



S11-
L1

Remediation & Mitigation: Attacchi Dos

TRACCIA

Attacco DoS (Denial of Service)

Scenario: Immagina di essere un amministratore di sistema per una media azienda che ha subito un attacco DoS. Gli attaccanti inondano i server aziendali di richieste, rendendo i servizi web inaccessibili agli utenti legittimi.

1. Identificazione della Minaccia:

- Ricerca e documenta cos'è un attacco DoS e come funziona.
- Spiega come un attacco DoS può compromettere la disponibilità dei servizi aziendali.

2. Analisi del Rischio:

- Valuta l'impatto potenziale di questa minaccia sull'azienda.
- Identifica i servizi critici che potrebbero essere compromessi (ad es. server web, applicazioni aziendali).

3. Pianificazione della Remediation:

- Sviluppa un piano per rispondere all'attacco DoS. Il piano dovrebbe includere:
- Identificazione delle fonti dell'attacco.
- Mitigazione del traffico malevolo.

4. Implementazione della Remediation:

Descrivi i passaggi pratici che intraprenderesti per mitigare la minaccia di DoS. Questo potrebbe includere:

- Implementazione di soluzioni di bilanciamento del carico per distribuire il traffico.
- Utilizzo di servizi di mitigazione DoS offerti da terze parti.
- Configurazione di regole firewall per bloccare il traffico sospetto.

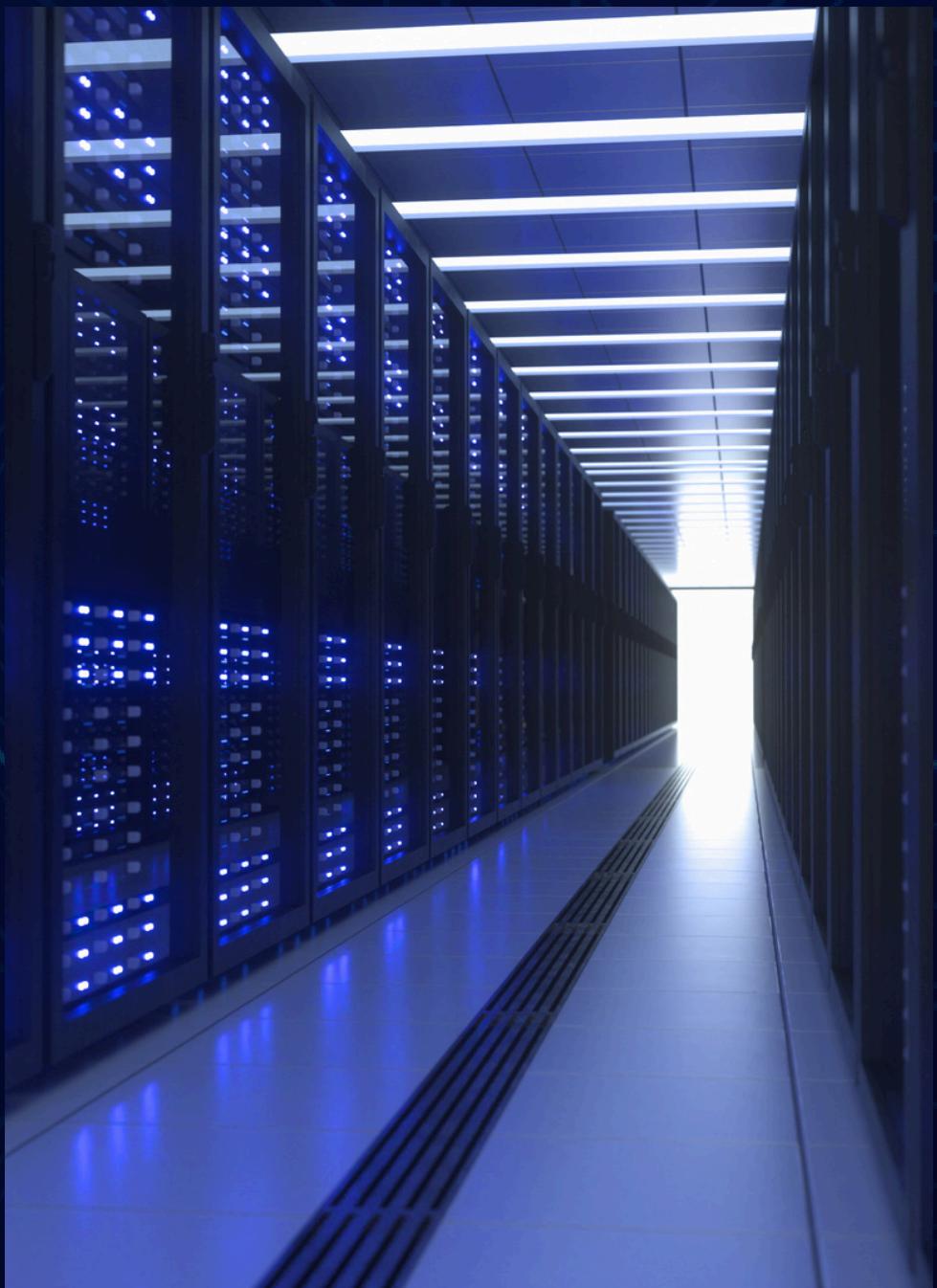
5. Mitigazione dei Rischi Residuali:

Identifica misure di mitigazione da implementare per ridurre il rischio residuo, come:

- Monitoraggio continuo del traffico di rete per rilevare e rispondere rapidamente a nuovi attacchi.
- Collaborazione con il team di sicurezza per migliorare le difese contro DoS.
- Test periodici di resilienza per valutare l'efficacia delle misure di mitigazione adottate.

6. Documentazione e Report:

Compila un report che includa: Descrizione delle minacce di DoS. Analisi del rischio della minaccia. Piano di remediation dettagliato per la minaccia. Misure di mitigazione adottate per la minaccia.



1. IDENTIFICAZIONE DELLA MINACCIA

Cos'è un attacco DoS?

Un attacco Denial of Service (DoS) è un'azione deliberata mirata a rendere indisponibili i servizi di un sistema, una rete o un'applicazione per gli utenti legittimi. Questo viene fatto sovraccaricando il sistema con richieste che ne consumano tutte le risorse disponibili.

Tipologie principali di attacchi DoS:

1. Flooding (Inondazione): Consiste nell'inviare grandi volumi di pacchetti o richieste in un breve periodo. Esempi comuni sono:
 - **SYN Flood**: sfrutta il meccanismo di handshake TCP (protocollo di connessione affidabile). L'attaccante invia pacchetti SYN senza completare la connessione, bloccando le risorse del server.
 - **HTTP Flood**: l'attaccante invia richieste HTTP legittime in quantità eccessiva, sovraccaricando il server web.
 - **UDP Flood**: utilizza pacchetti UDP (User Datagram Protocol), che non richiedono un meccanismo di connessione, per saturare la banda.
2. Amplification (Amplificazione):
 - L'attaccante invia richieste a un servizio mal configurato (es. DNS o NTP) con l'indirizzo IP della vittima come mittente. Il servizio risponde con pacchetti di grandi dimensioni, amplificando il volume del traffico verso la vittima.
 - **Esempio**: Una richiesta di 60 byte al server DNS genera una risposta di 4.000 byte inviata alla vittima.

Impatto sulla disponibilità:

- Rallentamento o interruzione completa dei servizi critici.
- Difficoltà di accesso da parte degli utenti legittimi.
- Effetti a cascata su altre infrastrutture aziendali, come database o applicazioni connesse.

2. ANALISI DEL RISCHIO

Andremo a vedere l'impatto che avrà sull'azienda in termini di costi operativi, finanziari e reputazionali:

1. Operativo:

- Interruzione di operazioni aziendali chiave.
- Impatto diretto sulla produttività dei dipendenti.

2. Finanziario:

- Costi per la risposta e la mitigazione dell'attacco.
- Perdita di entrate causata dall'inaccessibilità dei servizi per i clienti.

3. Reputazionale:

- Danno alla percezione dell'affidabilità dell'azienda da parte di clienti e partner.

Servizi critici che potrebbero essere compromessi:

- Server Web: interruzione dei portali per clienti, partner e dipendenti.
- Sistemi ERP/CRM: blocco delle applicazioni che gestiscono risorse aziendali e relazioni con i clienti.
- Email aziendale: difficoltà nella comunicazione interna ed esterna.
- Database aziendali: ritardi o impossibilità nell'accesso ai dati.

3. PIANIFICAZIONE DELLA REMEDIATION

Piano di risposta dettagliato:

1. Identificazione delle fonti dell'attacco:

- **Analisi dei log del server:** Esaminare i file di registro per individuare indirizzi IP che inviano volumi anomali di traffico.
- **Strumenti di monitoraggio:** Utilizzare Wireshark poichè consente di catturare e analizzare pacchetti di rete per identificare flussi sospetti. Un altro tool che si può utilizzare è NetFlow ovvero uno strumento che fornisce una panoramica del traffico di rete e consente di individuare anomalie.

2. Mitigazione del traffico malevolo:

- **Filtraggio degli IP sospetti:** Utilizzare firewall o regole di rete per bloccare gli indirizzi IP identificati come sorgenti dell'attacco.
- **Rate Limiting:** Limitare il numero di richieste accettate da un singolo IP per un determinato periodo di tempo.

