Das Internet der Dinge verstärkt DDoS-Angriffe

Digitales Bombardement

Christoph Puppe

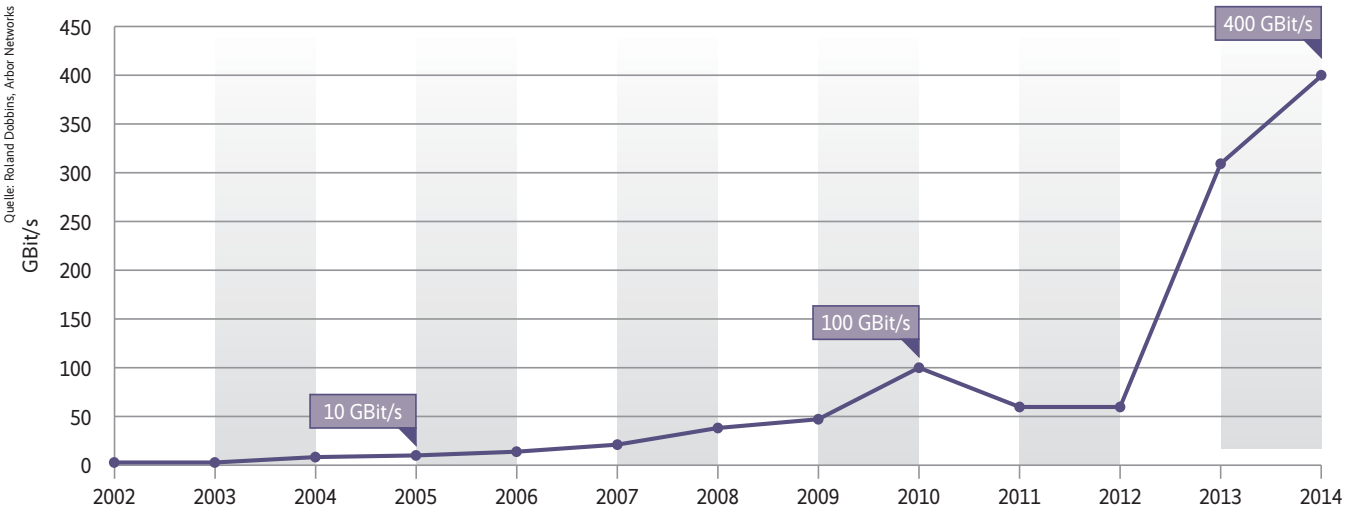
Im Herbst 2016 fanden die bisher heftigsten verteilten Angriffe auf den unverzichtbaren Internetdienst DNS statt. Noch größeres Unheil steht zu befürchten, doch Anwender und Anbieter sind nicht vollkommen wehrlos.

Im September und Oktober 2016 fanden Distributed-Denial-of-Service-Angriffe noch nie da gewesener Größenordnung im Internet statt. Selbst der große Anbieter von DDoS-Abwehrdiensten Akamai musst aufgeben und seine Dienste für den prominenten Security-Experten und Pro-bono-Kunden Brian Krebs einstellen. Kurz zuvor waren bereits entsprechende Drohungen eingegangen. Erpressung mit DDoS ist seit Jahren ein Geschäftsmodell, doch spätestens mit den letzten Angriffen muss sich die aufs Internet angewiesene Gesellschaft Gedanken machen, ob sie sich einer Technik ausgeliefert hat, die sich im Ernstfall nicht verteidigen lässt.

DDoS-Angriffe sind für die Täter preiswert und einfach. Für die notwendigen Datenmengen bedienen sie sich eines Netzwerks übernommener Geräte, deren Betriebs- und Verbindungskosten sie nicht tragen. Um so operieren zu können, benötigen sie eine große Zahl verwundbarer Geräte, die aus dem Internet erreichbar sind. Früher waren dies fast ausschließlich private PCs mit Windows als Betriebssystem, aber auch Server unter Linux und Windows. Heute kommt eine wachsende Schar kleiner, alltäglicher Gadgets hinzu – und das sind nicht nur Smartphones: Besonders die Geräte im „Internet of Things“ lassen sich oft einfach übernehmen und in ein Botnetz integrieren. Deren Hersteller achten kaum auf die Sicherheit und bieten höchst selten Updates an.

