DELL Technologies

# DDoS: Stärkung von Cybersicherheit und Resilienz mit Dell Technologies

## Zunehmende Bedrohung durch DDoS-Angriffe

Distributed-Denial-of-Service-Angriffe (DDoS) gehören mittlerweile zu den weitverbreitetsten und zerstörerischsten Bedrohungen im digitalen Zeitalter. DDoS-Angriffe nutzen umfangreiche Netzwerke kompromittierter Geräte, um Zielsysteme, Server oder Netzwerke mit einer überwältigenden Datenmenge zu überfluten. Dieser unerbittliche Anstieg verlangsamt den Betrieb oder bringt ihn ganz zum Erliegen, was häufig zu einer Lähmung des Geschäftsbetriebs führt.

Von Start-ups bis hin zu multinationalen Konzernen ist kein Unternehmen vor dem steigenden Risiko von DDoS-Angriffen gefeit. Da Unternehmen zunehmend von digitaler Infrastruktur abhängig sind, haben diese Angriffe verheerende Folgen, die von finanziellen Verlusten bis hin zu Reputationsschäden reichen. Dell Technologies ist sich der Bedeutung dieser Herausforderung bewusst und bietet skalierbare, innovative Lösungen, die Unternehmen helfen, ihre Abwehrmaßnahmen zu verstärken und die Herausforderung zu bewältigen.

## Was sind DDoS-Angriffe?

Bei einem DDoS-Angriff wird versucht, den normalen Betrieb eines Netzwerks, Dienstes oder Servers zu stören, indem dieser mit einer enormen Datenmenge aus mehreren Quellen überlastet wird. Diese Angriffe werden mithilfe von Botnets durchgeführt, also Netzwerken infizierter Geräte, die von AngreiferInnen ferngesteuert werden.

## So funktionieren DDoS-Angriffe

1. **Botnet-Rekrutierung:** Cyberkriminelle infizieren Tausende oder Millionen von Geräten mit Malware und bilden so ein Botnet, das für einen Angriff mobilisiert werden kann, der Ihr Unternehmen lahmlegt.
2. **Datenflut:** AngreiferInnen weisen die Botnets an, eine Flut von Anfragen an den Zielserver zu senden, was dazu führt, dass das System verlangsamt wird, abstürzt oder für legitime NutzerInnen nicht mehr verfügbar ist.
3. **Systemüberlastung:** Das System wird durch unzulässigen Datenverkehr überlastet und kann legitime Anfragen nicht mehr bearbeiten, was zu Serviceausfällen oder erheblichen Verzögerungen führt.

## Gängige Techniken

- **Volumenbasierte Angriffe:** Diese Angriffe nutzen das enorme Datenverkehrsvolumen, um die Bandbreite eines Netzwerks auszuschöpfen.
- **Protokollangriffe** nutzen Sicherheitslücken in Protokollen wie TCP/IP aus, um Ressourcen zu verbrauchen.
- **Angriffe auf Anwendungsebene** zielen auf bestimmte Anwendungen ab, z. B. eine Website oder Datenbank, um die Funktionalität zu unterbrechen.

Diese Angriffe entwickeln sich ständig weiter und machen sie zu einer gewaltigen Herausforderung für Unternehmen, die versuchen, den Betrieb zu schützen.

## Auswirkungen auf Unternehmen

### Finanzielle Folgen

Ein einziger DDoS-Angriff kann Millionen von Dollar an entgangenen Einnahmen, Ausfallzeiten und Wiederherstellungskosten verursachen. Selbst wenige Minuten Ausfallzeit können erhebliche Auswirkungen auf Unternehmen haben, die auf Echtzeittransaktionen angewiesen sind, wie E-Commerce-Plattformen und Finanzdienstleister.

### Betriebsunterbrechung

Durch einen DDoS-Angriff verursachte Unterbrechungen verringern die Produktivität, verzögern wichtige Prozesse und behindern den Zugriff auf wesentliche Dienste. In Branchen wie dem Gesundheitswesen oder der Fertigung können betriebliche Ausfallzeiten weitreichende Folgen haben.

