M5 - Progetto Finale - Impatti sul Business

Calcolo dell'impatto sul business

- Tempo di inattività: 10 minuti;
- Spesa media per minuto da parte degli utenti: 1500€.

Per calcolare l'impatto economico diretto, moltiplichiamo il tempo di inattività per la spesa media al minuto:

Impatto economico = Tempo di inattività (minuti) × Spesa media per minuto
Impatto economico = 10 minuti×1.500 €/minuto
Impatto economico = 15.000€

Questa cifra rappresenta la perdita diretta di entrate subita dalla piattaforma di e-commerce a causa della non raggiungibilità del servizio durante l'attacco DDoS. È importante notare che questo calcolo non include altri potenziali danni, come il danno alla reputazione del brand, la perdita di fiducia dei clienti o i costi di recupero e mitigazione dell'attacco.

Valutazioni di azioni preventive per attacchi DDoS

Gli attacchi Distributed Denial of Service (DDoS) mirano a rendere un servizio non disponibile saturando le sue risorse (banda, server, applicazione). Le azioni preventive si concentrano sulla capacità di assorbire, filtrare o deviare il traffico malevolo.

Servizi di protezione DDoS basati su Cloud

- Implementazione: L'utilizzo di un provider specializzato in servizi di protezione DDoS basati su cloud (es. Cloudflare, Akamai, AWS Shield, Google Cloud Armor) è la misura più efficace. Questi servizi agiscono come un "filtro" del traffico, posizionandosi tra l'Internet e la propria infrastruttura.
- Funzionalità: I provider DDoS dispongono di una vasta capacità di banda e di algoritmi sofisticati per identificare, mitigare e deviare il traffico DDoS, instradando solo il traffico legittimo verso la propria applicazione. Possono assorbire attacchi di grande entità che supererebbero la capacità della propria rete e del proprio firewall.
- Benefici: Offre protezione scalabile contro attacchi di volume (Layer 3/4) e applicativi (Layer 7), riducendo drasticamente il tempo di inattività del servizio e l'impatto sul business. Sposta il carico di mitigazione su infrastrutture esterne e specializzate.

Bilanciamento del Carico e Scalabilità Automatica

- Implementazione: Utilizzare bilanciatori di carico (hardware o software) per distribuire il traffico in entrata su più istanze dell'applicazione e-commerce. Configurare l'infrastruttura (specialmente in ambienti cloud) per scalare automaticamente (es. auto-scaling group) aggiungendo nuove istanze dell'applicazione durante picchi di traffico.
- Funzionalità: Il bilanciamento del carico distribuisce la richiesta tra diversi server, prevenendo che una singola risorsa diventi un collo di bottiglia. La scalabilità automatica aumenta dinamicamente la capacità computazionale e di rete disponibile, permettendo di gestire un maggior volume di richieste, anche se parte di esse è malevola, e di mantenere la disponibilità del servizio.
- Benefici: Migliora significativamente la resilienza e la capacità di gestire fluttuazioni di traffico, inclusi attacchi DDoS di intensità moderata.

Limiti di Velocità e Configurazioni del Firewall

- Implementazione: Configurare il firewall perimetrale (quello tra Internet e la DMZ) e, se presente, il Web Application Firewall (WAF), per applicare limiti al numero di richieste che un singolo indirizzo IP (o un gruppo di IP) può fare in un determinato periodo di tempo.
- Funzionalità: Questa misura può aiutare a mitigare attacchi DDoS di tipo applicativo (Layer 7) che generano un elevato numero di richieste legittime ma eccessive. Il firewall può anche essere configurato per bloccare pattern di traffico noti come malevoli o per rifiutare connessioni da IP sorgente sospetti.
- Benefici: Protezione contro attacchi mirati a risorse specifiche dell'applicazione e mitigazione di attacchi basati su connessioni.

Network Segmentation e Servizi CDN (Content Delivery Network)

- Implementazione: Sebbene non direttamente una protezione DDoS, l'uso di una CDN per i contenuti statici (immagini, CSS, JavaScript) può ridurre il carico sui server dell'applicazione durante un attacco. La segmentazione della rete può aiutare a contenere un attacco nel caso in cui una porzione della rete venga comunque saturata.
- Funzionalità: Le CDN distribuiscono i contenuti statici su server geograficamente dispersi, assorbendo una parte significativa del traffico e proteggendo i server di origine.
- Benefici: Riduzione della superficie di attacco e della banda necessaria sui server principali durante un attacco.

Conclusioni

Un attacco DDoS, anche di breve durata, può avere un impatto economico significativo sul business di un'applicazione e-commerce, come dimostrato dalla perdita diretta di 15.000 € in soli 10 minuti. Per mitigare tale rischio, è indispensabile adottare una strategia proattiva e stratificata. L'implementazione di servizi di protezione DDoS basati su cloud è la misura più robusta e scalabile, in grado di assorbire e filtrare attacchi di grande portata. Parallelamente, l'utilizzo di bilanciatori del carico e la configurazione della scalabilità automatica aumentano la resilienza intrinseca dell'infrastruttura. L'applicazione di limiti di velocità a livello di firewall e l'ottimizzazione tramite CDN contribuiscono ulteriormente a rafforzare le difese, garantendo la continuità operativa e minimizzando le perdite finanziarie e reputazionali derivanti da attacchi di negazione del servizio.