DELL Technologies

DDoS: rafforzamento della sicurezza informatica e della resilienza con Dell Technologies

La crescente minaccia degli attacchi DDoS

Gli attacchi DDoS (Distributed Denial of Service) sono una delle minacce più pervasive e dirompenti nell'era digitale. Sfruttando vaste reti di dispositivi compromessi, gli attacchi DDoS inondano i sistemi, i server o le reti presi di mira con un esorbitante volume di traffico. Questa implacabile impennata rallenta le operazioni o le arresta del tutto, spesso paralizzando un'azienda durante l'azione.

Dalle startup alle multinazionali, nessuna organizzazione è immune dal crescente spettro degli attacchi DDoS. Poiché le aziende crescono affidandosi sempre più all'infrastruttura digitale, questi attacchi hanno conseguenze devastanti, che vanno dalle perdite finanziarie ai danni alla reputazione. Dell Technologies riconosce la criticità di questa sfida e offre soluzioni scalabili e innovative che aiutano le aziende a rafforzare le difese e a superare la tempesta.

Che cosa sono gli attacchi DDoS?

Un attacco DDoS cerca di interrompere il normale funzionamento di una rete, di un servizio o di un server sovraccaricandolo di un enorme volume di traffico da più origini. Questi attacchi vengono eseguiti sfruttando le botnet, ovvero reti di dispositivi infetti controllati da remoto dai malintenzionati.

Come funzionano gli attacchi DDoS

1. **Reclutamento di botnet:** i criminali informatici infettano migliaia o milioni di dispositivi con malware, formando una botnet che può essere mobilitata per un attacco che blocca l'operatività della tua azienda.
2. **Inondazione di traffico:** gli autori degli attacchi istruiscono le botnet per inviare un'ondata di richieste al server preso di mira, causando il rallentamento, l'arresto anomalo o la non disponibilità del sistema agli utenti legittimi.
3. **Sovraccarico del sistema:** il sistema, sopraffatto dal traffico illegittimo, diventa incapace di soddisfare le richieste legittime, con conseguenti interruzioni o gravi ritardi del servizio.

Tecniche comuni

- **Gli attacchi basati sul volume** sfruttano l'elevato volume di traffico per esaurire la larghezza di banda di una rete.
- **Gli attacchi ai protocolli** sfruttano le vulnerabilità di protocolli come TCP/IP per esaurire le risorse.
- **Gli attacchi a livello di applicazione** puntano ad applicazioni specifiche, ad esempio un sito web o un database, per interromperne la funzionalità.

Questi attacchi sono in costante evoluzione e rappresentano pertanto una grande sfida per le aziende che tentano di proteggere le operazioni.

L'impatto sulle aziende

Conseguenze finanziarie

Un singolo attacco DDoS può costare milioni di dollari in termini di perdita di entrate, downtime e spese di ripristino. Anche pochi minuti di non disponibilità dei servizi possono avere un impatto notevole sulle aziende che dipendono da transazioni in tempo reale, ad esempio le piattaforme di e-commerce e i servizi finanziari.

Interruzione operativa

Le interruzioni causate da un attacco DDoS riducono la produttività, ritardano i processi critici e ostacolano l'accesso a servizi essenziali. Per settori come quello sanitario o manifatturiero, il downtime operativo può comportare conseguenze di vasta portata.

Danno alla reputazione

Quando i clienti o i client subiscono interruzioni del servizio, la fiducia si indebolisce. Incidenti prolungati o ripetuti possono causare danni di lungo termine alla reputazione di un'organizzazione, con conseguente defezione dei clienti e riduzione della fiducia del mercato.

Esempio del mondo reale

Un caso di rilievo si è verificato nel 2020, quando un istituto finanziario di grandi dimensioni è stato vittima di un attacco DDoS prolungato che ha arrestato i suoi servizi di online banking per diverse ore. Le perdite dirette di entrate, unitamente a una reputazione compromessa, hanno causato danni superiori a **$ 50 milioni.**

Statistiche allarmanti

Il report DDoS Insights di Zayo Group (febbraio 2024) indica che nel 2023 le organizzazioni non protette hanno perso in media **$ 6.000** al minuto, con un costo medio di circa **$ 408.000** per incidente. Inoltre, la frequenza di tali attacchi è in aumento, con oltre **10 milioni di attacchi segnalati ogni anno**. Queste statistiche evidenziano l'urgente necessità di solidi meccanismi di prevenzione.

