Hochschule Luzern
Technik & Architektur
Network & Services

(Distributed) Denial-of-Service Attack

Horw, 14. Januar 2013

Simon Moor | Felix Rohrer

Inhalt

Abstract

Distributed Denial of Service Attacken sind Angriffe auf ein Server oder ein Netzwerk, bei dem das Ziel aufgrund der grossen Last auf reguläre Anfragen nicht mehr Antworten kann. Während solche Angriffe Ende der 90er Jahre noch gänzlich unbekannt waren, sind sie inzwischen zu einer realen Gefahr herangewachsen, die unser tägliches Leben beeinflussen oder gar beeinträchtigen kann. Es sind heute nicht mehr nur Webseiten betroffen, auch Infrastruktursysteme, welche ans Internet angeschlossen sind, sind verletzlich geworden.

In diesem Dokument werden sowohl Angriffs- wie auch Abwehrmöglichkeiten aufgezeigt und die technischen Einzelheiten genauer erklärt.

Im Laufe der Jahre wurden viele gross angelegte DDoS-Angriffe, darunter auch einige gegen namhafte Firmen, bekannt. Die wichtigsten davon werden zusammengefasst und ihre Folgen dargelegt. Ebenso wird die nationale Strategie zur Abwehr zusammengefasst sowie die rechtliche Situation in der Schweiz dargestellt.

1 Einleitung

1.1 Was ist ein DDoS Angriff (Distributed Denial of Service Attack)

Seit den Anfängen des Internets existieren die so genannten "Denial-of-Service"-(DoS-)Angriffe. Ziel der Attacken ist die massive Einschränkung der Verfügbarkeit bestimmter Online-Systeme und / oder Dienste oder gar die komplette Verwehrung des Zugriffs. Meist wird dabei versucht, durch das Ausnutzen von Schwachstellen in Betriebssystemen, Programmen und Diensten bzw. von grundsätzlichen Entwurfsschwächen der verwendeten Netzwerkprotokolle die angegriffenen Systeme über das Internet zum Absturz zu bringen. Obwohl es verschiedene Gründe für die Nichtverfügbarkeit geben kann, spricht man von DoS in der Regel als die Folge einer Überlastung von Servern / Systemen.

Wird die Überlastung von einen grösseren Anzahl verteilter Systeme verursacht, so wird dies als „Distributed Denial of Service“-(DDos-)Angriff bezeichnet.

1.2 Motivation von DDoS-Attacken

Durch das Überlasten der Systeme kann deren eigentliche Funktionalität nicht mehr gewährleistet werden. Reine DDoS-Attacken können also nicht dazu benutzt werden um Daten zu entwenden. Die Angreifer nutzen die DDoS-Attacken um Ihre eigenen Ziele zu erreichen. Dafür gibt es verschiedene Motive:

- Ansehen in der Gruppe / Reputation: Früher wurden DoS-Attacken oft benutzt um das eigene Können zu demonstrieren. Dies hatte nicht nur den Zweck zu beweisen, dass man es kann, sondern es war zugleich auch ein Konkurrenzkampf.
- Wirtschaftliche Zwecke: Durch die Nichtverfügbarkeit von Systemen kann die Konkurrenz geschwächt oder ganz ausgeschaltet werden. Es gibt professionell tätige Hacker-Organisationen bei welchen DDoS-Attacken online bestellt und via Kreditkarte bezahlt werden können. In diesem Zusammenhang werden nicht selten Erpressungen oder Lösegeld-Forderungen ausgesprochen.
- Politische Zwecke: Eine Gruppe oder auch eine einzelne Person ist mit den Ansichten, Handeln einer Organisation nicht einverstanden und startet eine entsprechende DoS-Attacke oder ruft zu einer DDoS auf.

1.3 Prinzipielle Funktionsweise von DDoS-Attacken

Die Funktionsweise von DDoS-Attacken können in drei Kategorien aufgeteilt werden:

1. Überlastung der Bandbreite
2. Überlastung der Server / Systeme
3. Ausnutzung von Sicherheitslücken und dadurch das System zum Absturz bringen

Bei der Überlastung der Bandbreite wird gezielt das Netzwerk, die Border-Router, der Firma angegriffen. Jedes System kann nur eine begrenzte Anzahl von Datenpakete verarbeiten. Der Angreifer startet eine Attacke und überlastet das Netzwerk mit zu vielen Anfragen oder unnötigen Datenpaketen. Somit wird die ganze Bandbreite durch den Angriff in Anspruch genommen und echte Anfragen gehen verloren.

Bei einem Angriff auf ein System oder Server wird gezielt dieses System angegriffen. Die Funktionsweise ist vergleichbar wie der Angriff auf die Bandbreite. Hier wird jedoch die Eigenschaft ausgenutzt, dass ein Server nur eine bestimmte Anzahl an Verbindungen herstellen kann sowie das er für jede Anfrage, resp. Antwort Rechenzeit benötigt. Umso komplexer die Berechnungen sind, umso weniger Anfragen können gleichzeitig beantwortet werden. Der Angreifer überlastet das System, den Server mit sinnlosen oder ungültigen Abfragen so, dass echte Anfragen nicht mehr beantwortet werden können.

Wenn eine Sicherheitslücke von einem System bekannt ist, ist dies die leichteste durchzuführende Angriffsmethode. Hier werden Fehler im Programm dazu benutzt, um ein kompletten Absturz des Systems zu erreichen. Auch wenn dieser Angriff am leichtesten durchzuführen ist, so hat er den Nachteil, dass der Unterbruch eher kurzzeitig ist und nach einem Neustart des Systems dieses wieder zur Verfügung steht.

Oft werden die Angriffe auch kombiniert, speziell die Überlastung des Systems zusammen mit der Überlastung der Bandbreite.

1.4 Voraussetzung für eine DDoS-Attacke

Damit ein System anfällig für eine DDoS-Attacke ist, muss es via Internet erreichbar sein. Immer mehr SCADA[1] Systeme werden via TCP/IP in ein bestehendes Netzwerk eingebunden welches ebenfalls via Internet erreichbar ist.

Angriffe basierend auf einer DDoS-Attacke werden in der Regel über sogenannte Bot-Netzwerke initiiert. Diese bestehen aus einigen Dutzend bis zu mehreren 100‘000 mit Trojanern oder Viren infizierten Computer. Den Eigentümern dieser Computer ist es oft nicht bewusst, dass sie ein Teil eines Bot-Netzwerkes sind. Die Bot-Netzwerke werden durch die Tatsache begünstigt, dass immer mehr Breitbandnetze vorhanden und die Computer daran angeschlossen sind. Dadurch werden weniger Computer benötigt um die gleiche Bandbreite auszulasten. Die infizierten Computer sind weltweit verteilt (Siehe Abb. 1).

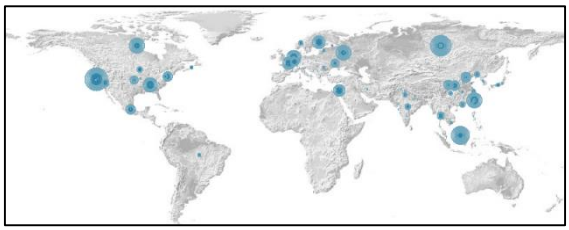

Abb. 1: Global aktive Botnet-Quellen (Quelle: Arbor Networks)

[1] Unter SCADA (Supervisory Control and Data Acquisition) ersteht man das Überwachen und Steuern technischer Prozesse mittels eines Computer-Systems.

