Scenario: Attacco DoS in Azienda

Identificazione della Minaccia

Cos'è un attacco DoS e come funziona:

Un attacco DoS è un tentativo di bloccare i servizi aziendali inviando una quantità eccessiva di richieste ai server, saturando così le risorse come la banda di rete o la memoria, e impedendo agli utenti legittimi di accedere ai servizi. Gli attacchi DoS possono essere eseguiti da un singolo computer o tramite una rete di dispositivi compromessi chiamata botnet. Esistono vari tipi di attacchi DoS, tra cui:

- **Attacchi Volumetrici**: Usano una grande quantità di traffico per saturare la banda di rete, rendendo impossibile il passaggio del traffico legittimo.
- **Attacchi di Protocollo**: Sfruttano vulnerabilità nei protocolli di rete per sovraccaricare i server e bloccarli.
- **Attacchi Applicativi**: Colpiscono i servizi applicativi inviando richieste che sovraccaricano il sistema, come query intensive ai database.

Impatto sulla disponibilità dei servizi:

Un attacco DoS può impedire agli utenti di accedere ai servizi aziendali, causando interruzioni che riducono la produttività, compromettono le entrate e danneggiano la reputazione aziendale. L'accesso ai server web e alle applicazioni critiche può essere bloccato, causando perdite finanziarie e problemi per i clienti. Inoltre, un attacco prolungato può causare la perdita di dati e richiedere molto tempo per il recupero. Il personale IT può essere sovraccaricato nel tentativo di risolvere il problema, riducendo la capacità di occuparsi di altre attività importanti.

- **Interruzioni Prolungate**: L'indisponibilità dei servizi può avere effetti a lungo termine, soprattutto se non si interviene rapidamente per mitigare l'attacco. Anche il recupero completo può essere costoso e impegnativo.
- **Effetti su Clienti e Partner**: La fiducia dei clienti e dei partner potrebbe essere compromessa se l'azienda non riesce a garantire un servizio adeguato. La perdita di credibilità può portare a una riduzione della clientela e delle opportunità di business.

2. Analisi del Rischio

Valutazione dell'impatto:

L'impatto di un attacco DoS dipende dalla criticità dei servizi interrotti. Se vengono colpiti servizi fondamentali come il server web o le applicazioni aziendali, i rischi possono includere:

- **Perdite Economiche**: Se i clienti non possono fare acquisti o accedere ai servizi, l'azienda perde entrate importanti, con conseguenze finanziarie significative.
- **Danneggiamento della Reputazione**: L'incapacità di fornire servizi danneggia la fiducia dei clienti, che potrebbero rivolgersi ai concorrenti. Una buona reputazione richiede anni per

essere costruita, ma può essere compromessa in pochi minuti di indisponibilità.
- **Riduzione della Produttività**: I dipendenti potrebbero non essere in grado di accedere agli strumenti necessari per lavorare, riducendo la produttività. Questo può causare ritardi in progetti e consegne.
- **Sanzioni Legali o Contrattuali**: Se l'azienda non riesce a rispettare gli accordi sui livelli di servizio (SLA), potrebbe dover affrontare azioni legali o pagare penali. Le violazioni degli SLA potrebbero anche compromettere le relazioni con partner e clienti.

Servizi critici identificati:

- **Server Web**: È fondamentale per l'interazione con clienti e partner. Un server web inaccessibile può avere un impatto significativo su tutte le operazioni aziendali, limitando la capacità di fornire informazioni e servizi cruciali.
- **Applicazioni Aziendali**: Sistemi come ERP (Enterprise Resource Planning) e CRM (Customer Relationship Management) sono essenziali per la gestione di vendite, logistica e supporto clienti. La loro indisponibilità potrebbe interrompere la catena di approvvigionamento e complicare la gestione delle relazioni con i clienti.

3. Pianificazione della Remediation

Piano di Risposta all'attacco DoS:

- **Identificazione delle Fonti dell'Attacco**: Utilizzare strumenti di monitoraggio della rete, come sistemi di rilevamento delle intrusioni (IDS) e sistemi di prevenzione delle intrusioni (IPS), per identificare gli indirizzi IP coinvolti e capire se le richieste sono legittime o malevole. Analizzare i pattern di traffico per rilevare anomalie e individuare la provenienza dell'attacco. Strumenti avanzati di monitoraggio possono fornire dettagli sulla natura del traffico, inclusi paesi di origine e volumi.
- **Mitigazione del Traffico Malevolo**: Implementare misure per filtrare e bloccare il traffico sospetto. Queste misure possono includere la limitazione del numero di richieste per unità di tempo (rate limiting) e il blackhole routing, che indirizza il traffico malevolo verso una destinazione che lo scarta automaticamente. Tecnologie di geofencing possono essere utilizzate per bloccare il traffico da regioni sospette.