### Reputationsschäden

Wenn Kunden oder Klienten Serviceunterbrechungen erleben, schwächt sich das Vertrauen. Länger andauernde oder wiederholte Vorfälle können zu langfristigen Schäden für den Ruf eines Unternehmens führen, was Kundenabwanderung und ein geringeres Vertrauen auf dem Markt zur Folge haben kann.

## Praxisbeispiel

Ein viel beachteter Fall ereignete sich im Jahr 2020, als ein großes Finanzinstitut Opfer eines anhaltenden DDoS-Angriffs wurde, der seine Onlinebanking-Dienste für mehrere Stunden lahmlegte. Die direkten Umsatzverluste in Verbindung mit dem angeschlagenen Ruf führten zu Schäden in Höhe von über **50 Millionen USD**.

## Alarmierende Statistiken

Der DDoS Insights Report der Zayo Group (Februar 2024) zeigt, dass ungeschützte Unternehmen im Durchschnitt **6.000 USD** pro Minute verloren haben, was zu durchschnittlichen Kosten von rund **408.000 USD** pro Incident im Jahr 2023 führte. Darüber hinaus nimmt die Häufigkeit solcher Angriffe zu, wobei **jährlich mehr als 10 Millionen Angriffe** gemeldet werden. Diese Statistiken verdeutlichen die dringende Notwendigkeit robuster präventiver Mechanismen.

**20,5 Mio.**

DDoS-Angriffe wurden im ersten Quartal 2025 abgewehrt

Quelle: 2024: Cloudflare DDoS Threat Report

## Bekämpfung von DDoS-Angriffen mit Dell Technologies

Dell Technologies bietet eine Reihe fortschrittlicher Lösungen, mit denen Unternehmen DDoS-Vorfälle verhindern, erkennen und beheben können.

### Verstärkte Endpunkte mit Dell Trusted-Devices

Endpunkte sind wichtige Einstiegspunkte für DDoS-bezogene Bedrohungen. Dell Trusted-Devices bieten robuste, in die Hardware integrierte Sicherheitsfunktionen wie Secure BIOS und SafeID, die vor unbefugtem Zugriff schützen und die Systemintegrität gewährleisten.

### Serversicherheit

Die Serverlösungen von Dell sind mit integrierten Sicherheitsmaßnahmen wie der Dell Trusted Server-Technologie ausgestattet, die Folgendes umfasst:

- **Hardware Root of Trust:** Diese Funktion stellt sicher, dass die Hardwarekomponenten des Servers zum Startzeitpunkt überprüft werden, wodurch eine grundlegende Sicherheitsebene gegen Manipulationen oder unbefugte Änderungen bereitgestellt wird.
- **Integrierte Sicherheitsfunktionen:** Dell Server sind mit selbstverschlüsselnden Laufwerken und End-to-End-Startüberprüfung ausgestattet, die vor unbefugtem Zugriff schützen und Vertrauen in die Datenintegrität schaffen.
- **Ausfallsicherheit bei Cyberangriffen:** Der Ansatz umfasst Funktionen zur Erkennung von Anomalien, Sicherheitsverletzungen und unbefugten Vorgängen, sodass Unternehmen sich schnell von Cyber-Incidents erholen können.
- **Umfassende Data Protection:** Die Trusted Server-Lösungen von Dell verfügen über integrierte Sicherheitsmechanismen, die Daten im Ruhezustand und während der Übertragung schützen. Dazu gehören fortschrittliche Verschlüsselungstechniken und automatisierte Wiederherstellungsoptionen, um die Geschäftskontinuität zu gewährleisten.

Mit diesen Funktionen können Server Datenverkehrsspitzen standhalten und gleichzeitig die Betriebsstabilität aufrechterhalten. Storage-Lösungen schützen die Verfügbarkeit und Integrität kritischer Daten während eines Angriffs und minimieren so Unterbrechungen.

