BEST PRACTICES
ANSÄTZE ZUM DDoS-SCHUTZ

Version 3.0

KONTAKT

LINK11 GmbH
Lindleystraße 12
60314 Frankfurt am Main
Deutschland

Telefon: +49 (0) 69-264929777
E-Mail: info@link11.de
Web: www.link11.de

September 2015
Raymond Hartenstein
rh@link11.de

Was sind DDoS-Angriffe?

Bei Distributed Denial-of-Service (DDoS) Attacken benutzt ein Angreifer eine Vielzahl von Rechnern, die mit Schadsoftware infiziert sind und somit fern gesteuert werden können. Bei einer Attacke greifen diese Rechner (Botnetz) zeitgleich auf ein Ziel zu, z.B. einen Web- oder Mailserver und blockieren diesen durch Überlast. Er ist mitunter über Stunden oder Tage nicht mehr erreichbar.

Die Angriffe zielen auf Anwendungen (Applikations-Attacke) und/oder auf die physikalische Internet-Anbindung des betroffenen Unternehmens, die durch eine große Anfragemenge überlastet werden kann (Volumen-Attacken).

Bei Applikations-Attacken versucht der Angreifer eine Anwendung zu überlasten, indem er z.B. eine größere Datei (Bild, Grafik, etc.) sehr oft in kurzer Zeit aufruft. Oder er startet eine Suchabfrage, die sehr viele Ergebnisse liefert, häufig mehrmals innerhalb kurzer Zeit. Dadurch werden die Systeme, die den entsprechenden, nicht cache-fähigen Inhalt ausliefern sollen, überlastet.

Bei den Volumen-Attacken ist es die Zahl der Anfragen, die von vielen Tausend Rechnern zeitgleich kommen und so einen Internetzugang und das System überlasten. Hier ist durch die Menge der Anfragen das Datenvolumen derart groß, dass die Leitung „verstopft".

In den vergangenen Monaten haben „Distributed Reflection DoS" (DRDoS) Angriffe zugenommen. Diese schalten zwischen Angreifer und Ziel-Server ein weiteres System: Domain Name Server (DNS) oder Network Time Protocol (NTP) Server, die zehntausendfach und oft ungeschützt im Internet vorhanden sind. Diese sogenannten Reflektoren verstärken die Wucht des Angriffes. Sie erhalten vom Angreifer eine kleine Anfrage und schicken die größere Antwort an den Ziel-Server.[1]

Warum DDoS-Angriffe?

Als Angriffsmethode auf Unternehmen bzw. deren Internetpräsenz oder Infrastruktur werden DDoS-Attacken immer beliebter. Sie sind für wenig Geld im Internet zu mieten, oder auch recht einfach selbst zu bewerkstelligen. Für Angreifer ist die Wahrscheinlichkeit identifiziert zu werden extrem gering. Die Angriffe sind wirkungsvoll und richten oft großen Schaden an. Das unterscheidet DDoS-Attacken von anderen Methoden, die mehr Aufwand bedeuten oder deren Effekt wesentlich kleiner ist.

Bisher gibt es noch kaum Statistiken, wie stark deutsche Unternehmen von DDoS-Angriffen betroffen sind. Nach Schätzungen des Bundesministeriums des Innern wird nur jede zehnte Tat zur Anzeige gebracht. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) geht von mindestens 133 DDoS-Angriffen pro Tag auf deutsche Unternehmen und Behörden aus. Im Jahr 2014 gab es bis zum Herbst in Deutschland bereits über 32.000 DDoS-Angriffe.[1]

International gibt es Erhebungen, dass sich die Zahl der DDoS-Attacken im zweiten Quartal 2015 verglichen mit der Situation vor einem Jahr mehr als verdoppelt hat. Die Angriffe sind zudem länger geworden und dauern nun im Schnitt 20,64 statt 17,35 Stunden. Gefährliche Mega-Angriffe mit mehr als 100 GBit/s nehmen erkennbar zu. Ihre Anzahl hat sich innerhalb eines Quartals verdoppelt. Nur wenige Unternehmen verfügen über genügend Kapazitäten, um solche Angriffe mit eigenen Mitteln abzuwehren.[2]

