Denial of Service

aus Wikipedia, der freien Enzyklopädie

Als **Denial of Service** (**DoS**, zu Deutsch etwa: *Dienstverweigerung*) bezeichnet man einen Angriff auf einen Host (Server) oder sonstigen Rechner in einem Datennetz mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen. In der Regel geschieht dies durch Überlastung. Erfolgt der Angriff koordiniert von einer größeren Anzahl anderer Systeme aus, so spricht man von **Verteilter Dienstblockade** bzw. **DDoS** (**Distributed Denial of Service**). Normalerweise werden solche Angriffe nicht per Hand, sondern mit Backdoor-Programmen oder Ähnlichem durchgeführt, welche sich von alleine auf anderen Rechnern im Netzwerk verbreiten und dem Angreifer durch solche Botnetze weitere Wirte zum Ausführen seiner Angriffe bringen.

Inhaltsverzeichnis

Funktionsweise

Primitive DoS-Angriffe wie SYN-Flooding, PIH-Flooding oder die Smurf-Attacke belasten die Dienste eines Servers, beispielsweise HTTP, mit einer größeren Anzahl Anfragen, als dieser in der Lage ist zu bearbeiten, woraufhin er eingestellt wird oder reguläre Anfragen so langsam beantwortet, dass diese abgebrochen werden. Wesentlich effizienter ist es jedoch, wie bei WinNuke, der Land-Attacke, der Teardrop-Attacke oder dem Ping of Death Programmfehler auszunutzen, um eine Fehlerfunktion (wie einen Absturz) der Serversoftware auszulösen, worauf diese ebenso auf Anfragen nicht mehr reagiert.

Eine besondere Form stellt die **DRDoS** (**Distributed Reflected Denial of Service**)-Attacke dar. Hierbei adressiert der Angreifer seine Datenpakete nicht direkt an das Opfer, sondern an regulär arbeitende Internetdienste, trägt jedoch als Absenderadresse die des Opfers ein (IP-Spoofing). Die Antworten auf diese Anfragen stellen dann für das Opfer den eigentlichen DoS-Angriff dar. Der Ursprung des Angriffs ist für den Angegriffenen durch diese Vorgehensweise praktisch nicht mehr ermittelbar.

Im Unterschied zu anderen Angriffen will der Angreifer hier normalerweise nicht in den Computer eindringen und benötigt deshalb keine Passwörter oder Ähnliches. Jedoch kann ein DoS-Angriff Bestandteil eines Angriffs auf ein System sein, zum Beispiel bei folgenden Szenarien:

- Um vom eigentlichen Angriff auf ein System abzulenken, wird ein anderes System durch einen DoS lahmgelegt. Dies soll dafür sorgen, dass das mit der Administration betraute Personal vom eigentlichen Ort des Geschehens abgelenkt ist, bzw. die Angriffsversuche im durch den DoS

erhöhten Datenaufkommen untergehen.
- Werden Antworten eines regulären Systems verzögert, können Anfragen an dieses durch eigene, gefälschte Antworten kompromittiert werden. Beispiel hierfür ist das Hijacking fremder Domainnamen durch Liefern gefälschter DNS-Antworten.
- Als Form des Protests sind DoS-Attacken in letzter Zeit populär geworden. Zum Eigenschutz der Protestierenden werden Angriffe dieser Art im Allgemeinen von Würmern durchgeführt, die sich selbstständig auf fremden Systemen verbreiten. Entsprechend handelt es sich bei Protestaktionen dieser Art um DDoS-Attacken.

Beispiele

Chronologie

- Im Februar 2000 wurden verschiedene, große Internet-Dienste (zum Beispiel Yahoo, CNN, amazon.de, eBay) durch DDoS-Attacken lahmgelegt. Hierbei hatten sich die Angreifer Zugang zu hunderten von Computern im Internet verschafft, um die Wirksamkeit ihrer Attacken durch die Vielzahl der gleichzeitig angreifenden Rechner stark zu erhöhen.
- Mai 2001: drei Tage andauernde DDoS-Attacke gegen das CERT/CC (Computer Emergency Response Team/Coordination Center).
- August 2003: Der E-Mail-Wurm Lovsan / W32.Blaster soll die Update-Site der Firma Microsoft unerreichbar machen, wird jedoch durch Deaktivierung des Domainnamens ins Leere geführt.
- Februar 2004: Der E-Mail-Wurm Mydoom bringt die Website der Firma SCO zum Erliegen.
- Januar/Februar 2005: Ein aktiv gesteuerter DoS-Angriff legt in mehreren Angriffswellen das Online-Angebot des Heinz-Heise-Verlags für zwei Tage teilweise lahm. Der Zeitschriftenverlag stellt Strafanzeige und setzt eine Belohnung in Höhe von 10.000 Euro für sachdienliche Hinweise aus, die zur Ergreifung des Täters führen.
- April 2005: Das Online-Spielenetzwerk *PlayOnline* der Firma Square Enix, auf dem unter anderem das Spiel Final Fantasy XI läuft, ist Ziel eines DDoS-Angriffs.
- August 2005: Wegen mehreren DDoS wird das Bundeskriminalamt eingeschaltet, zum Beispiel bei der FLUXX AG, die Ziel eines gescheiterten Erpressungsversuchs um 40.000 Euro war.
- Dezember 2005: DDoS gegen die Server von dialerschutz.de, computerbetrug.de, gulli.com und antispam.de; Ermittlungsbehörden eingeschaltet.
- Februar 2007: Das Onlinespiel Ragnarok Online (euRO) der Burda Holding ist Ziel eines DoS-Angriffs.
- März 2007: DDoS gegen den Service von DynDNS.org. Es wurde vor allem der Client-Server angegriffen welcher die IP-Adressen der dynamischen Hostnamen annimmt.
- April / Mai 2007: Die Server der estländischen Regierung und von Unternehmen in Estland werden in mehreren Wellen angegriffen und brechen zeitweilig zusammen. Es soll sich um den schwersten DDoS-Angriff gegen ein Land gehandelt haben.
- November 2007: DDoS-Angriff gegen antispam.de und aa419.org, die Betreiber gehen von einem Zusammenhang aus.[1]
- Dezember 2007: Das beliebte Browserspiel OGame wird Ziel eines DDoS-Angriffes.[2]
- Februar 2008: Das Browserspiel OGame wird wieder zum Ziel einer DDoS Attacke.[3]
- März 2008: Vampirefreaks.com, eine beliebte Seite für die Gothic/Industrial-Subkultur wird Opfer einer DDoS Attacke

