

Schutz vor gross angelegten Cyber-Attacken



Die «DDoS Defense Appliances» von Corero Network Security sind im Leaders-Quadrant von Gartner platziert und bieten auf Netzwerk- und Anwendungsebene maximalen Schutz vor DoS- und DDoS-Attacken.

«Sony PlayStation Network wegen DDoS-Attacken seit Tagen down». «Wikileaks-Sympathisanten fahren Attacken gegen Postfinance, Mastercard und Visa». «Denial-of-Service-Angriff verursacht massive Umsatzeinbusse» ... Meldungen dieser Art nehmen zu – und bilden nur die Spitze des Eisbergs. Denn: Viele «Distributed Denial of Service»-Attacken (DDoS) finden den Weg nicht in die breite Öffentlichkeit oder werden durch Schutzgeldzahlungen verhindert.

DoS- und DDoS-Angriffe haben das primäre Ziel, Server und Kommunikationsinfrastrukturen der angegriffenen Institutionen lahmzulegen. Dabei werden im Rahmen von SYN-Flood- oder Smurf-Attacken derart viele http-Anfragen mit nicht komplettiertem Handshaking an den angegriffenen Website-Server übermittelt, dass dieser aufgrund von Überlastung nicht mehr in der Lage ist, Inhalte auszuliefern. Angriffe dieser Art erfolgen in aller Regel über sogenannte Botnetze. Dabei handelt es sich um eine Vielzahl von Rechnern, die mit Schadsoftware infiziert sind, sich dadurch von einem Hacker fernsteuern und Tausende gleichzeitiger Zugriffe auf einen Zielrechner erzeugen können, um diesen zum Absturz zu bringen. Grosse Botnetze sind in der Lage, enormen Traffic zu generieren und selbst gut geschützte Systeme in die Knie zu zwingen.

DDoS-Angriffe lassen sich auch von Serverfarmen in Ländern reiten, die keine griffige Internet-Gesetzgebung kennen. Auch

Programmfehler bieten eine gute Angriffsmöglichkeit. Bei diesen sogenannten «Application-Level-Attacken» wird die Schwachstelle einer Applikation genutzt, um Fehlerfunktionen wie zum Beispiel den Absturz einer Serversoftware auszulösen.

Allen Attacken gemeinsam ist die Tatsache, dass sie in dubiosen Kreisen als Dienstleistung eingekauft werden können und es folglich auch für Nicht-Hacker ein Leichtes ist, beispielsweise Web-Shops von Mitbewerbern lahmzulegen.

Sicherheit – oft eine existenzielle Frage

DDoS-Attacken stellen namentlich für jene Firmen und Institutionen eine Bedrohung dar, die ihr Geschäft oder wesentliche Teile davon online abwickeln. Dazu gehören Betreiber von E-Shops, Finanzdienstleister, international tätige Firmen, öffentliche Dienste und politische Akteure. Nebst schwerwiegenden Reputationsschäden verursachen DDoS-Angriffe oft massive Umsatzeinbussen und haben Kundenabwanderung zur Folge. Nicht zu vernachlässigen sind ferner die finanziellen Folgen, die sich durch die Androhung von DDoS-Attacken beziehungsweise durch digitale Schutzgelderpressungen ergeben.

Um Gefahren dieser Art wirksam zu begegnen, stellt der Netzwerk-Security-Spezialist Corero ein innovatives DDoS Defense System (DDS) mit integrierter IPS-Funktionalität (Intrusion Prevention System) zur Verfügung. Die hoch performante Appliance ermöglicht die nahtlose

DDoS Defense Systems (DDS) von Corero setzen neuen Leistungsstandard

Ob zur Schädigung von Mitbewerbern, aus politischen Motiven oder zur Erpressung von Schutzgeldern – «Distributed Denial of Service»-Attacken (DDoS) stellen IT-Infrastrukturen, Firmen und staatliche Organisationen vor grosse Herausforderungen.

Überwachung und Vermeidung von DDoS-Angriffen und stellt somit eine maximale Verfügbarkeit internetbasierter Dienste sicher.

Corero setzt mit ihrer DDS-Appliance zur Abwehr von DDoS-Attacken Bestmarken:

- «Out of the box»-Lösung zur Erkennung und automatischen Abwehr von DDoS-Attacken auf Netzwerk- und Application-Layer-Ebene
- Patentierter DDoS-Defense-Algorithmus erkennt und filtert bösartigen Datenverkehr, lässt regulären Traffic jedoch zu
- Dedizierte, hoch performante Appliance garantiert «Business Continuity» – selbst bei massivsten DDoS-Attacken von über 100 MBit/s
- Transparente Einbindung in bestehende Netze gewährt unmittelbaren Schutz
- Maximale Verfügbarkeit dank Leistungsmerkmalen wie Clustering, bis zu 30 Jahre MTBF (Meantime between failure), redundante Power-Supplies
- Komfortables User-Interface mit weitreichenden Reporting-Funktionen

Kontakt

BOLL Engineering AG

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