DELL Technologies

DDoS: Wzmacnianie cyberbezpieczeństwa i odporności dzięki Dell Technologies

Rosnące zagrożenie atakami DDoS

Ataki DDoS (Distributed Denial of Service) stały się jednym z najbardziej rozpowszechnionych i destrukcyjnych zagrożeń w erze cyfrowej. Wykorzystując rozległe sieci zagrożonych urządzeń, ataki DDoS zalewają docelowe systemy, serwery lub sieci przytłaczającą ilością ruchu. Ten bezwzględny zalew spowalnia operacje lub zatrzymuje je w trakcie procesu, co często zakłóca działalność firmy.

Od start-upów po międzynarodowe korporacje — żadna organizacja nie jest odporna na rosnące widmo ataków DDoS. Wraz z rosnącą zależnością firm od infrastruktury cyfrowej ataki te mają katastrofalne skutki, od strat finansowych po utratę reputacji. Firma Dell Technologies zdaje sobie sprawę z wagi tego wyzwania i oferuje skalowalne, innowacyjne rozwiązania, które pomagają firmom wzmocnić ochronę i przetrwać burzę.

Czym są ataki DDoS?

Atak DDoS ma na celu zakłócenie normalnego funkcjonowania sieci, usługi lub serwera poprzez przytłaczanie go ogromną ilością ruchu z wielu źródeł. Ataki te są wykonywane poprzez wykorzystanie botnetów, czyli sieci zainfekowanych urządzeń, które są zdalnie kontrolowane przez atakujących.

Jak działają ataki DDoS

1. **Rekrutacja botnetów:** Cyberprzestępcy infekują tysiące lub miliony urządzeń złośliwym oprogramowaniem, tworząc botnet, który może zostać zmobilizowany do ataku, który uniemożliwi działanie Twojej firmy.
2. **Zalewanie ruchu:** Atakujący kierują botnety do wysyłania zalewu żądań do serwera docelowego, powodując spowolnienie, awarię lub niedostępność systemu dla uprawnionych użytkowników.
3. **Przeciążenie systemu:** System, przeciążony nielegalnym ruchem, staje się niezdolny do realizacji normalnych żądań, co skutkuje awariami usług lub poważnymi opóźnieniami.

Typowe techniki

- **Ataki wolumetryczne** wykorzystują ogromną ilość ruchu, aby wyczerpać przepustowość sieci.
- **Ataki na protokół** wykorzystują luki w zabezpieczeniach protokołów, takich jak TCP/IP, aby wykorzystać zasoby.
- **Ataki na warstwy aplikacji** są ukierunkowane na określone aplikacje, takie jak witryna internetowa lub baza danych, a na celu mają zakłócenie działania.

Ataki te nieustannie ewoluują, co czyni je wielkim wyzwaniem dla firm próbujących zabezpieczyć działalność.

Konsekwencje dla firm

Skutki finansowe

Pojedynczy atak DDoS może kosztować miliony dolarów utraconych przychodów, przestojów i wydatków na odzyskiwanie danych. Nawet minuty niedostępności usług mogą znacznie wpłynąć na firmy zależne od transakcji w czasie rzeczywistym, takich jak platformy e-commerce i usługi finansowe.

Zakłócenia operacyjne

Przerwy spowodowane atakiem DDoS zmniejszają produktywność, opóźniają krytyczne procesy i utrudniają dostęp do podstawowych usług. W przypadku branż takich jak opieka zdrowotna lub produkcja przestoje operacyjne mogą spowodować daleko idące konsekwencje.

Uszczerbek na reputacji

Gdy klienci doświadczają zakłóceń w świadczeniu usług, zaufanie do firmy słabnie. Przedłużone lub powtarzające się incydenty mogą spowodować długoterminowe szkody dla reputacji organizacji, co prowadzi do spadku lojalności klientów i zmniejszenia zaufania na rynku.

