DuD
Datenschutz und Datensicherheit

Distributed Denial-of-Service Angriffe (DDoS)

Klaus Möller, Stefan Kelm

Gateway (Tor, Durchgang) ist ein Vermittlungscomputer, der zwei unterschiedliche, aber gleichartige Kommunikationssysteme verbindet. Dazu setzt er die Kommunikationsregeln (Protokolle) des einen in die des anderen um. So ermöglicht er den Teilnehmern beider Systeme, sich zu verständigen. In unserem „Gateway" werden Juristen technische und Technikern juristische Begriffe erläutert.

Hintergrund

Seit den Anfängen des Internets existieren sie, die sog. „Denial-of-Service" (DoS) Angriffe, deren Ziel es ist, die Verfügbarkeit bestimmter Rechner und/oder Dienste drastisch einzuschränken. Meist wird bei dieser Form von Angriffen über das Internet versucht, durch das Ausnutzen von Schwachstellen in Betriebssystemen, Programmen und Diensten bzw. das Ausnutzen grundsätzlicher Entwurfsschwächen der verwendeten Netzwerkprotokolle, die angegriffenen Systeme zum Absturz zu bringen oder derartig zu überlasten, dass diese Systeme ihre eigentliche Funktionalität nicht mehr erbringen können.

Reine DoS-Angriffe haben also nicht das Ziel, vertrauliche Daten zu stehlen oder Benutzer-Authentisierungs-Mechanismen zu umgehen, sondern Diensteanbieter lahm zu legen. Häufig führt dies nicht zu einem direkten Schaden des angegriffenen Systems, wohl aber durch die Verursachung von Verzögerungen wichtiger Transaktionen oder Nachrichten zu indirekten Schäden. Angesichts des zunehmenden Angebots von Waren und Dienstleistungen über das Internet („E-Commerce") ist zu befürchten, dass DoS-Angriffe zukünftig auch erhebliche direkte Schäden (Geschäftsausfälle) verursachen können.

Ein neuer Trend in Denial-of-Service Angriffen wird seit Mitte 1999 beobachtet und hat Anfang diesen Jahres bei Angriffen auf Firmen wie Yahoo und eBay für internationales Aufsehen gesorgt: Anstelle von einzelnen Systemen, die als Ausgangspunkt eines Denial-of-Service Angriffs benutzt werden, kommt nun eine Vielzahl von unterschiedlichen Systemen in einem grossflächig koordinierten Angriff auf einzelne Systeme oder Netzwerke zum Einsatz. Die Anzahl der an einem Angriff beteiligten Systeme kann dabei variieren; einige hundert bis tausend gleichzeitig angreifende Systeme wurden bereits beobachtet.

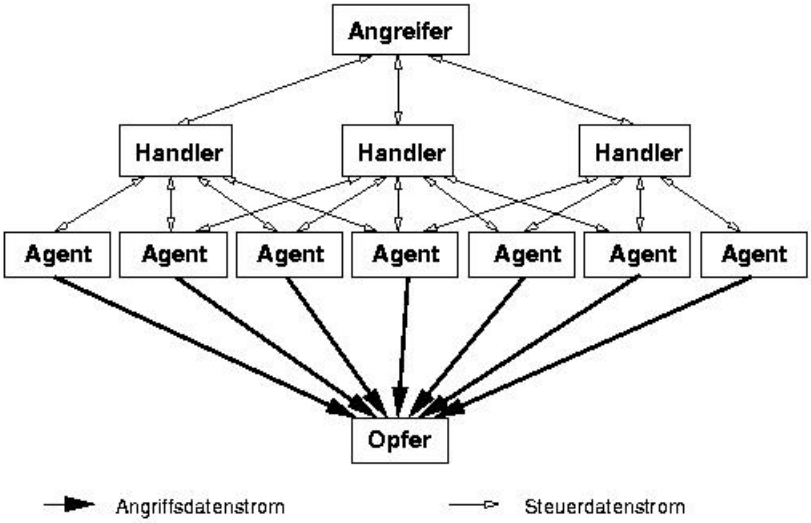

Abb. 1: Struktur eines DDoS-Angriffs

Da die an einem Angriff beteiligten Rechner oft über große Teile des Internets verteilt sind, spricht man von einem sogenannten „Distributed Denial-of-Service" (DDoS) Angriff. Die dabei verwendeten Angriffstechniken sind seit Jahren bekannt. Häufig werden einzelne oder mehrere der folgenden Methoden eingesetzt:

- „UDP packet storm": Eine große Anzahl von (korrekten) UDP-Paketen wird an ein fremdes System geschickt, welches unter der Last ausfallen kann.
- „TCP SYN Flooding": Auf einem fremden System wird eine große Anzahl von (gefälschten) TCP-Verbindungen aufgebaut, die bereits während des Verbindungsaufbaus wieder unterbrochen werden. Diese „halb offenenen" Verbindungen blockieren dann das System.
- „PING-Flooding": ein fremdes System wird mit (gefälschten) IP-Kontrollnachrichten (ICMP-Paketen) belastet; diese Nachrichten samt der erzeugten Anwort-Pakete können ein komplettes Subnetz erheblich belasten.

Allen diesen Angriffen liegt üblicherweise das ebenfalls seit langem bekannte Fälschen von IP-Adressen („IP-Spoofing") zugrunde, welches das Aufspüren des Angreifers erheblich erschwert.

Die Abbildung zeigt die typische Struktur eines verteilten Denial-of-Service Angriffs, bestehend aus dem Angreifer, welcher eine relativ kleine Anzahl sog. *Handler* kontrolliert, die ihrerseits wiederum eine sehr viel größere Anzahl von *Agents* steuern. Diese *Agents* führen dann den eigentlichen Denial-of-Service Angriff auf das Opfer durch.

Die Installation der *Agents* und *Handler* durch den Angreifer erfolgt zumeist auf Systemen, in die zuvor (üblicherweise automatisiert über das Internet) eingebrochen wurde. Mittels sogenannter „Rootkits"

wird zusätzlich die Existenz bzw. der Betrieb der *Agents* und *Handler* auf den kompromittierten Systemen zu verbergen versucht.

Zum Glück gibt es mittlerweile einige Programme, die das Aufspüren solcher Angriffs-Tools erheblich erleichtern (siehe die URL am Ende des Beitrags). Sowohl die Rootkits als auch die Tools zur Durchführung der DDoS-Angriffe (die so illustre Namen wie „Stacheldraht“ und „Tribe Flood Network“ tragen) sind dabei frei im Internet verfügbar und stammen teilweise aus Deutschland.

Schutz vor DoS-Attacken

Ein wirksamer Schutz vor Angriffen auf die Verfügbarkeit von offenen Systemen ist mit informationstechnischen Mitteln prinzipiell nur sehr eingeschränkt möglich. Denn offene Systeme sind ja gerade dafür gedacht, dass sie die Kommunikation mit praktisch jedem System zulassen und dynamisch auf Lastschwankungen reagieren.

Technisch bleibt als einzige Möglichkeit, Datenpakete von einem angreifenden System möglichst frühzeitig abzuweisen, so daß das Angriffsziel das Paket gar nicht erst erhält. Die Abwehr am Netzübergang zum Opfer greift nicht mehr, da die Überflutung hier bereits eingetreten ist. Idealerweise sollten die Angriffspakete schon in dem Netz abgefangen werden, in dem sich der Agent befindet oder beim Internet Service Provider dieses Netzes. Die Wirksamkeit solcher Maßnahmen hat allerdings mehrerlei Voraussetzungen:

- So muss das Abwehrsystem „böse“ und „gute“ Pakete unterscheiden können. Dies ist heute z. T. mit Hilfe von Intrusion Detection Systemen möglich, die auf „ungewöhnliches“ Verhalten im Netz reagieren (z. B. eine große Zahl von Verbindungsaufbauwünschen in kurzer Zeit von einer Adresse, oder das „Angriffsmuster“ eines Angreifertools).
- Weiter muss das Abwehrsystem schnell genug auf die erkannte „Abnormalität“ reagieren und Netzkomponenten (wie z. B. einen Paketfilter) dynamisch umkonfigurieren.