Jeder kann angegriffen werden. Jede Branche. Jedes Unternehmen ist gefährdet, auch Non-Profit-Organisationen. Besonders im Fokus stehen Banken, Versicherungen, E-Commerce-Shops, Medien, ISPs, Rechenzentrums-Betreiber und Anbieter von Cloud-Services. In Deutschland ist schon jedes dritte Unternehmen von DDoS-Angriffen betroffen.[3] Weitere Umfragen zeigen zudem, dass die Attacken zu 70 Prozent auf Webservices und Anwendungen wie Online-Shops und Unternehmensseiten zielen. 47 Prozent sollen die Infrastruktur (Router, Firewalls, Bandbreite) schädigen. Zu je 13 Prozent stehen Business Services wie VPN und E-Mail) und externe Rechenzentren und Cloud-Services im Fokus.[4]

---

[1] Bundesamt für Sicherheit in der Informationstechnik, Distributed Denial of Service, Themenlagebild: September 2014

[2] Akamai's State oft the Internet Security Report Q2 2015

[3] BSI, Umfrage Cyber-Sicherheit in Deutschland, 2014

[4] Arbor Worldwide Infrastructure Security Report 2014, S. 98

In der Regel finden DDoS-Angriffe dann statt, wenn sie das angegriffene Unternehmen am meisten schädigen können: Zur Weihnachtszeit sind Online-Shop-Betreiber besonders stark betroffen. Die Versicherungsbranche ist vor den klassischen Versicherungswechseltagen im November häufig unter Beschuss. Zudem wird generell gerne an Wochenenden angegriffen, wenn die IT-Abteilung nicht voll besetzt ist. So vergeht viel Zeit, bis die Überlastung der Server abgewendet werden kann.

Prominentes Beispiel ist der DDoS-Angriff auf Sony und dessen Playstation Netzwerk zur Weihnachtszeit. Dann, wenn die Nutzer an den Feiertagen endlich Zeit haben, intensiv zu spielen, bzw. ihr Geschenk auszuprobieren ist das Playstation Netzwerk lahm gelegt worden.

Im Wesentlichen sind es vier unterschiedliche Motivationen im Bereich der DDoS-Angriffe auf professionelle Webseiten/ Infrastrukturen:

Politische Motive/Hacktivismus:

Die Aussagen oder politischen Ziele der angegriffenen Seite sind nicht konform mit der Meinung und Motivation des Angreifers. Im Januar 2014 wurde die Webseite des Bundestages und die von Dr. Angela Merkel angegriffen.

Finanzielle Motive/Erpressung:

Opfer sind hier häufig Webshop-Betreiber, die erpresst werden. Sofern sie kein Geld zahlen, drohen die Angreifer damit, die Seite zu überlasten, damit sie nicht mehr verfügbar ist. Kürzlich wurden in Deutschland Banken und Anbieter von Online Bezahlterminals erpresst, der Umsatzverlust bei solchen Unternehmen ist enorm.

Feindselige Konkurrenz/Blockade:

Unternehmen, deren Internetpräsenz durch Wettbewerber angegriffen wird. Teilweise um Imageschäden zu verursachen, oder den Online-Handel des Unternehmens zu blockieren. Die Angreifer kommen in diesen Fällen meist nicht aus der gleichen geographischen Region.

Datendiebstahl/Verschleierung:

Durch eine DDoS-Attacke wird die IT/Security Abteilung des Unternehmens beschäftigt. In der Zwischenzeit wird dadurch unbemerkt eine andere Schwachstelle ausgenutzt, um sensible Daten zu stehlen.

Abwehrmethoden

Es gibt viele Methoden, die aufgeführt werden, um sich gegen DDoS-Angriffe zu schützen. Nur wenige davon sind wirklich wirksam gegenüber professionellen Angriffen. Systeme wie eine Firewall können in der Regel schnell überlastet werden und bieten daher gegen DDoS-Angriffe nur unzureichend Schutz. Die Firewall regelt, wer von extern auf welche Anwendung zugreifen darf, und geht dabei nach einem strikten Regelwerk vor. Gibt es zu viele Anfragen, ist die Firewall schnell überlastet, da der permanente Abgleich mit dem Regelwerk entsprechend Ressourcen benötigt. Als Ergänzung zur Firewall werden häufig Intrusion Detection Systeme (IDS) eingesetzt. Diese gleichen den Datenverkehr mit bekannten Angriffsmustern ab. Die wenigsten Systeme erkennen neuartige Angriffe und auch hier spielen die vorhanden Ressourcen eine große Rolle, ein IDS System lässt sich meist sehr schnell mit einem DDoS-Angriff überlasten.

