Nichts geht mehr

Aktuelle Situation zu Distributed-Denial-of-Service-(DDoS)-Angriffen

Während interne Netze und Server durch verschiedene Security-Layer mehr oder weniger gut vor Angreifern geschützt sind, eröffnen sich über DDoS-Attacken für jedermann Methoden, um Unternehmen mit geringem Mitteleinsatz maximal zu schaden. Durch Trends wie das „Internet der Dinge" (IoT) oder Industrie 4.0 erhöht sich noch die Abhängigkeit von der IT, sodass Organisationen und sogar Einzelne noch leichter erpressbar werden. Unser Autor informiert über aktuelle Entwicklungen globaler DDoS-Bedrohungen.

Von Markus Manske, Kiel

Distributed-Denial-of-Service-(DDoS)-Angriffe sind kein neues Phänomen, jedoch immer noch beliebt [1]. Ein Grund dafür ist, dass sie so gut wie jeder durchführen kann: Es sind keine größeren „Hacking-Skills" notwendig, um zum Ziel zu kommen, und es stehen unzählige Systeme bereit, die sich missbrauchen lassen. Wer das nicht selbst kann, nutzt einfach entsprechende Angebote – rund um DDoS-as-a-Service hat sich ein komplettes kriminelles Ökosystem gebildet, über das man DDoS-Angriffe beliebiger Größe bestellen kann. Angefangen bei „Booter/Stresser-Services", die sich für 15 bis 30 US-$ im Monat mieten lassen, über professionellere Anbieter, die ab 50 US-$ die Stunde zu buchen sind, bis hin zu Erpressergangs, deren Angriffe gerne auch mal die Internet-Infrastruktur eines ganzen Staates beeinträchtigen [2].

Im Bereich der DDoS-Angriffe unterscheidet man Volumenattacken, bei denen so viel Traffic auf das Netz des Ziels geleitet wird, bis es unter der Last zusammenbricht, von Angriffen gegen Applikationen, die zu einer Überlastung der Serverressourcen führen. Eine Unterart sind Reflection/Amplification-Angriffe, bei denen aus einer kleinen Anfrage eine um den Faktor 10 bis 4000 größere Antwort resultiert (Amplification: Verstärkung) und die IP-Adresse verfälscht (gespoofft) wird, sodass sich der eigentliche Angreifer nicht identifizieren und blocken lässt (Reflection: „über Bande").

80 Millionen Werkzeuge

Cyberkriminelle benutzen für DDoS-Angriffe meist Botnetze, die überwiegend aus gehackten oder falsch konfigurierten Servern bestehen und manchmal auch aus DSL-Routern [3]. Sowohl Server als auch Router-Botnetze werden durch automatisierte Scanner/Exploit-Tools infiziert, indem ungepatchte Sicherheitslücken ausgenutzt und dann Bots installiert werden, die weitere Angriffe und Scans ausführen.

Für Volumenangriffe mittels UDP-Reflection/Amplification ist vonseiten der Angreifer noch weniger Aufwand nötig, da die „Lücke" durch falsch konfigurierte UDP-basierte Dienste entsteht (NTP, DNS, CharGen, SSDP). Mit Scannern wie zmap oder masscan lassen sich innerhalb von 4 bis 24 Stunden alle Server im Internet finden, die dann

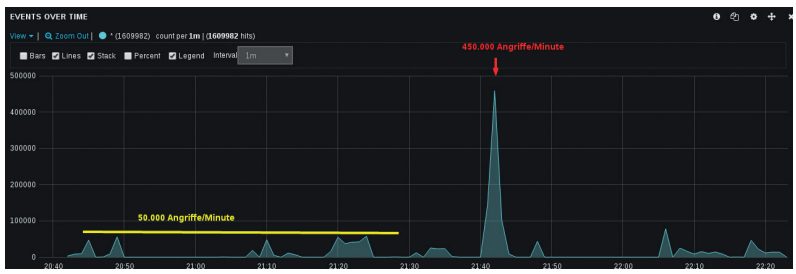

Abbildung 1: Angreifer können für DDoS-Attacken heute auf enorme Ressourcen zurückgreifen.

den Angreifern als Botnetz zur Verfügung stehen. Das OpenResolverProject beziffert die Zahl der als Reflection/Amplification-Bot verfügbaren, falsch konfigurierten DNS-Server auf 23 000 000, während das OpenNTPProject 4 000 000 offene NTP-Server meldet. Für die populärer werdenden Simple-Service-Discovery-Protocol-(SSDP)-Attacken gibt es Zahlen aus dem Jahr 2015, die von 50 bis 80 Millionen verwundbarer DSL-Router ausgehen.

