DELL Technologies

DDoS: Stärk cybersäkerheten och motståndskraften med Dell Technologies

Ökande hot om DDoS-attacker

DDoS-attacker (Distributed Denial of Service) har blivit ett av de mest avgörande och störande hoten i den digitala eran. DDoS-attacker utnyttjar enorma nätverk av komprometterade enheter och översvämmar system, servrar eller nätverk med en överväldigande trafikvolym. Denna obevekliga ökning saktar ner driften eller gör att den stannar upp, och förlamar ofta företag helt.

Från nystartade företag till multinationella företag – ingen organisation är immun mot det ökande hotet från DDoS-attacker. I takt med att företag blir alltmer beroende av digital infrastruktur får dessa attacker förödande konsekvenser, allt från ekonomiska förluster till skadat anseende. Dell Technologies inser vikten av denna utmaning och levererar skalbara, innovativa lösningar som hjälper företag att stärka sitt försvar och klara stormen.

Vad är DDoS-attacker?

En DDoS-attack syftar till att störa den normala funktionen hos ett nätverk, en tjänst eller en server genom att överbelasta den med en enorm trafikvolym från flera källor. Dessa attacker utförs genom att utnyttja botnät, som är nätverk av infekterade enheter som styrs av angripare på distans.

Så här fungerar DDoS-attacker

1. **Botnätrekrytering:** Cyberbrottslingar infekterar tusentals eller miljontals enheter med skadliga program och bildar ett botnät som kan mobiliseras för en attack som gör ditt företag obrukbart.
2. **Trafiköverbelastning:** Angripare styr botnäten att skicka en otrolig mängd förfrågningar till målservern, vilket gör att systemet blir långsammare, kraschar eller blir otillgängligt för legitima användare.
3. **Systemöverbelastning:** Systemet överväldigas av falsk trafik och kan inte uppfylla legitima förfrågningar, vilket resulterar i serviceavbrott eller allvarliga förseningar.

Vanliga tekniker

- **Volymbaserade attacker** utnyttjar ren trafikvolym för att uttömma nätverkets bandbredd.
- **Protokollattacker** utnyttjar sårbarheter i protokoll som TCP/IP för att förbruka resurser.
- **Applikationslagerattacker** riktar sig mot specifika program, t.ex. en webbplats eller databas, för att störa funktionen.

Dessa attacker utvecklas hela tiden, vilket gör dem till en enorm utmaning för företag som försöker skydda verksamheten.

© 2025 Dell Inc. eller dess dotterbolag.

Påverkan på företag

Ekonomiska konsekvenser

En enda DDoS-attack kan kosta miljontals dollar i förlorade intäkter, driftavbrott och återställningskostnader. Bara några minuter av otillgänglighet kan påverka företag som är beroende av realtidstransaktioner, t.ex. e-handelsplattformar och finansiella tjänster.

Driftstörningar

Avbrott som orsakas av en DDoS-attack minskar produktiviteten, försenar kritiska processer och hindrar åtkomst till viktiga tjänster. För branscher som hälso- och sjukvård eller tillverkning kan driftavbrott leda till långtgående konsekvenser.

Skadat anseende

När kunder eller klienter upplever störningar i tjänsten försämras förtroendet. Långvariga eller upprepade incidenter kan leda till långsiktiga skador på organisationens anseende, vilket leder till färre kunder och att försämrat marknadsförtroende.

Verkliga exempel

En uppmärksammad incident inträffade 2020, när ett stort finansinstitut föll offer för en ihållande DDoS-attack som stängde ner deras internetbanktjänster i flera timmar. De direkta intäktsförlusterna, kombinerat med ett skadat anseende, resulterade i skador på över **50 miljoner USD.**

Skrämmande statistik

Zayo Groups rapport med DDoS-insikter (feb 2024) visar att icke-skyddade organisationer i genomsnitt förlorade **6 000 USD** per minut, vilket ledde till en genomsnittlig kostnad på cirka **408 000 USD** per incident under 2023. Frekvensen för sådana attacker eskalerar dessutom, med över **10 miljoner rapporterade attacker årligen**. Denna statistik visar på det brådskande behovet av robusta förebyggande mekanismer.

20,5 miljoner

DDoS-attacker blockerades under första kvartalet 2025

Källa: 2024: Cloudflare DDoS Threat Report

Bekämpa DDoS-attacker med Dell Technologies

Dell Technologies tillhandahåller en avancerad svit med lösningar som hjälper företag att förebygga, upptäcka och återställa efter DDoS-incidenter.