### Sicherheit für Storage

Dell Storage schützt vor DDoS-Angriffen durch verschiedene integrierte Sicherheitsmaßnahmen und fortschrittliche Technologien, die darauf ausgelegt sind, Schwachstellen zu minimieren, Bedrohungen frühzeitig zu erkennen und im Falle eines Angriffs eine schnelle Wiederherstellung zu gewährleisten. Die wichtigsten Methoden:

- **Proaktive Bedrohungserkennung:** Dell Storage-Lösungen nutzen intelligentes Monitoring und KI-gesteuerte Anomalieerkennung, um ungewöhnliche Zugriffsmuster zu identifizieren, die auf einen DDoS-Angriff hinweisen könnten. Diese Tools bieten Sicherheitseinblicke in Echtzeit und können automatisierte Bedrohungsreaktionen auslösen, um die Auswirkungen eines Angriffs zu mindern.
- **Root-of-Trust-Architektur:** Diese in Storage-Controller integrierte Architektur gewährleistet die Authentizität der Firmware und verhindert unbefugte Änderungen. Dadurch wird die Sicherheit der Storage-Hardware verbessert und das Risiko einer Kompromittierung während eines DDoS-Angriffs verringert.
- **Multifaktor-Authentifizierung (MFA) und Zugriffskontrollen:** Die Implementierung von MFA und rollenbasierter Zugriffskontrolle (Role-Based Access Control, RBAC) trägt dazu bei, unbefugten Zugriff auf Storage-Systeme zu verhindern, und bietet zusätzlichen Schutz vor Bedrohungen im Zusammenhang mit DDoS-Angriffen.
- **Mikrosegmentierung und Netzwerkisolierung:** Durch die Isolierung von Storage-Systemen und die Einschränkung des Zugriffs zwischen Workloads minimiert Dell potenzielle Angriffsvektoren und schützt Storage-Systeme im Falle einer Sicherheitsverletzung vor lateralen Bewegungen.
- **Sichere Snapshots und unveränderliche Protokolle:** Die Storage-Lösungen von Dell bieten sichere Snapshots und unveränderliche Protokolle, die die Datenintegrität gewährleisten und Unternehmen dabei unterstützen, sich schnell von DDoS-Angriffen zu erholen. Diese Funktionen erleichtern die forensische Analyse und die Untersuchung von Vorfällen, sodass IT-Teams Angriffsvektoren erkennen und auswerten können.
- **Cyber Recovery Vault:** Lösungen wie Dell PowerMax und PowerProtect Cyber Recovery Vault erstellen Air-Gap-Backups, die unveränderlich und vor Ransomware und anderen Angriffen geschützt sind. Diese Backups können wiederhergestellt werden, um die Geschäftskontinuität ohne das Risiko einer erneuten Infektion sicherzustellen.

Durch die Integration dieser umfassenden Sicherheitsfunktionen und -technologien unterstützen die Storage- und Cyber-Resilience-Lösungen von Dell Unternehmen effektiv dabei, sich gegen DDoS-Angriffe zu verteidigen und resiliente und sichere IT-Umgebungen aufrechtzuerhalten.

### Proaktives Monitoring mit CrowdStrike

Echtzeitüberwachung und erweiterte Analysen sind unerlässlich, um ungewöhnliche Datenverkehrsmuster vor der Eskalation zu erkennen. CrowdStrike lässt sich in das Ökosystem von Dell integrieren und nutzt Verhaltensanalysen und KI-gestützte Erkenntnisse, um legitime Aktivitäten von Angriffsdatenverkehr zu unterscheiden und so eine schnelle Behebung zu ermöglichen.

### Dell PowerProtect für Datenintegrität

Dell PowerProtect sorgt dafür, dass kritische Daten während eines DDoS-Angriffs sicher und zugänglich bleiben. Unveränderliche Backupfunktionen und isolierte Recovery-Umgebungen ermöglichen es Unternehmen, Systeme wiederherzustellen und Ausfallzeiten nach einem Incident zu minimieren.

### Erweiterte Netzwerksicherheit und Mikrosegmentierung mit Dell PowerSwitch Networking und SmartFabric OS

Stärkung der Abwehr von Zero-Day-Angriffen durch erweiterte Netzwerksegmentierung, strenge Zugriffskontrollen und Echtzeit-Analysen des Datenverkehrs in Ihrer gesamten Infrastruktur

## Praxisbeispiel

Eine globale E-Commerce-Plattform nutzte kürzlich die PowerProtect-Lösungen von Dell in Verbindung mit proaktiven Erkennungsfunktionen, um einen ausgeklügelten DDoS-Angriff abzuwehren. Durch die Isolierung kritischer Systeme und die Bereitstellung von Notfallwiederherstellungsprozessen konnte das Unternehmen die volle Betriebsfähigkeit in Rekordzeit wiederherstellen, wodurch finanzielle Verluste gemindert und das Vertrauen der Kunden bewahrt wurde.