Es haben sich drei Methoden durchgesetzt, die einen wirksamen Schutz bieten können:

Hardware:

Es wird ein Gerät (DDoS-Appliance) in der Infrastruktur des Unternehmens installiert. Diese Appliance überwacht den Datenverkehr. Bei Auffälligkeiten, wie dem plötzlichen Anstieg des Datenverkehrs, limitiert sie den Traffic, bzw. erkennt die Anfragen des Angreifers und blockiert diese.

CDN:

Das Content Distribution Netzwerk (CDN) verteilt Inhalte der Webseite auf weltweit platzierte Server. Somit müssen Anfragen nicht vom Original Server beantwortet werden, sondern von dem physikalisch am nächsten platzierten. Das hilft Lastenspitzen, wie sie durch DDoS-Attacken entstehen können, bis zu einem gewissen Level auszugleichen.

DDoS Cloud-Schutz:

Der Datenverkehr für die Webseite wird über den externen Filter eines Dienstleisters geleitet. Durch eine Analyse der Anfragen können Angreifer erkannt und blockiert werden. Nur legitimer Datenverkehr wird weitergeleitet.

Diese verschiedenen Abwehrmethoden können auch miteinander kombiniert werden. Das ist in vielen Fällen zielführender in der Abwehr, als der Einsatz nur einer Methode.

Herausforderungen bei der Abwehr

Die Thematik der DDoS-Abwehr hat sich in den letzten Jahren gewandelt. Die Angriffsmethoden sind komplexer geworden: Die Angreifer kombinieren Volumen- und Applikations-Attacken, die Schlagkraft erhöht sich z.B. durch den Einsatz von Reflektoren und einen immer stärkeren Breitbandanschluss vieler Botnetz-Rechner. Angriffe auf Applikationsebene tarnen sich zudem immer besser wie normale User-Anfragen und bleiben so länger unentdeckt.

Die EINE Abwehrmethode gibt es nicht, auch unter dem Gesichtspunkt, dass verschiedene Branchen sehr unterschiedliche Anforderungen an eine Lösung haben: Eine Bank mit starken Datenschutzanforderungen möchte ihren Datenverkehr nicht dauerhaft über einen Cloud-Anbieter umleiten. Bewertungsportale oder Nachrichtenseiten haben damit weniger Probleme. Ein rein national agierendes Unternehmen benötigt womöglich kein CDN, um seine Webseite weltweit schnell verfügbar zu machen. Aber vielleicht ist es wie ein Finanzinstitut um seine Datensicherheit besorgt, da täglich viele Bezahlvorgänge über die Webseite laufen.

Vor der Auswahl der DDoS-Schutzlösung sollte daher immer die Erstellung eines Anforderungskataloges stehen, in dem die Vor- und Nachteile der einzelnen Lösungen abgewogen werden. Diese sind unter anderem:

Hardware:

Eine lokal installierte Hardware kann Angriffe gut erkennen. Jedoch arbeiten viele Hardware Lösungen nicht immer sehr granular. Aus Ressourcengründen analysieren sie nur Teile des Datenstroms. Solange die physikalische Netzwerkanbindung groß genug ist, funktioniert diese Lösung. Sobald das Datenvolumen des Angriffs die Kapazität der Anbindung überschreitet, ist die Hardware-Lösung im Nachteil. In der Regel fallen auch sehr hohe Beschaffungskosten an, die Hardware muss in die bestehende Infrastruktur integriert, Personal für den 24/7-Betrieb der Appliance geschult werden. Nehmen die Angriffe an Volumen zu, kann die Bandbreite des Internetanschlusses vergrößert werden. Es entstehen in der Folge weitere Kosten durch den Kauf zusätzlicher Hardware.

Viele Hardware Anbieter bauen mittlerweile einen eigenen Cloud-Schutz gegen Volumenangriffe auf oder sie kooperieren mit Anbietern von Cloud-Lösungen.

