Denial of Service

Carl Denis
Betreuer: Marc Fouquet
Seminar Future Internet SS2009
Lehrstuhl Netzarchitekturen und Netzdienste
Fakultät für Informatik
Technische Universität München
Email: denis@in.tum.de

***Kurzfassung*— Thema dieser Arbeit ist die Analyse verschiedener Denial of Service (DoS) Techniken, den Motiven, ihrer Ausführung und die Häufigkeit mit der sie Auftreten. Es wird ein Überblick gegeben, der einen Einstieg in die Analyse vereinfachen soll, um mögliche Prognosen über die zukünftige Entwicklung dieser Angriffsart aufzustellen.**

***Schlüsselworte*— Denial of Service, ICMP/TCP/SYN-Flood, Cyberattack**

I. Einleitung

Wohlbekannt sind Denial of Service (DoS) Angriffe aus den Medien. Immer wieder werden sie für Schlagzeilen bezüglich des "Cyberkrieges" verwendet und breiten bei Laien, die trotzdem täglich mit Computern zu tun haben, eine gewisse Panik aus. Schutzlos ist man der Willkür von Hackern ausgesetzt. Was nun passiert, wie und warum Einzelne, vielleicht auch Jugendliche in der Schule ganze Regierungsnetze lahmlegen können, und wie häufig es wirklich geschieht, werden wir im Folgenden abhandeln.

A. Definition

Denial of Service bedeutet wörtlich übersetzt "Dienstverweigerung" und beschreibt eine jegliche Art und Weise, einen Dienst über ein Netzwerk unerreichbar zu machen. Dem inbegriffen sind auch die weniger beachteten physikalischen Angriffe, die ein lokaler Angreifer zum Beispiel durch abzwicken eines Netzwerkkabels erreichen könnte. Untersucht werden in dieser Arbeit jedoch lediglich entfernte Attacken, die einen direkten/lokalen Zugriff auf den Host oder das anvisierte Netzwerk ausschließen.

B. Beispiele

- Im Mai 2007 wurde Estland von DDoS Angriffen heimgesucht, teilweise ist Estland digital vom Rest der Welt abgeschnitten gewesen [1], [2].
- Im März 09 wurde die Videostreamingleitung von ESL auf der CeBit Hannover lahmgelegt.

II. Motivation

Das Motiv, einen Dienst unerreichbar zu machen kann auf sehr verschiedene Gründe zurückzuführen sein. Diese lassen sich aber in verschiedene Kategorien einteilen. Die Motivation, globalpolitisch oder im kleinen, ist proportional zur Wichtigkeit und Resistenz des Ziels. Damit ein Angriff auf ein prominentes Ziel, wie zum Beispiel ein Regierungsserver, überhaupt als Angriff gewertet werden kann, müssen ganz anderen Mittel in Bewegung gesetzt werden als um einen heimischen Webserver außer Gefecht zu setzen.

- Cyberwarfare: Der digitale Krieg ist auch heute nicht nur mehr in Filmen präsent, was sich unter anderem durch die aktiven Überlegungen über Restrukturierung der Sicherheitsvorkehrungen der US-Regierung zeigt [3]. Simultan mit dem Georgienkrieg gestartete Cyberattacken [4], [5], sowie der DDoS [1] auf die Estländische Regierung 2007 bekräftigen, dass diese Methoden mit der immer größeren weltweiten Vernetzungen verschiedener Systeme mit Breitbandanbindungen zu immer durchschlagkräftigeren Waffen mutieren.
- Organisierte Kriminalität: Durch Erpresserbriefe werden Firmen aufgefordert Zahlungen zu tätigen um im Gegenzug ihre Internetpräsenz ungehindert betreiben zu können. Besonders konzentriert tauchten diese nahe für Betreiber wichtige Terminen auf, wie zum Beispiel für Online-Wettbüros zur Fußball Europameisterschaft 2004 [6].
  Botnets[2] scheinen auch immer mehr untergliedert zu werden um evntl. Teile davon zu vermieten [7], [8], demnach ist es auch denkbar, dass für Marketingzwecke Demonstrationen und anschließend für Kunden breit angelegte Angriffe durchgeführt werden [9].
- Die kleine Rache: als neuer Volkssport in der elektronischen "Sportwelt" scheint das DoS aufgetaucht zu sein. Tutorials wie man einen verhassten Gegner aus einem Onlinespiel nimmt, indem man zum Beispiel seine Internetleitung an der die X-Box hängt überlädt sind frei zugänglich [10], [11].

