Denial of Service DoS/DDoS

Unter Denial of Service (DoS) versteht man ein Angriff, der die Verfügbarkeit von Systemen stört. Häufig werden jedoch Distributed Denial of Service (DDoS) Attacken ausgeführt. Dies bedeutet, dass der Angriff im Gegensatz zur normalen DoS-Attacke von vielen Rechnern aus erfolgt. Beim DDoS-Angriff werden in der Regel Bot-Netze oder schlecht konfigurierte Drittsysteme verwendet, damit sehr viele Anfragen an das Zielsystem gesendet werden können. Bei Protestaktionen ist es jedoch auch möglich, dass eine Gruppe von Leuten bewusst eine Webseite mit bestimmten Tools, wie LOIC, down bringen. Durch das grosse Datenvolumen ist es ohne entsprechender Hilfe nicht mehr möglich die Anfragen zu bewältigen und daher ist der Service während dieser Zeit nicht verfügbar. Ein Angriff erfolgt meistens in einer Kombination von Netzwerkebene und Anwendungsebene und kann durch entsprechend konfigurierte Firewalls nur bedingt abgewehrt werden.

Motivation

- Politischer Aktivismus
- Schädigung des Konkurrenten
- Erpressung
- Aufmerksamkeit

Angriffstypen

- Applikations-Attacken, z.B. HTTP-Flooding
- Protokoll-Attacken z.B. SYN-Flooding
- Bandbreiten-Attacken z.B. ICMP-Flooding

Auswirkungen

- Ausfall der Webseite
- Gewinnverlust
- Reputationsverlust

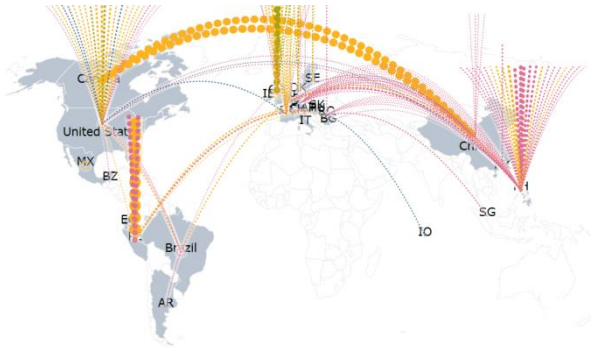

Abbildung 1 Digital Attack Map - 14. Juni 2014

Massnahmen

- Firewall, die Pakete filtert.
- Genügend Ressourcen, meistens finanziell nicht möglich!
- SYN-Cookies einsetzen, sobald Speicher knapp wird.
- Filter-Services z.B. CloudFlare nutzen, schützt vor Angriffen auf der Anwendungsschicht.
- Capatchas oder Rätselfragen einsetzen, wenn der Benutzer mehrere HTTP Anfragen in kurzer Zeit sendet.

Begriffe

DoS/DDoS:	Die Verfügbarkeit eines Services mit einem oder mehreren Computern stören.
Bot-Netz	Riesige Anzahl infizierter Systeme, die von einem Angreifer ferngesteuert werden können.
Zombie	Infizierter Rechner in einem Bot-Netz.
Drittsysteme	z.B. Open DNS Resolver oder HTML Validierungsseiten
LOIC	Tool, welches das Ausführen einer DoS-Attacke per Knopfdruck ermöglicht.

Beispiel

Am 14. März 2016 standen mehrere Schweizer Online-Händler unter Beschuss und waren für mehrere Stunden nicht erreichbar. Neben anderen Online-Anbietern, wie Microspot, SBB oder Interdiscount hat es Digitec am übelsten erwischt. Neben der Webseite waren auch die Filialen und Callcenter betroffen. Der oder die Täter sind bis heute unbekannt und werden vermutlich auch nie erwischt. Man kann davon ausgehen, dass die Schäden des eher kurzen Angriffes in Millionenhöhe liegen.

Links

Infos & Filter-Service «DoS/DDoS»:	http://www.incapsula.com/ddos/ddos-attacks/
	http://www.cloudflare.com/ddos/
Melde- und Analysestelle Schweiz:	http://www.melani.admin.ch/melani/de/home/themen/DDoSAttacken.html
Digitale DDoS Angriffskarte:	http://www.digitalattackmap.com/
	http://cybermap.kaspersky.com/
Artikel über «DNS amplification attack»:	http://www.evilsec.net/2015/04/drdos-denial-of-service-on-steroids/
Infos über «Open DNS Resolver»:	http://openresolverproject.org/

Quellen zuletzt geprüft am 23.3.2016.