CDN:

Ein CDN ist zunächst keine wirkliche Sicherheitslösung, sondern nur ein Verteilen der Anfragelast. Zudem bietet es keinen Schutz, wenn die Angriffe auf nicht-cachefähige Inhalte, z.B. eine Datenabfrage per Suchfunktion zielen. Außerdem wird nur der Webserver geschützt, andere Server in der Infrastruktur (Mail, VPN, etc.) sind weiterhin ungeschützt. CDN-Anbieter kombinieren ihr Angebot zunehmend mit einer „Web Application Firewall" (WAF). Diese kann Zugriffe auf einzelne Anwendungen limitieren, erfordert jedoch auch eigene Expertise und administrativen Aufwand.

DDoS Cloud-Schutz:

Der cloud-basierte Schutz, bzw. externe Filter, muss mit ausreichender Bandbreite angeschlossen sein. Nur so schützt er vor Volumen-Attacken. Um die Latenz so niedrig wie möglich zu halten, sollte der Filter in derselben Region (US/EU/APAC) wie der zu schützende Webserver stehen.

Durch die externe Filterung rückt der Datenschutz stark in den Mittelpunkt. Hier muss darauf geachtet werden, dass die Datenschutz-Standards des Landes, in dem der Filter steht, ausreichend sind.

Der Support spielt gerade bei externen Lösungen eine große Rolle. Der Kunde will im Angriffsfall oder bei Problemen, die potenziell vom externen Filter kommen könnten, jederzeit einen kompetenten Ansprechpartner am Telefon haben.

Die Nachteile der einzelnen Lösungen können nur durch sinnvolle Kombination gemildert werden. Auch gelten die Nachteile nicht notwendigerweise für alle Anwendungsfälle.

Zusammenfassung und empfohlene Schutzmaßnahmen

DDoS-Angriffe sind immer einfacher zu bewerkstelligen. Der finanzielle Schaden bei Ausfall der Webseite oder Überlastung der Infrastruktur kann enorm sein: Eine Bank, die über einen Tag keine Transaktionen mehr durchführen kann, erleidet einen erheblichen Schaden. So setzte im Sommer 2015 die international tätige DDoS-Erpresserbande DD4BC (DDoS for Bitcoins) zahlreiche Finanzunternehmen in Deutschland und Österreich unter Druck.[5] Auch ein Technologie-Unternehmen, dessen Entwicklungsstandort vom Netz abgetrennt ist, oder der Mittelständler, dessen Produktionsstandort über Tage nicht mehr erreichbar ist, können nachhaltig geschädigt werden. Existenzbedrohend kann es für einen Online-Shop sein, der komplett abhängig ist von der Erreichbarkeit seiner Webseite. Sein gesamtes Geschäftsmodell ist darauf aufgebaut, dass Kunden jederzeit bestellen können. So wurde jeder achte Online-Shop bereits mit DDoS-Attacken erpresst.[6]

Präventive Schutzmaßnahmen sind daher umgehend zu ergreifen. Die DDoS-Angriffe der letzten Monate haben an Volumen zugenommen, sodass häufig die lokale Netzanbindung des betroffenen Unternehmens überlastet war. Zudem werden Angriffe intelligenter und kombinieren Volumen- und Applikations-Attacken. Neben dem Webserver werden verstärkt andere Server in der Infrastruktur des Unternehmens angegriffen, die Internetzugänge überlastet und damit mitunter ganze Standorte außer Betrieb gesetzt.

Der erste Schluss, den man daraus ziehen muss, ist, dass eine lokale Hardware, die in der eigenen Infrastruktur installiert ist, meist nicht ausreichend ist. Es empfiehlt sich die Kombination mit einem Cloud-Schutz oder einem CDN. Welche Punkte gibt es hier zu beachten?

- *Ist es eine internationale Webseite, deren Inhalt in mehreren Ländern verteilt werden muss?* Dann empfiehlt sich die Kombination mit einem CDN.

- *Gibt es viele dynamische Inhalte auf der Seite?* Da die Anfragen vom Original-Webserver beantwortet werden müssen, kann ein Cloud-Schutz hier optimal schützen.