In der Summe stehen heute mindestens 80 bis 100 Millionen Server und Router zur Verfügung, um Reflection/Amplification-Angriffe durchzuführen. Wenn man nur ein Prozent dieser Ressourcen für einen Angriff benutzt und von jedem System aus einen Datenstrom mit 1 MBit/s erzeugt, lässt sich ein Angriff mit circa 800 GB/s Traffic herstellen, dem momentan nur wenige Dienste und Netze gewachsen sind. Dazu kommen mehr als 70

Einteilung der Angreifer

Profis

Professionelle Angreifer haben die technischen Möglichkeiten und das Können, massive Angriffe mit hoher Durchschlagskraft auszuführen. Sie sind in der Lage, einen Angriff über eine längere Zeitspanne aufrechtzuerhalten. In diese Gruppe gehören auch Staaten, die hin und wieder direkt als Verursacher von DDoS-Attacken auftreten, zum Beispiel wenn Nachrichtendienste die Kommunikation missliebiger Gruppen stören. Anders als Erpresser-Gangs treten professionelle Angreifer jedoch nicht mit den Betroffenen in Kontakt. DDoS-Profis lassen sich im Darknet anheuern und können zum Beispiel auch von Unternehmen genutzt werden, um Konkurrenten zu behindern und deren Geschäft zu stören. Die Ziele hinter den Attacken können dabei politischer Natur sein, aber auch finanzielle Hintergründe haben.

Erpresser

Erpresser-Gangs, wie zum Beispiel die DD4BC-Crew, machen sich die vielen ausnutzbaren Server und Systeme zunutze, um vom Internet abhängige Unternehmen zu bedrohen und Geld zu erpressen. Sie können Unternehmen, die nicht auf den Angriff vorbereitet sind, gefährlich werden. Für bessere Anti-DDoS-Provider oder größere Unternehmen mit einer Anti-DDoS-Strategie sind die Angriffe von Erpresser-Gangs jedoch nicht gefährlich, zumindest momentan.

Booter/Stresstester

Seit einigen Jahren gibt es nicht nur „Fuck-of-as-a-Service“, „ALL CAPS AS A SERVICE“, „BOFH-Excuses-as-a-Service“ oder „Star-Wars-Weather-as-a-Service“, sondern auch DDoS-as-a-Service. Einige Botmaster bieten ihre Botnetze zu einem Preis von 15 bis 100 US-$ im Monat an, dabei kann mit Kreditkarte oder Bitcoins bezahlt werden. Über ein Webinterface kann man dann das Ziel eingeben und den Angriff starten. Meist sind die verfügbaren Pakete so strukturiert, dass der Angriff nur für eine voreingestellte Zeit läuft und danach dann neu initiiert werden muss. Der Booter-Markt ist dabei sehr schnelllebig. Webseiten sind häufig nur für drei bis sechs Monate online, gehen vom Netz und entstehen unter anderem Namen und mit leicht anderem Layout kurz danach wieder neu. Einige Tests dieser Booter-Services ergaben, dass die Angriffe von 50 MB/s bis maximal 5 GB/s eher schwach ausfielen, aber ausreichten, um DSL-Anschlüsse oder kleinere Gaming-Server lahmzulegen. Die Booter-Dienste werden häufig von Gamern genutzt, vornehmlich während der Ferienzeit, um Mitspieler vom Netz zu trennen. Booter-Dienste können also als Low-Budget-Low-Impact angesehen werden, die für kommerzielle Dienste selten gefährlich sind. Die Ziele der Booter-Betreiber sind eindeutig finanzieller Natur.

Politische Aktivisten / Hacktivisten

Die Gruppe Anonymous hat ab 2008 DDoS-Angriffe benutzt, um nicht nur auf der Straße, sondern auch im Internet gegen Organisationen und Unternehmen zu protestieren, die ihrer Meinung nach die Freiheit bedrohen. Zu nennen wären hier die Angriffe gegen Scientology (2008) oder „Operation Payback“ als Antwort auf die Kampagne von Kreditkartenunternehmen und Banken gegen Wikileaks (2010), um diese vom internationalen Zahlungsverkehr und damit Spendenzahlungen abzuschneiden. Dazu gesellen sich unterschiedliche, sich manchmal auf Anonymous berufende oder sich davon distanzierende Gruppen, die Unternehmen, Organisationen oder Regierungs-Webseiten angreifen. In den Anfangstagen der DDoS-Angriffe kam ein Tool namens „LOIC – Low Orbit Ion Canon“ zum Einsatz, das als Javascript-Programm im Browser desjenigen läuft, der sich freiwillig an der Attacke beteiligt. Mittlerweile benutzen die Gruppen aber vermehrt eigene Botnetze, manchmal sehr kreativ zusammengestellt, wie die Crew „Lizard Squad“ gezeigt hat. Solche Angriffe können, wenn sie von einer genügend qualifizierten Gruppe durchgeführt werden, durchaus auch größeren Unternehmen gefährlich werden. Neben Banken, Staats- und Regierungsorganisationen werden häufig Organisationen angegriffen, die den weltweiten Austausch von Informationen oder digitalen Gütern regulieren wollen – manchmal als spontaner Ausdruck von Unwillen, manchmal als plakativ angekündigte, koordinierte Aktion.

