

Abwehr von DDoS-Attacken auf allen Ebenen

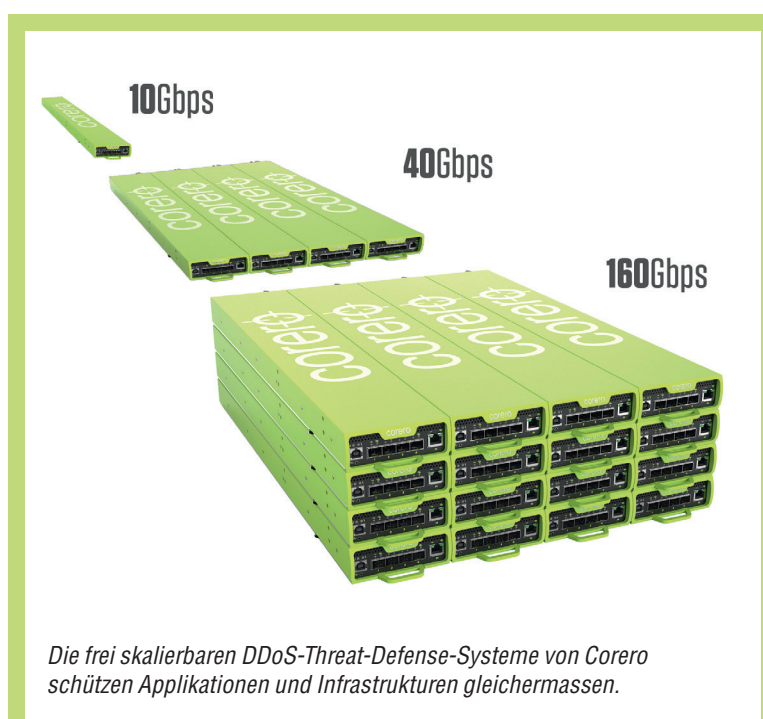
DDoS-Threat-Defense-Systeme (TDS) von Corero

«Distributed Denial of Service»-Attacken (DDoS) gehören zu den aktuell grössten Gefahren für IT-Infrastrukturen und Applikationen. Um entsprechende Angriffe zu erkennen und wirksam abzuwehren, empfiehlt sich der Einsatz der hochperformanten DDoS-Threat-Defense-Systeme (TDS) von Corero.

DoS- und DDoS-Angriffe haben zum Ziel, Applikationen und Server lahmzulegen und Systeme wie Firewalls, Load-Balancer, Web- und Applikations-server, Datenbanken und Storage-Lösungen so zu stören, dass sie ihre Aufgaben nicht mehr erfüllen können («Denial of Service»). Dazu bedienen sich Hacker einerseits der bekannten, volumenbasierten Attacken. Andererseits lancieren sie vermehrt intelligente Multivektor-Angriffe sowie Attacken auf Anwendungsebene.

Bei der erstgenannten Variante werden beispielsweise mittels Botnetz derart viele HTTP-Anfragen mit nicht komplettiertem Handshaking an das angegriffene System übermittelt, dass dieses aufgrund der so generierten Überlast nicht mehr in der Lage ist, Inhalte auszuliefern. Angriffsformen wie SYN-Flood- oder Smurf-Angriffe gehören in diese Kategorie.

Stark zunehmend sind intelligente, mehrschichtige Attacken. Diese «langsamen» und «leistungsschwachen» Angriffe benötigen bescheidene Ressourcen und lassen sich für die Infizierung der angegriffenen Systeme oft viel Zeit. Dadurch sind sie in der Regel nur schwer als Gefahr zu erkennen, da das Netzwerk-Verkehrsvolumen nicht merklich zunimmt. Zu den smarten Angriffsformen gehören unter anderem Reflecting-DDoS-Attacken, Application Layer DDoS, das gezielte Ausnutzen von Server-Verletzlichkeiten, Pre-Attack Recon Scans (verschaffen fundiertes Wissen über die anzugreifende Infrastruktur) und Advanced Evasion Techniques (Kombination aus bekannten Evasion-



Die frei skalierbaren DDoS-Threat-Defense-Systeme von Corero schützen Applikationen und Infrastrukturen gleichermassen.

Wirksamer Schutz vor Cyber-Attacken

Dank der mit «First Line of Defense» bezeichneten Einbindung am äussersten Perimeter der Kunden- bzw. Serviceprovider-Netzwerkinfrastruktur stellen die TDS von Corero eine maximale Verfügbarkeit und eine uneingeschränkte Performance aller nachgelagerten Dienste und Infrastrukturen sicher.

- Hochperformante «First Line of Defense»-Lösung für Serviceprovider, Hostingprovider, Datacenter und Enterprises
- Erkennung und Abwehr von breit angelegten Angriffen (High-Volume-Attacken bzw. «Reflective and amplified Spoof Attacks») auf Netzwerk-Level bis hin zu «smarten» und «langsamen» DDoS-Attacken auf Anwendungsebene (Layer 3 bis 7)
- Wehrt DDoS-Angriffe wirksam ab und erlaubt gleichzeitig legitime Zugriffe (Business Continuity bzw. Aufrechterhaltung der Services unter Attacken)
- Dedizierte TDS-Plattform mit hardwarebeschleunigten Multicore-CPU's
- Minimalste Latenzzeiten und höchste Durchsatzraten von 10 Gbps bis 1 Tbps pro Rack
- Modulare, nahtlos skalierbare Lösung – erweiterbar in 1- und 10-Gbps-Schritten
- SDN- und Cloud-ready
- Automatische Provisionierung
- Zentralisiertes Reporting-System

Techniken mit neuen Tarnmethoden, um Schadcode ins gewünschte Zielnetzwerk zu schleusen).

First Line of Defense

Um DOS- und DDoS-Attacken auf allen Ebenen – von der Anwendungs- über DNS- und HTTP- bis hin zur Protokoll-ebene (Layer 3 bis 7) – zu erkennen und abzuwehren, bietet der Netzwerk-Security-Spezialist Corero die höchst performanten DDoS-Threat-Defense-Systeme (TDS). Diese leisten sowohl in Unternehmen (on-premise) als auch bei Service- und Hosting-Providern wertvolle Dienste. Sie blockieren gefährliche IP-Adressen und ungewollten Datenverkehr aus definierten geografischen Regionen, limitieren die Anzahl Requests und Verbindungen, stoppen Protokoll-Missbrauch und -Verletzungen, und sie verhindern AETs (Advanced Evasion Techniques). Zudem blockieren sie unberechtigte Zugriffe (Intrusion Prevention), wehren Buffer Overflows und Exploits ab und blockieren das Einschleusen von ausführbarem Code (Code Injection). Kurz: Sie bilden ein einzigartiges Sicherheitsdispositiv gegen DDoS-Attacken unterschiedlichster Art.

BOLL
IT Security Distribution

BOLL ENGINEERING AG

Jurastrasse 58, 5430 Wettingen
Tel. 056 437 60 60
info@boll.ch, www.boll.ch