2 Verschiedene Angriffsmethoden

2.1 UDP Flood

Das User Datagram Protocol (UDP) ist ein verbindungsloses Protokoll. Daten können ohne einen Verbindungsaufbau übertragen werden. Bei einem UDP-Flood Angriff schickt der Angreifer dem Zielsystem an einen zufällig gewählten Port ein UDP-Packet. Das Zielsystem versucht herauszufinden welche Anwendung auf diesen Port wartet. Sollte keine Applikation diesen UDP-Port benützen, sendet es ein ICMP-Packet (Destination Unreachable) an die (evt. gefälschte) Absenderadresse. Werden genügend viele UDP-Pakete an ein Zielsystem geschickt, kann dies zu einer Überlastung oder Absturz des Zielsystems führen (Cert CA-1996-01, 1997).

2.2 TCP Flood

Bei einer TCP-Flood Attacke wird das Verhalten des Dreiwege-Handshake von einem TCP Verbindungsaufbau ausgenutzt. Bei einem normalen Verbindungsaufbau wird vom Client zum Server ein „SYN“-Paket geschickt. Der Server beantwortet dieses mit einem „SYN-ACK“-Paket, worauf wiederum der Client dem Server die Verbindung mit einem „ACK“-Paket bestätigt (Vgl. Abb. 2). Bei einer TCP-Flood Attacke wird das letzte „ACK“-Packet nicht geschickt und der Server behält die Verbindung bei sich offen und wartet auf die Bestätigung (Vgl. Abb. 3). Der Server wird mit Verbindungsanfragen überhäuft und behält die Anfragen bei sich im Speicher. Dadurch kommt es zu einer Überlastung der Ressource des Servers, sowie kann er dadurch keine neue Verbindungen mehr annehmen. Zusätzlich kommt hinzu, dass ein TCP SYN-Paket mit wenig Aufwand generiert werden kann und wenig Bandbreite in Anspruch nimmt, für den Server jedoch viel Last erzeugt und entsprechend viel Ressourcen benötigt (Cert CA-1996-21, 2000).

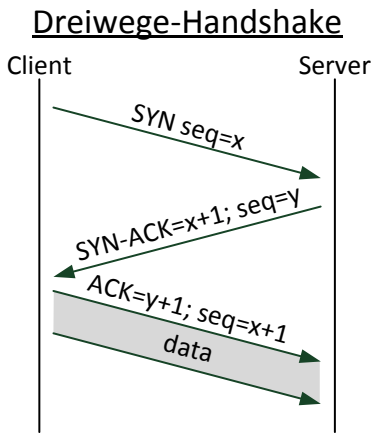

Abb. 2: Dreiwege-Handshake

(Nach RFC 793)

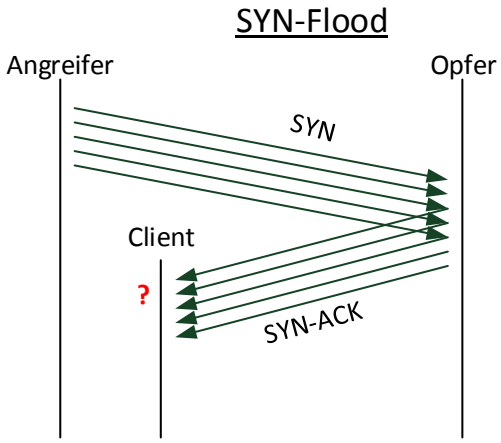

Abb. 3: SYN-Flood Attacke mit IP Spoofing

2.3 ICMP Flood

Bei einer ICMP Flood Attacke schickt der Angreifer ein Ping-Paket (ICMP Echo Request) an einen Broadcast-Adresse. Als Absender wird die IP Adresse des anzugreifenden Computers gefälscht. Der Router vom Ziel-Netzwerk leitet die Anfragen an alle Geräte in diesem Netz weiter. Dadurch antworten alle angeschlossenen Geräte im Netzwerk und schicken den Echo Replay an die gefälschte Absender Adresse.

Je nach Anzahl der Clients kann der Angreifer auf diese Art mit nur einem ICMP-Paket eine hohe Anzahl von Antworten an das Opfer erzeugen. Durch die Verstärkung kann ein Angreifer seine zur Verfügung stehende Bandbreite vervielfacht auf das Opfer richten. Durch die vielen Anfragen, resp. Antworten wird der Computer des Opfers überlastet und kann nicht mehr auf die restlichen Netzwerkanfragen antworten.

2.4 Reflected DDoS-Attacke / DRDoS

Bei einem Reflected (Distributed) DoS Angriff werden die Datenpakete nicht direkt an das Opfer gesendet, sondern an regulär arbeitende Internet-Dienste. Durch die gefälschte Absenderadresse wird die Antwort nun an das Opfer geschickt. Die Antworten auf diese Anfragen stellen dann für das Opfer den eigentlichen DDoS-Angriff dar. Durch diese Vorgehensweise ist der Ursprung des Angriffs für den Angegriffenen nicht mehr direkt ermittelbar.

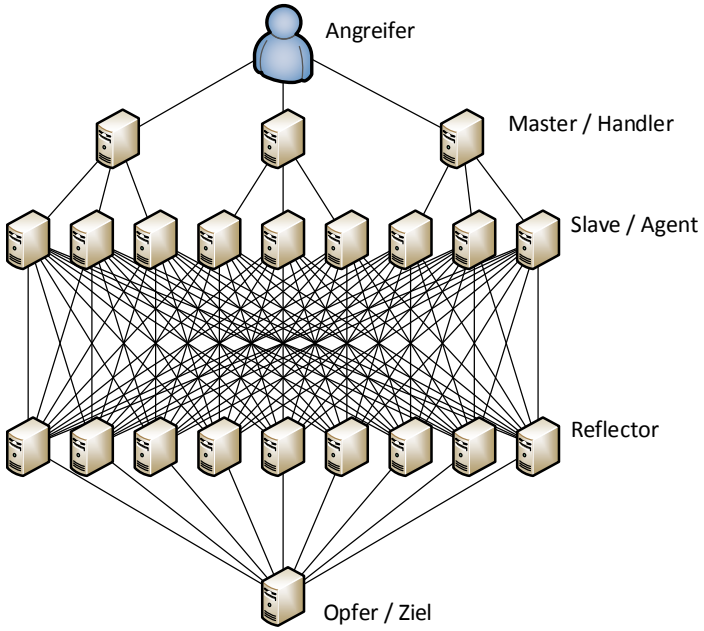

Abb. 4: Angriffsnetzwerk führt eine DRDoS Attacke aus

3 Angriffs-Strategie

3.1 Benötigte Software

DDoS Angriffe lassen sich mit Hilfe von zahlreichen Tools relativ einfach organisieren und durchführen. Im Jahr 1999 wurden ein paar solche Software-Tools publik. Die Tools waren unter dem Namen „Trinoo“ oder „Tribe Flood Network (TFN)“ bekannt. Bereits damals wurde auf eine Client-Server Architektur aufgebaut. Heute laufen alle Bot-Netzwerke nur noch mittels Command & Control Servern. Die Tools wurden immer weiter entwickelt. „Stacheldraht“ z.B. vereinigt Funktionen aus Trinoo und TFN. Diese Tools wurden für die Steuerung der Angriffe benutzt. Sie besassen noch keine eigene Routine um weitere Client (Agenten) zu infizieren und das Bot-Netzwerk zu erweitern.