Millionen Wordpress-Blogs [4], die sich zu einem großen Teil mittels der standardmäßig aktivierten „Pingback“-Funktion für Angriffe auf webbasierte Infrastruktur missbrauchen lassen [5].

Wohin die Reise geht

Diese Voraussetzungen führen zu einer Vielzahl von Angriffen, die Unternehmen auch in Zukunft stark beschäftigen werden. So treten seit 2014 wieder vermehrt die klassischen Schutzgelderpressungen auf: Pünktlich zur CeBIT startete zum Beispiel eine Kampagne gegen Schweizer E-Commerce-Unternehmen, Banken und Zeitungen [5]. Die Angreifer verlangten bis zu 9000 Euro, zahlbar in Bitcoins. Damit hervorgetan haben sich in jüngster Vergangenheit besonders die Gruppen DD4BC, Lizard Squad und Amarda Collective, die auch schon mal Banken gefährlich werden können. Manchmal geht es den Internet-Kriminellen aber auch nur darum, missliebige Informationen zu unterdrücken. Beispielsweise war die Site seitcheck.de, ein Community-basiertes Portal, das über Betrügereien, Abzocke, illegale Abo-Modelle und sonstigen Nepp aufklärt, über lange Zeit immer wieder Ziel von DDoS-Angriffen ohne jedwede Erpressung.

Am oberen Ende der Skala ist zu beobachten, dass die Angriffe immer ausgefeilter werden: Im April 2015 fand eine DDoS-Attacke auf ein komplettes Rechenzentrum (RZ) statt [6], die über neun Tage hinweg gegen alle IPs des RZ geführt wurde. Die Angriffe kamen in Wellen mit je zwei bis sechs Stunden Dauer, zu unterschiedlichen Zeiten und mit einer Stärke von 100 GB/s – sie wurden mit hoher Professionalität ausgeführt und das eigentliche Ziel verschleiert. Da in dem Rechenzentrum jedoch Webseiten einiger ukrainischer Tageszeitungen gehostet wurden, liegt der Verdacht nahe, dass hinter dem Angriff politische Motive steckten.

Wozu professionelle staatliche Angreifer fähig sind, zeigt auch ein weiterer bemerkenswerter DDoS-Angriff, der letztes Jahr auf den Dienst Github [7] stattfand: Dort befand sich neben vielen Open-Source-Projekten auch die chinakritische Webseite GreatFire.org, die sich mit der „Great Firewall of China“ beschäftigt. Für den Angriff auf den Dienst wurde Besuchern der Suchmaschine Baidu ein Javascript-Snippet untergeschoben, dass dann über den Browser der Benutzer in geringer Frequenz Seiten von Github.com abrief. Durch die Vielzahl von infizierten Browsern kamen bei Github circa zwei Millionen Anfragen pro Sekunde an, was den Dienst komplett überlastete und letztlich lahmlegte. Spätere Analysen ergaben, dass die DDoS-Attacke von einem Tool ausging, das anscheinend in die „Great Firewall“ integriert war und darum „Great Cannon“ getauft wurde.

Weiterhin ist zu beobachten, dass sich Operationen nicht mehr nur auf einen Vektor beschränken: Bei den Attacken auf den österreichischen Telekommunikationsanbieter A1 im Februar [8] wurden zum Beispiel über zehn Tage hinweg immer wieder neue Ziele angegriffen, sodass Abwehrmaßnahmen nur kurzfristig halfen. Die Angreifer waren auf jeden Fall sehr gut vorbereitet.

Webapplikationen stehen ebenfalls noch im Fokus der Cyberkriminellen: Die Angriffe werden überwiegend von Botnetzen ausgeführt, die aus 1000 bis 5000 Bots bestehen und üblicherweise 300 bis 1000 Anfragen pro Sekunde erzeugen. Hin und wieder wurden aber auch Attacken von Botnetzen mit mehr als 10 000 Bots und knapp 10 000 Anfragen pro Sekunde registriert, die für viele ungeschützte webbasierte Applikationen bedrohlich sind (vgl. Abb. 1).