4. Implementazione della Remediation

Passaggi Pratici per Mitigare l'Attacco DoS:

- **Bilanciamento del Carico**: Utilizzare soluzioni di bilanciamento del carico per distribuire il traffico legittimo su più server, riducendo la pressione su ciascuno di essi. Queste soluzioni possono essere hardware o software e aiutano a gestire picchi di traffico senza interrompere i servizi. Il bilanciamento del carico garantisce che nessun singolo server sia sovraccaricato e che le risorse siano utilizzate in modo efficiente.
- **Servizi di Mitigazione DoS**: Utilizzare servizi forniti da terze parti, come Cloudflare, Akamai o AWS Shield, per filtrare il traffico malevolo prima che raggiunga i server aziendali. Questi servizi utilizzano infrastrutture distribuite per assorbire grandi volumi di traffico e ridurre

l'impatto dell'attacco. Questi provider spesso usano tecniche come il filtraggio del traffico a livello globale e l'analisi comportamentale per identificare le richieste sospette.
- **Regole Firewall**: Configurare regole firewall per bloccare il traffico sospetto e consentire solo connessioni legittime. Impostare limiti per ridurre il numero di richieste per IP e aggiornare regolarmente le regole per rispondere ai nuovi tipi di attacchi. Le regole firewall possono essere configurate in modo dinamico per adattarsi ai pattern di attacco in evoluzione, garantendo una risposta tempestiva.
- **Segmentazione della Rete**: Isolare i servizi critici in segmenti separati della rete per limitare l'impatto di un attacco. In questo modo, se un segmento viene colpito, gli altri restano operativi. La segmentazione può anche migliorare la sicurezza complessiva, limitando la propagazione degli attacchi all'interno dell'infrastruttura.

5. Mitigazione dei Rischi Residuali

Misure di Mitigazione:

- **Monitoraggio Continuo**: Implementare strumenti di monitoraggio continuo, come sistemi SIEM (Security Information and Event Management), per rilevare picchi di traffico anomali e rispondere rapidamente. Automatizzare gli avvisi per segnalare comportamenti sospetti e adottare azioni correttive immediatamente. Un monitoraggio continuo permette di identificare rapidamente i segnali di un possibile attacco e intervenire prima che possa causare gravi danni.
- **Collaborazione con il Team di Sicurezza**: Coordinarsi con il team di sicurezza per migliorare le difese e attivare piani di risposta rapida. Organizzare riunioni regolari per discutere nuove minacce e adattare le strategie di difesa. Usare l'intelligence sulle minacce per prevenire futuri attacchi. La collaborazione interna ed esterna con esperti di sicurezza può migliorare significativamente la resilienza dell'infrastruttura IT.
- **Test Periodici di Resilienza**: Eseguire simulazioni di attacco e test di stress per verificare l'efficacia delle misure adottate e migliorarle nel tempo. Questi test aiutano a garantire che i sistemi siano pronti a resistere a un attacco reale. È utile condurre test regolari per adattarsi alle nuove tecniche di attacco, assicurandosi che la strategia di difesa rimanga aggiornata.
- **Piani di Continuità Operativa**: Creare piani per garantire la continuità dei servizi durante un attacco DoS, come il passaggio a server di backup o il reindirizzamento del traffico su percorsi alternativi. La continuità operativa deve includere l'identificazione di servizi alternativi e soluzioni di failover che possano essere attivate rapidamente in caso di emergenza.

Documentazione e Report

Descrizione delle Minacce di Phishing e DoS:

- **Phishing**: È un attacco in cui un aggressore cerca di ottenere informazioni sensibili ingannando l'utente con comunicazioni apparentemente legittime, come email o messaggi. Il phishing può compromettere la sicurezza aziendale causando la perdita di dati sensibili. Gli attacchi di phishing sono spesso sofisticati e possono essere difficili da rilevare se i dipendenti non sono adeguatamente formati a riconoscere le minacce.

- **DoS**: Un attacco che impedisce agli utenti di accedere ai servizi aziendali sovraccaricando le risorse del sistema. Può essere lanciato da un singolo attaccante o tramite una rete distribuita (DDoS), rendendo la mitigazione ancora più complessa. Gli attacchi DDoS utilizzano reti globali di dispositivi compromessi per lanciare attacchi su vasta scala che possono sopraffare anche le infrastrutture più robuste.

Analisi del Rischio:

- **Phishing**: Rischio di compromissione di credenziali e dati sensibili, con conseguenze finanziarie e danni alla reputazione. Un attacco di phishing ben riuscito potrebbe portare alla compromissione dell'intera rete aziendale. Gli attacchi di phishing mirati, come lo spear phishing, possono colpire individui specifici per ottenere accesso privilegiato alle informazioni aziendali.
- **DoS**: Rischio di interruzione dei servizi, con conseguenze sulla continuità operativa e sulla fiducia dei clienti. Un attacco DoS può fermare l'intera infrastruttura aziendale, causando non solo la perdita di accesso ai servizi, ma anche danni all'immagine aziendale. La continuità operativa potrebbe essere compromessa per giorni se non vengono adottate misure adeguate.

Piano di Remediation e Misure di Mitigazione:

- **Phishing**: Formare i dipendenti per riconoscere email sospette e segnalare tentativi di phishing. Usare filtri anti-phishing e implementare l'autenticazione a due fattori per aumentare la sicurezza. Organizzare workshop e campagne di sensibilizzazione per migliorare la consapevolezza. Un programma di simulazioni di phishing per testare la preparazione dei dipendenti può essere utile per migliorare la resilienza.
- **DoS**: Utilizzare soluzioni di bilanciamento del carico, firewall avanzati e servizi di protezione cloud. Collaborare con fornitori di sicurezza per mantenere i sistemi aggiornati e preparati contro le nuove minacce emergenti. Assicurarsi che l'infrastruttura sia progettata con ridondanza e failover per garantire la resilienza anche in caso di attacchi complessi.