Autentyczny przykład

W 2020 roku doszło do głośnego incydentu, w którym duża instytucja finansowa padła ofiarą długotrwałego ataku DDoS, który na kilka godzin uniemożliwił korzystanie z usług bankowości internetowej. Bezpośrednie straty w przychodach, w połączeniu z nadszarpniętą reputacją, spowodowały szkody przekraczające **50 milionów dolarów.**

Alarmujące statystyki

Raport DDoS Insights Report firmy Zayo Group (luty 2024 r.) wskazuje, że niechronione organizacje ponosiły średnie koszty w wysokości **6000 USD** na minutę, co w 2023 r. doprowadziło do średnich kosztów na poziomie około **408 000 USD** na jeden incydent. Co więcej, częstotliwość takich ataków rośnie, a ponad **rocznie zgłaszanych jest 10 milionów ataków**. Statystyki te podkreślają pilną potrzebę solidnych mechanizmów zapobiegawczych.

20,5 mln

Ataki DDoS zostały zablokowane w pierwszym kwartale 2025 roku.

Źródło: 2024: Raport Cloudflare DDoS Threat Report

Przeciwdziałanie atakom DDoS za pomocą Dell Technologies

Firma Dell Technologies oferuje zaawansowany pakiet rozwiązań, które pomagają firmom zapobiegać incydentom DDoS, wykrywać je i odzyskiwać po nich dane.

Wzmocnione punkty końcowe dzięki zaufanym urządzeniom firmy Dell

Punkty końcowe są głównymi obszarami podatnymi na ryzyko ataków typu DDoS. Dell Trusted Devices oferuje zaawansowane funkcje zabezpieczeń wbudowane w sprzęt, takie jak Secure BIOS i SafeID, które chronią przed nieautoryzowanym dostępem i utrzymują integralność systemu.

Zabezpieczenia serwerów

Rozwiązania serwerowe firmy Dell wyposażone we wbudowane zabezpieczenia, takie jak technologia Dell Trusted Server, która obejmuje:

- **Sprzętowe źródło zaufania:** Ta funkcja zapewnia, że komponenty sprzętowe serwera są weryfikowane podczas rozruchu, co w ten sposób wprowadza podstawową warstwę bezpieczeństwa przed manipulacją lub nieautoryzowanymi modyfikacjami.
- **Wbudowane funkcje zabezpieczeń:** Serwery firmy Dell są wyposażone w dyski samoszyfrujące i kompleksową weryfikację rozruchu, które chronią przed nieautoryzowanym dostępem i dają pewność integralności danych.
- **Cyberodporność:** Podejście to obejmuje możliwości wykrywania anomalii, naruszeń i nieautoryzowanych operacji, umożliwiając organizacjom szybkie odzyskiwanie danych po incydentach cybernetycznych.
- **Kompleksowa ochrona danych:** rozwiązania Trusted Server firmy Dell są wyposażone w zintegrowane mechanizmy bezpieczeństwa, które chronią dane w spoczynku i w ruchu. Obejmuje to zaawansowane techniki szyfrowania i opcje automatycznego odzyskiwania w celu zapewnienia ciągłości biznesowej.

Dzięki tym funkcjom serwery mogą wytrzymać skoki ruchu przy jednoczesnym zachowaniu stabilności operacyjnej. Rozwiązania w zakresie pamięci masowej chronią krytyczną dostępność i integralność danych podczas ataku, minimalizując zakłócenia.