3.1.1 LOIC – Low Orbit Ion Cannon

Nicht immer werden Computer welche mittels Viren resp. Trojaner verseucht sind für eine DDoS Attacke benutzt. Das Tool LOIC – Low Orbit Ion Cannon wurde ursprünglich als Netzwerk-Lasttest Software entwickelt. Die ursprüngliche Version wurde von weiteren Programmieren so angepasst und erweitert, dass sie sich via IRC fernsteuern lässt. Die Software musste selbständig heruntergeladen werden, sowie der entsprechende IRC-Server und Channel eingetragen werden. Die teilnehmenden User können sich dadurch freiwillig zu einem grossen Bot-Netzwerk zusammenschliessen und an einer Attacke mitwirken.

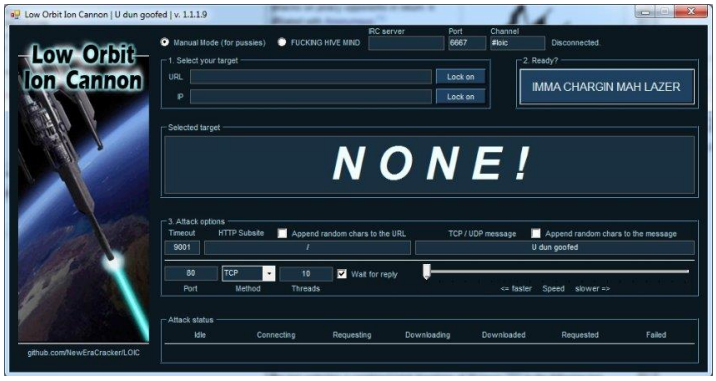

Abb. 5: LOIC – Low Orbit Ion Cannon

3.2 Bot-Netzwerk

Ein Botnet oder Botnetz, resp. Bot-Netzwerk ist eine Gruppe von Computer die mit einem Software Bot infiziert sind. Die Betreiber der Botnetze installieren die Bots ohne Wissen der Inhaber auf Computern und nutzen sie für ihre eigenen Zwecke. Die meisten Bots können von einem Botnetz-Operator über einen Kommunikationskanal überwacht und ferngesteuert werden.

Je nach Bot stehen verschiedene Möglichkeiten zur Verfügung. Aktuelle Bots besitzen die Möglichkeit, nachträglich weitere Programm-Module nachzuladen und sich so entsprechend anzupassen und neue, weitere Aufgaben übernehmen.

Grundsätzlich lassen sich die Verwendungsmöglichkeiten eines Bot-Netzwerkes auf folgende sechs Bereiche aufteilen: Proxy, SPAM, DDoS- / (D)RDoS-Attacken, Klickbetrug, Sniffer und Speicher für illegalen Content.

Für die Command & Control Technologien waren in den 90er Jahren primär IRC-Server zum Einsatz gekommen. IRC erlaubt die Full-Duplex Kommunikation, sowie können mehrere IRC-Server zu einem Verbund zusammengeschlossen werden. Damit die Adressen der IRC-Server nicht hardcoded im Bot stehen müssen, wird DNS verwendet. Das Bot-Netz wird auf mehrere Domain-Namen aufgeteilt, das ganze wird Multihomed betrieben. Durch diese Anpassung konnte die Verfügbarkeit der C&C-Server weiter gesteigert werden. Aktuell basieren die meisten Botnetze auf Webbasierten C&C-Servern. Eine Webbasierte Oberfläche ist sehr einfach zu bedienen und kann entsprechend mit dem Back-End kommunizieren. Die Kommunikation über HTTP hat zusätzlich den Vorteil, dass der Traffic weniger auffällt und die entsprechenden Ports auf den Firewalls geöffnet sind. Die Bots registrieren sich beim Server und dieser baut bei Bedarf die Verbindung zu den Bots auf. Dies verringert den Datenverkehr zwischen dem C&C-Server und dem Bot. Dadurch sinkt die Chance ein Bot in einem Netzwerk zu erkennen. Ein einzelner Webserver ist in der Lage mehrere hunderttausende bis Millionen Bots zu verwalten. Einige Botnetze sind intern auch als P2P-Netze aufgebaut. So kann jeder Bot als Client wie auch als Server funktionieren.

3.2.1 Schattenwirtschaft Botnetze

Ein Botnetz zu Betreiben kostet Zeit und Geld. Damit dies gewinnbringend betrieben werden kann, wird ein Botnetz aufgebaut und dann entweder verkauft oder vermietet. In vielen Untergrund-Foren wird offen für die Vermietung von Botnetzen geworden. Je nach Grösse und Anforderungen an das Botnet sind die Preise unterschiedlich. Bereits ab 50 Dollar kann ein Botnetz mit ca. 1‘000 Bots für 24 Stunden gemietet werden, welches dann für DDoS-Attacken verwendet werden darf. Für einen ungesicherten, normalen Webserver genügen selbst weniger Bots um den Server zu überlasten. Nach Angaben von shadowserver.org gab es im Jahr 2008 zirka 190.000 DDoS-Attacken, mit denen Cyberkriminelle rund 20 Millionen Dollar verdient haben (Namestnikov, 2009).

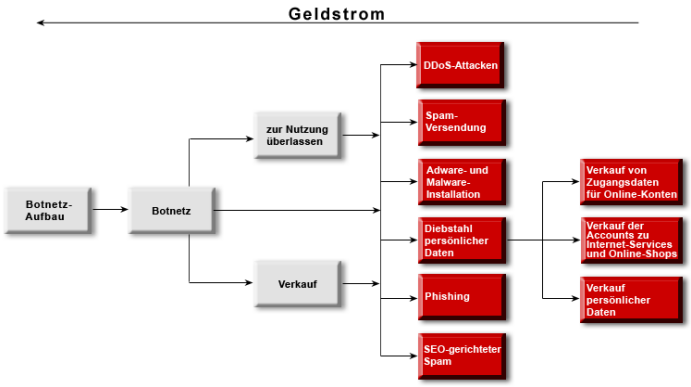

Abb. 6: Geschäfte mit Botnetzen (Quelle: http://www.viruslist.com/de/analysis?pubid=200883656)

3.3 Benötigte Bandbreite

Untersuchungen von Kasperky Lab ergaben, dass die durchschnittliche Bandbreite von DDoS-Attacken im zweiten Halbjahr 2011 110 Mbit/sec war. Die maximale Bandbreite betrug 600 Mbit/sec, mit 1‘100‘000 packets/sec bei einer UDP-Flood Attacke mit einer Packet Grösse von 64 bytes.

Im zweiten Halbjahr 2011 wurden 384 DDoS-Attacken erkannt. Die längste Attacke dauerte 80 Tage, 19 Stunden, 13 Minuten und 5 Sekunden, das Ziel war eine Reise-Webseite. Die durchschnittliche Dauer betrug 9 Stunden und 29 Minuten (Kaspersky Lab, 2012).

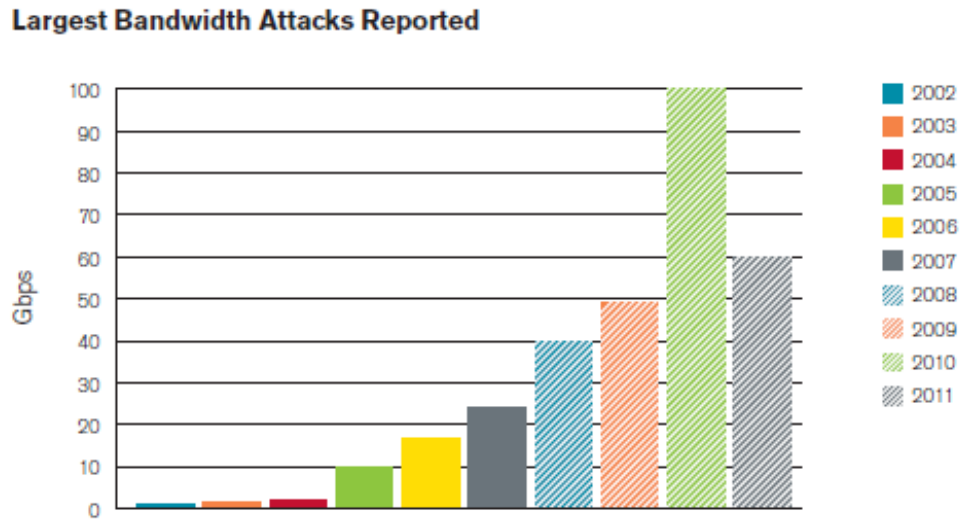

Abb. 7: Largest Bandwidth Attacks Reported (Arbor SERT, 2011).

