Consegna 21 ottobre

Attacco DoS

Un attacco *Denial of Service* (DoS) si verifica quando un aggressore tenta di rendere inaccessibili risorse o servizi, sovraccaricando il server bersaglio con una quantità eccessiva di traffico o richieste. Questo sovraccarico impedisce agli utenti legittimi di accedere al servizio, causando interruzioni e rallentamenti.
Questo può compromettere gravemente i servizi aziendali in diversi modi, tra cui:

1. **Sovraccarico del server**:
   Gli attacchi DoS inondano i server aziendali con una quantità massiccia di richieste. Questo può saturare la **banda di rete** o **esaurire le risorse di sistema**, come CPU e memoria. Quando un server è sovraccarico, non può rispondere tempestivamente alle richieste legittime, causando ritardi o l'impossibilità di accedere ai servizi.

2. **Blocco dei sistemi di comunicazione**:
   Un attacco DoS può compromettere sistemi critici come **server di posta elettronica** o **VPN aziendali**, impedendo ai dipendenti di comunicare tra loro o con clienti/fornitori. Ciò può paralizzare le operazioni aziendali quotidiane.

3. **Impatto sui siti web aziendali**:
   Se un sito web aziendale viene colpito da un attacco DoS, diventa irraggiungibile per i clienti, causando perdita di vendite (se l'azienda ha un portale di e-commerce) e danneggiando la reputazione. I clienti potrebbero non essere in grado di effettuare ordini, richiedere assistenza o accedere a informazioni importanti.

4. **Interruzione delle applicazioni interne**:
   Molte aziende utilizzano applicazioni web-based per gestire il proprio business, come i sistemi di gestione dei clienti (*CRM*) o software di gestione aziendale (*ERP*). Un attacco DoS che compromette questi sistemi può interrompere l'accesso ai dati aziendali essenziali, rallentando i processi decisionali e le operazioni.

5. **Database**:
   Se i database aziendali sono inaccessibili, i dati critici necessari per prendere decisioni aziendali e operare in tempo reale diventano non disponibili.

Impatto Potenziale:
L'indisponibilità dei servizi può portare a una perdita economica diretta (interruzione delle vendite online, ritardi nei processi interni) e indiretta (danni alla reputazione). Inoltre, può aumentare il carico sul team IT e mettere a rischio dati sensibili se l'attacco serve come diversivo per altri tipi di incursioni (es. furto di dati).

Esempio di attacco DoS: Attacco a un e-commerce durante il Black Friday

In questo esempio inventato, un'azienda di e-commerce subisce un attacco DoS che inonda i server con milioni di richieste, rendendo il sito inaccessibile ai clienti. Durante questo evento, l'azienda perde vendite significative e subisce danni alla reputazione.

Pianificazione della Remediation

1. **Identificazione delle fonti dell'attacco**:
    - **Monitoraggio del traffico**: Utilizzare strumenti di analisi del traffico per identificare picchi sospetti e indirizzi IP malevoli. La visibilità in tempo reale aiuta a comprendere la natura dell'attacco e a identificare le fonti.
    - **Analisi dei log**: Rivedere i log del firewall e del server per individuare modelli di traffico anomalo, come richieste elevate da IP specifici.

Mitigazione del traffico malevolo

1. Load Balancing

- **Utilità**: Il bilanciamento del carico distribuisce le richieste tra più server. Questo è cruciale durante il Black Friday, quando il volume delle richieste può aumentare drasticamente. Senza un bilanciatore di carico, un singolo server potrebbe sovraccaricarsi e diventare inaccessibile.

2. CDN (Content Delivery Network)

- **Utilità**: Le CDN possono assorbire traffico malevolo e migliorare la velocità di caricamento dei contenuti. Durante eventi come il Black Friday, le CDN possono gestire picchi di traffico e proteggere l'infrastruttura interna da attacchi DoS.
- **Esempio**: Una CDN può memorizzare nella cache i contenuti statici del sito e servirli ai visitatori, riducendo il carico sui server originari. Se un attaccante inonda il sito di richieste, la CDN può filtrare gran parte di questo traffico, mantenendo accessibili i contenuti legittimi.

3. WAF (Web Application Firewall)

- **Utilità**: Il WAF filtra e monitora il traffico HTTP per identificare e bloccare attacchi malevoli. In situazioni di alto traffico, un WAF può prevenire che le richieste dannose raggiungano il server applicativo.
- **Esempio**: Se un attaccante tenta di sfruttare una vulnerabilità del sito durante il Black Friday, un WAF può bloccare le richieste sospette prima che possano causare danni, garantendo che il sito rimanga disponibile per i clienti.

4. Rate Limiting

- **Utilità**: Limita il numero di richieste che un singolo IP può fare in un determinato periodo. Questo è fondamentale per prevenire attacchi DoS e garantire che le richieste legittime possano passare.

- **Esempio**: Se un singolo IP invia 100 richieste in un secondo, il rate limiting può bloccare ulteriori richieste da quell'IP, prevenendo l'inondazione del server e permettendo a utenti legittimi di accedere al sito.