Förstärkta slutpunkter med Dell Trusted Devices

Slutpunkter är viktiga ingångspunkter för DDoS-relaterade hot. Dell Trusted Devices erbjuder robusta säkerhetsfunktioner inbyggda i hårdvaran, t.ex. Secure BIOS och SafeID, som skyddar mot obehörig åtkomst och upprätthåller systemets integritet.

Serversäkerhet

Dells serverlösningar, utrustade med inbäddade säkerhetsåtgärder som Dell Trusted Server-teknik, som omfattar:

- **Hårdvarubaserad förtroenderot:** Den här funktionen säkerställer att hårdvarukomponenterna i servern verifieras vid start, vilket ger ett grundläggande säkerhetslager mot manipulering eller obehöriga ändringar.
- **Inbyggda säkerhetsfunktioner:** Dell-servrar levereras med självkrypterande enheter och heltäckande startverifiering som skyddar mot obehörig åtkomst och skapar förtroende för dataintegritet.
- **Cyberelasticitet:** Metoden inkluderar funktioner för att upptäcka avvikelser, intrång och obehöriga åtgärder, vilket gör det möjligt för organisationer att snabbt återhämta sig från cyberincidenter.
- **Omfattande dataskydd:** Dells Trusted Server-lösningar har integrerade säkerhetsmekanismer som skyddar data i vila och under flytt. Detta inkluderar avancerade krypteringstekniker och automatiserade återställningsalternativ för att säkerställa verksamhetens kontinuitet.

© 2025 Dell Inc. eller dess dotterbolag.

Dessa funktioner säkerställer att servrarna klarar av trafikstörningar samtidigt som driftstabiliteten bibehålls. Lagringslösningar skyddar kritisk datatillgänglighet och -integritet under en attack, vilket minimerar störningar.

Lagringssäkerhet

Dell Storage hjälper till att skydda mot DDoS-attacker genom olika integrerade säkerhetsåtgärder och avancerad teknik som utformats för att minimera sårbarheter, upptäcka hot tidigt och säkerställa snabb återställning om en attack inträffar. Viktiga metoder:

- **Proaktiv hotdetektering:** Dells lagringslösningar använder intelligent övervakning och AI-driven avvikelsedetektering för att identifiera ovanliga åtkomstmönster som kan tyda på en DDoS-attack. Dessa verktyg ger säkerhetsinsikter i realtid och kan utlösa automatiserad hotrespons för att mildra effekterna av en attack
- **Arkitektur med förtroenderot:** Den här arkitekturen är integrerad i lagringsstyrenheter och säkerställer autenticiteten för fast mjukvara och förhindrar obehöriga ändringar, vilket förbättrar säkerheten hos lagringshårdvaran och minskar risken för komprommettering under en DDoS-attack
- **Multifaktorautentisering (MFA) och åtkomstkontroller:** Implementering av MFA och rollbaserad åtkomstkontroll (RBAC) hjälper till att förhindra obehörig åtkomst till lagringssystem, vilket ytterligare skyddar mot hot i samband med DDoS-attacker
- **Mikrosegmentering och nätverksisolering:** Genom att isolera lagringssystem och begränsa åtkomsten mellan arbetsbelastningar minimerar Dell potentiella attackvektorer och skyddar lagringssystem från lateral förflyttning i händelse av intrång
- **Säkra snapshots och oföränderliga loggar:** Dells lagringslösningar tillhandahåller säkra snapshots och oföränderliga loggar som säkerställer dataintegritet och hjälper organisationer att snabbt återhämta sig från DDoS-attacker. Dessa funktioner underlättar forensisk analys och incidentutredning, vilket gör det möjligt för IT-team att upptäcka och analysera attackvektorer
- **Cyber Recovery Vault:** Lösningar som Dell PowerMax och PowerProtect Cyber Recovery Vault skapar säkerhetskopior med luftgap som är oföränderliga och skyddade mot utpressningsvirus och andra attacker. Dessa säkerhetskopior kan återställas för att säkerställa verksamhetens kontinuitet utan risk för återinfektion

Genom att integrera dessa omfattande säkerhetsfunktioner och -tekniker hjälper Dell Storage and Cyber Resilience effektivt organisationer att försvara sig mot DDoS-attacker och upprätthålla tåliga och säkra IT-miljöer.