Geschäftsmodell Erpressung und politische Motivation

Auch andere, zum Teil seit 20 Jahren bekannte Faktoren spielen eine Rolle. So ist es immer noch trivial, die Quelladresse eines Datenpakets zu fälschen und somit eine Verstärkung des Angriffs zu erreichen. Dazu tragen Provider von Endkundenanschlüssen und auch RZ-Dienstleistungen bei, die den ausgehenden Datenverkehr nicht auf Plausibilität filtern. Der Angreifer versendet dann eine verhältnismäßig kleine Anzahl von Datenpaketen, in denen er die Absenderadresse auf die Adresse des Angriffsopfers fälscht (Spoofing). Wenn die Datenpakete ihr Ziel erreichen, landet die Antwort somit beim Opfer. Für diese Reflexions- und Amplifying-Angriffe bieten sich Protokolle wie Chargen, DNS, SNMP, NTP und SSDP an, die auf kleine Anfragepakete erheblich größere Antworten senden – teils geht es um den Faktor 1000. Einen Überblick über die Lage bietet unter anderem die „Digital Attack Map“ des Serviceanbieters Arbor (siehe Abbildungen und „Alle Links“).



Sowohl die Zahl als auch die Heftigkeit der DDoS-Angriffe steigt seit 2012 beängstigend schnell (Abb. 1).

DDoS als Drohung im Rahmen einer Erpressung kann erhebliche Summen einspielen. Gerade mittelständische Firmen lassen sich auf diese Weise schröpfen, aber auch internationale Konzerne sind Opfer von Cybercrime. Die Täter folgen oft einem eingespielten Muster: Zuerst stören sie die Webpräsenz oder die Außenverbindung der Firma für etwa eine Stunde mittels DDoS-Angriff. Dann trifft eine E-Mail ein, die darauf hinweist, dass dies nun wiederholt passieren wird, sofern die Firma nicht eine bestimmte Bitcoin-Summe an eine anonyme Adresse überweist.

Auch Aktivisten jeglicher Couleur haben DDoS als die Waffe des kleinen Mannes gegen Konzerne, Staaten und Andersdenkende für sich entdeckt. „DDoS as a Service“ mit einfach zu bedienenden Weboberflächen zur Steuerung des Angriffs gibt es auf dem Schwarzmarkt unter Produktnamen wie Botter oder Stresser. Damit kann jeder, der möchte, entweder in das Geschäft mit Erpressungen einsteigen oder seiner Meinung online Nachdruck verleihen. Die Kosten liegen gerade einmal im dreistelligen Dollar-Bereich für einen eintägigen DDoS-Angriff mit mehreren 100 GBit/s.

Hier findet sozusagen eine Demokratisierung einer mächtigen Waffe statt, gegen die sich kleinere Firmen, Blogs und Webseiten kaum oder nur mit horrendem Aufwand verteidigen können. Allerdings gab es auch Fälle, in denen Staaten die Webseiten von Kritikern mit DDoS aus dem Netz warfen. Neben dem ungleich aufwendigeren Infiltrieren kritischer Infrastrukturen sind solche Angriffe die wichtigste Waffe im „Cyberwar“, in dem Konfliktbeteiligte ohne große Ressourcen einen erheblichen Schaden anrichten können.

DNS als dankbares Ziel

Nach den DDoS-Angriffen auf Dyn, einen großen Anbieter von DNS-Dienstleistungen, wurde vielen der Ernst der Lage bewusst. Es folgten einige Vorschläge, wie sich die Sicherheit erhöhen lassen könnte. Einer lautet, die Störerhaftung auf die Inhaber der an den Angriffen beteiligten Geräte auszuweiten. So wären die Kunden gezwungen, ihre Computer, IP-Kameras und Babyphones regelmäßig mit Sicherheitsupdates zu versorgen. Das kann aber nur dann klappen, wenn die Hersteller überhaupt Updates liefern. Dass das weit an der Realität vorbeigeht, belegt ja schon die Smartphone-Branche auf eindrückliche Weise (siehe auch den Kommentar).

Eine Alternative bestünde darin, die Hersteller in die Verantwortung zu nehmen und bei dieser Gelegenheit die von vielen geforderte Produkthaftung auch in der IT einzuführen. Eine ganz andere Richtung verfolgt der Vorschlag von Internetexperten, die meinten, dass doch der Staat die für DDoS missbrauchten Geräte selbst hacken möge, um dann eine sichere Konfiguration einzuspielen. Dazu sagte Linus Neumann, einer der Sprecher des Chaos Computer Clubs, in der „Zeit“: „Sofern das FBI den Prozess ordentlich dokumentiert und keinen Anlass für Misstrauen bietet, ist es vermutlich im Interesse des Großteils der Nutzer“, und fügt hinzu: „Sofern die Geräte eine bekannte Sicherheitslücke aufweisen, können sie einzeln und automatisiert übernommen, desinfiziert und per Update von der Sicherheitslücke befreit werden“ (siehe „Alle Links“).