---

[5] Link11 Report zur DD4BC-Erpressung, www.ddos-info.de

[6] Studie Informationssicherheit im E-Commerce 2014 http://ibi.de/isiec2014.html

- *Welche Such-/Datenbankabfragen können das System stark belasten?* Nur wenige Hardware-Lösungen erkennen, wie sehr eine Suchabfrage die Datenbank belastet. Auch hier bietet der Cloud-Schutz Vorteile.

- *Sind nur Webserver oder weitere Server für E-Mail und VPN zu schützen?* Das CDN schützt nur den Webserver. Hier empfiehlt sich die Kombination aus Hardware und Cloud-Schutz.

- *Über wie viel Security Expertise verfügt das Unternehmen?* Sind zu wenig eigene Ressourcen vorhanden, sollte man von einer Hardware Lösung Abstand nehmen, da sie nicht ausreichend administriert werden kann.

- *Soll eine externe Lösung permanent den Datenstrom filtern oder nur im Angriffsfall?* Oft empfiehlt sich eine Standby-Lösung, die nur im Angriffsfall aktiv wird. Der DDoS-Schutz-Anbieter kann in diesem Fall auch als potenzielle Fehlerquelle ausgeschlossen werden.

- *Wie relevant ist der Datenschutz? Wird er durch den Anbieter gewährleistet?* Dies ist für die meisten Unternehmen wichtig und der externe Anbieter sollte die Einhaltung wirksamer Datenschutz Regelungen sicherstellen können.

Dies ist nur eine kleine Auswahl an Fragen, die sich ein Unternehmen stellen sollte, um darauf aufbauend seine Evaluierung der Schutzmöglichkeiten zu beginnen. Zu bedenken ist immer, dass DDoS-Angriffe bisher ein Nischenthema sind. In vielen Unternehmen ist die Expertise nicht vorhanden, die meist völlig überraschenden Angriffe selbst abzuwehren bzw. eine Hardware-Lösung effektiv zu bedienen. Im Zweifel sollte man sich an Spezialisten wenden, die täglich mit dieser Form der Cyber-Abwehr zu tun haben. Ein externer, cloud-basierter Schutz, bietet viele Vorteile:

- *Die Experten beschäftigen sich täglich mit der Abwehr von Angriffen.*

- *Große Datenvolumen können problemlos abgefangen werden, aber auch Angriffe auf Applikationsebene werden von guten Anbietern erkannt.*

- *Einige Cloud-Anbieter können im Angriffsfall zudem das gesamte Netzwerk des Unternehmens kurzzeitig übernehmen und damit komplett schützen, da Attacken nicht mehr nur auf die Webserver zielen. Dieser Schutz ist in einer Standby-Variante realisierbar, so dass der Datenverkehr im Normalfall nicht über den DDoS-Schutzanbieter läuft.*

Wichtig ist, dass die Evaluierung der Schutzmöglichkeiten nicht erst beginnt, wenn ein Angriff in vollem Gange ist. Das Risiko betroffen zu sein, steigt von Monat zu Monat. Geeignete Schutzmaßnahmen sollten vorher gefunden sein.

Über Link11:

Die Link11 GmbH ist ein deutscher IT-Security Anbieter. Spezialisiert auf DDoS-Schutz, gewann das Unternehmen mit seiner cloudbasierten Lösung 2012 den „eco-Award“ für das innovativste Produkt. Zu den Kunden von Link11 zählen führende Unternehmen aus dem Finanzsektor, der E-Commerce Branche und dem deutschen Mittelstand. Als Mitglied in der „Allianz für Cybersicherheit“, dem TeleTrusT e.V. und als „Preferred Business Partner“ des Bundesverband E-Commerce und Versandhandel Deutschland e.V. (bevh) beteiligt sich Link11 intensiv am Austausch und an der Entwicklung von DDoS-Schutzmaßnahmen.

Über den Autor:

Raymond Hartenstein ist seit 1997 in der IT-Branche tätig. Er arbeitete u.a. für globale Netzwerkanbieter, CDN-Betreiber und IT-Security Hersteller. Seit März 2013 ist er für die Link11 GmbH als Vertriebsleiter tätig.

KONTAKT

LINK11 GmbH

Lindleystraße 12
60314 Frankfurt am Main
Deutschland

Telefon: +49 (0) 69-264929777
E-Mail: info@link11.de
Web: www.link11.de