Fiese Maschen

Wer denkt, wenn die Firmenwebsite weg ist, wäre das nicht so schlimm, der irrt beziehungsweise geht von falschen Zielen der Angreifer aus: Denn nur ein kleiner Teil der Attacken betrifft Websites, der weitaus größere richtet sich gegen die Internet-Infrastruktur. Wenn zum

Level	Bezeichnung	Angriffsstärke	Vektoren
1	Poking/Anklopfen	< 10 MBit/s	1
2	Script-Kiddy, Booter-Service	< 100 MBits/s	2
3	Basic-Level-Professionals	< 1 GBit/s	5
4	Sophisticated Professionals	< 10 GBit/s	10
5	Advanced Professionals	< 50 GBit/s	unlimitiert
6	Extreme Professionals	< 100 GBit/s	unlimitiert
7	Staatliche Angreifer	unlimitiert	unlimitiert

Tabelle 1: DDoS-Resiliency-Score

Beispiel die DNS-Infrastruktur nicht ausreichend geschützt ist, kann ein Angreifer ein Unternehmen quasi spurlos von der digitalen Bildfläche verschwinden lassen.

So gibt es viele Firmen, die sowohl DNS- als auch E-Mail-Infrastruktur selbst oder bei einem externen Anbieter betreiben, die weniger als zehn Gigabyte Uplink-Kapazitäten und keinen DDoS-Schutz vorhalten – dadurch sind sie akut von DDoS-Angriffen bedroht. Beispielsweise wurde eine regional tätige Wohnungsverwaltungsgesellschaft mit knapp 40 Mitarbeitern fünf Tage lang von einem erbosten Mieter mit DDoS-Angriffen überzogen. Das Unternehmen ist in einer strukturschwachen Region mit einer schmalen DSL-Leitung angesiedelt und war auf VoIP, extern genutzte Einsatzpläne für Wartungspersonal und Dienstleister, externes Customer-Relationship-Management (CRM) und größtenteils auf E-Mail basierende Kommunikation angewiesen – und somit komplett handlungsunfähig. Kosten für den Angreifer: 50 US-$ pro Tag.

Ebenso ist es in der aktuellen Lage ein Trugschluss, dass ein Content-Delivery-Network (CDN) ausreichend schützt: Im November 2015 wurde das Tool ARDT [11] veröffentlicht, mit dem eine so genannte CDN-Reflection-Attacke möglich ist. Dabei nutzten die Cyberkriminellen den Umstand aus, dass ein weltweit verteiltes CDN Zugang zu den eigentlich geschützten Systemen (Origin) hat und gestalteten ihre Zugriffe derart, dass alle CDN-Edge-Server gleichzeitig auf die geschützten Systeme zugreifen. Im Falle des CDN-Anbieters Akamai wurde so ein Angriff mit knapp 100 000 Anfragen pro Sekunde möglich. Auch der Anbieter Cloudflare ist als weltweites CDN aufgebaut und für diese Angriffe anfällig. So lässt sich selbst die Cloudflare-Challenge, ein auf Cookie und Javascript basierter Schutz, automatisiert aushebeln: Da das Anti-DDoS-Cookie für die gesamte Cloudflare-Infrastruktur für ein Jahr gültig ist, können Angreifer eine CDN-Reflection-Attacke ausführen.

Ein weiterer Trend ist das „Smokescreening“, eine Technik, die vor allem von Hackergruppen genutzt wird, die bereits in ein Netz eingedrungen sind. Sie benutzen den

Literatur

[1] 8ack, DDoS-Angriffe – Die globale Bedrohung, Whitepaper, 2015, https://8ack.de/core/showroom/odosseus/DDoS-Whitepaper.pdf

[2] Florian Kalenda, DDoS-Angriff auf Spiele-Site legt halb Schweden lahm, ZDNet online, Dezember 2014, www.zdnet.de/88213792/ddos-angriff-auf-spiele-site-legt-halb-schweden-lahm/

[3] Akamai, SSDP Reflection DDOS Attacks, Threat Advisory, Oktober 2014, www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/ssdp-reflection-ddos-attacks-threat-advisory.pdf

[4] Craig Smith, By the Numbers: 29 Amazing WordPress Statistics, DMR Blog, Juli 2016, http://expandedramblings.com/index.php/wordpress-statistics/

[5] Ronald Eikenberg, DDoS-Attacken auf Schweizer Websites, heise Security, März 2016, http://heise.de/-3144854

[6] 8ack, DDoS-Angriffe auf ukrainische und russische Rechenzentren, April 2015, https://8ack.de/guides/ddos_angriffe_auf_ukrainische_rechenzentren