III. DoS Angriffe durchführen

Es wird hier keine Anleitung gegeben um Systeme in die Knie zu zwingen, lediglich ein Überblick über Methoden gegeben die anderweitig schon frei verfügbar und ausführlich dokumentiert sind.

DoS Angriffe kann man prinzipiell in 3 Unterklassifizierungen einordnen, die Einfachen, welche ein einzelner Computer

[1] Distributed Denial of Service, siehe III-C.

[2] Netzwerk von kompromitierten "Zombiekomputern" welche für einen Kriminellen Zweck missbraucht werden.

zur Ausführung ausreicht, diese die andere Netze als ungewollte Reflektoren benutzen und schlussendlich Distributed-DoS.

A. Die elementarsten Techniken

1) Fehlerhafte Implementierung: Bekannt wurde diese Art von Angriffen durch den sogenannten "Ping of Death" der hier [12] beschrieben ist. Es geht darum, ein unzulässiges IP-Paket nach dem RFC-791 [13] zu produzieren, welches die maximale Paketgröße von 65535 Bytes beim Wiederzusammenfügen eines fragmentierten Pakets überschreitet, und beim Client einen Bufferoverflow erzeugt. Damit wird erreicht, dass bei einem anfälligen Betriebssystem zufällige Bits im Speicher überschrieben werden können, was als Folge nichts, ein Einfrieren oder ein Neustart des Systems haben kann.

Der "Ping of Death" ist nur ein Beispiel von verschiedenen "Nuke" [3] Techniken, welche bei fehlerhafter Implementation genutzt werden können. Meistens handelt es sich aber um Speicherprobleme, welche sobald sie erkannt sind, durch einen Patch effektiv bekämpft und dauerhaft abgestellt werden können.

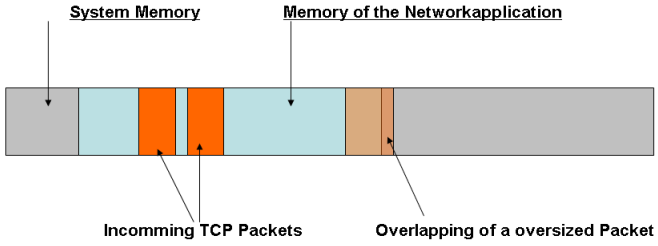

Abbildung 1. Ping of Death

2) Dauerhafter Hardwareschaden: Besonders interessant für einen Angreifer ist es auch dauerhaften Schaden anzurichten, welcher sich nicht nach dem Ende des Angriffs von alleine behebt. Im schlimmsten Fall ist sogar ein Austauschen der Hardware nötig. Permanent Denial of Service (PDoS) ist wohl am besten gegen an ein Netz angeschlosse, eingebettete Systeme, wie zum Beispiel Drucker oder Router, durchzuführen. Durch Sicherheitslücken im Fernwartungssystem, sei es durch Programmierfehler oder duch administrative Versäumnisse wie fehlende Patches oder nicht geänderte Standardpasswörter, kann sich ein Angreifer Zugang zu den Geräten verschaffen und evtl. ein fehlerhaftes Firmwareimage hochladen, welches beim nächsten Neustart dann gebootet wird.
Das Gerät ist dadurch unbrauchbar geworden. Wenn dies nun auf einem Router passiert sind alle dahinterliegende Systeme mit einem Schlag nicht mehr zu erreichen. Dieser Fehler ist einfach nicht mehr zu beheben und mit relativ geringem Aufwand zu bewerkstelligen, da nur ein einmaliger Vorgang nötig ist im Gegensatz zu anderen DoS Methoden, welche durchgehende Aktionen des Angreifers erfordern.
Vorgeführt wurde diese Art von Angriff von Rich Smith von HP Systems Security Labs auf der EUSecWest Sicherheitskonferenz [14], [15].