Zabezpieczenia pamięci masowej

Pamięć masowa Dell pomaga chronić przed atakami DDoS za pomocą różnych zintegrowanych środków bezpieczeństwa i zaawansowanych technologii zaprojektowanych z myślą o minimalizacji luk w zabezpieczeniach, wczesnym wykrywaniu zagrożeń i zapewnianiu szybkiego odzyskiwania danych w przypadku ataku. Najważniejsze metody to:

- **Proaktywne wykrywanie zagrożeń:** Rozwiązania pamięci masowej firmy Dell wykorzystują inteligentne monitorowanie i wykrywanie anomalii oparte na sztucznej inteligencji w celu identyfikacji nietypowych wzorców dostępu, które mogą wskazywać na atak DDoS. Te narzędzia zapewniają w czasie rzeczywistym informacje o zagrożeniach i mogą uruchamiać automatyczne reakcje na zagrożenia w celu zmniejszenia skutków ataku.
- **Architektura źródła zaufania:** Zintegrowana z kontrolerami pamięci masowej architektura ta zapewnia autentyczność oprogramowania wewnętrznego i zapobiega nieautoryzowanym modyfikacjom, zwiększając w ten sposób bezpieczeństwo sprzętu pamięci masowej i zmniejszając ryzyko naruszenia bezpieczeństwa podczas ataku DDoS
- **Uwierzytelnianie wieloskładnikowe (MFA) i kontrola dostępu:** Wdrożenie MFA i kontroli dostępu opartej na rolach (RBAC) pomaga zapobiegać nieautoryzowanemu dostępowi do systemów pamięci masowej, dodatkowo chroniąc przed zagrożeniami związanymi z atakami DDoS
- **Mikrosegmentacja i izolacja sieci:** Dzięki izolacji systemów pamięci masowej i ograniczeniu dostępu między obciążeniami roboczymi firma Dell minimalizuje potencjalne cele ataków i chroni systemy pamięci masowej przed ruchami bocznymi w przypadku naruszenia bezpieczeństwa
- **Bezpieczne migawki i niezmienne dzienniki:** Rozwiązania pamięci masowej firmy Dell zapewniają bezpieczne migawki i niezmienne dzienniki, które zapewniają integralność danych i pomagają organizacjom szybko odzyskać sprawność po atakach DDoS. Funkcje te ułatwiają analizę śledczą i badanie incydentów, umożliwiając zespołom IT wykrywanie i analizowanie wektorów ataków
- **Sejf Cyber Recovery:** Rozwiązania takie jak Dell PowerMax i sejf PowerProtect Cyber Recovery tworzą odizolowane kopie zapasowe, które są niezmienne, a także chronione przed atakami typu ransomware i innymi zagrożeniami. Te kopie zapasowe można przywrócić, aby zapewnić ciągłość prowadzenia działalności bez ryzyka ponownej infekcji

Dzięki integracji tych kompleksowych funkcji i technologii bezpieczeństwa Dell Storage i Cyber Resilience skutecznie pomagają organizacjom bronić się przed atakami DDoS i utrzymać odporne i bezpieczne środowiska IT.

Proaktywne monitorowanie dzięki CrowdStrike

Monitorowanie w czasie rzeczywistym i zaawansowana analiza mają kluczowe znaczenie dla wykrywania nietypowych wzorców ruchu przed eskalacją. Rozwiązanie CrowdStrike integruje się z ekosystemem firmy Dell, wykorzystując analizę zachowania i informacje oparte na sztucznej inteligencji do odróżniania legalnej aktywności od działalności o charakterze ataku, umożliwiając szybkie usuwanie zagrożeń.

Dell PowerProtect dla integralności danych

Dell PowerProtect zapewnia bezpieczeństwo i dostępność najważniejszych danych w przypadku ataku DDoS. Niezmienne możliwości tworzenia kopii zapasowych i izolowane środowiska odzyskiwania umożliwiają firmom przywracanie systemów i minimalizowanie przestojów po incydencie.

Zaawansowane zabezpieczenia sieciowe i mikrosegmentacja dzięki rozwiązaniom Dell PowerSwitch Networking i SmartFabric OS

Wzmacnia ochronę przed atakami typu zero day, zapewniając zaawansowaną segmentację sieci, ścisłą kontrolę dostępu i analizę ruchu w czasie rzeczywistym w całej infrastrukturze.

