Akamai

WHITE PAPER

11 miti sugli attacchi DDoS con cui continueremo ad avere a che fare

Gli attacchi DDoS (Distributed Denial-of-Service) sono notevolmente aumentati in termini di dimensioni, portata, distribuzione e complessità negli ultimi anni, come hanno evidenziato alcuni attacchi da record. Sfortunatamente, molte organizzazioni sono ancora legate ad un vecchio concetto dei meccanismi di difesa basato sulla convinzione che i propri sistemi di protezione siano adeguati, o peggio, che difficilmente possano subire un attacco. La realtà è che , invece, questi attacchi colpiscono tutti i principali settori, dai servizi finanziari all'e-commerce fino al settore del gaming. In realtà, gli attacchi contro le infrastrutture pubbliche critiche, tra cui quelle del settore sanitario, dei servizi di pubblica utilità e dell'energia, del settore dell'istruzione e di quello dei trasporti, si sono dimostrati particolarmente preoccupanti. Nel 2023, Akamai ha protetto un cliente nell'area Asia-Pacifico da un vasto attacco di 900 gigabit al secondo (Gbps) e, sempre nello stesso anno, Akamai ha impedito il verificarsi di un attacco da 634 Gbps e 55 milioni di pacchetti al secondo (Mpps), che ha presentato una complessa combinazione di vettori di attacco: uno dei più imponenti attacchi mai sferrati contro un cliente dei servizi finanziari negli Stati Uniti. Tutto ciò oltre al fatto che Akamai ha mitigato il più vasto attacco mai osservato fino ad oggi: un attacco da 1,44 Tbps e 385 Mpps distribuito a livello globale, che è durato quasi due ore. Questi eventi fanno chiaramente capire che i criminali informatici continueranno a prendere di mira i pilastri fondamentali dell'economia.

Anche se la portata di questi attacchi potrebbe condurre alcune organizzazioni più piccole a sottovalutare il rischio di diventare le prossime vittime di un attacco DDoS, in realtà i servizi e le applicazioni business-critical di tutti i settori sono bersagli facili da colpire. L'aumento del numero di hacktivisti che agiscono sulla base di motivazioni politiche e ideologiche e i costi relativamente bassi delle soluzioni DDoS-as-a-Service offerte da gruppi di criminali informatici, come Killnet e Anonymous Sudan, hanno reso praticamente chiunque un possibile bersaglio. E non è solo l'attacco iniziale che deve preoccupare le organizzazioni: gli attacchi DDoS vengono sempre più usati come copertura per distrarre gli addetti alla sicurezza e alle reti, mentre i criminali, nel contempo, tentano di sferrare attacchi RDDoS (ransomware DDoS) o altri tipi di exploit, come le campagne di attacchi a tripla estorsione. Infine, la sempre più diffusa e allarmante adozione degli strumenti di intelligenza artificiale per coordinare attacchi DDoS sofisticati e distribuiti crea una notevole sfida difensiva per le aziende e le pubbliche istituzioni che devono garantire un livello coerente di disponibilità e performance.

Man mano che le minacce diventano più complesse e si evolvono quasi ogni giorno, esistono ancora numerosi miti sulla protezione dagli attacchi DDoS, alcuni persino incoraggiati dai vendor di soluzioni per la sicurezza. La protezione dagli attacchi DDoS deve essere un principio fondamentale di qualsiasi strategia di sicurezza, pertanto comprendere il pericolo legato a questi miti può risultare essenziale per il proprio sistema di difesa dagli attacchi DDoS.

MITO 1

La capacità totale indica tutte le risorse di mitigazione disponibili

Anche se la capacità totale è importante, un semplice valore della capacità della rete può risultare fuorviante escludendo così alcuni dettagli fondamentali. Le organizzazioni che valutano le soluzioni tecnologiche per la protezione dagli attacchi DDoS devono chiedersi:

- Quanta capacità di rete viene consumata dal traffico degli attacchi?
- Quante risorse del sistema di mitigazione sono **dedicate esplicitamente** 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 e a ciascun tenant univoco?

Queste domande sono fondamentali perché, se la capacità di rete totale include altri requisiti, come la delivery di contenuti, l'effettiva capacità di difesa dagli attacchi DDoS potrebbe essere inferiore rispetto a quanto dichiarato dal provider.

Inoltre, la capacità di difesa dagli attacchi DDoS non si limita solo alla tecnologia. Ad un certo punto, se la tecnologia non funziona in modo efficace, ci saranno risorse umane dedicate per segnalare un problema, gestire la risposta agli incidenti e ottimizzare la mitigazione? La mitigazione più solida combina le funzionalità di automazione e intelligenza artificiale con le competenze umane per offrire una protezione approfondita.