[7] Bill Marczak, Nicholas Weaver, Jakub Dalek, Roya Ensafi, David Fifield, Sarah McKune, Arn Rey, John Scott-Railton, Ronald Deibert, Vern Paxson, China’s Great Cannon, Citizen Lab, April 2015, https://citizenlab.org/2015/04/chinas-great-cannon/

[8] Martin Stepanek, Angriffe auf A1 gehen unvermindert weiter, Futurezone Technology News, Februar 2016, http://futurezone.at/digital-life/angriffe-auf-a1-gehen-unvermindert-weiter/179.233.622

[9] Red Button, DDoS Resilience Score (DRS) Standard, Oktober 2015, http://red-button.net/wp-content/uploads/2016/07/DDoS-Resiliency-Score-Standard-1.00.00.pdf

[10] Red Button, DDoS Resilience Score (DRS) Standard Overview, Mai 2016, http://red-button.net/wp-content/uploads/2016/05/DDoS-Resiliency-Score-Overview-1.pdf

[11] „Mitch x90“, Akamai Reflective DDoS Tool – Attack the origin host behind the Akamai Edge hosts and DDoS protection offered by Akamai services, GitHub Projektseite, https://github.com/m57/ARDT

DDoS-Angriff, um die Administratoren unter Stress zu setzen und von der eigentlichen Aktion abzulenken, zum Beispiel um größere Datenbestände zu transferieren oder intern weitere Ziele anzugreifen. Beim Smokescreening findet der Angriff in mehreren Wellen statt, damit die Administratoren möglichst vollends mit der Abwehr der Attacke beschäftigt sind.

DDoS-Resiliency-Score

Ein DDoS-Schutz sollte immer integraler Bestandteil einer umfassenden Strategie zur Abwehr von Cyberangriffen sein. Eine effektive Lösung hängt dabei von der jeweiligen, individuellen Bedrohungslage und den Anforderungen des Unternehmens ab. Um den eigenen Schutzbedarf zu ermitteln, lässt sich der im letzten Jahr vorgestellte DDoS-Resiliency-Score [9,10] benutzen, der auf einfache Weise aufzeigt, ob das implementierte Schutzniveau mit der Bedrohungslage einhergeht oder ob es eine Lücke gibt (vgl. Tab. 1). Den Score kann man für einzelne Teilbereiche oder auf eine gesamte Organisation anwenden. Er gibt den Verantwortlichen ein Werkzeug an die Hand, um der beteiligten Leitungsebene (C-Level) kurz und knapp den aktuellen Stand zu verdeutlichen.

Egal, welcher Schutz letztlich implementiert wird: Das verantwortliche Admin-Team sollte regelmäßig die Arbeitsabläufe im Falle eines DDoS-Angriffs mithilfe eines Stresstests üben. Die Übungen können als echte Angriffe durchgeführt werden, um zu testen, ob die implementierten Schutzmechanismen wie erwartet funktionieren – oder als Simulation auf dem Papier, um primär die Abläufe und Alarmierungswege zu überprüfen.

Fazit

DDoS-Angriffe können für Unternehmen unterschiedliche Auswirkungen haben: von „lästig wie ein Mückenstich“ bis hin zu Verlusten von mehr als einer Million US-$ pro Tag. Das Grundproblem ist jedoch, dass es zu viele angreifbare Systeme gibt und die Hürde, sie zu finden und in ein eigenes Botnetz zu integrieren, sehr gering ist.

Das Thema DDoS wird uns also weiter verfolgen: Sicherheitsunternehmen werden immer neue Rekorde bei der Länge, Breite und Höhe der jeweils erkannten und gestoppten Angriffe melden und neue Sicherheitslücken sowie fehlkonfigurierte Systeme sorgen für regelmäßigen Nachschub an Bots.

Hinzu kommt, dass im jetzigen Stadium der vernetzten Welt professionelle DDoS-Angriffe gegen Einrichtungen eines Landes, Organisationen oder Regionen durchaus auch Schaden bei der Bevölkerung anrichten können – solche Cyber-Angriffe also auch als verdeckte Auseinandersetzung zwischen Staaten dienen können.

DDoS-Angriffe sind schon heute Teil des Cyberwars und werden langfristig nicht von der Bildfläche verschwinden. Dabei wird die Intensität weiter zunehmen und die DDoS-Dienstleister werden sich weiter professionalisieren. Gegen viele Angriffsvektoren lassen sich aber Schutzmaßnahmen aufbauen. ■

Markus Manske ist Leiter Technik bei der 8ack GmbH.