Akamai

WHITE PAPER

I 9 miti sulla difesa dagli attacchi DDoS

Negli ultimi due anni, il volume degli attacchi DDoS (Distributed Denial-of-Service) è raddoppiato, mentre il numero e la combinazione dei vettori di attacco sono aumentati in modo significativo. Nel 2020, un'organizzazione è stata colpita da un attacco di 809 milioni di pacchetti al secondo (Mpps), il più grande attacco di questo tipo mai registrato. Anche se alcune organizzazioni possono considerarsi obiettivi a basso rischio per un attacco DDoS, i servizi e le applicazioni business-critical in ogni settore sono obiettivi ambiti, esponendo tutte le aziende a problemi di downtime e riduzione delle performance se l'infrastruttura non è protetta.

La protezione dagli attacchi DDoS deve essere un principio fondamentale di una strategia di sicurezza complessiva, pertanto essere consapevoli dei miti da sfatare può risultare essenziale per adottare il miglior sistema di difesa dagli attacchi DDoS.

Esistono numerosi miti sulla protezione dagli attacchi DDoS, alcuni persino rafforzati dai fornitori di soluzioni per la sicurezza.

Mito 1. La capacità totale indica le risorse di mitigazione disponibili

Il semplice dato della capacità di rete tralascia dettagli importanti. Le domande a cui è necessario rispondere includono: Quanta capacità di rete viene consumata dal traffico nocivo? Quante risorse del sistema di mitigazione sono dedicate a fermare gli attacchi? Quante risorse di rete e del sistema sono disponibili per distribuire traffico pulito a tutte le origini dei clienti sulla piattaforma? Inoltre, la capacità non si limita solo alla tecnologia. Ad un certo punto, se le tecnologie non funzionano in modo efficace o non ottimizzano la mitigazione, quale capacità umana dedicata può essere sfruttata per segnalare un problema, gestire la risposta agli incidenti e ottimizzare la mitigazione?

Suggerimento. Analizzate in modo più approfondito le differenze tra la capacità di rete totale di un provider e la stabilità della piattaforma, la capacità disponibile per la mitigazione degli attacchi e l'utilizzo della delivery di traffico pulito.

Mito 2. Tutti gli SLA sulle tempistiche di mitigazione sono creati in maniera uguale

Le tempistiche di mitigazione indicano la velocità con cui il traffico dannoso viene arrestato o bloccato, senza influire sul traffico e sugli utenti legittimi. Tuttavia, come è emerso, ciò lascia molto spazio all'interpretazione. Ad esempio, un fornitore potrebbe non considerare un aumento del traffico come un attacco DDoS, se non dura almeno cinque minuti. Di conseguenza, le tempistiche dello SLA potrebbero partire solo dopo i primi cinque minuti di un attacco. Ciò significa che un tempo di mitigazione di 10 secondi, in realtà, potrebbe essere di cinque o più minuti. Altri fornitori definiscono le tempistiche di mitigazione come la velocità di implementazione di una regola di mitigazione. In definitiva, ciò che conta è il tempo richiesto per riportare le risorse online al loro normale funzionamento. Assicuratevi di leggere attentamente le clausole scritte in piccolo nello SLA del vostro fornitore.

Suggerimento. Esaminando i dettagli sulle tempistiche di mitigazione elencati in uno SLA, dovreste individuare la seguente equazione: tempo di rilevamento dell'attacco + tempo di applicazione dei controlli di mitigazione + tempo per il blocco dell'attacco + qualità della mitigazione = tempo per fermare l'attacco.

Mito 3. L'oscuramento e la limitazione della velocità sono sistemi di difesa accettabili

L'oscuramento è una risposta difensiva comune di alcuni fornitori di soluzioni per la mitigazione degli attacchi DDoS. Se una risorsa è sotto attacco e mette a rischio altri clienti, il fornitore può tentare di prevenire danni collaterali bloccando il traffico proveniente da tale risorsa in un "buco nero" virtuale. Questa strategia può realmente aiutare? Dal punto di vista dei criminali, l'oscuramento equivale ad una missione compiuta: la risorsa oggetto dell'attacco risulta effettivamente offline. A seconda dell'infrastruttura del provider, altri clienti potrebbero finire offline o riscontrare una riduzione delle performance. Un'altra risposta a questo problema prevede la limitazione del traffico dei clienti da parte di molti provider negli ambienti condivisi. Tuttavia, la riduzione del traffico legittimo del 20 - 40% per dare l'impressione che la risorsa o il servizio siano ancora attivi e funzionanti non è un risultato positivo per il cliente sotto attacco.

