Esercizio 21/10/2024

1. Identificazione della Minaccia

Un attacco DoS (Denial of Service) si verifica quando un sistema viene sovraccaricato da richieste eccessive, rendendo i servizi inaccessibili agli utenti legittimi. Le principali tecniche utilizzate negli attacchi DoS includono:

- **SYN Flooding**: L'attaccante invia un gran numero di richieste SYN al server, ma non completa mai la connessione TCP, esaurendo le risorse del server.
- **UDP Flooding**: Vengono inviati pacchetti UDP (User Datagram Protocol) verso porte randomizzate del server, sovraccaricando le risorse con traffico inutile.
- **ICMP Flooding (Ping Flood)**: L'attaccante invia pacchetti ICMP (ping) in massa al server, che diventa incapace di rispondere a richieste legittime.

2. Analisi del Rischio

- **Impatto potenziale sull'azienda:**
    - Interruzione di servizi critici come sistemi di pagamento, portali di clienti o server di posta.
    - **Perdite economiche** dovute a downtime, soprattutto per piattaforme di e-commerce durante periodi ad alto traffico come il Black Friday.
    - **Compromissione della reputazione**: Clienti e partner possono perdere fiducia nell'affidabilità dell'azienda.
- **Risorse aziendali a rischio**:
    - **Server Web**: Rischiano di essere sovraccaricati al punto da non poter più rispondere a nessuna richiesta.
    - **Infrastruttura di rete**: Attacchi di tipo flooding possono saturare la larghezza di banda della rete aziendale.
    - **Database**: Gli attacchi possono far collassare server database se la connessione ai front-end è interrotta.

3. Pianificazione della Remediation

La risposta a un attacco DoS deve essere veloce e coordinata. Ecco un piano di remediation completo:

- **Passo 1: Identificazione delle fonti del traffico**:

- Utilizzare sistemi di monitoraggio avanzati come **NetFlow** o **sFlow** per identificare le fonti del traffico anomalo.
- Implementare soluzioni di **packet capturing** per registrare e analizzare il traffico sospetto.

- **Passo 2: Mitigazione immediata del traffico**:
  - Configurare regole temporanee sui firewall aziendali e sui router per bloccare gli IP responsabili dell'attacco.
  - Se l'attacco proviene da una botnet, considerare l'implementazione di **blackhole routing** temporaneo per deviare il traffico malevolo.

4. Implementazione della Remediation

Soluzioni Tecniche Avanzate:

1. **Scrubbing Center (Centro di pulizia del traffico)**:
   - I **scrubbing centers** sono soluzioni di terze parti che filtrano il traffico DoS prima che raggiunga la rete aziendale. Servizi come **Akamai Kona Site Defender** o **Cloudflare Magic Transit** analizzano il traffico in tempo reale, separando quello legittimo da quello dannoso.
   - Questi servizi sono ideali per attacchi DDoS su larga scala e possono mitigare attacchi da diversi Gbps di traffico.
2. **Reverse Proxy con Cloudflare**:
   - **Cloudflare** offre una soluzione di reverse proxy che agisce come interfaccia tra il server e il traffico. Configurando il dominio aziendale attraverso Cloudflare, il traffico viene analizzato e solo quello legittimo raggiunge il server finale.
   - Questo servizio include funzionalità di mitigazione DoS e CDN per una protezione ottimale.
3. **Automated Threat Detection**:
   - Utilizzare strumenti di rilevamento delle minacce in tempo reale, come **Darktrace** o **Arbor Networks**, che utilizzano l'intelligenza artificiale per identificare schemi di traffico sospetti e bloccarli prima che causino danni.
   - Questi strumenti possono apprendere i pattern normali di traffico e reagire automaticamente quando vengono rilevate anomalie significative.
4. **Intrusion Prevention Systems (IPS)**:
   - L'**IPS** lavora in modo proattivo bloccando pacchetti dannosi in tempo reale. Sistemi come **Snort** o **Suricata** possono rilevare attacchi basati su regole

predefinite e bloccare il traffico in entrata che corrisponde ai pattern di attacco DoS noti.

5. **Diversione del traffico tramite Anycast**:
    - Utilizzare **Anycast**, una tecnologia di routing, permette di distribuire il traffico DoS su più punti di presenza (PoP) globali, diluendo l'impatto dell'attacco. Ad esempio, **Google Cloud** e **AWS** supportano Anycast per mitigare il traffico malevolo.

Pratiche Organizzative:

1. **Response Team Preparato**:
    - Formare un **Incident Response Team (IRT)** addestrato a rispondere rapidamente agli attacchi DoS. Il team deve essere preparato a riconoscere l'attacco, isolare i server colpiti e comunicare efficacemente con il resto dell'azienda.
2. **Scenari di Simulazione**:
    - Simulare attacchi DoS periodici per testare la resilienza dell'infrastruttura e l'efficacia delle misure di difesa. Strumenti come **LOIC** e **HOIC** possono essere utilizzati per condurre simulazioni controllate in un ambiente sicuro.
3. **Piano di Continuità Operativa**:
    - Stabilire un **Business Continuity Plan (BCP)** che garantisca che l'azienda possa continuare a operare, anche durante un attacco. Questo può includere l'uso di server di backup o la migrazione temporanea di servizi critici su piattaforme cloud.

5. Mitigazione dei Rischi Residuali

- **Sottoscrizione a Servizi Anti-DDoS**:
    - Servizi come **AWS Shield Advanced** o **Azure DDoS Protection** offrono protezione dedicata per mitigare attacchi su larga scala.
    - Questi servizi sono gestiti direttamente dai provider cloud e scalano automaticamente per fronteggiare anche gli attacchi più intensi.
- **Test di Resilienza su Base Regolare**:
    - Eseguire test di resilienza su tutta la rete e sui server per garantire che le difese siano in grado di resistere a nuovi tipi di attacchi.
    - Utilizzare strumenti come **hping** per simulare traffico TCP/UDP per verificare l'efficacia dei sistemi di protezione.

Esempio di Scenario Simulato

Scenario simulato: Attacco DoS durante un evento di lancio prodotto Immagina che un’azienda stia lanciando un nuovo prodotto sul suo sito di e-commerce durante il Black Friday. Durante il picco di traffico, gli attaccanti lanciano un attacco DDoS, inviando milioni di richieste SYN e saturando la capacità del server.

Fasi della risposta:

1. **Identificazione dell'attacco**: Il team di sicurezza rileva un aumento anomalo del traffico SYN. Il sistema IPS blocca temporaneamente le richieste in entrata e segnala una possibile minaccia DoS.
2. **Attivazione delle soluzioni di mitigazione**: Viene attivato il **scrubbing center** fornito da Akamai, che inizia a filtrare il traffico in tempo reale. La maggior parte del traffico malevolo viene deviato.
3. **Bilanciamento del carico**: Viene attivata una configurazione Anycast su AWS, che distribuisce il traffico su diversi data center globali.
4. **Comunicazione con il provider ISP**: Il team collabora con l'ISP per bloccare le richieste malevole a livello di rete.
5. **Ripristino del servizio**: Il sito torna operativo entro pochi minuti, grazie all'azione rapida dei sistemi di mitigazione.