Arbor Networks kommt in seinem „Worldwide Infrastructure Security Report 2011 Volume VII“ zum Schluss, dass DDoS-Angriffe auf Unternehmen weltweit deutlich zunehmen. Der Report basiert unter anderem auf den Angaben von Netzwerk- oder Sicherheitstechnikern von weltweit 114 Service- und Breitband-Providern. Die Frequenz von Angriffen ist laut diesen Befragungen nach wie vor steigend: 91 Prozent der teilnehmenden Unternehmen verzeichneten mindestens einen Angriff pro Monat, 44 Prozent bis zu zehn und 20 Prozent sogar mehr als 50 Angriffe monatlich. Zweidrittel aller Angriffe auf Netzwerke sind DDoS-Angriffe. Dabei werden Attacken mit grossen Volumina zur Regel: 40 Prozent der analysierten Angriffe hatten Bandbreiten von mehr als einem GBit/s und 13 Prozent über 10 GBit/s. 25 Prozent aller Angriffe überschritten sogar die gesamte Bandbreite der betroffenen Rechenzentren. Der grösste analysierte DDoS-Angriff besass eine Bandbreite von 60 GBit/s. Bei rund 40 Prozent aller Angriffe versagten die nachgeschalteten Firewalls und IPS-Systeme (Arbor SERT, 2011).

4 Abwehrmassnahmen

4.1 Präventive Massnahmen

VeriSign führt in ihrem Whitepaper verschiedene „Best Practices“ auf, mit denen Unternehmen ihre Server vor gezielten Angriffen schützen können (VeriSign, 2012):

- Datensammlung zentralisieren und Trends verstehen:
  Man muss den „normalen“ Traffic kennen, um Abweichungen schnell und präzise identifizieren zu können. Durch die Zusammenarbeit mit erfahrenen Sicherheitsexperten können Unternehmen Trends und Bedrohungen besser erkennen. Sie können wirksame Systeme zur Warnung, Abwehr und zur Aufzeichnung von DDoS-Attacken einführen.
- Klare Abwehrstrategie definieren:
  Eine schnelle und wirksame Reaktion ist wichtig zur Abwehr von DDoS-Attacken. Deshalb brauchen Unternehmen klar definierte Prozesse und Methoden wie zum Beispiel die präventive Festlegung eines Eingriffsteams und die Vorbereitung auf mögliche Ausfallzeiten. So kann der Betrieb schneller und mit geringerem Schaden wiederhergestellt werden.
- Mehrschichtige Filter nutzen:
  Wenn unerwünschter Datenverkehr blockiert wird, muss der reguläre Traffic dennoch ungestört weiterlaufen können. Einige Angriffe können durch die Implementierung von Filtern auf der Netzwerkebene abgewehrt werden, komplexe Attacken müssen bis zur Anwendungsschicht analysiert und gefiltert werden.
- Flexibilität und Skalierbarkeit einplanen:
  Eine skalierbare, flexible Infrastruktur hilft sicherzustellen, dass Systeme auch während einer Attacke einwandfrei funktionieren. IT-Manager sollten die Grenzen von IT-Komponenten testen, um ihre Schwachstellen zu kennen. Es ist besser, auf verschiedene Hard- und Softwaresysteme zu setzen, damit der Angriff auf eine Plattform nicht das gesamte Netzwerk lahm legt. Und darüber hinaus sind alle möglichen Massnahmen umzusetzen, die per Lastverteilung innerhalb der Infrastruktur die On-Demand-Kapazitäten absichern.
- Anwendungs- und Konfigurationsprobleme ansprechen:
  DDoS-Attacken haben sich von Brute-Force-Angriffen hin zu Methoden zur unterschwelligen Infiltration der Anwenderschicht entwickelt. Deshalb benötigen Unternehmen einen besseren Einblick in Anwendungen und ihre Schwachstellen.

4.2 Netzwerk technische Möglichkeiten zur Abwehr

- Es gibt verschiedene technische Möglichkeiten zur Abwehr von DDoS:
  - Auf der Ebene der Serversoftware z.B. das Apache Modul "mod_dosevasive", welches sich speziell gegen HTTP-DDoS und Brute-ForceAttacken richtet, oder das Apache Modul "mod_security", welches nützlich ist, um Anfragen nach bestimmten Kriterien zu filtern. So werden gefilterte Anfragen gar nicht verarbeitet. Dies hat den Nachteil, dass die Anfragen jedoch durch alle Netzwerkkomponenten, das Betriebssystem und Teile der Serversoftware durchgereicht werden.
  - Um Anfragen früher zu blocken, empfiehlt sich eine gute Firewall, z.B. iptables. Diese blockt die Anfragen bereits vor der Serversoftware und entlastet sie dementsprechend.
  - Noch früher greift eine Hardware Firewall ein, ein Gerät das speziell zu diesem Zweck gebaut wurde und welches unabhängig vom Server betrieben wird.
  - Es gibt auch spezielle Hardware für die erweiterte Abwehr von Attacken aller Art (IDS Intrusion Detection System, IPS Intrusion Prevention System)
- QoS (Quality of Service) einsetzen: Mit QoS werden IP-Pakete markiert und können so in verschiedene Klassen eingeteilt werden. Ein Netzwerkgerät kennt dann den Inhalt des Pakets und kann dieses prioritär behandeln oder eben zurückstellen. Dies wird häufig in Kombination mit Voice over IP benutzt, wo die Sprachpakete zuerst übertragen werden müssen. Andere Dienste werden dann mit kleinerer Priorität behandelt. QoS dient ebenfalls zur Abwehr von DDoS Attacken. Der normale Netzwerkverkehr wird laufend gemessen, und wenn plötzlich von einer Quelle mehr Datenverkehr auftaucht so wird dieser als weniger wichtig angeschaut oder sogar verworfen. Auch kann der Zugang über ein Management Interface sichergestellt werden, so dass Administratoren jederzeit eingreifen können.
- Mit einem SYN Proxy werden alle Anfragen über einen Proxyserver vermittelt. Dieser überwacht den Netzwerkverkehr und verwirft die Verbindung, wenn der Client nicht mit einem ACK antwortet. Dies verhindert das „SYN flood“
- Die Anzahl neuer Verbindungen sollten beschränkt werden. Werden in zu kurzer Zeit zu viele neue Verbindungen erstellt, werden diese geblockt. Sind zu viele aktive Verbindungen im Speicher, muss die Software entsprechend konfiguriert werden diese früher zu trennen (Agressive Idle Aging)
- Mittels Dark Address Prevention werden alle IP-Adressen geblockt, die noch nicht von der IANA verteilt wurden. Traffic von solchen Adressen deutet allgemein auf IP-Spoofing und somit auf Angreifen hin.

