

newsletter

zum Thema **Distributed Denial of Service-Attacken im Internet**

Distributed Denial of Service-Attacken (DDoS) stellen eine zunehmende Gefahr für das Internet dar. Sie treten vermehrt auf und zielen mittlerweile auch auf zentrale Elemente der Internet-Infrastruktur ab.

Anlass: DDoS auf DNS-Server

Ende November 2002 wurde der Internet-Dienstleister UltraDNS (zuständig für Verwaltung des Domain Name Systems (DNS)-Server der Top Level Domain.info) für 4 Stunden einer DDoS ausgesetzt. Einen Monat zuvor, am 21.10.2002 waren die Root-Server des Domain Name Systems (DNS) Ziel einer massiven sog. Distributed Denial of Service-Attacke (DDoS). Die attackierten DNS-Server sind eine wichtige Basisstruktur des Internets, da sie das Adressverzeichnis des Internets darstellen: Jedem Computer im Internet ist eine spezifische Adresse zugeordnet. Das DNS-System ermöglicht die eindeutige Zuordnung und Umwandlung der benutzerfreundlichen Web-Adressen (z.B. www.swissre.com) in die von Computern verstandenen numerischen IP-Adressen (z.B.193.246.224.28). Die laut US-Behörden bis dato heftigste und komplexeste DDoS-Attacke auf diese Systeme dauerte ungefähr eine Stunde. Dabei fielen 7 der weltweit 13 Root-Server komplett aus, weitere zwei waren nahezu lahmgelegt. Von den Internet-Nutzern wurde der Vorfall nicht bemerkt, da Server lokaler ISPs (Internet Service Provider) die Zuordnung der IP-Adressen einige Zeit im Zwischenspeicher vorhalten. Bei längerem Ausfall ist jedoch eine Beeinträchtigung in Form von Problemen in der Internetnutzung und der Auslieferung von Mails zu erwarten. Die Urheber dieser Attacken konnten bis dato nicht ermittelt werden.

Technischer Hintergrund

DDoS-Attacken im Internet gibt es seit mehreren Jahren. Sie nutzen Schwachpunkte in der Implementierung von Netzwerkfunktionalitäten diverser Betriebssysteme aus. Denial of Service (= den Dienst verweigern) bezeichnet einen Prozess, der darauf abzielt, Netzwerkdienste (z.B. einen Web- oder Mailserver) lahmzulegen und somit deren Nutzung zu erschweren bzw. unmöglich zu machen. Dabei wird die Netzanbindung des Angriffsziels mit einer großen Anzahl von Datenpaketen überflutet, was letztendlich zu einer Überlastung und u.U. zum Absturz des Systems führt. Um dies zu erreichen, muss ein Angreifer über entsprechend große IT-Ressourcen verfügen. Eine optimale Angriffs-Methode zur Generierung entsprechend ausreichender Ressourcen ist die sog. Distributed (= verteilte) Denial of Service-Attacke (DDoS).

Die DDoS geht im Vergleich zum einfachen Denial of Service Angriff von mehreren unterschiedlichen Quellen gleichzeitig aus, d.h. es wird eine Vielzahl von Rechnern koordiniert und gleichzeitig dazu veranlasst, Datenpakete an eine bestimmte Zieladresse zu schicken.

Dies geschieht mittels automatisierter DDoS Programme wie z.B. Trinoo, Tribe Flood oder Stacheldraht. Diese Tools sind im Internet frei verfügbar.

Ablauf eines Angriffs

Der eigentliche Angreifer operiert bei einer DDoS-Attacke getarnt im Hintergrund und macht andere Rechner zu den Werkzeugen seines Angriffs. Die Ermittlung des Urhebers ist bei dieser Angriffsvariante nur sehr schwer möglich. Zu Beginn der Attacke sucht der Angreifer im Internet entsprechend ungeschützte Rechner, die es ihm erlauben, seine Angriffs-Tools zu platzieren und somit sein „Angriffsnetzwerk“ aufzubauen.

Vereinfacht dargestellt läuft eine DDoS-Attacke in folgenden Schritten ab:

- der Angreifer versendet seinen Angriffsbefehl an die Masterprogramme seines Angriffsnetzwerks
- diesen Befehl leiten die Masterprogramme an die von ihnen kontrollierten Rechner (sog. Daemons) weiter
- eine Vielzahl von Daemons attackieren nun zeitgleich ein vom Angreifer zuvor festgelegtes Zielsystem - das Opfer der Attacke

