RELAZIONE SULL'ESERCIZIO DI REMEDIATION E MITIGAZIONE DI MINACCE

PHISHING E ATTACCHI DOS

Introduzione

L'obiettivo di questo esercizio è esplorare strategie per identificare, rispondere e mitigare due minacce comuni nel panorama della sicurezza informatica: **phishing** e **attacchi Denial of Service (DoS)**.

Queste minacce rappresentano rischi significativi per le aziende, e la loro gestione efficace richiede conoscenze tecniche, organizzative e comportamentali.

Parte 1: Minaccia di Phishing

Identificazione della Minaccia

Il **phishing** è una forma di attacco di ingegneria sociale in cui un attore malevolo tenta di ingannare le vittime inducendole a divulgare informazioni sensibili o ad eseguire azioni dannose.

Gli attacchi di phishing avvengono principalmente tramite email fraudolente, ma possono coinvolgere anche messaggi SMS (smishing) o chiamate vocali (vishing).

Caratteristiche principali:

- Imitazione di fonti affidabili (banche, colleghi, fornitori).
- Utilizzo di link fraudolenti che reindirizzano a siti falsi.
- Allegati contenenti malware.

Impatto sull'azienda

Un attacco di phishing può compromettere la sicurezza di un’organizzazione nei seguenti modi:

1. **Furto di credenziali**: accesso non autorizzato ai sistemi aziendali.
2. **Installazione di malware**: infezioni che possono condurre a ransomware o spyware.
3. **Esfiltrazione di dati**: sottrazione di informazioni sensibili come dati dei clienti, progetti riservati o strategie aziendali.
4. **Compromissione della reputazione**: violazioni di dati possono danneggiare la fiducia dei clienti e la reputazione dell'azienda.

Analisi del Rischio

Impatto potenziale:

- **Operativo**: Interruzione dei flussi di lavoro a causa di compromissioni.
- **Economico**: Costi per il ripristino, sanzioni legali e perdita di clienti.
- **Reputazionale**: Perdita di fiducia da parte dei clienti e del mercato.

Risorse a rischio:

- **Credenziali di accesso**: Permettono agli attaccanti di violare account critici.
- **Dati sensibili**: Come contratti, informazioni personali e piani strategici.
- **Infrastruttura IT**: Possibile compromissione di server, database e reti aziendali.

Pianificazione della Remediation

Un piano di remediation efficace deve includere:

1. **Identificazione e blocco delle email fraudolente**:
    - Configurare strumenti di sicurezza email come filtri anti-phishing.
    - Impostare regole di autenticazione email come SPF, DKIM e DMARC per ridurre la possibilità di spoofing.
2. **Comunicazione interna**:
    - Avvisare i dipendenti dell’attacco in corso e delle misure precauzionali da adottare.
    - Fornire istruzioni su come riconoscere email sospette e segnalarle al team di sicurezza.
3. **Verifica e monitoraggio dei sistemi**:

- Analizzare i log di rete e di sistema per identificare eventuali compromissioni.
- Isolare i dispositivi sospetti e avviare la scansione approfondita per la ricerca di malware.

Implementazione della Remediation

1. **Implementazione di soluzioni tecnologiche**:
   - Configurare filtri anti-phishing per bloccare email sospette.
   - Monitorare i log di rete e implementare sistemi di rilevamento delle intrusioni (IDS).
2. **Formazione e sensibilizzazione del personale**:
   - Organizzare sessioni per educare i dipendenti sui rischi del phishing.
   - Simulazioni di phishing per valutare il livello di consapevolezza dei dipendenti e identificare eventuali lacune.
3. **Aggiornamento delle policy di sicurezza**:
   - Definire regole chiare per la gestione delle email sospette.
   - Introduzione di procedure per la verifica delle comunicazioni prima di condividere informazioni sensibili.

Mitigazione dei Rischi Residuali

Misure preventive:

1. **Esecuzione di test di phishing simulati**:
   - Utilizzare piattaforme come KnowBe4 o Cofense per simulare attacchi e migliorare la preparazione dei dipendenti.
2. **Implementazione di autenticazione a due fattori (2FA)**:
   - Richiedere un secondo livello di verifica per accedere a sistemi critici.
   - Garantire la protezione degli account anche in caso di furto di credenziali.
3. **Aggiornamenti regolari e patching**:
   - Applicare patch per correggere vulnerabilità note nei sistemi aziendali.
   - Aggiornare regolarmente i software antivirus e gli strumenti di sicurezza.

4. **Implementare sistemi SIEM (Security Information and Event Management)**:
    - Per identificare comportamenti anomali in tempo reale.

