare ulteriori attività sospette.
2. **Comunicazione ai dipendenti**
    - Informare tempestivamente tutti i dipendenti dell'attacco in corso.
    - Fornire istruzioni su come riconoscere le email di phishing (es. controllare indirizzi email, evitare link sospetti).
    - Creare un canale dedicato per segnalare tentativi di phishing.
3. **Verifica e monitoraggio dei sistemi**
    - Condurre una scansione dei sistemi per rilevare eventuali malware installati.
    - Monitorare il traffico di rete per identificare connessioni non autorizzate.
    - Rimuovere accessi compromessi e reimpostare le credenziali compromesse.

4. Implementazione della Remediation

Passaggi pratici per mitigare la minaccia

1. **Filtri anti-phishing e sicurezza email**
    - Configurare soluzioni come SPF, DKIM e DMARC per autenticare le email.
    - Utilizzare strumenti di sicurezza avanzata come Microsoft Defender o Google Workspace Security.
2. **Formazione dei dipendenti**
    - Organizzare workshop o moduli di e-learning per insegnare come riconoscere e gestire le minacce di phishing.
    - Fornire esempi pratici di email di phishing.
3. **Aggiornamento delle policy di sicurezza**
    - Implementare regole rigide per la gestione delle credenziali (es. rotazione regolare delle password).
    - Limitare i privilegi di accesso ai sistemi critici.

---

5. Mitigazione dei Rischi Residuali

Misure per ridurre il rischio residuo

1. **Test di phishing simulati**

- Eseguire campagne periodiche di phishing simulato per valutare la preparazione dei dipendenti.
- Fornire feedback immediato su come gestire correttamente tali situazioni.

2. **Autenticazione a due fattori (2FA)**
    - Implementare l'uso obbligatorio della 2FA per tutti i sistemi critici e gli accessi remoti.
    - Utilizzare applicazioni di autenticazione (es. Google Authenticator) o token hardware.
3. **Aggiornamenti e patching**
    - Garantire che tutti i sistemi, i software e i dispositivi aziendali siano aggiornati con le ultime patch di sicurezza.
    - Monitorare costantemente le vulnerabilità pubblicamente note e reagire rapidamente.