Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan Bund ISB

Melde- und Analysestelle Informationssicherung MELANI
GovCERT.ch

Massnahmen gegen DDoS Attacken

MELANI / GovCERT.ch

Version:	v1.00
Author:	MELANI / GovCERT.ch

[1] http://creativecommons.org/licenses/by-nd/3.0/

Einleitung

Unter DDoS (Distributed Denial of Service = Verweigerung des Dienstes) versteht man einen Angriff auf Computer-Systeme mit dem erklärten Ziel, deren Verfügbarkeit zu stören. Für das Opfer kann dies weitreichende wirtschaftliche Folgen haben. Im Gegensatz zur einfachen DoS-Attacke erfolgt der Angriff bei DDoS von vielen verteilten Rechnern aus. Der Angriff kann dabei auf Netzwerkebene, auf Anwendungsebene oder einer Kombination davon erfolgen. In der Regel werden für solche Attacken sogenannte Bot-Netze (eine riesige Anzahl "gekaperter" Systeme, die vom Angreifer ferngesteuert werden können) oder schlecht konfigurierte Drittsysteme (z.B. Open DNS Resolver) verwendet, die durch manipulierte Anfragen dazu gebracht werden, grosse Antworten an die „falsche“ Adresse – nämlich die des Zielsystems – zu schicken (Amplification-Angriffe). Das Datenvolumen erreicht oft mehrere hundert Gbit/s. Dies sind Volumina, die eine einzelne Organisation ohne fremde Hilfe i.d.R. nicht mehr bewältigen kann. Entsprechend konfigurierte Firewalls und IPS (Intrusion Prevention Systeme) helfen nur bedingt.
Die Motivation hinter solchen DDoS Attacken sind meistens politischer Aktivismus, Erpressung oder Schädigung eines Konkurrenten. MELANI beobachtet aktuell eine Zunahme von erpresserischen DDoS-Attacken, bei welchen Lösegeld in Form von Cryptowährungen wie Bitcoin oder Litecoin eingefordert wird.

DDoS kann jede Organisation treffen!

Vorbeugende Massnahmen

Idealerweise haben Sie sich mit der DDoS-Problematik schon vorgängig auseinandergesetzt und eine gewisse DDoS-Abwehrbereitschaft erreicht.

- Sie kennen Ihre Infrastruktur und deren Schwächen. Welche Dienste sind so wichtig, dass deren Ausfall weitreichende Auswirkungen auf Ihre Organisation haben könnte. Versuchen Sie dabei auch an Basis Systeme zu denken, ohne die Ihre kritischen Geschäftsanwendungen nicht funktionieren.
- Sie kennen den "Normalzustand" Ihrer Netze und Systeme und erkennen Anomalien (IDS (Intrusion Detection Systeme), zentralisierte Logauswertung). Eine DDoS-Attacke sollte entdeckt werden, bevor Ihre Kunden sie bemerken können.
- Überwachen Sie die Verfügbarkeit Ihrer Kundenanwendungen auch aus der Sicht Ihrer Kunden, das heisst vom Internet her
- Ihre Systeme sind gehärtet (keine unnötigen Dienste, strikte Rechtevergabe, starke Authentisierung, usw.) und auf aktuellem Patch-Level. SYN-Cookies sind aktiviert etc.
- Eine vorgelagerte Firewall lässt nur benötige Protokolle zum System durch. Die Firewall verfügt über genügend Systemressourcen, um auch im Falle eines DDoS funktionsfähig zu bleiben. Dabei ist ein grosses Augenmerk auf die Connection Table sowie auf eine gute Regelverwaltung zu legen, damit sie im Notfall zusätzlich viele Blockierungsregeln implementieren können.
- Prüfen Sie die Möglichkeiten eines GeoIP Blockings. Wenn Ihre Kunden vorwiegend aus der Schweiz und dem nahen Ausland stammen, können Sie ein Profil vordefinieren, welches IP Adressen aus diesem Raum entweder Priorität einräumt oder andere IP Adressen blockiert. Im Angriffsfall können Sie dieses Profil aktivieren und gewinnen so sehr schnell an Handlungsoptionen und zusätzlichem Schutz.
- Eine Web-Application Firewall minimiert die Angriffsfläche auf webbasierte Dienste.
- Systeme, die potentiell Opfer einer DDoS Attacke werden könnten (z.B. Webauftritt), sollten an einem anderen Internet-Uplink hängen als die übrigen Systeme der Organisation. Die betroffenen Systeme können so einfacher unter den Schutzschild eines DDoS-Mitigation-Providers gestellt werden, ohne dabei die restlichen Systeme zu tangieren, die für das Tagesgeschäft nötig sind.