Conclusione

La mitigazione del phishing richiede un approccio integrato che combini tecnologia, formazione e politiche aziendali rigorose.

Attraverso la corretta identificazione delle minacce, un piano di remediation ben strutturato e misure preventive avanzate, è possibile ridurre significativamente il rischio di compromissione.

Parte 2: Minaccia DoS e DDoS

Identificazione della Minaccia

Un attacco **Denial of Service (DoS)** è un tentativo malevolo di rendere un servizio o una risorsa di rete indisponibile per gli utenti legittimi.

Gli attaccanti inondano un server o un'applicazione con un volume eccessivo di richieste o traffico, sovraccaricandolo e impedendo il normale funzionamento.

Caratteristiche principali:

- **Volume-based attacks**: Sovraccarico della larghezza di banda (es. UDP Flood, ICMP Flood).
- **Protocol-based attacks**: Sfruttamento di vulnerabilità nei protocolli di rete (es. SYN Flood).
- **Application-layer attacks**: Saturazione delle risorse delle applicazioni (es. HTTP Flood).

Come compromette la disponibilità dei servizi aziendali?

- **Interruzione dei servizi critici**: Gli utenti legittimi non riescono ad accedere a siti web, portali o applicazioni.
- **Perdita finanziaria**: Downtime prolungati possono ridurre entrate, soprattutto in aziende che offrono servizi online.
- **Impatto sulla reputazione**: Clienti e partner potrebbero percepire l'azienda come insicura o poco affidabile.

Analisi del Rischio

Impatto potenziale:

- **Finanziario**: Ogni minuto di downtime può tradursi in una perdita economica significativa.
- **Operativo**: Impossibilità di accedere a strumenti e applicazioni interni, rallentando le operazioni aziendali.
- **Legale**: Potenziali violazioni di SLA (Service Level Agreement) con partner e clienti.

Servizi critici a rischio:

- **Server web**: Siti aziendali o piattaforme di e-commerce potrebbero diventare inaccessibili.
- **Applicazioni aziendali**: Sistemi gestionali o CRM potrebbero essere inutilizzabili.
- **Infrastruttura di rete**: Router e switch possono essere sovraccaricati, interrompendo la connettività interna ed esterna.

Pianificazione della Remediation

1. **Identificazione delle fonti dell'attacco**:
    - Analizzare i log di rete per individuare pattern di traffico anomalo.
    - Utilizzare strumenti di monitoraggio del traffico come Wireshark per identificare gli IP di origine.
2. **Mitigazione del traffico malevolo**:
    - Configurare regole di **firewall** per bloccare IP sospetti.
    - Implementare **rate limiting** per limitare il numero di richieste per IP e il numero di richieste totali simultanee.
    - Utilizzare tecniche di **blackhole routing** per deviare il traffico malevolo verso una destinazione null.

Implementazione della Remediation

1. **Distribuzione del carico**:
    - Implementare soluzioni di **load balancing** per distribuire il traffico su più server, riducendo il rischio di sovraccarico di un singolo nodo.

2. **Uso di servizi di mitigazione DoS**:
    - Collaborare con fornitori di protezione DoS come Cloudflare o AWS Shield per assorbire il traffico malevolo.
    - Configurare una **Content Delivery Network (CDN)** per gestire il traffico e mitigare gli attacchi volumetrici.
3. **Configurazione del firewall**:
    - Creare regole per bloccare traffico da IP conosciuti come malevoli.
    - Configurare **Web Application Firewall (WAF)** per proteggere le applicazioni da richieste sospette.

Mitigazione dei Rischi Residuali

1. **Monitoraggio continuo**:
    - Implementare sistemi di **monitoraggio e alerting** per identificare e rispondere rapidamente a nuovi attacchi.
    - Utilizzare **IDS/IPS (Intrusion Detection and Prevention Systems)** per rilevare comportamenti anomali in tempo reale.
2. **Collaborazione interna/esterna**:
    - Coordinarsi con il team di sicurezza per migliorare la risposta agli attacchi.
3. **Test periodici di resilienza**:
    - Condurre simulazioni di attacchi DoS per valutare l'efficacia delle misure adottate.
    - Rivedere regolarmente le politiche di sicurezza e applicare aggiornamenti per mitigare nuove vulnerabilità.

Conclusione

Gli attacchi DoS rappresentano una seria minaccia per la disponibilità dei servizi aziendali, ma un approccio integrato che includa distribuzione del carico, mitigazione del traffico malevolo e monitoraggio continuo può ridurre significativamente l'impatto.

Una strategia preventiva, combinata con una risposta tempestiva, è essenziale per garantire la resilienza e la sicurezza dell'infrastruttura aziendale.