3) Überflutung des Opfers: Der "flood" ist die wohl meist eingesetzte Art des DoS. Es geht darum möglichst viele Pakete[4] an das Opfer zu schicken und damit zu bezwecken, dass dem Opfer irgendeine Ressource ausgeht, sei es Speicher, Bandbreite oder CPU-Leistung. Wenn das Opfer einmal mit dem illegitimen Verkehr überlastet ist, kann es berechtigte Anfragen nicht mehr bearbeiten.
Um nicht von einer wachsamen Firewall sofort ausgesperrt zu werden verwendet man zusätzlich IP-spoofing (Fälschung) indem man die versandten Pakete mit einer anderen Herkunfts-IP-Adresse versieht und somit bei dem Empfänger vortäuscht, dass das Paket von einer anderen Maschine stammt. Wegen der Struktur des Internets ist es für dem Empfänger nicht möglich die korrekte Herkunft des Pakets zu überprüfen.

- SYN flood ist ein Angriff auf der Netzwerkschicht 4 und nutzt die Statusallokation welche in TCP für jede Verbindung gebraucht wird, um den Arbeitsspeicher langsam aufzubrauchen. Das Opfer wird von SYN Paketen (initiieren den Aufbau einer Kommunikation) überflutet und sendet falls es möglich ist, zum Beispiel bei einem Webserver, ein SYN-ACK Paket und begibt sich in den Status "Wartend" bis entweder wieder ein ACK eintrifft oder ein Timeout ausläuft. Wenn man jetzt das Opfer dazu bringen kann schneller Verbindugen zu öffnen als diese wieder ablaufen, kann man erreichen dass der Arbeitsspeicher nicht mehr ausreicht um neue Verbindungen zu alloziieren und es beginnt eine Diensteverweigerung.
  Um einem solchen Angriff zumindest teilweise entgegenzuwirken, gibt es mehrere Ansätze. Einer davon sind die SYN-Cookies welche als Antwort auf ein SYN an den vermeintlichen Absender geschickt werden. Ist dieser der Reale, empfängt er dieses Cookie und kann es gekoppelt mit einem SYN-Paket erneut an den Server schicken, welcher erst zu diesem Zeitpunkt die Verbindung alloziiert [16].
  Diese Methode wird oft erst bei höherer Last auf einem Server zugeschaltet, um im normalen Verlauf keinen zusätzlichen Roundtrip zum Verbindungsaufbau zu benötigen.

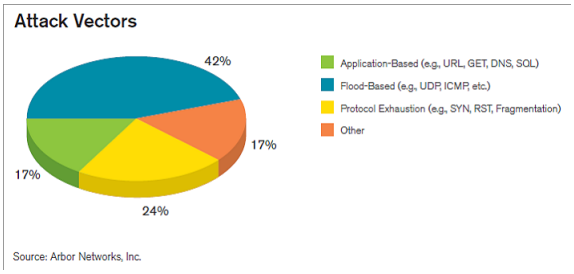

Abbildung 2. Angriffsvektoren

[3]Steht für Denial of Service.

[4]Der Pakettyp ist bei einem breit angelegten flood nicht ausschlaggebend, sei es TCP/UDP oder ICMP