Das geht allerdings nur, wenn das Abwehrsystem nicht schon selbst Opfer eines solchen Angriffs ist. An der Wurzel läßt sich ein DoS-Angriff nur bekämpfen, wenn das angreifende System identifiziert werden kann. Durch die Verschleierung der IP-Adresse mit Hilfe von IP-Spoofing ist dies in der Praxis allerdings in der Regel nicht möglich.

Abwehr von DDoS-Angriffen

Das Ausmaß eines DDoS-Angriffs macht die Abwehr extrem schwierig. Da die angreifenden *Agents* einerseits sehr weit verteilt liegen und andererseits die Absender-IP-Adressen von den *Agents* gefälscht werden, ergibt sich ein sehr großer Bereich von IP-Adressen, der zu filtern wäre, um den Angriff abzuwehren. Ein solcher Filter würde letztlich die Erreichbarkeit des angegriffenen Systems genauso stark beeinträchtigen wie der Angriff selbst. Hinzu kommt, dass für PING-Floods und UDP-Floods eine Filterung beim Provider (ISP) des Opfers oder beim Übergang zum angegriffenen Netz zu spät käme, da diese Netzbereiche durch den Angriff in der Regel bereits überlastet sind.

Da ferner sowohl *Handler* als auch *Agents* mehrfach vorhanden sind, kann der Angriff selbst dann noch fortgesetzt werden, falls es gelingen sollte, einige der *Agents* oder *Handler* zu finden und zu deaktivieren.

Das „Spoofing“ der Absender IP-Adressen erschwert die Erkennung derjenigen Systeme, auf denen sich die *Agents* befinden. Zusätzlich erschwert die verteilte Architektur von Distributed Denial-of-Service Angriffen die Ermittlung des tatsächlichen Angreifers. In den *Agents* finden sich immer nur die IP-Adressen einiger weniger *Handler*, meistens nicht einmal aller am Angriff beteiligten. Die *Handler* wiederum haben keine Kenntnis von der IP-Adresse des Angreifers. Darüber hinaus ist die Kommunikation zwischen Angreifer und *Handler* zumindest bei einigen Versionen der Angriffs-Tools verschlüsselt.

Als Konsequenz ist der Angreifer selbst meist nicht aufzuspüren, es sei denn es gelingt, die Kommunikation zwischen Angreifer und *Handler* abzuhören und mittels der aufgezeichneten IP-Adressen einen Hinweis auf das System zu erlangen, das der Angreifer gerade zur Initiierung des Angriffs nutzt. Dieses System kann allerdings selbst kompromittiert sein, so dass sich dort in der Regel keine verwertbaren Spuren finden werden.

Zur Aufarbeitung eines Distributed Denial-of-Service Angriffs müssten zunächst zumindest einige der Systeme ermittelt werden, auf denen sich am Angriff beteiligte *Agents* befinden. Über diese lassen sich die kontrollierenden *Handler* aufspüren, welche zu anderen *Agents* führen, usw. Dies erfordert eine gemeinsame Anstrengung des Opfers, der Provider, der Systemverwalter der Systeme, auf denen *Agents* oder *Handler* laufen, und der Notfall-Teams. Hier sind in erster Linie organisatorische Anstrengungen notwendig, um die Zusammenarbeit zu ermöglichen.

Als Schutz vor DDoS-Angriffen werden häufig das Schließen bekannter Betriebssytemlücken sowie allgemeine Maßnahmen des ISPs gegen das „IP Spoofing“ empfohlen. Diese Maßnahmen treffen generell für alle mit dem Internet verbundenen Rechner zu; sie vermögen das Risiko eines Angriffs jedoch nur eingeschränkt zu verringern, da es immer auch einen Teil von nicht gesicherten Systemen im Internet geben wird. Andererseits ist jedes über das Internet erreichbare System ein potenzielles Ziel von DDoS-Angriffen.

Literatur

Zahlreiche Links und Informationen zum Thema DDoS finden Sie auf dem Webserver des DFN-CERT:
http://www.cert.dfn.de/dfncert/ddos.html