Proaktiv övervakning med CrowdStrike

Övervakning i realtid och avancerad analys är avgörande för att upptäcka onormala trafikmönster före eskalering. CrowdStrike integreras med Dells ekosystem och använder beteendeanalys och AI-drivna insikter för att skilja mellan legitim aktivitet och attacktrafik, vilket möjliggör snabba åtgärder.

Dell PowerProtect för dataintegritet

Dell PowerProtect säkerställer att kritiska data förblir säkra och tillgängliga under en DDoS-attack. Funktioner för oföränderlig säkerhetskopiering och isolerade återställningsmiljöer gör det möjligt för företag att återställa system och minimera driftavbrott efter en incident.

Avancerad nätverkssäkerhet och mikrosegmentering med Dell PowerSwitch Networking och SmartFabric OS

Stärker försvaret mot nolldagsattacker genom att leverera avancerad nätverkssegmentering, strikta åtkomstkontroller och trafikanalys i realtid i hela infrastrukturen.

Verklig implementering

En global e-handelsplattform drog nyligen nytta av Dells PowerProtect-lösningar tillsammans med proaktiva detekteringsfunktioner för att avvärja en sofistikerad DDoS-attack. Genom att isolera kritiska system och driftsätta processer för nödåterställning återupptog företaget driften på rekordtid, vilket minskade de ekonomiska förlusterna och bevarade kundernas förtroende.

Säkerhetsmetod i flera lager

Framgång mot DDoS-attacker beror på skiktade och adaptiva försvar. Dell förespråkar följande strategier för att komplettera sina tekniska erbjudanden:

© 2025 Dell Inc. eller dess dotterbolag.

Viktiga steg för att förbättra försvaret

- **Nollförtroendearkitektur** Implementera en ”lita aldrig på något, verifiera alltid”-modell för att granska varje användare och enhet
- **Avancerad kryptering** Kryptera kommunikation över alla lager för att skydda känsliga data som överförs under potentiella attackförsök.
- **Utbildning för medarbetare** Utbilda medarbetarna i att identifiera misstänkt aktivitet och följa säkra protokoll för att förhindra oaktsamma intrång.
- **Regelbundna systemtester** Utför rutinbedömningar, inklusive intrångstest och belastningstest, för att utvärdera systemets beredskap för höga trafikvolymer.

Dessa åtgärder, i kombination med Dell Technologies-lösningar, skapar en robust försvarsmekanism mot sofistikerade hot.

Partnerskap som stärker cybersäkerheten

För att utöka sin kapacitet samarbetar Dell Technologies med branschledare som t.ex. **Microsoft**, **CrowdStrike** och **Secureworks**. Dessa partnerskap ger ytterligare skyddslager och införlivar den bästa hotinformationen och avancerade detekteringsmetoder i Dells omfattande ramverk.

Dra nytta av Dell Professional Services

Utöver tekniken erbjuder Dell Professional Services expertrådgivning till företag som står inför DDoS-utmaningar. Dells team säkerställer att organisationer snabbt kan återställas och förstärka framtida försvar, från incidentrespons till skräddarsydda konsultationer om säkerhetsarkitektur.

Bygg en motståndskraftig framtid

Dell Technologies är mer än en teknikleverantör – det är en partner som strävar efter att skydda ditt företag mot det växande hotet från DDoS-attacker. Genom att kombinera banbrytande teknik, djupgående partnerskap och användbara insikter hjälper Dell företag att skydda verksamheten, upprätthålla kundernas förtroende och aktivt driva tillväxt.

Ta det första steget mot motståndskraft idag. Kontakta Dell Technologies för att stärka ditt företag mot DDoS-hot och säkra din framtid.

Dell Technologies gör det möjligt för företag att övervinna utmaningarna med DDoS-cybersäkerhet, och bevisar att en säker grund är nyckeln till framgång i en sammankopplad värld.

Lär dig att hantera några av dagens främsta cybersäkerhetsutmaningar på **Dell.com/SecuritySolutions**

Läs mer om Dells lösningar

Kontakta en av Dell Technologies experter

Visa fler resurser

Delta i samtalet med #HashTag

© 2025 Dell Inc. eller dess dotterbolag. Med ensamrätt. Dell och andra varumärken är varumärken som tillhör Dell Inc. eller dess dotterbolag. Andra varumärken kan vara varumärken som tillhör sina respektive ägare.

DELL Technologies