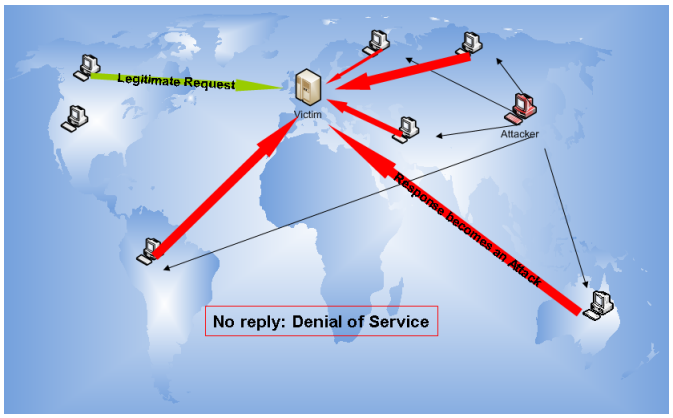

Abbildung 3. Amplifikation durch Reflektion

- CPU flood bezeichnet einen Angriff der darauf aus ist, die Rechenlast eines Knoten soweit zu erhöhen, dass er nichts mehr Sinnvolles leisten kann. Beliebte Ziele sind kryptographische Endgeräte, welche zum nachprüfen von Signaturen und Verschlüsselung erheblichen Rechenaufwand haben und somit ist diese Ressource besonders schnell aufgebraucht. Interessant kann auch je nach Bauart eines Routers dessen Überlastung sein. Durch komplizierte Fragmentierung oder geschickt manipulierte Pakete, welche dann nicht von den in Hardware implementierten Bausteinen bearbeitet werden können, kann Last auf dem begrenzten Prozessor eines Routers erzeugt werden. Zusätzlich kann bei vielen auch ein Cacheüberlauf hervorgerufen werden, da die Netzwerkinterfaces auf einen größeren Datendurchsatz ausgelegt sind, kann der Cache dieser CPU nicht ausreichen. Egal welcher Fall eintritt, der Router ist außer Gefecht gesetzt und wie vorher schon erwähnt, die hinter ihm liegenden Systeme ebenfalls.
- Clients welche nur eine sehr magere Anbindung haben, wie zum Beispiel Einwahlleitungen , kann man schon mit einem beliebigen flood mit “irgendeinem” Paket vom Netz abtrennen, weil die Leitung einfach überlastet (vorrausgesetzt man verfügt selber über genügend Bandbreite) wird und legitimer Traffic das Endgerät nicht mehr erreicht. In der Praxis ist diese Methode ohne Angriffs-Amplifikation wohl nur schwer anwendbar, weil Breitbandverbindungen immer verbreiteter werden, welche weniger anfällig sind.

B. Angriffs-Amplifikation für größere Ziele

Wenn die Leitung des Opfers nun aber größer ausgelegt ist als die Eigene, ist es natürlich wesentlich schwieriger einen effektiven Angriff durchzuführen. In diesem Fall ist es besonders nützlich, wenn man in den Weiten des Internets andere Geräte dazu überreden kann, an dem Angriff teilzunehmen.

1) Reflektion - Smurf Attack: Bei dieser Angriffsart werden wenn möglich, ein oder mehrere Subnetze dazu verwendet als Spiegel zu fungieren. Man sendet über eine Broadcastadresse[5] ein Paket an ganze Netze, welche der Amplifikation dienen, und fälscht dabei die Absenderadresse, welche nunmehr die des Opfers sein soll. In diesem Fall werden alle erreichbaren Clients in diesem Netz, welche den genutzten Dienst verwenden, eine Antwort an das Opfer schicken. Beim Schlumpf-Angriff (SmurfAttack) wird ein ICMP echo request (ping) über Broadcast an ein Netz versandt. Nebeneffekt ist die Anonymisierung des Angreifers, weil das Opfer nur die Adressen der Schlümpfe warnehmen kann.
Viele Netze sind heute dagegen imunisiert als Schlumpf für einen Angreifer aus einem externen Netz zu fungieren, da Router am Rande eines Netzes heute Broadcasts von Außen verbieten.

2) DNS-Amplifikation: Hier werden öffentlich zugängliche, rekursive[6] und antwortende DNS Server dazu missbraucht mit ihrer großen Bandbreite die Leitung des Opfers auszulasten. Dies ist möglich weil eine kleine Anfrage von wenigen Bytes eine sehr große Antwort des DNS Servers erzeugen kann. Ist diese Anfrage nun mit der gefälschten Absenderadresse des Opfers versehen, wird dieses die ganzen Antworten erhalten, was erheblich den Datendurchsatz von legitimen Paketen zum Endystem erschwert. Auch hier ist der Angreifer anonymisiert. 21% der Internetprovider haben angegeben, ihre rekursiven DNS-Server nicht vor Clients außerhalb ihres eigenen Netzes abzuschirmen [17].

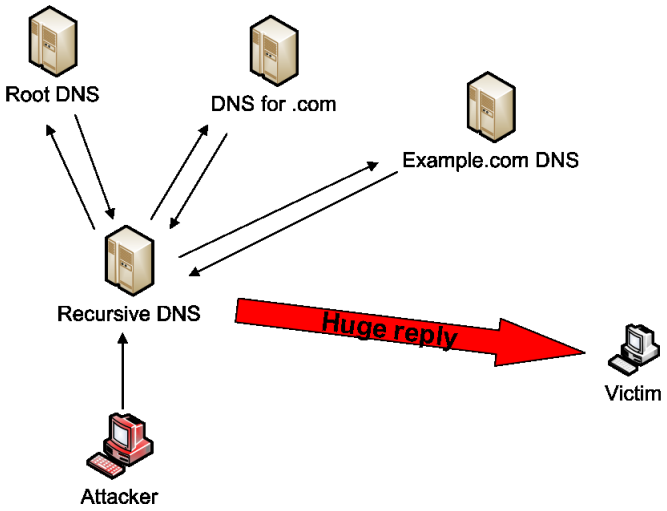

Abbildung 4. Amplifikation eines DoS durch öffentliche rekursive DNS

Wie auch bei Smurf wären durchgehend verbreitete Filter auf Providerebene, welche die Injektion von gefälschten Paketen direkt am Eingang abblocken eine wirksame Maßnahme gegen diese Angriffe [18].