- Gibt es mehrere Rechenzentren, so können diese mittels Anycast verbunden werden. Alle Rechenzentren verfügen dann über die gleichen IP-Adressen und der Netzwerkverkehr wird jeweils nur zum nächsten Zentrum geleitet. Für den Endbenutzer ist dieses System transparent und nicht sichtbar, man kann jedoch so die Last vermindern und auch die Antwortzeiten optimieren, da beispielsweise Anfragen aus Amerika auch in Amerika beantwortet werden, während Anfragen aus Europa niemals nach Amerika gelangen werden und aus einem näheren Rechenzentrum beantwortet werden.

4.3 Allgemeine Abwehr von DDoS

Es gibt auch allgemeine Punkte, die beachtet werden sollten:

- Genügens Systemressourcen einplanen, so dass das System auch unter grosser Last noch gut arbeiten kann.
- Firewallregeln mit Sperrlisten abgleichen, um so gefährliche IP-Adressen direkt auszusperren. Dies hilft jedoch nur bei bekannten Angreifern. Bei Botnetzen, die aus PCs von überall her bestehen, nützen diese Sperrlisten wenig bis nichts. Spätestens mit IPv6 wird dieser Punkt seine Relevanz verlieren, da dann zu viele IP-Adressen verfügbar sind.
- Eine dynamische Filterung z.B. nach Datenmenge pro Zeit aktivieren. Dies kann jedoch Probleme verursachen, wenn ein Proxy-Server geblockt wird, da sich viele Clients über diesen verbinden. In gewissen Ländern ist aus Zensurgründen nur eine Verbindung über eine staatlich kontrollierte Stelle möglich, dort würde dann das gesamte Land „abgetrennt“.
- DDoS-Mitigation: Datenverkehr bereits beim Provider filtern lassen, bevor dieser in die eigenen Netze eindringt. Dies hat den Vorteil, dass man im eigenen Netzwerk weniger Ressourcen aufbringen muss, um das Netzwerk zu schützen. Zudem hat der Provider durch andere Kunden mehr Erfahrung und kann eine Attacke eventuell schneller erkennen bzw. abwehren. Es gibt sehr viele Anbieter in diesem Bereich, auch Swisscom hat für ihre Geschäftskunden ein entsprechendes Angebot.
- Wenn die Attacke bereits läuft, sollte man die IP-Adressen(n) der Angreifer in der Firewall sperren, um die Pakete direkt verwerfen zu lassen. So wird der bombardierte Server entlastet.
- Ist dies nicht möglich, sollte man den gesamten Server vom Netz nehmen bzw. den Traffic auf einem Router mittels Blackholing verwerfen (weiter routen an nicht existentes Netzwerkinterface) und danach dem Server eine neue IP Adresse zuteilen. Neue Besucher kriegen durch die DNS Abfrage dann die neue Adresse als Antwort und man gewinnt Zeit für die Optimierung.

4.4 DDoS Attack Mitigation Appliance

Verschiedene grosse Firewall Hersteller haben auch spezielle Appliance im Angebot für die Abwehr von Netzwerk Attacken. Das Intrusion Detection System (IDS) ist ein System zur Erkennung von Angriffen. Das IDS kann eine Firewall ergänzen oder auch direkt auf dem zu überwachenden Computersystem laufen und so die Sicherheit von Netzwerken erhöhen. Wie der Name sagt ist es jedoch nur ein Erkennungssystem und nicht in der Lage den Angriff abzuwehren. Die zweite Generation der Geräte ist in der Lage, nicht nur einen Angriff zu erkennen, sondern diesen auch abzuwehren. Die Intrusion-Prevention-Systeme (IPS) überwachen den Netzwerkverkehr und analysieren die Übertragung auf Protokollebene und suchen dabei nach eventuellen Angriffsmusstern.

IPS Geräte sind jedoch nicht in der Lage DDoS Attacken zu filtern, dafür wurden nun Erweiterungen für die IPS und spezielle DDoS-Defense Systeme von den Herstellern entwickelt. Diese Arbeiten auf Layer-2 als Transparent Forwarding und können somit einfach in bestehende Umgebungen eingebaut werden.

Abb. 8:Check Point DDoS Protector (Check Point, 2012)

Die angebotenen Geräte unterscheiden sich anhand des jeweiligen Throughput, Latency, Max Concurrent Sessions sowie der Max Session Setup/Teardown Werte. Einzelne Hersteller weisen zusätzlich die Max SYN Flood DoS Protection Rate aus, diese ist in der Regel um Faktor 10 bis 25 grösser als die Session Setup/Teardown Rate. Technisch bedingt unterscheiden sich die Geräte auch in den Verfügbaren Anschlüsse. Je nach Throughput werden nicht nur Kupfer Ethernet verwendet, sondern auch Gigabit Ethernet mit SFP resp. 10 Gigabit SFP+ r oder XFP Ports.

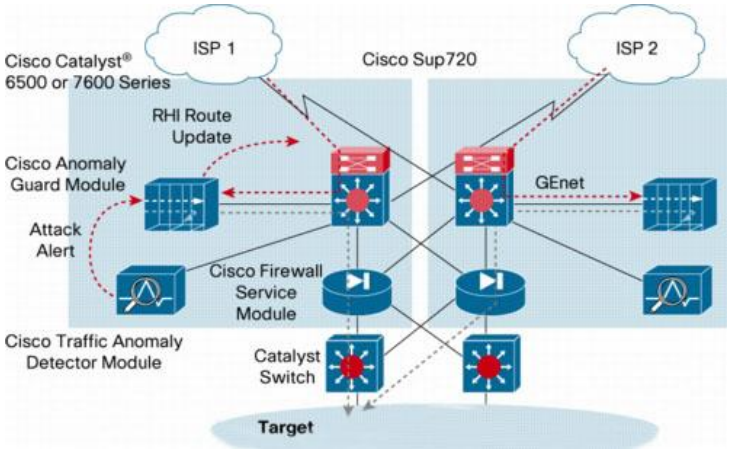

Abb. 9: DDoS Anomaly Detection and Mitigation (Cisco, 2012)

Cisco hat ein „Anomaly Guard Module“ im Agebot welches bei Cisco Catalyst 6500 Series Switches oder Cisco 7600 Series Router eingebaut werden kann.

Zusammen mit einem „Traffic Anomaly Detector Module“ können DDoS Attacken erkannt und dynamisch darauf werden.

Durch die Analyse des Layers-7 können die Filter auch in einem bestehenden Traffic-Flow die ungewünschten Anfragen herausfiltern.

5 Historische DDoS-Attacken

5.1 Erwähnenswerte Angriffe

Nebst unzähligen kleineren Angriffen gibt es einige grössere und auch in den Medien bekannt gemachte Angriffe.