- Stellen Sie Ausweichlösungen bereit, z.B. eine statische Website mit minimalen Informationen, welche bei einem anderen Provider bereit steht und die Sie mit einer einfachen Änderung im DNS aktivieren können.
- Achten Sie generell darauf, eine gute Balance in den TTLs der DNS Server zu haben, so dass Sie genügend schnell eine Domänenauflösung umstellen können.
- Sie haben eine Strategie für den Fall einer DDoS Attacke. Die zuständigen Personen kennen das Vorgehen sowie die internen und externen Kontakte (Service Provider, Polizeistellen etc.)
- Im Fall der Fälle können sie auf interne oder vertraglich zugesicherte externe Ressourcen zugreifen (insbesondere Personal und Infrastruktur).
- Sie haben den Fall einer DDoS Attacke mit Ihren internen Stellen und den externen Partnern besprochen und auch geübt. Jeder kennt seine Rolle und Ansprechpartner!

Gegenmassnahmen bei einem Angriff

Bei einem DDoS geht es primär darum, dem Angreifer zu signalisieren, dass er sein Ziel nicht erreicht. Halten Sie genügend lange durch, wird der Angreifer sich typischerweise von Ihnen abwenden.

1. Protokollieren Sie den Angriff (Netflows, Server-Logs, Mail-Verkehr mit den Erpressern usw.). Sie sind für eine spätere Analyse und allfällige Anzeige wichtig.
2. Stellen Sie sicher, dass Sie minimale Informationskanäle gegen aussen offen halten können, z.B. ein statischer Webauftritt, auf dem Sie Ihre Kunden informieren und Ihnen alternative Kontaktmöglichkeiten (z.B. Telefon, Fax, E-Mail) anbieten.
3. Analysieren Sie den Angriff und legen Sie eine Abwehrstrategie fest:

    a. Ist der Ursprung der Attacke eine beschränkte Anzahl von IP-Adressen, dann genügt evtl. das Filtern dieser Adressen an Ihrem Router oder Firewall. Übersteigt das Datenvolumen die Ihnen zur Verfügung stehende Bandbreite, dann muss dies Ihr ISP erledigen.
    b. Verschieben Sie ggf. Ihr angegriffenes System in ein anderes Subnetz (Bei rein IP-basierten Angriffen). Typischerweise suchen Sie hier eine Lösung in enger Zusammenarbeit mit Ihrem ISP und/oder einem spezialisierten DDoS-Mitigation-Provider.
    c. Es handelt sich um eine Attacke, deren Source-IP-Adressen wahrscheinlich gefälscht sind:
    Dies ist typischerweise bei SYN-, UDP-, BGP- und SNMP-Flooding der Fall. Ein Filtern der IP-Adressen macht hier keinen Sinn und kann sogar legitime Benutzer aussperren. Typischerweise suchen Sie hier eine Lösung in Zusammenarbeit mit Ihrem ISP. Er kann diesen Verkehr umlenken und ausfiltern. Dazu sollten Sie aber vorher schon wissen, welche Protokolle bei Ihnen eingesetzt werden und welche schadlos ausgefiltert werden können. Öffentliche Auftritte beschränken sich in der Regel auf TCP-basierte Protokolle (HTTP, HTTPS, SMTP etc.) so dass state-less Protokolle wie UDP bedenkenlos gefiltert werden können (evt. Ausnahme: DNS).
    d. Angriffe auf eine Applikation:
    Hier wird Ihre Applikation durch eine grosse Anzahl von (komplexen) Anfragen lahm gelegt. Die Attacken nutzen in der Regel TCP als Netzwerk-Protokoll. Die Absender Adresse ist also nur schwer fälschbar und kann daher nach diversen Kriterien gefiltert werden.
    e. Attacken auf das SSL/TLS Protokoll: Mögliche Abhilfe ist das Terminieren der SSL-Verbindung bei einem Cloud-Dienst, der die gefilterte Verbindung danach an Ihre Systeme weiterreicht.
    f. Falls sich der Grossteil der Kundschaft in bestimmten Ländern befindet, kann nach GEO-IP gefiltert bzw. priorisiert werden. So bleibt der Dienst möglichst

lange verfügbar, obwohl vielleicht der eine oder andere legitime Benutzer ausgefiltert bzw. niedrig priorisiert wird.

4. Analysieren Sie den Angriff und legen Sie eine Abwehrstrategie fest: Stellen Sie sich darauf ein, dass der Angreifer versuchen wird, sich auf Ihre Abwehrmassnahmen einzustellen und dass er neue Taktiken anwenden wird. Analysieren Sie in einem solchen Fall den DDoS erneut und wenden Sie entsprechende Gegenmassnahmen an.
5. Melden Sie den Vorfall MELANI und erstatten Sie Anzeige bei der zuständigen Polizei, wegen (versuchter) Datenbeschädigung (Art. 144bis Strafgesetzbuch) und gegebenenfalls (versuchter) Erpressung (Art. 156 Strafgesetzbuch). Eine Datenbeschädigung liegt auch dann vor, wenn Daten durch einen Angriff über eine gewisse Zeit nicht verfügbar und deshalb „unbrauchbar“ sind.
6. MELANI rät dringend davon ab, auf die Forderungen der Erpresser einzugehen.

Kontakt MELANI

http://www.melani.admin.ch