[5]Höchste Adresse in einem Subnetz, oft der Art: x.y.z.255
[6]Rekursive DNS führen die Anfrage selber durch, anstatt den Client nur auf einen anderen Server hinzuweisen

C. Distributed Denial of Service

Verteidigungsmechanismen gegen vorher angesprochene DoS Techniken basieren immer darauf den bösartigen Verkehr vom legitimen zu unterscheiden und diesen frühzeitig (nahe an der Quelle, damit so wenig wie möglich Last entsteht) im Netz rauszufiltern. Besonders kompliziert wird es bei dem sogenannten Distributed Denial of Service, wenn der Angriff nicht mehr nur von einem Angreifer und einer Leitung ausgeht, sondern von einer Vielzahl an Rechnern, die sehr breit durch die ganze Welt verteilt sein können. Die von Botnetzen aufgebauten Zombiearmeen können nämlich von ihrer Art her legitimen Traffic erzeugen. Es liegt eben in der Natur eines Webservers auf Seitenanfragen zu antworten. Wenn das jetzt zehntausende Clients gleichzeitig tun, ist es nicht nachvollziehbar ob es sich dabei um einen Angriff oder einen sogenannten "flash" handelt. Wenn eine kleinere Webseite spontan an Anziehungskraft gewinnt, weil sie zum Beispiel von einem vielgelesen Portal wie Slashdot oder Heise.de verlinkt wurde, kann diese von den anstürmenden Lesern überlastet werden.

Eine in der Forschung in Erwägung gezogene Möglichkeit legitimen Traffic von illegitimen zu unterscheiden, scheint eine Methode zu sein, welche den Client auffordert eine höhere Bandbreite zu benutzen, wobei davon ausgegangen wird, dass ein Angreifer diese sowieso schon ausschöpft und seine Übertragungsrate nicht mehr erhöhen kann. Diese Anfragen würden dann ignoriert [19]. Ein konkretes Umsetzungsbeispiel scheint es noch nicht zu geben.

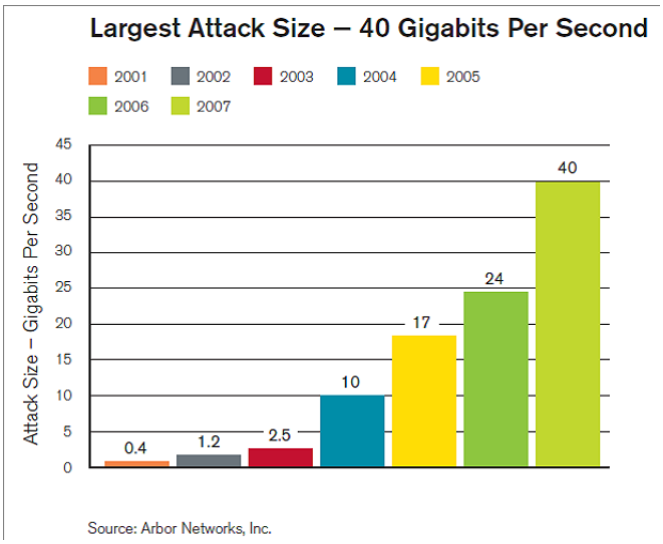

Abbildung 5. Entwicklung der stärksten Angriffe zwischen 2001 und 2007

Wenn nun die Leitung als solche überlastet ist, bringt auch solch ein Ansatz nichts mehr. Das passierte Turtle Entertainment auf der CeBit 2009 in Hannover bei ihrer Videoübertragung vom Messegelände. Wie ein persönliches Telephoninterview mit einem der beteiligten Administratoren vor Ort ergab, konnten sie wohl zuererst eine Verlangsamung ihrer 100Mbit Leitung vom Messegelände feststellen, sowie ein ansteigender Trafficload auf ihrem Monitoring. Kurz darauf brachen die Firewalls zusammen und der Messestand war Offline. Nachdem sie sich mit ihrem Provider verständigt hatten, stellt sich herraus, dass es sich um einen DDoS von ungefähr 60 bis 70 Clients aus China handelte. Diese erzeugten Spitzenlasten von 120 bis 130Mbits Traffic mit einem UPD Flooding auf Port 21 mit über 10.000 Paketen pro Sekunde. Als Gegenmaßnahme half, sich vom Provider einen neuen IP-Block geben zu lassen, was den Angriff anschließend ins Leere laufen ließ. Die Downtime betrug ungefähr 30 Minuten. Eine wirklich effiziente Verteidigung gibt es keine, ein erneuter Angriff auf den neuen IP-Block hätte sofort die selbe Auswirkung gehabt.

