● **Compila un report che include:**
○ Descrizione delle minacce di phishing e DoS.
○ Analisi del rischio per entrambe le minacce.
○ Piano di remediation dettagliato per entrambe le minacce.
○ Misure di mitigazione adottate per entrambe le minacce.:

Parte 1: Minaccia di Phishing

1. Identificazione della Minaccia

- **Definizione:** Il phishing è una tecnica di attacco che sfrutta email fraudolente o siti web ingannevoli per indurre le vittime a divulgare informazioni sensibili (es. credenziali, dati bancari) o scaricare malware. Questo tipo di attacco può essere suddiviso in:
    - **Spear phishing:** mirato a specifici individui o gruppi.
    - **Whaling:** indirizzato a figure dirigenziali di alto livello.
- **Funzionamento:**
    - Gli attaccanti inviano email che imitano comunicazioni legittime (es. banche, aziende, fornitori).
    - Le email contengono link a siti web falsi o allegati dannosi.
    - L'utente, ingannato dalla legittimità apparente, inserisce dati sensibili o scarica contenuti dannosi.
- **Compromissione della Sicurezza Aziendale:**
    - Furto di credenziali di accesso.
    - Perdita di dati riservati.
    - Installazione di malware, potenzialmente con accesso a sistemi critici.

---

2. Analisi del Rischio

Probabilità: Possibilità che un attacco di phishing abbia successo, ad esempio a causa di dipendenti non formati.

- **Danno:** Impatto sull'azienda, come perdita di dati, interruzioni operative o danni alla reputazione.
- **Impatto Potenziale:**
    - **Perdita di dati:** Compromissione di informazioni riservate di clienti e dipendenti.
    - **Reputazione:** Danni alla fiducia dei clienti.
    - **Costi:** Spese per recupero dati, indagini e implementazione di nuove difese.

- **Risorse compromesse:**
    - Credenziali di accesso ai sistemi aziendali.
    - Dati finanziari e personali dei clienti.
    - Proprietà intellettuali e strategie aziendali.

---

3. Pianificazione della Remediation

- **Piano di Risposta:**
    1. Identificare e bloccare le email fraudolente tramite soluzioni di sicurezza email come SPF, DKIM e DMARC.
    2. Monitorare i sistemi per identificare eventuali compromissioni..
    3. Comunicare ai dipendenti la minaccia in corso e le misure preventive.

---

4. Implementazione della Remediation

- **Passaggi Pratici:**
    - **Filtri anti-phishing:** Configurare soluzioni di sicurezza per bloccare email sospette.
    - **Formazione:** Educare i dipendenti a riconoscere email fraudolente e segnalare immediatamente.
    - **Aggiornamenti delle policy:** Rivedere e rafforzare le policy di sicurezza, vietando l'apertura di link o allegati non verificati.

---

5. Mitigazione dei Rischi Residuali

- **Misure di Mitigazione:**
    - Simulazioni regolari di phishing per verificare la preparazione dei dipendenti.
    - Implementazione dell'autenticazione a due fattori (2FA) per tutti i sistemi critici.
    - Aggiornamenti continui dei sistemi e delle patch di sicurezza.

Parte 2: Attacco DoS (Denial of Service)

1. Identificazione della Minaccia

- **Definizione:** Un attacco DoS mira a rendere un servizio inaccessibile saturandolo con un traffico eccessivo. Una variante più sofisticata è l'attacco DDoS (Distributed Denial of Service), in cui più macchine compromettono il sistema simultaneamente.

- **Funzionamento:**
    - Gli attaccanti inviano un numero elevato di richieste al server.
    - Il server esaurisce le risorse, impedendo l'accesso agli utenti legittimi.
- **Compromissione della Sicurezza Aziendale:**
    - Interruzione dei servizi critici.
    - Perdita di profitti e fiducia dei clienti.
    - Danni reputazionali a seguito di downtime prolungati.

---

2. Analisi del Rischio

- **Impatto Potenziale:**
    - **Downtime:** I servizi aziendali diventano inaccessibili.
    - **Costi operativi:** Necessità di ripristinare i sistemi e mitigare il danno.
    - **Perdita di clienti:** A causa dell'inaccessibilità dei servizi.
- **Servizi critici compromessi:**
    - Server web aziendali.
    - Applicazioni connesse al cloud.
    - Sistemi di pagamento o gestione ordini online.

---

3. Pianificazione della Remediation

- **Piano di Risposta:**
    1. Identificare le fonti dell'attacco analizzando i log di rete.
    2. Implementare soluzioni di mitigazione per filtrare il traffico malevolo.
    3. Comunicare ai clienti l'accaduto e le tempistiche di ripristino.

---

4. Implementazione della Remediation

- **Passaggi Pratici:**
    - **Bilanciamento del carico:** Distribuire il traffico su più server per evitare sovraccarichi.
    - **Firewall e IDS/IPS:** Configurare regole per bloccare il traffico sospetto e rilevare intrusioni.
    - **Collaborazione con provider DDoS:** Utilizzare servizi come CDN o blackhole routing per mitigare gli attacchi.

---

5. Mitigazione dei Rischi Residuali

- **Misure di Mitigazione:**
    - Monitorare continuamente il traffico di rete con strumenti come Wireshark.
    - Effettuare test di resilienza per verificare l'efficacia delle contromisure.
    - Aggiornare regolarmente il piano di risposta agli incidenti.

Conclusione

Grazie a un'approfondita analisi del rischio e all'applicazione di misure di remediation e mitigation, è possibile proteggere un'azienda da phishing e attacchi DoS. Formazione continua, monitoraggio costante e l'uso delle migliori tecnologie di sicurezza sono essenziali per mantenere la resilienza aziendale.