Suggerimento. Chiedete al vostro fornitore con quale frequenza effettua l'oscuramento o limita la velocità del traffico in "tempo di pace" o durante un attacco. Determinate in quali condizioni un provider bloccherà il traffico e quali criteri dovrete soddisfare per ripristinare i vostri servizi.

Mito 4. Non importa chi condivide la piattaforma cloud

Ogni organizzazione necessita di un sistema di sicurezza. Anche le attività più controverse che attirano attacchi frequenti, ad esempio i mercati grigi come i siti pornografici e di giochi d'azzardo, hanno bisogno di sistemi di difesa. Persino le organizzazioni che promuovono attività criminali e attacchi terroristici hanno acquistato soluzioni per la cybersicurezza da fornitori di cloud legittimi. È facile pensare che questo problema non vi riguardi. Tuttavia, se la vostra azienda condivide una piattaforma per la sicurezza nel cloud con un'impresa illegale o soggetta a frequenti attacchi, il potenziale di danni collaterali è elevato. Le risorse del fornitore potrebbero essere già vincolate o sovraccariche, lasciando esposta la vostra organizzazione.

Se la vostra azienda condivide una piattaforma per la sicurezza nel cloud con un'impresa illegale o soggetta a frequenti attacchi, il potenziale di danni collaterali è elevato.

Suggerimento. Leggete attentamente la policy di utilizzo di un fornitore di servizi di sicurezza nel cloud per verificare che non dovrete condividere le risorse della piattaforma per la sicurezza con obiettivi ad alto rischio.

Mito 5. Una piattaforma per la sicurezza all-in-one implica una migliore experience di sicurezza

Alcuni provider offrono una varietà di servizi integrati in un'unica piattaforma cloud, il che potrebbe significare una ridotta complessità tecnica per l'implementazione e l'integrazione di controlli di sicurezza nel breve termine. Tuttavia, nel caso di più servizi che condividono la stessa infrastruttura di back-end e le stesse reti, aumenta la vulnerabilità in termini di interruzioni della piattaforma, danni collaterali e problemi di resilienza se altre parti dell'ambiente subiscono interruzioni. Spesso, i fornitori unici sacrificano le loro funzionalità per le limitazioni della progettazione di un approccio basato su una singola piattaforma. Una mesh trasparente di cloud di scrubbing DDoS, CDN e DNS appositamente progettati, concepita per risolvere specifici problemi tecnici e di sicurezza, implica una maggiore qualità della mitigazione e delle performance su larga scala necessarie per ottimizzare i sistemi di difesa.

Suggerimento. Tenete presente che non è necessario condividere la stessa infrastruttura per un'experience di sicurezza unificata. Diverse architetture sottostanti possono offrire un'eccellente user experience insieme ad una mitigazione dalle elevate performance.

Mito 6. Una soluzione in sede offre un maggiore controllo

Anche se una soluzione in sede consente alle organizzazioni di tenere tutto sotto controllo, tale controllo può risultare illusorio. L'anello più debole di qualsiasi soluzione in sede è spesso la portata del collegamento a Internet. Con l'aumentare delle dimensioni e della complessità (multivettore) degli attacchi DDoS, anche un tipico attacco di meno di 4 Gbps può saturare il collegamento a Internet e causare un DoS (Denial of Service) anche per i data center che includono le migliori risorse hardware locali. Nelle implementazioni in sede, si tratta essenzialmente di guadagnare minuti per spostare la mitigazione degli attacchi gravi nel cloud. Poiché gli esperti nel campo della sicurezza non solo sono scarsi ma anche sotto pressione, le organizzazioni affidano la mitigazione degli attacchi DDoS in outsourcing a piattaforme basate su cloud anziché sviluppare competenze interne per la mitigazione degli attacchi DDoS.

Suggerimento. Non potete tenere tutto sotto controllo se il personale di rete, il team IT e gli addetti alla risposta agli incidenti sono sovraccarichi. Gli attacchi DDoS vengono gestiti meglio da esperti della mitigazione. Raddoppiate le vostre capacità interne e affidatevi agli esperti.

Mito 7. Non sono necessari più livelli di difesa

La maggior parte delle organizzazioni non ci crede davvero, ma, a volte, costruisce la propria strategia di difesa come se ciò fosse vero. Considerate, ad esempio, l'approccio ibrido. Un'organizzazione che cerca di rafforzare la propria soluzione per la sicurezza in sede può potenziarsi aggiungendo una soluzione basata su cloud dello stesso fornitore. Gli acquisti effettuati presso un unico fornitore possono risultare convenienti, ma non necessariamente forniscono una difesa più approfondita. Se più livelli di difesa si basano sulla stessa tecnologia sottostante, avranno le stesse falle e le medesime debolezze, lasciandovi altrettanto esposti.