Einen anderen Weg geht die Telefongesellschaft Singapurs, die den Inhabern gekaperter Geräte laut Zeitungsberichten Hausbesuche abstattet – als Reaktion auf einen DDoS-Angriff, der die Telefongesellschaft selbst traf und an dem offenbar die Geräte der eigenen Kunden maßgeblich beteiligt waren.

Derlei noch vor Kurzem undenkbare Lösungsvorschläge belegen eine regelrechte Verzweiflung. Es steht nicht zu erwarten, dass eine staatliche Stelle die Erlaubnis und den Auftrag erhält, Geräte der Bürger anzugreifen und Software darauf zu installieren – nicht einmal zum Zweck des Sicherheitsupdates.

Dass die Besitzer der Geräte für ihre Beteiligung in die Haftung geraten, steht bei Tausenden an einem Angriff beteilig-

iX-TRACT

- Die rasch wachsende Zahl von Internet-Devices im IoT und höhere Datenraten für Endkunden tragen zu immer stärkeren DDoS-Angriffen bei.
- Bisherige Ideen, die einen Beitrag zum Senken des DDoS-Risikos liefern sollen, erscheinen unrealistisch.
- Eine Vorsorge ist notwendig und in gewissem Rahmen möglich, nicht nur seitens potenzieller Opfer, sondern auch der Internetprovider.

ten Systemen nicht zu erwarten. Denn es kommt neben ethischen Aspekten und den Bedenken der Datenschützer ein Umstand hinzu, der solche Ideen ins Reich der Fantasie verweist: Das Internet ist international verteilt – und die Botnetze sind es auch. Die meisten der bis zu 500 000 Geräte in einem Botnetz befinden sich aus Sicht des Angegriffenen nun einmal im Ausland. Hier Haftung für Besitzer und Hersteller einzuführen oder Updates ungefragt in diese Geräte einzuspielen, erscheint also unmöglich. Als Beispiel diene erneut der Angriff gegen Dyn, der seinen Ursprung zum Großteil in Asien hatte, oder der erfolgreich abgewehrte 540-GBit/s-Angriff auf die Internetinfrastruktur der Olympischen Spiele (siehe „Alle Links“).

Auch wenn wirksame Gegenmaßnahmen derzeit nahezu unmöglich erscheinen, gehen die Vorschläge zumindest in eine Richtung, die eine nachhaltige Verbesserung der Internetsicherheit mit sich bringen könnte. Allerdings nicht als Alleingang, sondern – wie in Gestalt des Cybercrime Treaty – als international koordinierter Ansatz, der auch Datenschutzaspekte beachten muss. Sollten Länder oder Blöcke gemeinsam vorausgehen, steht zu befürchten, dass eines Tages Firewalls an allen internationalen Peering-Knoten stehen werden, die dort offiziell Schadsoftware und DDoS-Traffic aus Ländern ohne diese Gesetze abfangen sollen, sich aber auch prima dafür eignen würden, missliebige Inhalte zu unterdrücken.

Gut vorbereitet ist halb gewonnen

Laut Sun Tzu, dem Autor von „Die Kunst des Krieges“, darf man nur in die Schlacht ziehen, wenn man weiß, dass man gewinnt. So sollte sich eine Firma, Behörde oder ein sonstiger Betreiber eines Internetdienstes schon beim Planen seines Angebots mit dem DDoS-Risiko auseinandersetzen. Selbst Privatpersonen können ihre Webserver so im Internet platzieren, dass ihnen ein Angriff wenig anhaben kann. Und für Firmen oder Organisationen bieten kommerzielle Angebote einen gewissen Schutz bei vertretbaren Kosten. Wer also beachtet, dass es Bot- und Amplifier-Netze gibt und nicht jeder Provider ordentliche Filter implementiert, muss sich entsprechend rüsten, wenn ihm die Erreichbarkeit der eigenen Angebote am Herzen liegt.

Wie es sich für eine gute Verteidigungsstrategie gehört, sollten sich die Betroffenen in mehreren Stufen absichern. Bereits die Anwendungen selbst sollten resistent gegen Angriffe sein, die zum Beispiel Server mit einer einzigen Anfrage lahmlegen können. So können Anwendungen eine Session über mehrere Server verteilen, sodass der Ausfall eines Servers nicht den Kunden hinauswirft. Die Zahl der Server sollte sich außerdem dynamisch an die Zahl der Anfragen anpassen, um Lastspitzen abzufangen.