## Mehrschichtiger Sicherheitsansatz

Eine erfolgreiche Abwehr von DDoS-Angriffen beruht auf mehrschichtigen und adaptiven Schutzmaßnahmen. Dell empfiehlt die folgenden Strategien als Ergänzung zu seinen technologischen Angeboten:

### Wichtige Schritte zur Verbesserung der Verteidigung

- **Zero-Trust-Architektur** Implementieren Sie ein Modell nach dem Motto „Niemals vertrauen, immer überprüfen“, um alle NutzerInnen und Geräte zu überprüfen.
- **Erweiterte Verschlüsselung** Verschlüsseln Sie die Kommunikation über alle Ebenen hinweg, um sensible Daten zu schützen, die bei potenziellen Angriffsversuchen übertragen werden.
- **Mitarbeiterschulungen** Schulen Sie Ihre MitarbeiterInnen darin, verdächtige Aktivitäten zu identifizieren und sichere Protokolle zu befolgen, um unbeabsichtigte Sicherheitsverletzungen zu verhindern.
- **Regelmäßige Systemtests** Führen Sie routinemäßige Bewertungen, einschließlich Penetrationstests und Lasttests, um die Bereitschaft des Systems für hohe Datenverkehrsvolumina zu bewerten.

In Kombination mit den Lösungen von Dell Technologies bilden diese Maßnahmen einen robusten Verteidigungsmechanismus gegen komplexe Bedrohungen.

## Partnerschaften zur Stärkung der Cybersicherheit

Um sein Angebot auszuweiten, arbeitet Dell Technologies mit branchenführenden Unternehmen wie **Microsoft**, **CrowdStrike** und **Secureworks** zusammen. Diese Partnerschaften bieten zusätzliche Schutzebenen, indem sie die besten Threat-Intelligence- und fortschrittlichen Erkennungsmethoden in das umfassende Framework von Dell integrieren.

## Nutzung von Dell Professional Services

Über die Technologie hinaus bieten die Professional Services von Dell fachkundige Beratung für Unternehmen, die mit DDoS-Herausforderungen konfrontiert sind. Von der Reaktion auf Incidents bis hin zu maßgeschneiderten Beratungen zur Sicherheitsarchitektur sorgt das Team von Dell dafür, dass Unternehmen sich schnell erholen und ihre Abwehrmaßnahmen für die Zukunft verstärken können.

## Zusammen für eine krisenfeste Zukunft

Dell Technologies ist nicht nur ein Technologieanbieter, sondern ein Partner, der sich dafür einsetzt, Ihr Unternehmen vor den sich ständig weiterentwickelnden Bedrohungen durch DDoS-Angriffe zu schützen. Durch die Kombination von Spitzentechnologie, intensiven Partnerschaften und umsetzbaren Erkenntnissen unterstützt Dell Unternehmen dabei, ihren Betrieb zu schützen, das Vertrauen ihrer Kunden zu wahren und aktiv Wachstum zu verfolgen.

Machen Sie noch heute den ersten Schritt in Richtung Resilienz. Wenden Sie sich an Dell Technologies, um Ihr Unternehmen gegen DDoS-Bedrohungen zu stärken und Ihre Zukunft zu sichern.

Dell Technologies unterstützt Unternehmen dabei, die Herausforderungen der DDoS-Cybersicherheit zu meistern, und beweist damit, dass eine sichere Grundlage der Schlüssel zum Erfolg in einer vernetzten Welt ist.

Erfahren Sie, wie Sie einige der größten Herausforderungen von heute im Bereich der Cybersicherheit bewältigen können: **Dell.com/SecuritySolutions**

---

Weitere Informationen zu Dell Lösungen

Kontaktieren Sie die Dell Technologies ExpertInnen.

Weitere Ressourcen anzeigen

Kommen Sie ins Gespräch über #HashTag



DELL Technologies