- Februar 2000:
  Amazon.com, Buy.com, ZDNet.com, E-Trade.com, eBay.com, CNN.com wurden lahmgelegt. Auslöser war Michael Demon Calce, ein Student aus Quebec, Kanada. Er wollte sich und seine Hackergruppe TNT im Internet bekannt machen. Dies ist zugleich auch die erste grosse DDoS Attacke und hat Medien wie auch IT-Administratoren auf das Thema sensibilisiert. Bis anhin waren solche Attacken unbekannt und in keiner IT-Strategie eingeplant. (BBC, 2000)

- Juni 2001:
  Im Juni 2001 fand eine Online-Demonstration gegen Lufthansa statt. Die Lufthansa Webseite (www.lufthansa.com) war während zwei Stunden blockiert. Die Aktion fand im Rahmen der antirassistischen Deportation.class-Kampagne statt, welche die Beteiligung von Fluggesellschaften an staatlichen Abschiebungen durch vielfältige Aktionsformen kritisierte. Da die Initianten den Angriff im Voraus angekündigt haben, erhielten sie ein riesiges Medienecho und konnten ihr Anliegen dort bereits mehrfach vortragen. Nach diversen Hausdurchsuchungen wurde der Hauptinitiant angeklagt, später jedoch freigesprochen. (Netzpolitik, 2010)

- Oktober 2002:
  Ein Angriff auf die Root DNS Server hatte das Ziel, „das Internet lahmzulegen“. Ohne DNS-Auflösung kann eine Domain nicht mehr auf die dazugehörige IP-Adresse aufgelöst werden. Während 75 Minuten wurden die Server mit zusammen 900Mbit/s angegriffen. Die Firewalls verwarfen die Pakete und die Server liefen alle weiter. Verursacht durch den grossen Netzwerkverkehr waren die Server teilweise jedoch schlecht oder gar nicht erreichbar. Dies hatte keinen grossen Einfluss auf den normalen Internetbetrieb, da DNS Records von anderen Servern, z.B. beim eigenen ISP, zwischengespeichert werden. Viele Anwender haben von den Problemen gar nichts mitbekommen. Wäre diese Attacke jedoch über eine längere Zeit aktiv gewesen und hätte alle Server lahmgelegt, so hätte dies weltweit grossen Einfluss gehabt. Ohne funktionierende Internetverbindung ist ein Grossteil der Infrastruktur in westlichen Ländern nicht mehr funktionstüchtig. (ISC, 2002)

- Dezember 2010:

  postfinance.ch wurde angegriffen, weil die Postfinance das Konto von Julian Assange (Chef Wikileaks) gesperrt hatte, nachdem WikiLeaks Depeschen US-amerikanischer Botschaften veröffentlichte. Für diesen Angriff wurde die LOIC – Low Orbit Ion Cannon Software verwendet. Weiter waren die Websites der Kreditkartenunternehmen Mastercard und Visa Ziel von Angriffen. Auch thepaypalblog.com war von einem achtstündigen Ausfall betroffen, da ebenfalls ein PayPal Spendenkonto von Assange gesperrt wurde. Gegen Ende des Monats wurde aus den gleichen Gründen zusätzlich noch die Website der Bank of America beeinträchtigt. Dieser Angriff war ebenfalls mehrere Stunden davor über Twitter angekündigt worden. Im Anschluss an den Angriff wurden mehrere Festnahmen getätigt, darunter auch einen 16- und einen 19-Jährigen aus den Niederlanden. (Maron, HJ., 2010)

Abb. 10: DDoS Ankündigung via Twitter (Quelle: haymarket.net.au)

- Oktober 2012:

  Webseiten der Regierung, des Polizeigeheimdiensts Säpo sowie der Zentralbank Schwedens wurden lahmgelegt. Weiter waren diverse Server der Nachrichtenagentur TT, der Bank Swedbank, der Bahngesellschaft SJ sowie des Militärs betroffen. Die Angriffe erfolgten als Protest gegen das Vorgehen der schwedischen Justiz gegen Filesharing-Plattformen. Diese führte kurz davor Razzien bei einem ehemaligen Hoster von WikiLeaks sowie PirateBay (grösste Filesharing Platform der Welt) durch. (Heise, 2012)

5.2 Neuartige Angriffsstrategien

Anfangs der 90er Jahre war DDoS noch nicht bekannt, heute ist dies zu einem wichtigen Punkt bei der Absicherung eines Netzes geworden. Während zu Beginn die Software noch innerhalb einer Aktivistengruppe manuell verteilt wurde, wird diese heute nur noch unbeabsichtigt als Trojaner oder „Software-Bundle“ installiert. Insbesondere im aktuellen Jahr 2012 haben die Attacken erneut stark zugenommen, und auch die Ziele werden vielfältiger. Während früher in die Bank eingebrochen wurde, wird heute die Bank digital ausgeraubt und das Geld transferiert. Durch umfangreiche DDoS Attacken könnte man den Geldfluss (Kreditkarten, Debitkarten, Überweisungen) und die Börse innert kürzester Zeit lahmlegen und so einen enormen wirtschaftlichen Schaden anrichten.

Mit dem „Internet of things“, wo nahezu jedes Gerät ans Internet angeschlossen wird, gibt es neuartige Angriffskonzepte. Es hat viele Vorteile, wenn integrierte Systeme aus der Ferne wartbar sind, jedoch öffnet dies die Tore für Angreifer. Dabei spielt es keine Rolle, ob in die zentrale Steuerung eines Systems eingebrochen wird oder ob z.B. Sensorwerte manipuliert werden, die zu einer Fehlreaktion des Systems führen.

Die Anwendungsmöglichkeiten in diesem Bereich sind vielfältig und eine vollzählige Auflistung unmöglich. Durch unterschiedliche Angriffe kann ein unterschiedlich starker Schaden angerichtet werden: Wenn bei einem Verkehrsleitsystem alle Ampeln einer Stadt auf Rot gestellt werden, wird es wohl ein Chaos geben, jedoch kaum Verletzte. Man könnte aber auch Personenleitsysteme manipulieren, die in einem Notfall schnell vielen Leuten den schnellsten Weg aus einem Tunnel oder einem grossen Gebäude zeigen sollen, jedoch dann die Menschen einschliessen oder direkt ins Unheil führen.

Schlimmer wäre dieses Szenario: Eine manipulierte Steuerung eines Atomkraftwerks könnte einen Supergau auslösen und über ein grosses Gebiet viele Menschen töten und ein Leben verunmöglichen.

6 Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken

Cyber Defense stellt eine neue sicherheitspolitische Herausforderung sowohl für unser Land wie auch global dar. Obwohl die Schweiz die Situation längst erkannt hat, sind die bisher hervorgebrachten Lösungen der raschen Entwicklung der Bedrohung nicht mehr gewachsen. Am 10. Dezember 2010 hat der Bundesrat einen Projektleiter Cyber Defense beauftragt, bis Ende 2011 eine nationale Cyber Defense Strategie zu entwickeln.

Am 27. Juni 2012 hat der Bundesrat die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken gutgeheissen. Der Bundesrat sprach sich unter anderem für eine personelle Verstärkung von MELANI im EFD und VBS ab 2013 aus. Mit der vorliegenden Strategie wird auch mehreren parlamentarischen Vorstössen Rechnung getragen, in denen verstärkte Massnahmen gegen Cyber-Risiken gefordert wurden. (admin.ch, 2012)

6.1 Die Ziele des Bundesrates

Der Bundesrat verfolgt dabei die folgenden strategischen Ziele:

- „die frühzeitige Erkennung der Bedrohungen und Gefahren im Cyber-Bereich,
- die Erhöhung der Widerstandsfähigkeit von kritischen Infrastrukturen,
- die wirksame Reduktion von Cyber-Risiken, insbesondere Cyber-Kriminalität, Cyber-Spionage und Cyber-Sabotage.“ (Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken, 2012).

Die Strategie bezeichnet die verantwortlichen Bundesstellen, welche 16 in der Strategie genannte Massnahmen im Rahmen ihres Grundauftrags bis Ende 2017 umsetzen. In diesen Umsetzungsprozess sollen Partner aus Behörden, Wirtschaft und Gesellschaft einbezogen werden. Eine Koordinationsstelle im EFD überprüft dabei die Umsetzung der Massnahmen und den Bedarf nach weiteren Vorkehrungen zur Risikominimierung.

