

DDOS-APPLIANCES VON CORERO

Wirksamer Schutz vor DDoS-Attacken

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

DoS- und DDoS-Angriffe stellen Unternehmen und Organisationen vor grosse Herausforderungen. Sie haben zum Ziel, Applikationen und Server lahmzulegen und Systeme wie Firewalls, Load-Balancer, Web- und Applikationsserver, Datenbanken und Storage-Lösungen so zu stören, dass sie ihre Aufgaben nicht mehr erfüllen können («Denial of Service»). Dazu bedienen sich Hacker einerseits breit angelegter Attacken. Andererseits lancieren sie 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-Attacken 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



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

sie i. d. R. nur schwer als Gefahr zu erkennen. Zu den smarten Angriffsformen gehören u. a. Reflecting-DDoS-Attacken, Application Layer DDoS, das gezielte Ausnützen von Server-Verletzlichkeiten, Pre-Attack Recon Scans (verschaffen fundiertes Wissen über die anzugreifende Infrastruktur) und Advanced Evasion Techniques (Kombination aus bekannten Evasion-Techniken mit neuen Tarnmethoden, um Schadcode ins gewünschte Ziel-Netzwerk zu schleusen).

Angriffe erkennen und abwehren

Um DOS- und DDoS-Attacken auf allen Ebenen – von der Anwendungs- über DNS- und HTTP- bis hin zur Protokollebene – zu erkennen und abzuwehren, bietet der Netzwerk-Security-Spezialist Corero leistungsstarke DDoS-Defense-Systeme (DDS) mit integrierter IPS-Funktionalität an. Diese leisten sowohl in Unternehmen (on-premise) als auch bei ISPs und Cloud-Anbietern wertvolle

Dienste. Sie blockieren gefährliche IP-Adressen und ungewollten Datenverkehr aus 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: Die DDS-Appliances von Corero bilden ein einzigartiges Sicherheitsdispositiv gegen DDoS-Attacken unterschiedlichster Art.

Um diesem Anspruch jederzeit und langfristig gerecht zu werden, beinhalten die Appliances ein internes Bewertungssystem. Dieses überwacht kontinuierlich die sich ändernde DDoS-Bedrohungslage und aktualisiert die entsprechend notwendigen Abwehrmechanismen automatisch. Zudem steht mit ReputationWatch ein externes Bewertungssystem zur Verfügung. Dieses überwacht wechselnde IP-Adressen kontinuierlich auf deren Reputation und sperrt den Datenverkehr beim Überschreiten eines Grenzwertes automatisch.

Corero – DDoS-Attacken verhindern

Die leistungsstarken DDoS-Defense-Systeme (DDS) von Corero ermöglichen die nahtlose Überwachung und Abwehr von DDoS-Attacken:

- Appliances zum Schutz vor DDoS-Attacken – von der Anwendungs- über DNS- und HTTP- bis hin zur Protokollebene
- Internes Bewertungssystem und externer Service «ReputationWatch» erkennen DDoS-Attacken und stoppen diese effektiv
- Integrierte IPS-Funktionalität
- Schutz vor Protokoll-Missbrauch, AETs (Advanced Evasion Techniques), Buffer Overflows und Exploits
- Verhindert Einschleusen ausführbaren Codes (Code Injection)
- GEO-IP-Filtering



BOLL ENGINEERING AG

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