IV. Häufigkeit und Intensität von DoS heute

Die Präsenz solcher Angriffe im Internet steht außer Zweifel aber um das Gefahrenpotenzial genauer einschätzen zu können bräuchte man ein Monitoring aller DoS Angriffe die stattfinden. Leider scheint dies aber unmöglich und man muss auf andere Methoden zurückgreifen, um Näherungswerte zu erlangen. Backscatter-Analysis [20] scheint ein Weg zu sein, wenigstens einen Teil der DoS Techniken in ihrer Frequenz und Intensität zu erforschen.

Um ein Opfer effektiver anzugreifen und dem Angreifer bessere Anonymität zu gewährleisten kann die Quell-IP-Adresse in dem für den Angriff verwendeten Paket modifiziert worden sein. Demnach werden die Antworten des Opfers, solange dieses den Dienst nicht vollständig verweigert bei zufällig gewählten (den gespooften[7]) IP-Adressen landen. Wie groß der Anteil der Angriffe ist, welche IP-Spoofing verwenden ist leider nicht so einfach zu bestimmen.

In diesem Experiment [20] wurde auf 1/256 aller Adresses des IPv4 Addressraums nach Backscatterpaketen[8] gelauscht um so eine Idee zu bekommen wieviele Pakete dieser Art im Netz herumschwirren. Davon ausgehend können dann Hochrechnungen gemacht werden. Mögliche Informationen welche man extrahieren kann, sind das Ausmaß des Angriffs, wer ihm zum Opfer fällt (Source-IP des Backscatterpakets) und was für ein Angriffstyp verwendet wird.

Nach [20] kann diese Art von DoS Angriffen mit 2000-3000 pro Woche beziffert werden, mit einer Intensität von über 100.000 Paketen pro Sekunde, was eine immense Durchschlagkraft in sich birgt. Vorwiegend werden diese Angriffe über TCP (zu 95%) durchgeführt; an zweiter Stelle steht ICMP.

Ferner ist es wichtig zu beachten, dass dies nur ein Teil der tatsächlich verübten Angriffe darstellen kann, da diese Methode es leider nicht ermöglicht DoS-Angriffe, welche kein Backscatter erzeugen, zu erfassen.

Ein weiterer Ansatz zur Ermittlung der Gefahren welche überhaupt im Internet kursieren ist eine seit 2005 alljährliche Umfrage von Arbor Networks Inc [17]. Im Jahre 2008 wurden

[7] gefälschten
[8] Antwortpakete die wegen IP-Spoofing bei einer Zieladresse ankommen

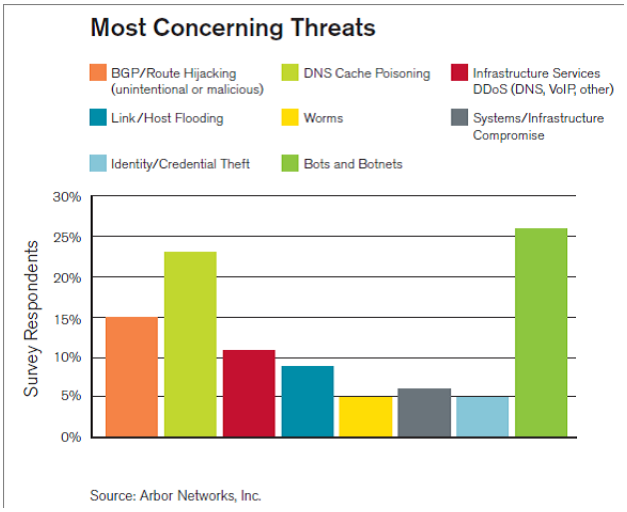

Abbildung 6. Die größten Bedrohungen

66 verschiedene ISP[9] und sonstige bedeutende Internetdienstleister zu verschiedenen Angriffen aus den letzten 12 Monaten und Gefahren aus dem Internet befragt. Wie in Abbildung 4 sichtbar wird, können neben den in dieser Arbeit angesprochenen Gefahren: "Bots and Botnets" (26%), "Infrastructure Service DDoS" (11%) und "Link/Host Flooding" (9%), alle der als kritisch eingeschätzten Bedrohungen indirekt zu einem DoS führen. Die Intensität der DoS Angriffe wird immer gewaltiger und 2008 wurde zum ersten mal die Schranke der 40 Gigabits pro Sekunde erreicht und damit der Rekord des bisher stärksten Angriffs gebrochen [17].