Die nationale Zusammenarbeit zwischen der Wirtschaft und den Behörden sowie die Kooperation mit dem Ausland bleibt dabei die Voraussetzung, um Cyber-Risiken minimieren zu können. Mit einem permanenten gegenseitigen Informationsaustausch sollen Transparenz und Vertrauen geschaffen werden. Der Staat soll nur eingreifen, wenn öffentliche Interessen auf dem Spiel stehen oder er im Sinne der Subsidiarität handelt.

Der Umgang mit Cyber-Risiken soll gemäss der Strategie als Teil eines integralen Geschäfts-, Produktions- oder Verwaltungsprozesses verstanden werden, bei dem alle Akteure – von der technischen bis hin zur Führungsstufe – einzubeziehen sind. Jede Organisationseinheit aus Politik, Wirtschaft und Gesellschaft trägt die Verantwortung, die Cyber-Ausprägung ihrer Aufgaben und Verantwortlichkeiten zu erkennen und die damit einhergehenden Risiken in ihren jeweiligen Prozessen zu adressieren respektive soweit machbar zu reduzieren. Die dezentralen Strukturen in Verwaltung und Wirtschaft sollen für diese Aufgaben gestärkt und bereits bestehende Ressourcen und Prozesse konsequent genutzt werden. Die

fortlaufende Zusammenführung von technischen und nicht technischen Informationen ist notwendig, um Cyber-Risiken umfassend zu analysieren und zu bewerten. Diese Erkenntnisse sollen möglichst zentral aufbereitet und bedarfsgerecht an die Akteure zur Unterstützung ihrer Risikomanagementprozesse weitergegeben werden.

6.2 Integration von Cyber-Risiken in bestehende Risikomanagementprozesse

Die Strategie identifiziert Cyber-Risiken in erster Linie als Erweiterung bestehender Prozesse und Verantwortlichkeiten. Entsprechend sollen diese Cyber-Risiken auch in bereits bestehende Risikomanagementprozesse Eingang finden. Primär soll die Informationsgrundlage über Cyber-Risiken bei den Verantwortlichen verbessert und ihre Wahrnehmung dafür geschärft werden. Dazu erteilt der Bundesrat den Departementen den Auftrag, die Umsetzung der Massnahmen auf ihrer Ebene und im Verbund und Dialog mit kantonalen Behörden und der Wirtschaft an die Hand zu nehmen. Die Massnahmen erstrecken sich dabei von Risikoanalysen zu kritischen IKT-Infrastrukturen bis zur stärkeren Einbringung der Schweizer Interessen in diesem Bereich auf internationaler Ebene.

Der Bundesrat anerkennt somit, dass in der Schweiz die Zusammenarbeit zwischen Behörden und Wirtschaft generell etabliert ist und gut funktioniert. Mit der Strategie zum Schutz der Schweiz vor Cyber-Risiken will er im Cyber-Bereich diese Zusammenarbeit vertiefen und das bereits gelegte Fundament weiter stärken, um so die Minimierung von Cyber-Risiken zielgerichtet anzugehen. Er setzt daher auf bestehende Strukturen und verzichtet auf ein zentrales Steuerungs- und Koordinationsorgan, wie es in anderen Ländern mit teils weniger ausgeprägter Zusammenarbeit zwischen den relevanten Akteuren nun aufgebaut wird. Stattdessen soll der Informationsfluss und die gesamtheitliche Auswertung vorliegender Informationen zu Cyber-Risiken und -Bedrohungen zur Unterstützung von Behörden, Wirtschaft und Betreibern kritischer Infrastrukturen intensiviert und bedarfsgerechter verbreitet werden. (Informatiksteuerungsorgan des Bundes ISB, 2012)

7 Rechtliche Situation

Hier stellt Artikel 143bis StGB das unbefugte Eindringen in ein Datenverarbeitungs-System als solches, Art. 143 den Daten-Diebstahl und 144bis die Daten-Beschädigung unter Strafe. Hinzu kommen die zivilrechtlichen Schadenersatz-Ansprüche.

Per 1. Januar 2011 wurde Art. 143bis StGB durch den Bundesbeschluss vom 18. März 2011 (Übereinkommens des Europarates über die Cyberkriminalität) mit dem „Hacker-Paragraphen" erweitert.

Computer-Spionage: Art. 143 StGB

Durch die unterschiedlichen Motive bei einer DDoS Attacke, resp. die dadurch erhaltenen Daten ist der Art. 143 StGB anwendbar.

> StGB Art. 143: Unbefugte Datenbeschaffung (Auszug)
>
> 1 Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, sich oder einem andern elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten beschafft, die nicht für ihn bestimmt und gegen seinen unbefugten Zugriff besonders gesichert sind, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.

Hacker-Paragraph: Art. 143bis StGB

Durch den Bundesbeschluss vom 18.03.2011 wurde in Übereinkunft mit dem Europarat der Artikel mit Abs. 2 ergänzt. Eine Teilnahme / Mitwirkung an einer DDoS Attacke erfüllt diesen Tatbestand.

> StGB Art. 143bis:Unbefugtes Eindringen in ein Datenverarbeitungssystem (Auszug)
>
> [1] Wer auf dem Wege von Datenübertragungseinrichtungen unbefugter weise in ein fremdes, gegen seinen Zugriff besonders gesichertes Datenverarbeitungssystem eindringt, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.
>
> [2] Wer Passwörter, Programme oder andere Daten, von denen er weiss oder annehmen muss, dass sie zur Begehung einer strafbaren Handlung gemäss Absatz 1 verwendet werden sollen, in Verkehr bringt oder zugänglich macht, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Computer-Sabotage: Art. 144bis StGB

Durch die eingesetzten Programme für eine DDoS Attacke kommt Art. 2 zum Tragen. Nicht klar ist, dass mit einer DDoS Attacke ein System beschädigt wird und der Tatbestand gemäss Art. 1 erfüllt ist. Bei gewerbsmässigem handeln oder grossen Schaden kann die Freiheitsstraffe bis zu fünf Jahre betragen.

> StGB Art. 144bis: Datenbeschädigung (Auszug)
>
> [1] Wer unbefugt elektronisch oder in vergleichbarer Weise gespeicherte oder übermittelte Daten verändert, löscht oder unbrauchbar macht, wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.
>
> [2] Wer Programme, von denen er weiss oder annehmen muss, dass sie zu den in Ziffer 1 genannten Zwecken verwendet werden sollen, herstellt, einführt, in Verkehr bringt, anpreist, anbietet oder sonst wie zugänglich macht oder zu ihrer Herstellung Anleitung gibt, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Computer-Betrug: Art. 147 StGB

Durch eine DDoS Attacke wird die Datenverarbeitungsanlage betrügerisch missbrauch. Dieser Tatbestand wird verstärkt, indem z.B. eine Erpressung mithilfe der Attacke stattfindet.

> StGB Art. 147: Betrügerischer Missbrauch einer Datenverarbeitungsanlage (Auszug)
>
> [1] Wer in der Absicht, sich oder einen andern unrechtmässig zu bereichern, durch unrichtige, unvollständige oder unbefugte Verwendung von Daten oder in vergleichbarer Weise auf einen elektronischen oder vergleichbaren Datenverarbeitungs- oder Datenübermittlungsvorgang einwirkt und dadurch eine Vermögensverschiebung zum Schaden eines andern herbeiführt oder eine Vermögensverschiebung unmittelbar darnach verdeckt, wird mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.