Suggerimento. Distribuite le migliori tecnologie con punti di forza e di debolezza diversi su più livelli, in modo che le falle presenti in un livello verranno coperte dai sistemi di difesa di un altro livello.

Mito 8. Ogni SOC offre lo stesso livello di supporto

Molti fornitori pubblicizzano il supporto del SOC (centro operativo per la sicurezza) nelle proprie schede tecniche. Tuttavia, disporre di un SOC 24/7 non è la cosa più importante. Ciò che importa è il livello di servizio e di competenze che potete aspettarvi di ricevere quando le vostre risorse sono sotto attacco. Alcune considerazioni chiave per la valutazione dei fornitori di soluzioni di mitigazione degli attacchi DDoS dovrebbero includere: Che tipo di supporto e analisi potrei ricevere prima, durante e dopo un attacco? Da quale personale è costituito il SOC per garantire una continuità del sistema di difesa? Se si contatta il SOC, la persona che viene chiamata è l'analista che sta effettivamente eseguendo la mitigazione o solo il riferimento a cui si deve segnalare il problema? Il vostro provider dispone di professionisti della sicurezza che hanno ricevuto una formazione sulla mitigazione o sono solo "vigili urbani" che dirigono il traffico verso dispositivi di mitigazione commerciali pronti all'uso? Inoltre, offrono un runbook personalizzato? Il SOC del vostro provider di soluzioni per la sicurezza dovrebbe fungere da estensione del vostro team di risposta agli incidenti per fornire un valore reale.

Suggerimento. Valutate la qualità del supporto che prevedete di ricevere dal SOC del provider di servizi. Oltre al rilevamento e alla mitigazione degli attacchi, determinate se vengono offerti servizi di integrazione e test, risoluzione dei problemi relativi agli incidenti, analisi post-hoc (lezioni apprese) e supporto alla progettazione per ridurre la superficie di attacco.

Mito 9. La protezione dagli attacchi DDoS include tutto ciò che serve

Sebbene un prezzo più basso possa sembrare allettante, potrebbero esserci dei costi nascosti. Alcuni fornitori offrono un prezzo basso, ma il numero o la portata degli attacchi che mitigano sono limitati. Se siete presi di mira da un numero troppo elevato di attacchi o da un attacco di dimensioni troppo grandi, vi chiederanno di eseguire l'aggiornamento a un livello di servizio più alto (e più costoso) prima di arrestare l'attacco mentre state tentando di riportare online la vostra azienda. Quando confrontate fornitori e prezzi, assicuratevi di comprendere i compromessi e il loro impatto sul vostro approccio ai rischi.

Suggerimento. Cercare di comprendere bene cosa è incluso nel prezzo offerto prima di firmare.

Se siete presi di mira da un numero troppo elevato di attacchi o da un attacco di dimensioni troppo grandi, alcuni fornitori vi chiederanno di eseguire l'aggiornamento a un livello di servizio più alto (e più costoso) prima di arrestare l'attacco mentre state tentando di riportare online la vostra azienda.

La sicurezza DDoS è complessa, dispendiosa in termini di tempo e in costante evoluzione. Restare connessi con i clienti e i dipendenti è la base della vostra azienda. Non c'è spazio per errori e non è necessario provare da soli sostenendo costi elevati. In qualità di piattaforma di cloud delivery più grande e affidabile per la sicurezza web, Akamai può aiutarvi. Ulteriori informazioni sono disponibili all'indirizzo www.akamai.com/secureapps.

Akamai garantisce experience digitali sicure per le più grandi aziende a livello mondiale. L'Akamai Intelligent Edge Platform permea ogni ambito, dalle aziende al cloud, permettendovi di lavorare con rapidità, efficacia e sicurezza. I migliori brand a livello globale si affidano ad Akamai per ottenere un vantaggio competitivo grazie a soluzioni agili in grado di estendere la potenza delle loro architetture multicloud. Più di ogni altra azienda, Akamai avvicina agli utenti app, experience e processi decisionali, tenendo lontani attacchi e minacce. Il portfolio Akamai di soluzioni per l'edge security, le web e mobile performance, l'accesso aziendale e la delivery di contenuti video è affiancato da un servizio clienti di assoluta qualità e da un monitoraggio 24 ore su 24, 7 giorni su 7, 365 giorni all'anno. Per scoprire perché i principali brand mondiali si affidano ad Akamai, visitate www.akamai.com o blogs.akamai.com e seguite @Akamai su Twitter. Le informazioni di contatto internazionali sono disponibili all'indirizzo www.akamai.com/locations. Data di pubblicazione: 12/20.