5. IPS/IDS (Intrusion Prevention/Detection Systems)

- **Utilità**: Questi sistemi monitorano il traffico di rete e possono rilevare e prevenire attacchi in tempo reale. Forniscono una risposta immediata agli attacchi, cruciali durante eventi ad alto rischio come il Black Friday.
- **Esempio**: Se un IPS rileva un numero anomalo di richieste provenienti da un singolo IP, può automaticamente bloccarlo, prevenendo un attacco DoS.

6. Blackhole Routing

- **Utilità**: Deviando il traffico malevolo verso una "blackhole", si riduce il carico sui server legittimi. Questo è utile quando si identificano indirizzi IP sospetti, permettendo ai server di concentrarsi sulle richieste legittime.
- **Esempio**: Se si identifica un attacco da determinati IP, il blackhole routing può deviare queste richieste prima che raggiungano i server, mantenendo il servizio operativo per gli altri utenti.

Implementazione delle Remediation

1. **Bilanciamento del Carico**
    - **Configurazione**: Installare un bilanciatore di carico (ad esempio, HAProxy o NGINX) e configurarlo per distribuire le richieste tra i server web disponibili.
    - **Passaggi**:
        - Definire i server backend nel file di configurazione del bilanciatore.
        - Stabilire algoritmi di bilanciamento, come round-robin o least connections, per gestire il traffico.
        - Monitorare le prestazioni e regolare la configurazione in base al carico.
2. **CDN (Content Delivery Network)**
    - **Configurazione**: Scegliere un provider di CDN (come Cloudflare o Akamai) e configurare il sito per utilizzare la rete di distribuzione dei contenuti.
    - **Passaggi**:
        - Registrare il dominio con la CDN.
        - Impostare le regole di caching per ottimizzare la distribuzione dei contenuti statici.
        - Attivare le funzionalità di protezione DDoS offerte dal provider.
3. **WAF (Web Application Firewall)**
    - **Configurazione**: Implementare un WAF (ad esempio, AWS WAF o ModSecurity) per filtrare il traffico web.
    - **Passaggi**:
        - Definire le regole per bloccare traffico sospetto (come richieste provenienti da IP noti per attività malevole).
        - Attivare la registrazione degli eventi per monitorare le attività e apportare modifiche alle regole in base ai risultati.
4. **Rate Limiting**
    - **Configurazione**: Implementare il rate limiting a livello del server web o del firewall.

- **Passaggi**:
  - Definire i limiti di richieste per IP o per utente, ad esempio consentendo un massimo di 100 richieste al minuto.
  - Monitorare i log per identificare eventuali tentativi di superamento dei limiti e regolare le impostazioni secondo necessità.

5. **IPS/IDS (Intrusion Prevention/Detection Systems)**
   - **Configurazione**: Installare e configurare un sistema IPS/IDS (come Snort o Suricata).
   - **Passaggi**:
     - Aggiornare regolarmente le firme per rilevare le minacce più recenti.
     - Configurare avvisi per attività sospette e potenziali attacchi DoS.
6. **Blackhole Routing**
   - **Configurazione**: Collaborare con il provider di servizi Internet (ISP) per implementare il blackhole routing.
   - **Passaggi**:
     - Identificare gli IP sorgente sospetti.
     - Chiedere all'ISP di deviare il traffico proveniente da quegli IP verso un blackhole, riducendo l'impatto sugli altri utenti.
7. **Monitoraggio e Alerting**
   - **Configurazione**: Utilizzare strumenti di monitoraggio (come Prometheus o Grafana) per monitorare il traffico di rete e le performance del server.
   - **Passaggi**:
     - Impostare allarmi per picchi di traffico anomali.
     - Analizzare i dati di traffico per identificare modelli di attacco e rispondere rapidamente.
8. **Ridondanza e Alta Disponibilità**
   - **Configurazione**: Implementare una configurazione di alta disponibilità per server critici.
   - **Passaggi**:
     - Utilizzare server cluster o failover per garantire che se un server fallisce, un altro prenda il suo posto.
     - Pianificare test regolari per garantire la resilienza delle soluzioni di alta disponibilità.

Mitigazione dei Rischi Residuali

1. **Monitoraggio e alerting**: Stabilire sistemi di monitoraggio per rilevare e rispondere rapidamente a nuovi attacchi, garantendo che il team di sicurezza sia sempre informato.

2. **Test di resilienza**: Effettuare test regolari di simulazione DoS (stress test) per valutare l'efficacia delle misure adottate e identificare eventuali punti deboli.

3. **Collaborazione con il team di sicurezza**: Lavorare con il team IT per migliorare continuamente le difese, affrontando eventuali vulnerabilità e aggiornando le politiche di sicurezza.

Queste misure aiutano a garantire che l'azienda possa affrontare attacchi DoS, migliorando la sua resilienza e la capacità di mantenere i servizi disponibili per i clienti.