Zeitdiebstahl: Art. 150 StGB

Durch eine DDoS Attacke wird die Datenverarbeitungsanlage übermässig beansprucht, es kann als ein erschleichen von Zeit / Zeitdiebstahl ausgelegt werden. In Betracht gezogen werden muss, inwiefern die Leistung nur gegen Entgelt erbracht wird. Oftmals ist eine „fair-use“ Nutzung erlaubt, eine übermässige Beanspruchung wird hingegen verrechnet.

> StGB Art. 150: Erschleichen einer Leistung (Auszug)
>
> Wer, ohne zu zahlen, eine Leistung erschleicht, von der er weiss, dass sie nur gegen Entgelt erbracht wird, namentlich indem er
>
> ein öffentliches Verkehrsmittel benützt,
>
> eine Aufführung, Ausstellung oder ähnliche Veranstaltung besucht,
>
> eine Leistung, die eine Datenverarbeitungsanlage erbringt oder die ein Automat vermittelt, beansprucht,
>
> wird, auf Antrag, mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Check- und Kreditkarten Missbrauch: Art. 148 StGB

Für die Benutzung der gemieteten Bot-Netzwerke wird oft mit gestohlenen Kreditkarten bezahlt. Dadurch wird der Tatbestand anhand Art. 148 StGB erfüllt.

> StGB Art. 148: Check- und Kreditkartenmissbrauch
>
> [1] Wer, obschon er zahlungsunfähig oder zahlungsunwillig ist, eine ihm vom Aussteller überlassene Check- oder Kreditkarte oder ein gleichartiges Zahlungsinstrument verwendet, um Vermögenswerte Leistungen zu erlangen und den Aussteller dadurch am Vermögen schädigt, wird, sofern dieser und das Vertragsunternehmen die ihnen zumutbaren Massnahmen gegen den Missbrauch der Karte ergriffen haben, mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.

8 Fazit

Die Bedrohung, die von DDoS Angriffen ausgeht, ist nicht zu unterschätzen. Administratoren müssen einen genügenden Schutz planen und umsetzen, auch für bestehende Netze. Die vielfältigen Angriffsmethoden verlangen eine umfassende Planung von Abwehrmassnahmen. Da die Botnetze immer grösser und leistungsfähiger werden und die Angreifer mit der Technik gehen, muss auch die Abwehr aufgerüstet werden. Die verschiedenen Angriffe aus der Vergangenheit haben gezeigt, dass ein absoluter Schutz nicht möglich ist. Bei genügend Angreifern wird früher oder später jedes noch so gut geschützte System zusammenbrechen. Damit solche Angriffe in Zukunft abgewehrt werden können ist es wichtig, dass die Provider zusammenarbeiten. Wenn im Backbone vom Internet die Angreifer bereits blockiert oder zumindest limitiert werden, kann immerhin der „normale“ Traffic weiterhin auf den Server bearbeitet werden. Es ist davon auszugehen, dass die reinen DDoS Angriffe in Zukunft immer intelligenter werden. Ein reines Flooding der Server wird ergänzt mit speziell angepassten Anfragen womit z.B. ein Webserver komplexe Berechnungen durchführen muss und somit zusätzlich belastet wird. Durch das Übereinkommen des Europarates über die Cyberkriminalität ist seit 2011 die rechtliche Situation beschrieben. Auch wenn es noch gewisse Unsicherheiten gibt ist es eindeutig, dass das Mitwirken bei DDoS Angriffen strafbar ist.

Abbildungsverzeichnis

Literatur- und Quellenverzeichnis

admin.ch. (2012). *Der Bundesrat verabschiedet die Nationale Strategie*. Verfügbar unter: http://www.news.admin.ch/message/index.html?lang=de&msg-id=45138 (26.11.2012)

Arbor Networks. (2012). *Global Activity Maps*. Verfügbar unter http://atlas.arbor.net/worldmap/ (11.11.2012)

Arbor SERT (2011). *Worldwide Infrastructure Security Report VII, 2011.* Verfügbar unter: http://ddos.arbornetworks.com/report/ (04.12.2012)

BBC News (2000). *Yahoo attack exposes web weakness*. Verfügbar unter: http://news.bbc.co.uk/2/hi/science/nature/635444.stm (24.11.2012)

Cert (1997). CA-1996-01. *UDP Port Denial-of-Service Attack*. Verfügbar unter: http://www.cert.org/advisories/CA-1996-01.html (11.11.2012)

Cert (2000). CA-1996-21. *TCP SYN Flooding and IP Spofing Attacks.* Verfügbar unter: http://www.cert.org/advisories/CA-1996-21.html (11.11.2012)

Check Point (2012). *Check Point DDoS Protector Appliances.* Verfügbar unter: http://www.checkpoint.com/products/ddos-protector/index.html (25.11.2012)

Cisco (2004). *Defeating DDOS Attacks.* Verfügbar unter: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5879/ps6264/ps5888/prod_white_paper0900aecd8011e927.html (25.11.2012)

Corero (2012). *IPS 5500 Product Family.* Verfügbar unter: http://www.boll.ch/corero/assets/IPS_Family.pdf (25.11.2012)

FortiNet (2012). *FortiDDoS Family of DDoS Prevention Appliances.* Verfügbar unter: http://www.fortinet.com/products/fortiddos/index.html (25.11.2012)

Heise (2012). *Hacker legen wieder schwedische Bank- und Regierungsserver lahm*. Verfügbar unter: http://www.heise.de/newsticker/meldung/Hacker-legen-wieder-schwedische-Bank-und-Regierungsserver-lahm-1724615.html (04.12.2012)

IETF (1981). RFC: 793 Transmission Control Protocol. Verfügbar unter: http://tools.ietf.org/html/rfc793 (11.12.2012).

Informatiksteuerungsorgan des Bundes ISB (2012). *Lage in der Schweiz und international.* Verfügbar unter: http://www.melani.admin.ch (04.12.2012)

ISC (2002). *21 Oct 2002 Root Server Denial of Service Attack – Report*. Verfügbar unter: http://www.isc.org/f-root-denial-of-service-21-oct-2002 (05.12.2012)

Kasperky Lab (2012). *DDoS attacks in H2 2011.* Verfügbar unter: http://www.securelist.com/en/analysis/204792221/DDoS_attacks_in_H2_2011 (04.12.2012)

Maron, HJ. (2010). *Wegen Assange: Postfinance.ch unter Hackerbeschuss.* Verfügbar unter: http://www.inside-it.ch/articles/23397 (02.12.2012)

Namestnikov, Y. (2009). *Schattenwirtschaft Botnetze.* Verfügbar unter: http://www.viruslist.com/de/analysis?pubid=200883656 (02.12.2012)

Netzpolitik (2010). *Damals: DDos als Aktionsform für Netzaktivisten?* Verfügbar unter: https://netzpolitik.org/2010/damals-ddos-als-aktionsform-fur-netzaktivisten/ (04.12.2012)

Wikipedia. (2012). *Operation Payback.* Verfügbar unter: http://de.wikipedia.org/wiki/Operation_Payback (04.12.2012)

StGB (2012). *Schweizerisches Strafgesetzbuch.* Verfügbar unter: http://www.admin.ch/ch/d/sr/311_0/ (18.11.2012)

Verisign (2012). *Whitepaper: DDoS Mitigation – Best Practices for a Rapidly Changing Threat Landscape.* Verfügbar unter: https://www.verisigninc.com/en_US/forms/ddosbestpracticeswp.xhtml (01.12.2012)

Vernez, G. (2012). *Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken.* Verfügbar unter: https://www.isss.ch/fileadmin/events/2012/partner/Swiss%20Crows%20Cyber%20Defense%20Conference%2025.04.2012%20-%20Vortrag%20G.Vernez.pdf (02.12.2012)