20,5 milioni

di attacchi DDoS sono stati bloccati nel Q1 2025

Fonte: report sulle minacce DDoS di CloudFlare, 2024

Contrasto agli attacchi DDoS con Dell Technologies

Dell Technologies fornisce un'avanzata suite di soluzioni per aiutare le aziende a prevenire e rilevare gli attacchi DDoS ed effettuare l'eventuale ripristino dopo un incidente.

Endpoint rafforzati con Dell Trusted Device

Gli endpoint sono punti di ingresso cruciali per le minacce di tipo DDoS. I Dell Trusted Device offrono solide funzioni di sicurezza integrate nell'hardware, come Secure BIOS e SafeID, che proteggono dall'accesso non autorizzato e preservano l'integrità del sistema.

Sicurezza dei server

Le soluzioni server Dell sono dotate di misure di sicurezza integrate come la tecnologia Dell Trusted Server, tra cui:

- **Root of Trust hardware:** questa funzione assicura la verifica dei componenti hardware del server al momento dell'avvio, fornendo pertanto un livello fondamentale di sicurezza contro manomissioni o modifiche non autorizzate.
- **Funzioni di sicurezza integrate:** i server Dell sono dotati di unità SED (Self-Encrypting Drive) e verifica completa all'avvio, che proteggono dall'accesso non autorizzato e infondono fiducia circa l'integrità dei dati.
- **Cyber-resilienza:** l'approccio include funzionalità per il rilevamento di anomalie, violazioni e operazioni non autorizzate, consentendo le organizzazioni di eseguire rapidamente il ripristino a seguito di incidenti informatici.
- **Protezione dei dati completa:** le soluzioni Dell Trusted Server sono dotate di meccanismi di sicurezza integrati che proteggono i dati inattivi e in transito. Tali meccanismi includono tecniche di crittografia avanzata e opzioni di ripristino automatizzate per garantire la continuità aziendale.

Queste funzionalità assicurano ai server la capacità di resistere ai picchi traffico e al contempo mantenere la stabilità operativa. Le soluzioni di storage proteggono la disponibilità e l'integrità dei dati critici durante un attacco, riducendo al minimo le interruzioni.

Sicurezza dello storage

Dell Storage contribuisce alla protezione dagli attacchi DDoS attraverso varie misure di sicurezza integrate e tecnologie avanzate progettate per ridurre al minimo le vulnerabilità, rilevare tempestivamente le minacce e garantire un ripristino rapido in caso di attacco. I metodi principali includono:

- **Rilevamento proattivo delle minacce:** le soluzioni Dell Storage utilizzano il monitoraggio intelligente e il rilevamento delle anomalie basato sull'AI per identificare modelli di accesso insoliti che potrebbero indicare un attacco DDoS. Questi strumenti forniscono informazioni in tempo reale sulla sicurezza con la possibilità di attivare risposte automatizzate alle minacce per mitigare l'impatto di un attacco.
- **Architettura Root of Trust:** integrata nei controller di storage, questa architettura garantisce l'autenticità del firmware e impedisce le modifiche non autorizzate, migliorando pertanto la sicurezza dell'hardware di storage e riducendo le possibilità di compromissione durante un attacco DDoS.
- **Autenticazione a più fattori (MFA) e controlli degli accessi:** l'implementazione dei meccanismi MFA e RBAC (Role-Based Access Control) impedisce l'accesso non autorizzato ai sistemi di storage, fornendo un'ulteriore protezione contro le minacce associate agli attacchi DDoS.
- **Micro-segmentazione e isolamento della rete:** isolando i sistemi di storage e limitando l'accesso tra carichi di lavoro, Dell riduce al minimo i potenziali vettori di attacco e protegge i sistemi di storage dal movimento laterale in caso di violazione.
- **Snapshot protette e registri non modificabili:** le soluzioni di storage Dell forniscono snapshot protette e registri non modificabili che garantiscono l'integrità dei dati e consentono alle organizzazioni di eseguire rapidamente il ripristino in caso di attacchi DDoS. Queste funzionalità facilitano l'analisi forense e le indagini sugli incidenti, affinché i team IT abbiano la possibilità di rilevare e analizzare i vettori di attacco.
- **Vault di Cyber Recovery:** soluzioni come Dell PowerMax e PowerProtect Cyber Recovery Vault creano backup con air-gap non modificabili e protetti da ransomware e altri attacchi. Questi backup possono essere ripristinati per garantire la continuità aziendale senza il rischio di reinfezione.

Grazie all'integrazione di queste funzioni e tecnologie di sicurezza complete, Dell Storage e la cyber-resilienza aiutano le organizzazioni a difendersi efficacemente dagli attacchi DDoS e a mantenere resilienti e sicuri gli ambienti IT.