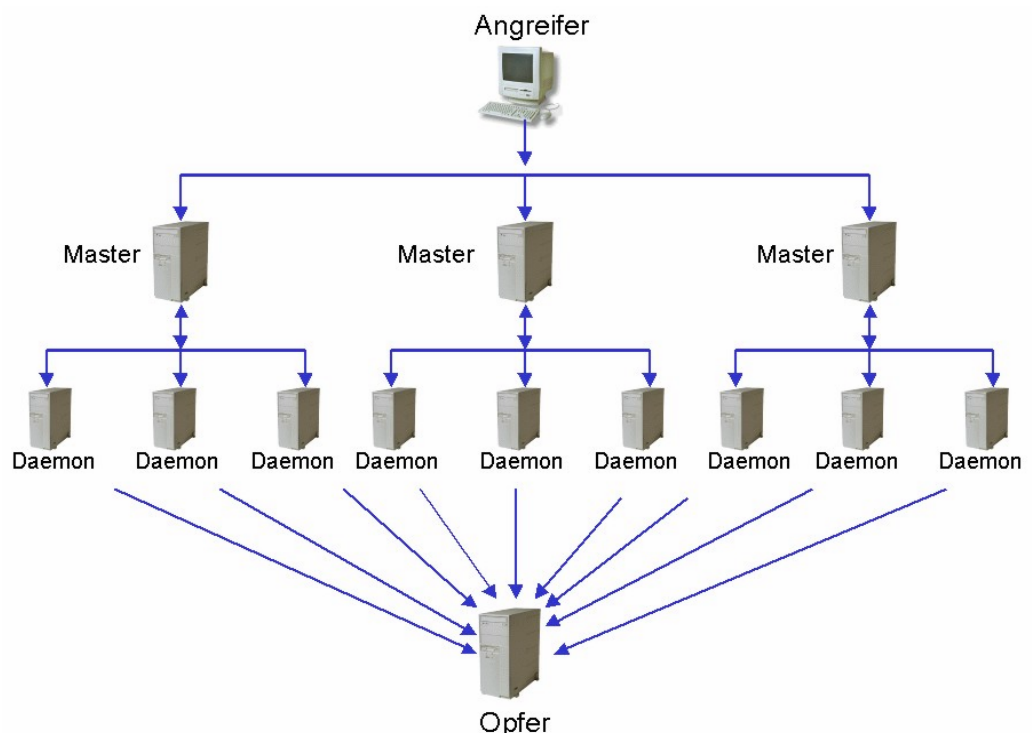


Bild: Übersichtsschema einer DDoS-Attacke

Weitere Beispiele

Denial of Service-Attacken stellen für Unternehmen eine erhebliche, ständig gegenwärtige Sicherheitsbedrohung dar. So gaben 40% der im Rahmen des CSI/FBI Computer Crime and Security Survey befragten US-Unternehmen an, dass sie im Jahr 2001 von Denial of Service-Attacken betroffen waren.

Beispiele von DDoS-Attacken:

- mehrere renommierte Internet-Anbieter, wie Yahoo.com, ebay.com, Amazon.com, CNN.com fielen im Februar 2000 z.T. über 3 Stunden aufgrund einer massiven DDoS-Attacke praktisch aus.
- eine große Zahl der Microsoft Web-Pages waren im Januar 2001 betroffen und teilweise bis zu 24 Stunden nicht verfügbar
- im Februar 2002 führte eine längerwährende Serie von DDoS-Attacken zur Schließung des britischen Internet Providers CloudNine

Fazit

Die Vorfälle zeigen klar die Risiken einer in immer stärkeren Maß vernetzten und digitalisierten Weltwirtschaft auf, die zunehmend von der Verfügbarkeit der IT-Infrastruktur abhängt. DDoS-Attacken bedeuten eine zunehmende Gefahr für Unternehmen, deren Geschäftstätigkeit in hohem Maß auf einer Präsenz im Internet basiert. Bisher wurde vornehmlich versucht, bestimmte E-Commerce-Anbieter und Institutionen mittels dieser Angriffstechnik lahmzulegen. Gezielte Angriffe auf die Kernelemente der Infrastruktur des Internets stellen jedoch ein wesentlich massiveres Bedrohungsszenario mit wirtschaftlichen Schäden als Konsequenz dar.

Hinweise für das Underwriting

Die durch Denial of Service-Attacken verursachten Ausfälle von IT-Systemen sind in der Regel in Standard Property- und Haftpflichtdeckungen nicht versichert; es gibt spezielle Versicherungsprodukte, die spezifisch IT- und Internetrisiken inkl. Netzausfälle decken. Um diesen Risiken Rechnung zu tragen, sollte ein profundes Risk Assessment durchgeführt werden neben angemessenen zeitlichen Selbstbehalten.

Ungenügender Schutz von IT-Systemen gegen unbefugten Zugriff schafft die Möglichkeit, solche Systeme als Angriffswerkzeuge zur Schädigung Dritter zu missbrauchen, was zu Haftungsansprüchen der Geschädigten gegen die Betreiber der missbrauchten Systeme führen kann (downstream liability). Bei Internet- oder IT-Haftpflichtdeckungen ist daher bei der Risikoprüfung auch der Schutz vor Angriffen angemessen zu berücksichtigen.

Eine durch Denial of Service-Attacken hervorgerufene Betriebsunterbrechung durch den Ausfall externer Netzwerke kann zu entsprechenden Rückwirkungsschäden (suppliers /customer extension) führen. Auch hier kommt der Risikoprüfung eine hohe Bedeutung zu, speziell im Hinblick auf Schnittstellen und Abhängigkeiten zu Internet Service Providern, Hostern und Carriern.

Bei Versicherungskonzepten, die Betriebsunterbrechungen bei IT-Systemen ohne zugrundeliegenden Sachsubstanzschaden decken, ist eine Kumulexposure aufgrund von Angriffen auf die Internet-Infrastruktur gegeben, insbesondere im Hinblick auf den Ausfall von zentralen Infrastrukturelementen. Für dieses Kumulschadenszenario gibt es derzeit noch keine anwendbare Kontrollmöglichkeit.

Kontakt

AssTech GmbH
Postfach 1211
85766 Unterföhring bei München
Telefon + 49 89 3844-1585
Telefax + 49 89 3844-1586
info@asstech.com
www.asstech.com