V. Zusammenfassung und Ausblick

In dieser Seminararbeit wurde dargestellt, was es für verschiedene Arten an Denial-of-Service Angriffen gibt und auf welchen Prinzipien sie basieren. Obwohl über die letzten zwei Jahre DoS, durch erscheinen neuer Gefahren, bei den Betreibern etwas an Wichtigkeit verloren hat [17], [21], ist die Bedrohung nicht zu unterschätzen. Es werden auch weiterhin Recherchen in Maßnahmen zur Abschwäschung dieser Angriffe benötigt werden.

[9]Internet Service provider

Literatur

[1] F. Rötzer, "Estland beschuldigt Russland des Cyberterrorismus," *Telepolis*, May 2007.

[2] B. Tittelbach, "Angriff auf Estland," in *IAIK - Kritische Infrastrukturen*, October 2008.

[3] J. A. Lewis, "Securing cyberspace for the 44th presidency," in *A Report of the CSIS Commission on Cybersecurity for the 44th Presidency*, Washington DC., december 2008.

[4] J. Swaine, "Georgia: Russia 'conducting cyber war'," *Telegraph.co.uk*, August 2008.

[5] K. Coleman, "Cyber war 2.0 – russia v. georgia," *DefenceTech*, August 2008.

[6] P. Brauch, "Geld oder Netz!" *C'T 14/04*, 2004.

[7] J. Steward, "Storm Worm DDoS Attack," February 2007, http://www.secureworks.com/research/threats/storm-worm/.

[8] ——, "The changing Storm," October 2007, http://www.secureworks.com/research/blog/index.php/2007/10/15/the-changing-storm/.

[9] K. Poulsen, "FBI busts alleged DDoS Mafia," *Security Focus*, 2004.

[10] H. Gieselmann, "Schlechte Verlierer: Xbox-Spieler setzen Gegner per DDOS außer Gefecht," February 2009, http://www.heise.de/newsticker/Schlechte-Verlierer-Xbox-Spieler-setzen-Gegner-per-DDOS-ausser-Gefecht–/meldung/133316.

[11] HostBooter4free, "XR Bio Zombie 1.6 Halo 3/More Host Booter," http://www.youtube.com/watch?v=iCbSrbg8nA8, Videoanleitung für DDoS Angriffe.

[12] M. Kenney, "Ping-of-death," *available at http://insecure.org/sploits/ping-o-death.html*, 1996.

[13] "Internet protocol, darpa internet program protocol specification," September 1981, RFC-791.

[14] R. Smith, "Phlashdance, discovering permanent denial of service attacks against embedded systems," in *EUSecWest Security conference 2008*, May 2008.

[15] K. J. Higgins, "Permanent denial-of-service attack sabotages hardware," *darkreading.com*, May 2008.

[16] T. Aura, P. Nikander, and J. Leiwo, "DOS-resistant authentication with client puzzles," in *Lecture Notes in Computer Science*. Springer-Verlag, 2000, pp. 170–177.

[17] D. McPherson, D. C. Labovitz, and M. Hollyman, "Worldwide infrastructure security report," *ARBOR Networks*, October 2008, volume IV.

[18] D. S. Paul Ferguson, "Network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing," January 1998.

[19] M. Walfish, M. Vutukuru, H. Balakrishnan, D. Karger, and S. Shenker, "Ddos defense by offense," in *ACM SIGCOMM 2006*, Pisa, Italy, September 2006.

[20] D. Moore, C. Shannon, D. Brown, G. M. Voelker, and S. Savage, "Inferring internet Denial-of-Service activity," in *Inproceedings of the USENIX Security Symposium*, 2001.

[21] D. McPherson, D. C. Labovitz, and M. Hollyman, "Worldwide infrastructure security report," *ARBOR Networks*, September 2007, volume III.