Monitoraggio proattivo con CrowdStrike

Il monitoraggio in tempo reale e l'analisi avanzata sono fondamentali per rilevare modelli di traffico anomali prima di un'escalation. CrowdStrike si integra con l'ecosistema Dell per utilizzare l'analisi comportamentale e informazioni basate sull'AI al fine di distinguere l'attività legittima dal traffico degli attacchi, in modo da rendere possibile una correzione rapida.

Dell PowerProtect per l'integrità dei dati

Dell PowerProtect assicura la protezione e l'accessibilità dei dati critici in caso di un attacco DDoS. Le funzionalità di backup non modificabile e gli ambienti di ripristino isolati consentono alle aziende di ripristinare i sistemi e ridurre al minimo il downtime dopo un incidente.

Sicurezza di rete avanzata e microsegmentazione con Dell PowerSwitch Networking e SmartFabric OS

Rafforza le difese dagli attacchi zero-day offrendo segmentazione avanzata della rete, rigorosi controlli degli accessi e analisi del traffico in tempo reale nell'intera infrastruttura.

Implementazione nel mondo reale

Una piattaforma di e-commerce globale ha recentemente sfruttato le soluzioni Dell PowerProtect unitamente a funzionalità di rilevamento proattivo per contrastare un sofisticato attacco DDoS. Grazie all'isolamento dei sistemi critici e all'implementazione di processi di ripristino di emergenza, l'azienda ha ripreso le operazioni complete in tempi record, riducendo le perdite finanziarie e preservando la fiducia dei clienti.

Approccio alla sicurezza multilivello

Il successo contro gli attacchi DDoS deriva dalla presenza di difese adattive e a più livelli. Dell sostiene le seguenti strategie a integrazione delle sue offerte tecnologiche:

Passaggi chiave per rafforzare la difesa

- **Architettura Zero Trust:** implementa un modello "mai fidarsi, verificare sempre" per esaminare ogni utente e ogni dispositivo.
- **Crittografia avanzata:** crittografa le comunicazioni a tutti i livelli per proteggere i dati sensibili trasmessi durante i potenziali tentativi di attacco.
- **Formazione dei dipendenti:** istruisci i dipendenti sull'identificazione delle attività sospette e sul rispetto di protocolli sicuri per prevenire violazioni involontarie.
- **Test regolari del sistema:** conduci valutazioni di routine, tra cui test di penetrazione e test di carico, per valutare la preparazione del sistema in caso di elevati volumi di traffico.

Queste azioni, in abbinamento alle soluzioni Dell Technologies, creano un solido meccanismo di difesa contro le minacce sofisticate.

Partnership che rafforzano la sicurezza informatica

Per estendere le proprie funzionalità, Dell Technologies collabora con leader del settore come **Microsoft**, **CrowdStrike** e **Secureworks**. Queste partnership forniscono ulteriori livelli di protezione, integrando le migliori metodologie di Threat Intelligence e rilevamento avanzato nel completo framework Dell.

Utilizzo dei Dell Professional Services

Oltre alla tecnologia, i Dell Professional Services offrono indicazioni di esperti alle aziende alle prese con le sfide degli attacchi DDoS. Dalla risposta agli incidenti alle consulenze per un'architettura di sicurezza personalizzata, il team Dell assicura alle organizzazioni la possibilità di effettuare un rapido ripristino e di rafforzare le difese per il futuro.

Crea un futuro resiliente

Dell Technologies è molto più di un fornitore di tecnologia: è un partner impegnato a proteggere la tua azienda dalla minaccia in continua evoluzione degli attacchi DDoS. Combinando tecnologia all'avanguardia, partnership consolidate e informazioni pratiche, Dell aiuta le aziende a proteggere le operazioni, mantenere la fiducia dei clienti e perseguire attivamente la crescita.

Fai il primo passo verso la resilienza oggi stesso. Contatta Dell Technologies per rafforzare la tua azienda contro le minacce DDoS e proteggere il tuo futuro.

Dell Technologies consente alle aziende di superare le sfide della sicurezza informatica degli attacchi DDoS, dimostrando che una base sicura è la chiave del successo in un mondo interconnesso.

Scopri come affrontare alcune delle principali sfide della sicurezza informatica di oggi alla pagina **Dell.com/SecuritySolutions**

Ulteriori informazioni su Soluzioni Dell

Contatta un esperto Dell Technologies

Visualizza più risorse

Partecipa alla conversazione con #HashTag