Difesa DDoS: la rapidità è essenziale

a cura di Ivan Straniero, Regional Manager, Southern & Eastern Europe di NETSCOUT Arbor

Nella difesa DDoS la rapidità è tutto. Attacchi in grandi volumi e rapidissimi possono materializzarsi in un istante e crescere fino a centinaia di gigabit nel giro di pochi secondi. Può sembrare che le applicazioni funzionino correttamente per poi diventare improvvisamente indisponibili senza un motivo immediatamente evidente. Quando si arriva a capire di essere sotto attacco, possono già essere avvenuti danni collaterali notevoli.

Gli attacchi DDoS possono anche colpire più bersagli contemporaneamente, dalla connessione a internet alle applicazioni fino all'infrastruttura di rete, inclusi firewall, firewall web (WAF) e sistemi anti-intrusione (IPS). Gli attacchi stanno diventando sempre più stratificati e superano le difese aziendali facendo leva su molteplici metodologie di attacco e tattiche diversive. La capacità di difendere la propria organizzazione e preservare la disponibilità dei servizi è direttamente correlata alla velocità di risposta a queste minacce multiple e prolungate.

I tre fattori chiave per la velocità

Come è possibile guadagnare secondi preziosi nel tempo di risposta e girare la situazione a proprio vantaggio? Occorre prestare attenzione ai tre fattori chiave per la velocità:

Rilevazione: la velocità di individuazione degli attacchi DDoS è la prima e più importante abilità necessaria per avviare un rapido programma di mitigazione. La scelta della soluzione da utilizzare su questo fronte incide sensibilmente sul profilo di rischio. È meglio aggiungere una nuova funzione al firewall esistente o è invece opportuno scegliere una protezione DDoS appositamente concepita e realizzata per questo scopo? Quali sono le differenze e perché sono importanti?

I dispositivi IPS, i firewall e gli altri prodotti di sicurezza sono elementi essenziali di una strategia di difesa stratificata, ma sono concepiti per risolvere problemi di sicurezza fondamentalmente diversi da quelli affrontati dai prodotti specifici per la rilevazione e mitigazione degli attacchi DDoS. I dispositivi IPS, ad esempio, bloccano i tentativi di attacco all'origine dei furti di dati. Nel mentre, i firewall svolgono un'azione di controllo per impedire l'accesso non autorizzato ai dati. Tuttavia, pur riuscendo a tutelare efficacemente l'integrità e la riservatezza della rete, questi prodotti di sicurezza non affrontano uno dei principali bersagli degli attacchi DDoS, ovvero la disponibilità della rete.

Le limitazioni dei firewall e dei dispositivi IPS mettono in luce i fondamentali benefici offerti dalle soluzioni IDMS (Intelligent DDoS Mitigation Solution).

- Le soluzioni IDMS sono stateless, ovvero non tracciano lo stato di tutte le connessioni. I dispositivi stateful, come i firewall e gli IPS, sono invece vulnerabili agli attacchi DDoS e non fanno altro che accrescere il problema.
- Le soluzioni IDMS non dipendono dalle firme create dopo che l'attacco ha colpito gli obiettivi e supportano invece molteplici contromisure, offrendo una protezione immediata contro la maggior parte delle tipologie di attacco.
- Le soluzioni IDMS consentono diverse configurazioni, ma soprattutto permettono l'implementazione fuori banda, ove necessaria. Questa flessibilità espande la scalabilità della soluzione, un aspetto indispensabile a fronte di attacchi DDoS di dimensioni sempre maggiori.
- Per gestire realmente gli attacchi DDoS "distribuiti", è necessario affidarsi a una soluzione IDMS totalmente integrata che supporti un metodo di rilevazione distribuito. I dispositivi IPS che sfruttano tecniche di rilevazione basate su singoli segmenti non riescono a individuare molti attacchi di grandi dimensioni.

Automazione: l'automazione è ormai divenuta il Sacro Graal della sicurezza perché riduce il personale necessario e incide sensibilmente sulla velocità di risposta. Una buona soluzione IDMS riesce infatti a rilevare gli attacchi e avviare l'azione di mitigazione in modo automatico, spesso prima che gli operatori di sicurezza si accorgano dell'attacco. Le soluzioni IDMS possono essere arricchite con decine di contromisure integrate e automatizzate, ognuna mirata a una specifica tipologia di attacco.

In una configurazione di difesa DDoS ibrida, che abbina la mitigazione on-premise alla protezione basata su cloud, la soluzione IDMS può inviare un segnale per attivare le contromisure basate su cloud istantaneamente e automaticamente non appena il volume di attacco raggiunge una determinata soglia. Questa è una tecnica ottimale, soprattutto in considerazione delle dimensioni sempre più consistenti degli attacchi e della crescente stratificazione delle metodologie impiegate.

Risposta: il primo passo per una gestione efficace degli attacchi DDoS è certamente l'implementazione di valide soluzioni tecnologiche. Tuttavia, anche nelle organizzazioni che si avvalgono di molteplici meccanismi di difesa DDoS automatici, dalle contromisure preinstallate alla connessione con mitigazione basata su cloud, il fattore umano ha ancora un ruolo determinante nella risposta e nella difesa globale. I team di sicurezza devono essere preparati a riconoscere e contrastare le minacce senza alcuna esitazione. La preparazione è un fattore chiave per lo sviluppo dei "riflessi organizzativi" che permettono di accelerare la risposta agli incidenti anche nelle situazioni di maggiore pressione associate agli attacchi.

Tre domande chiave:

- Avete stilato un piano di risposta agli incidenti DDoS?
- Sapete come effettuare l'escalation del problema all'interno dell'organizzazione, informando i team addetti alla rete, alle applicazioni e ai servizi che potrebbero subire le conseguenze di un attacco?
- Avete implementato un piano di comunicazione per i problemi di tipo normativo o relativi alla conformità e per i clienti, gli investitori e i partner?

NETSCOUT Arbor vanta un'esperienza decennale nella mitigazione DDoS che dimostra che la pratica è essenziale per una rapida ed efficace gestione della risposta agli incidenti. Ignorare il fondamentale aspetto umano della difesa DDoS nuoce all'azienda quanto scegliere la soluzione sbagliata.