4. IMPLEMENTAZIONE DELLA REMEDIATION

Per mitigare una minaccia, seguirei i seguenti passaggi:

Per prima cosa procederei con un Load balancing per distribuire il traffico su più server per evitare che uno solo venga sovraccaricato.

Strumenti comuni utilizzati nel processo sono:

- **Hardware dedicato**: dispositivi come F5 Big-IP.
- **Soluzioni cloud**: AWS Elastic Load Balancing o Azure Load Balancer.

Per una miglior gestione potrei affidarmi a servizi terzi come:

- **Cloudflare**: offre protezione da attacchi DoS e distribuisce il traffico tramite una rete globale di server.
- **AWS Shield**: una soluzione AWS per mitigare gli attacchi DoS/DDoS.

entrambi questi servizi hanno un riconoscimento e blocco automatico di traffico anomalo e riduzione del carico diretto sui server aziendali.

Procederei a una configurazione del firewall tramite regole definite come:

- Blocco di indirizzi IP specifici noti per il traffico malevole (non preferibile nel DDoS poiché sarebbero troppi gli indirizzi IP da bloccare)
- Implementazione di un Geo-blocking per limitare il traffico proveniente da determinate regioni geografiche.

5. MITIGAZIONE DEI RISCHI RESIDUALI

Per la prevenzione a lungo termine seguirei queste indicazioni:

Implementarei un IDS/IPS (Intrusion Detection/Prevention System) per un monitoraggio continuo.

Come ad esempio:

- Snort che viene utilizzato per rilevare attività anomale nella rete e può bloccare traffico malevolo.
- Suricata che viene utilizzato come strumento avanzato per il rilevamento delle intrusioni.

Farei un piano di incident Response definendo delle procedure per rispondere rapidamente a futuri attacchi.

Testerei periodicamente i team della sicurezza attraverso:

- Simulazioni di attacco: utilizzare strumenti come LOIC o HOIC in un ambiente controllato per simulare attacchi DoS e verificare la resilienza dei sistemi.
- Valutare regolarmente l'efficacia delle misure adottate con penetration test.

6. REPORT ATTACCO DOS

Il 15 novembre 2024, alle ore 10:30, il server web aziendale dell'azienda Terasys Solutions ha iniziato a registrare un improvviso e significativo aumento del traffico in entrata. Nel giro di pochi minuti, il sito è diventato inaccessibile per i clienti. Questo ha comportato un'interruzione completa dei servizi critici, tra cui:

- Portale clienti: utilizzato per gestire gli ordini e le richieste di supporto tecnico.
- Piattaforma di pagamento: essenziale per l'elaborazione delle transazioni.

L'attacco registrato è stato un SYN Flood: L'analisi dei log del server ha mostrato che il traffico proveniva da più indirizzi IP distribuiti globalmente (indicativo molto probabilmente di un attacco DoS amplificato o botnet).

Nel volume del traffico è stato registrato un incremento significativo di richieste che passano da una media di 500 al minuto a oltre 20.000 al secondo.

Ogni richiesta consumava risorse significative del server, impedendo la gestione delle connessioni legittime.

Tramite il monitoraggio di rete con Wireshark, è stato rilevato che il traffico proveniva da un pattern anomalo con pacchetti SYN incompleti.

Siamo intervenuti immediatamente con la mitigazione inserendo regole firewall per bloccare gli indirizzi IP con un alto tasso di richieste e abbiamo impostato un rate limiting massimo di 50 richieste al secondo per ogni IP.

Per il ripristino abbiamo configurato un Load Balancer per distribuire il traffico legittimo su un server secondario minimizzando l'interruzione e, durante l'attacco, abbiamo inoltre disattivato alcune funzionalità non essenziali del sito per ridurre il carico complessivo.

L'impatto sull'azienda è stato abbastanza significativo anche se abbiamo agito nel più breve tempo possibile:

- Durata dell'interruzione: circa 2 ore.
- Clienti impattati: circa 1.200 utenti non hanno potuto accedere ai servizi durante l'attacco.
- Perdite finanziarie: stimate in 15.000 euro, principalmente derivanti da transazioni mancate e risorse utilizzate per la risposta all'incidente.

Misure preventive che consigliamo di adottare in futuro:

- Implementazione di un servizio DDoS Protection: contratto un servizio con Cloudflare per filtrare attacchi futuri.
- Upgrade infrastrutturale: potenziamento del bilanciatore di carico e dei firewall aziendali.
- Simulazioni periodiche: pianificate simulazioni mensili di attacchi DoS per migliorare la preparazione del team IT.

THANK FOR YOUR ATTENTION

Mattia Di Donato