Suggerimento

Analizzate in modo più approfondito le differenze esistenti tra la capacità di rete totale di un provider e la stabilità della sua piattaforma, nonché la capacità disponibile per la mitigazione degli attacchi e la delivery di traffico pulito. Questi aspetti vanno considerati in modo univoco. Ad esempio, la capacità deve essere dedicata ad uno scopo, come, ad esempio, l'instradamento del traffico degli attacchi effettuato dalla rete, il blocco o la mitigazione del traffico degli attacchi e il reinstradamento di traffico pulito al data center.

MITO 2

La protezione dagli attacchi DDoS fornita dagli ISP (Internet Service Provider) e/o dai provider di servizi cloud è adeguata

Sfortunatamente, molte organizzazioni ancora ritengono che la protezione offerta dai propri ISP sia tutto ciò che serve. La realtà è che gli ISP, di solito, forniscono una protezione dagli attacchi DDoS riadattata, commerciale e pronta all'uso con una larghezza di banda limitata. I loro dispositivi hardware vengono condivisi tra la loro infrastruttura e la vostra, il che si traduce in una capacità limitata e in cicli della CPU ridotti. Gli attacchi DDoS ora sono così imponenti da sopraffare le infrastrutture e gli ISP cercano di instradare il traffico verso un percorso nullo (o blackholing) per prevenire danni collaterali ad altre risorse di produzione. Effettuando il blackholing di tutto il traffico, le aziende perdono il traffico e i servizi legittimi da parte degli utenti finali, determinando la riuscita degli attacchi che interrompono così le attività online per tutti gli scopi pratici.

Inoltre, anche se i provider di servizi cloud (CSP) spesso consentono agli utenti di impostare propri controlli e mantenere l'autonomia sul proprio sistema di sicurezza all'interno degli ambienti cloud dei CSP, la maggior parte di essi, di solito, rifiutano qualsiasi responsabilità e finiscono per addebitare ai clienti il traffico DDoS illegittimo, il che può implicare notevoli costi di overage per le vittime, considerando la portata e le dimensioni dei moderni attacchi DDoS.

Suggerimento

Verificate attentamente e negoziate le clausole dei contratti relativi alla protezione dagli attacchi DDoS con il vostro ISP o CSP. Inoltre, stabilite se il vostro ISP utilizza un dispositivo hardware affidabile per la protezione dagli attacchi DDoS on-premise con funzioni di backup nel cloud, in modo che gli attacchi DDoS piccoli, ma rapidi vengano mitigati on-premise, mentre i grandi attacchi volumetrici vengano mitigati in modo appropriato da un servizio di protezione dagli attacchi DDoS nel cloud.

MITO 3

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

A volte, le cifre possono risultare fuorvianti. Il valore TTM (Time-to-Mitigate) è spesso commercializzato dai vendor di soluzioni per la sicurezza e, idealmente, indica la velocità con cui il traffico DDoS 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 consecutivi. Di conseguenza, le tempistiche dello SLA potrebbero partire solo quando siete già sotto attacco. Poiché la durata media di un attacco è inferiore ai cinque minuti, potete capire bene come la questione sia problematica: ciò significa che un tempo di mitigazione di 10 secondi, in realtà, potrebbe essere superiore ai cinque minuti.

Altri fornitori definiscono le tempistiche di mitigazione come la velocità di implementazione di una regola di mitigazione. Questo valore non si riflette nella capacità di fermare un attacco oppure nella qualità o nella coerenza con cui questo controllo viene attivato. In definitiva, ciò che conta è il tempo richiesto per riportare le risorse online ai loro normali livelli di protezione e funzionamento **con il minimo impatto sugli utenti o sui servizi legittimi**. 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 effettivo = tempo per rilevare l'attacco + tempo per applicare i controlli di mitigazione + tempo per bloccare/fermare l'attacco + qualità/coerenza della mitigazione. Selezionate un fornitore in grado di offrire uno **SLA immediato** per la mitigazione degli attacchi DDoS senza influire sugli utenti legittimi.

MITO 4

Il null routing/blackholing e la limitazione della velocità sono sistemi di difesa accettabili

Il null routing (o blackholing) è una risposta difensiva comune e piuttosto primitiva di alcuni fornitori di soluzioni per la mitigazione degli attacchi DDoS. Se una risorsa è sotto attacco e la capacità dell'attacco mette a rischio altri clienti o servizi, il fornitore può tentare di prevenire danni collaterali indirizzando 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 anche finire offline o riscontrare una riduzione delle performance.

Un'altra risposta a questo problema offerta da molti provider di soluzioni per la sicurezza prevede la limitazione del traffico dei clienti 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. La limitazione della velocità è efficace come seconda o terza contromisura di difesa dagli attacchi DDoS ai livelli 3, 4 e 5. Ad un confronto con gli attacchi DDoS al livello 7, la limitazione della velocità può risultare più efficace come controllo iniziale, ma è sempre consigliabile ricorrere prima alla mitigazione della firma dell'attacco. La vostra infrastruttura digitale deve essere totalmente protetta dagli attacchi DDoS in modo efficace, indipendentemente dal livello del modello di interconnessione dei sistemi che è interessato, certamente non solo il 60% o meno.

