REMEDIATION & MITIGATION ATTACCHI DOS

1. Identificazione della minaccia

Attacco Dos cos'è e come funziona

L'attacco DoS (Denial of Service) è tra i più diffusi attacchi informatici, ha lo scopo di rendere un sistema, servizio o rete non disponibili tramite il sovraccaricamento delle risorse, questo avviene inviando una quantità eccessiva di pacchetti o richieste nella rete fino a consumarne le risorse.

Un attacco DoS può causare significative interruzioni ai servizi aziendali come ad esempio Server Web, E-commerce ed E-mail.

2. Analisi del rischio

L'impatto di un attacco DoS dipende molto dai sistemi che vengono compromessi, ad esempio per le aziende che offrono servizi online l'impossibilità degli utenti di raggiungerli potrebbe comportare a ingenti perdite economiche e allo stesso tempo ci sarebbe anche un danno reputazionale in quanto gli stessi clienti potrebbero perdere fiducia nel brand.

Servizi critici compromessi

Server Web
App aziendali (CRM)
Database Aziendali
Servizi Cloud

3. Pianificazione della Remediation

Fonti di Attacco

- Monitoraggio del traffico di rete: (identificazione di picchi anomali di traffico o indirizzi ip sospetti)
- Strumenti e analisi
- Identificare l'origine di attacco: nel caso di un DDoS sarà più difficile individuare il punto di origine essendo coinvolti più dispositivi bot

Mitigazione Traffico malevolo

- Bloccare IP sospetti
- Filtraggio del traffico tramite Firewall
- Rate Limiting: limitare la velocità di richieste inviate al server

4. Implementazione della Remediation

Come mitigare un attacco DoS

Bilanciamento del carico: la distribuzione del traffico su più server aiuta ad evitare che il singolo server possa essere sovraccaricato.

Servizi di mitigazione DoS: l'utilizzo di soluzioni esterne come quelle offerte da Cloudflare analizzano e filtrano il traffico malevolo prima che questo raggiunga la rete aziendale mentre l'implementazione di CDN aiuta a ridurre l'impatto dell'attacco diretto sul server aziendale.

Configurazione di regole firewall: L'utilizzo di firewall avanzati in combinazione con sistemi di IDS/IPS bloccheranno il traffico proveniente da fonti sospette o indirizzi ip noti, altra best practice è quella di implementare un sistema di limitazione delle richieste DNS anomale

Test periodici: eseguire stress test regolari per valutare e analizzare il comportamento dei sistemi sotto carico ed eventuali simulazioni di attacco aiuteranno il team di sicurezza a migliorare i piani di risposta.

Monitoraggio continuo della rete con strumenti come Splunk

Continua formazione del team di sicurezza per la risposta agli incidenti e un ripristino tempestivo dei servizi.

Gli attacchi DoS/DDoS rappresentano una minaccia significativa per le aziende moderne, in particolare per quelle che offrono servizi online. Tuttavia, con un piano di risposta ben strutturato, l'adozione di soluzioni di mitigazione avanzate e un monitoraggio continuo, è possibile ridurre significativamente l'impatto di tali attacchi. Un approccio combinato di prevenzione, rilevamento e recupero è fondamentale per garantire la disponibilità dei servizi aziendali e proteggere i dati sensibili.