Die beobachteten Angriffe basierten auf zwei wesentlichen Schwachstellen: Zum einen konnten die Absenderadressen der „angreifenden“ Datenpakete gefälscht werden (IP-Spoofing), zum anderen konnte vor dem eigentlichen Angriff auf einer großen Anzahl dritter – nur unzureichend geschützter – Internet-Rechner unberechtigterweise Software installiert werden, die dann ferngesteuert durch massenhaft versendete Datenpakete den eigentlichen Angriff ausführten. Das Besondere an diesen DDoS-Angriffen ist, dass diese auch diejenigen treffen können, die sich ansonsten optimal vor Eindringlingen aus dem Internet geschützt haben. Insofern sind Rechner, auf denen nicht einmal so genannte Grundschutzmaßnahmen umgesetzt sind, nicht nur für den jeweiligen Betreiber eine Gefahr, sondern auch für alle anderen Computer im Internet.

Zur Veranschaulichung

Werden in einer HTML-Datei bestimmte aktive Inhalte in einem Browser ausgeführt, indem beispielsweise mit der Maus über einen Hyperlink gefahren wird (Klicken ist dabei nicht zwingend notwendig), versucht der Browser bei entsprechend niedrigen Sicherheitseinstellungen zum Beispiel durch das Aneinanderhängen von Zeichenketten sehr viel längere Zeichenketten zu erzeugen, die nach und nach den Arbeitsspeicher des Rechners füllen. Dieser Speicher steht anderen Anwendungen dann nicht mehr zur Verfügung und muss gegebenenfalls sogar auf die Festplatte ausgelagert werden. Dadurch wird der Rechner stark ausgelastet und für andere Aufgaben unter Umständen blockiert. Der Arbeitsspeicher wird erst wieder freigegeben, wenn das Browserfenster geschlossen wurde.

Dienstverweigerung bei herkömmlicher Überlastung

Führt der sprunghafte Anstieg von Anfragen an eine bisher nur gering frequentierte Website aufgrund der Berichterstattung in einem publikumswirksamen Medium (wie dem IT-Online-Magazin Slashdot) zu deren Überlastung und damit zur Dienstverweigerung, wird das zumeist Slashdot-Effekt genannt und gelegentlich scherzhaft mit einem DDoS-Angriff verglichen.

Quellen

1. ↑ Zitat von der temporären Startseite von antispam.de: „Die Betreiber von Antispam.de gehen aufgrund der zeitlichen Überschneidung von einem Zusammenhang mit der DDoS auf die Anti-Scam-Seite aa419.org (Artists Against 419) aus, die sich mit dem als 'Nigeria-Mails' bekannten Vorschussbetrug befasst und diesen bekämpft.“
2. ↑ *DDOS Attacke auf OGame* im OGame-Forum (http://board.ogame.de/thread.php?threadid=563304)
3. ↑ [http://board.ogame.de/thread.php?threadid=592901 *DDOS auf die Startseite* im OGame-Forum

Weblinks

- Funktionsweise des DoS (Bundesamt für Sicherheit in der Informationstechnik) (http://www.bsi.de/fachthem/sinet/gefahr/toolsana.htm)
- Eine Liste freier deutschsprachiger Dokumente zum Thema (http://www.computec.ch/download.php?list.7)
- Ausführliche Beschreibung des Denial of Service (http://www.highgames.com/?set=hardwareview&view=8)
- Detaillierte Beschreibung eines Denial of Service Angriffs, anhand von grafischen Mitteln (http://www.irc-mania.de/DDOS.php)

Von „http://de.wikipedia.org/wiki/Denial_of_Service“
Kategorie: Sicherheitslücke