Suggerimento

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

MITO 5

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 di giochi d'azzardo e di contenuti per adulti, hanno bisogno di sistemi di difesa dagli attacchi DDoS. 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 questi siti non vi riguardino. Tuttavia, se la vostra azienda condivide una piattaforma cloud con un'impresa illegale o soggetta a frequenti attacchi, la possibilità di subire danni collaterali è elevata. Le risorse del fornitore potrebbero essere vincolate o sovraccariche, lasciando la vostra organizzazione vulnerabile agli attacchi.

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. Rivedete anche i suggerimenti riportati dopo il mito 1 e il mito 2 relativamente alla capacità e alle funzionalità.

MITO 6

Una soluzione WAF (Web Application Firewall) è sufficiente per la protezione dagli attacchi DDoS

Le soluzioni WAF (Web Application Firewall), che spesso fanno parte del gruppo più vasto delle soluzioni WAAP (Web Application and API Protection), offrono un'efficace protezione dagli attacchi DDoS a livello di applicazioni (livello 7). Anche se queste soluzioni possono offrire una protezione basilare a livello di rete (livello 3) o di trasporto (livello 4), non hanno la capacità di proteggere completamente tutti gli IP, le porte e i protocolli.

Gli attacchi DDoS vengono sferrati sotto vari formati e in varie modalità e possono colpire i livelli dell'infrastruttura (livelli 3 e 4), il livello di applicazioni HTTP(s) (livello 7) e l'infrastruttura del DNS. Inoltre, i criminali spesso cambiano tipo di attacco in modo dinamico, ad esempio, iniziano con un attacco al DNS e, successivamente, ne ampliano la portata ad altri livelli o protocolli. Una reale protezione dagli attacchi DDoS deriva da una strategia di difesa approfondita che adotta una piattaforma di solide soluzioni con specifiche caratteristiche e funzionalità in grado di offrire protezione ai livelli 3, 4 e 7, nonché al DNS. Una qualsiasi soluzione da sola non è sempre sufficiente per proteggere tutti i livelli e può lasciare la vostra organizzazione vulnerabile agli attacchi e a rischi maggiori per l'eccessiva mitigazione di traffico o servizi legittimi.

Suggerimento

Assicuratevi che la protezione dagli attacchi DDoS non sia focalizzata su un tipo particolare di attacchi DDoS o di progettazione di implementazione. La difesa migliore proviene da un fornitore in grado di offrire diverse funzionalità dedicate per la protezione dagli attacchi DDoS che mantengono l'interoperabilità e sono supportate da un team unificato di servizi di sicurezza immediatamente disponibili per proteggere le vostre risorse di produzione. La situazione diventa complessa se queste risorse vengono implementate in reti ibride e ambienti ospitati nel cloud. I servizi di protezione devono essere indipendenti dal modello di rete o distribuzione.

MITO 7

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

Alcuni provider offrono vari servizi disponibili su una piattaforma nel cloud. In tal modo, è possibile ridurre la complessità tecnica derivante dalla distribuzione e dall'integrazione dei 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, come in questo caso, sacrificano le loro funzionalità per le limitazioni di un approccio basato su una singola piattaforma.

Una mesh trasparente di soluzioni o piattaforme di protezione dagli attacchi DDoS, CDN e DNS appositamente progettate, 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. Un approccio basato su diversi sistemi di difesa utilizza le architetture sottostanti che possono offrire eccellenti user experience insieme ad una mitigazione della sicurezza dalle elevate performance.

MITO 8

La protezione dagli attacchi DDoS non è necessaria per l'IPv6

Secondo Google, il 45% circa del traffico Internet ha avuto origine da dispositivi compatibili con l'IPv6. In termini di attacchi DDoS, l'IPv6 introduce alcuni miglioramenti rispetto all'IPv4, come un maggiore spazio degli indirizzi e funzioni di sicurezza incorporate come l'IPsec, ma non protegge intrinsecamente da questi tipi di attacchi.

Gli attacchi DDoS possono prendere di mira le reti IPv4 e IPv6 sovraccaricandole con una grande quantità di traffico, sfruttando le vulnerabilità o utilizzando vari vettori di attacco che sono indipendenti della versione IP. I criminali informatici stanno già usando lo spazio IP dell'IPv6 notevolmente ampliato per sferrare attacchi DDoS volumetrici sempre più imponenti. In alcuni casi, i criminali hanno inviato volumi di traffico ad indirizzi casuali su una rete, creando una broadcast storm (tempesta di trasmissioni) sul livello fisico della rete ed esaurendo le risorse di rete o il router.