Autentyczne wdrożenie

Globalna platforma handlu elektronicznego wykorzystała niedawno rozwiązania Dell PowerProtect wraz z proaktywnym wykrywaniem, aby odeprzeć zaawansowany atak DDoS. Poprzez wyizolowanie krytycznych systemów i wdrożenie procesów odzyskiwania awaryjnego firma wznowiła pełną działalność w rekordowym czasie, zmniejszając straty finansowe i zachowując zaufanie klientów.

Wielowarstwowe podejście do zabezpieczeń

Sukces w walce z atakami DDoS wynika z warstwowej i adaptacyjnej ochrony. Firma Dell propaguje następujące strategie uzupełniające jej ofertę technologiczną:

Najważniejsze kroki w celu wzmocnienia obrony

- **Architektura modelu „zero trust”** umożliwia wdrożenie modelu „nigdy nie ufaj, zawsze weryfikuj” w celu sprawdzenia każdego użytkownika i urządzenia
- **Zaawansowane szyfrowanie** komunikacji we wszystkich warstwach w celu ochrony wrażliwych danych przesyłanych podczas potencjalnych prób ataku.
- **Szkolenie pracowników** edukuje pracowników w zakresie identyfikowania podejrzanych działań i stosowania bezpiecznych protokołów w celu zapobiegania przypadkowym naruszeniom.
- **Regularne testy systemu** Przeprowadzaj rutynowe oceny, w tym testy penetracyjne i testy obciążenia, aby oceniać jego gotowość na duże natężenie ruchu.

Działania te, w połączeniu z rozwiązaniami Dell Technologies, tworzą solidny mechanizm obrony przed zaawansowanymi zagrożeniami.

Partnerstwa, które wzmacniają cyberbezpieczeństwo

Aby rozszerzyć swoje możliwości, firma Dell Technologies współpracuje na przykład z liderami branży, takimi jak **Microsoft**, **CrowdStrike** i **Secureworks**. Te partnerstwa zapewniają dodatkowe warstwy ochrony, włączając najlepsze dane o zagrożeniach i zaawansowane metody wykrywania do kompleksowego systemu Dell.

Wykorzystanie usług Dell Professional Services

Poza technologią Dell Professional Services oferuje fachowe doradztwo firmom, które stają w obliczu wyzwań związanych z DDoS. Od reakcji na incydenty po dostosowane konsultacje w zakresie architektury bezpieczeństwa zespół Dell zapewnia organizacjom szybkie przywracanie i wzmacnianie przyszłych środków obronnych.

Buduj odporną przyszłość

Firma Dell Technologies to nie tylko dostawca technologii, ale także partner, który dba o ochronę firmy przed zmieniającym się zagrożeniem atakami DDoS. Łącząc najnowocześniejsze technologie, dogłębne relacje partnerskie i przydatne informacje, firma Dell pomaga firmom chronić operacje, utrzymywać zaufanie klientów i aktywnie dążyć do rozwoju.

Zrób pierwszy krok w kierunku odporności już dziś. Skontaktuj się z firmą Dell Technologies, aby wzmocnić swoją firmę przed zagrożeniami DDoS i zabezpieczyć swoją przyszłość.

Firma Dell Technologies umożliwia firmom sprostanie wyzwaniom związanym z cyberbezpieczeństwem DDoS, co potwierdza, że bezpieczna podstawa jest kluczem do sukcesu w połączonym świecie.

Więcej informacji o tym, jak radzić sobie z największymi wyzwaniami związanymi z cyberbezpieczeństwem, można znaleźć na stronie **Dell.com/SecuritySolutions**

Dowiedz się więcej o Rozwiązania firmy Dell

Skontaktuj się z ekspertem firmy Dell Technologies

Zobacz więcej materiałów

Dołącz do rozmowy, stosując #hasztag

DELL Technologies