L'attuale frammentazione tra l'IPv4 e l'IPv6 aggiunge ulteriori complessità perché, di solito, gli ambienti IPv6 non vengono considerati puliti.

Suggerimento

La protezione dagli attacchi DDoS per l'IPv6 richiede strategie e tecnologie simili a quelle dell'IPv4, tra cui il monitoraggio della rete, il filtraggio del traffico, la limitazione della velocità e l'utilizzo di servizi di mitigazione degli attacchi DDoS specializzati.

MITO 9

Non sono necessari più livelli di difesa

La maggior parte delle organizzazioni non crede davvero a questo mito, ma, a volte, costruisce la propria strategia di difesa come se fosse vero. Se, per proteggere la vostra casa, chiudete a chiave la porta principale, non significa che potete lasciare aperte le finestre e la porta sul retro. Per ottenere una reale difesa dagli attacchi DDoS, è necessario costruire diversi livelli di sicurezza che, insieme, possono impedire ai criminali di raggiungere il loro obiettivo con un colpo solo.

Un'eccellente difesa dagli attacchi DDoS inizia con l'adozione di un firewall di rete cloud in grado di alleggerire il carico di lavoro che grava sui vostri firewall sull'edge della rete. Inoltre, un modello di protezione dagli attacchi DDoS di tipo ibrido deve includere un sistema basato su apparecchiature hardware on-premise in grado di proteggere dagli attacchi DDoS brevi, ma potenti e un sistema di protezione dedicato e basato sul cloud per difendere dagli attacchi DDoS volumetrici, complessi e di vasta portata. Anche la vostra infrastruttura DNS ha bisogno di essere protetta con una strategia multilivello simile che include l'utilizzo di un servizio proxy in grado di implementare in modo dinamico appropriate policy di sicurezza sull'edge della rete e aggiungere ulteriori livelli con una soluzione di DNS autoritativo in modalità primaria o secondaria. Infine, dovete proteggere tutte le vostre applicazioni e API con una solida soluzione WAAP con funzionalità WAF.

Suggerimento

Distribuite le migliori tecnologie e soluzioni con punti di forza diversi e dedicati su più livelli per realizzare una strategia di difesa approfondita completa in grado di rendere estremamente difficoltoso per i criminali riuscire a sferrare un attacco.

MITO 10

Ogni SOC (centro operativo per la sicurezza) offre lo stesso livello di supporto

Molti fornitori pubblicizzano il supporto del proprio SOC. 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 la persona di 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 i "vigili urbani" che dirigono il traffico verso dispositivi di mitigazione 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 11

Gli attacchi DDoS sono basati su una vecchia tecnologia, quindi è sufficiente anche la protezione più economica

La massima "Tutto ha un prezzo" è probabilmente la più calzante per la protezione dagli attacchi DDoS. Sebbene un prezzo più basso possa sembrare allettante, spesso ci sono 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. I vendor di soluzioni per la sicurezza DDoS più affidabili offrono ai clienti la flessibilità di scegliere tra una protezione dagli attacchi DDoS "always-on" e una protezione "on-demand", nonché di passare facilmente da un tipo di protezione all'altro, per mantenere bassi i costi operativi, mantenendo, al contempo, il massimo livello di protezione. Quando confrontate fornitori e prezzi, assicuratevi di comprendere i compromessi e il loro impatto sul vostro sistema di sicurezza DDoS.

Suggerimento

Cercate di comprendere bene cosa è incluso nel prezzo offerto prima di firmare un contratto.

La sicurezza DDoS è complessa e richiede una notevole quantità di tempo e risorse nell'odierno panorama in rapida evoluzione. Le soluzioni che hanno funzionato ieri potrebbero non essere adatte oggi o domani. Restare connessi con utenti finali, clienti e dipendenti è la base del successo della vostra azienda. Non c'è spazio per errori e non è necessario provare da soli sostenendo costi elevati. Akamai può aiutarvi con la piattaforma di protezione dagli attacchi DDoS più completa, flessibile e affidabile.

Scoprite ulteriori informazioni sulle soluzioni per la sicurezza DDoS di Akamai.

Informazioni su Akamai Security

Akamai Security protegge le applicazioni che danno impulso alle vostre attività aziendali e rafforzano le interazioni, senza compromettere le performance o le customer experience. Tramite la scalabilità della nostra piattaforma globale e la visibilità delle minacce, possiamo unire le nostre forze per prevenire, rilevare e mitigare le minacce affinché voi possiate rafforzare la fiducia nel brand e realizzare la vostra visione. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com e akamai.com/blog o seguite Akamai Technologies su X (in precedenza Twitter) e LinkedIn. Data di pubblicazione: 10/24.