Der Einsatz eines Load Balancers gehört zu den notwendigen und verbreiteten Schutzmechanismen. Auch eine Web-Application-Firewall sowie eine Firewall mit erweiterten Funktionen zum Erkennen eines DDoS-Angriffs sind zu empfehlen. Die bekannten Hersteller von Netzwerktechnik verkaufen solche Produkte. Deren „Intelligent DDoS Mitigation Systems“ sind auf das Erkennen und Ableiten von DDoS-Angriffen spezialisiert und bieten damit einen zusätzlichen Schutz.

Derlei Maßnahmen helfen gegen Angriffe, die vornehmlich auf die Anwendungsschicht zielen. Einen DDoS-Angriff, der die Internetanbindung überlastet, halten sie aber nicht auf. Und Leitungen, die heutige DDoS-Größenordnungen aushalten, sind unwirtschaftlich. Ein Ausweg besteht darin, zwei Anschlüsse zu nutzen: einen für die öffentlich sichtbaren Dienste

Quelle: Arbor Networks, http://www.digitalattackmap.com/

Einen laufenden Überblick über DDoS-Angriffe gewährt Arbor Networks. Hier sind unter anderem Ziele in Indonesien und Südkorea unter Beschuss (Abb. 2).

und einen für die internen Verbindungen zu Partnern, Niederlassungen und VPN-Nutzern. Dann funktioniert zumindest das interne Netz noch, wenn ein DDoS-Angriff nach außen sichtbare Dienste wie E-Mail oder Web trifft.

Manche Provider bieten Internetzugänge an, die sie von mutmaßlichen Datenpaketen eines DDoS-Angriffs säubern. Oft ist eine Filterung von Schadsoftware im Web- und E-Mail-Traffic im Angebot enthalten. Solche „Clean Pipes“ senken bei wenig höheren Kosten das DDoS-Risiko – wenn man sich denn darauf einlassen mag, dass der Provider die Inhalte überwacht, die über die Leitung gehen, und dass mit jeder Filterung eine gewisse Fehlerquote einhergeht.

Separate Anschlüsse für unterschiedliche Anwendungszwecke sind allerdings vorzuziehen, wenn die Anforderungen an die Verfügbarkeit sehr hoch sind. Für kleinere Unternehmen bieten zusätzliche Filter einen Vorteil, da sie so eigene Investitionen in Sicherheitstechnik einsparen können.

Over-Provisioning mithilfe der Cloud

Wer die Verfügbarkeit seiner Online-Präsenz hoch halten möchte, kann dies mit Cloud-Angeboten der großen „Content Distribution Networks“ (CDN, das Kürzel steht auch für „Content Delivery Networks“) erreichen: Das eigene Angebot wird hinter den Adressen des CDN verschleiert und ein Angriff trifft dieses. Allerdings sind weitere Maßnahmen nötig, die verborgenen Adressen tatsächlich geheim zu halten. Eine IP-Adresse im Header der Webseite oder einer E-Mail zum Passwort-Reset kann dem Angreifer bereits die reale IP-Adresse des eigenen Angebots mitteilen. Wenn möglich sollten diese Adressen nur für die CDN-Server erreichbar sein.

Dem Anbieter des CDN stehen mehr Mittel zur Verfügung, Datenpakete eines DDoS-Angriffs zu erkennen und zu filtern. Große Anbieter dieser Dienstleistungen nutzen bis zu 10 Terabit/s Leitungskapazität zu anderen Providern und sind somit in der Lage, Angriffen mit vielen 100 Gigabit/s standzuhalten. Außerdem haben diese Anbieter die Kontrolle über ihr Routing, da sie als autonome Systeme im weltweiten Verbund agieren und per Border-Gateway-Protokoll das Routing der Daten bereits auf dem Weg zu ihren Übergabepunkten steuern. So können sie einen heftigen Angriff auf mehrere Eingangsknoten verteilen und damit verhindern, dass ein Knoten versagt.

Derlei findet teilweise automatisiert statt, benötigt aber das Fachwissen von IT-Sicherheitsexperten, die sich auf das Thema spezialisiert haben. Wenn etwa ein hauptsächlich in Asien aktives Botnetz einen Server in Brasilien angreift, würden fast alle Daten den für diese Region zuständigen Übergabepunkt erreichen und ihn überlasten. Eine Änderung der BGP-Regeln zum Routing des brasilianischen Servers verteilt die Last, indem das Sicherheitsmanagement zum Beispiel alle Pakete von einem Dutzend Providern der Region auf einen anderen Knoten lenkt und so den zuerst angesprochenen Knoten entlastet. (Ein Twitter-Beitrag mit sehenswerter animierter Grafik findet sich unter „Alle Links“.)

Kleinunternehmen, Mittelständler und Privatpersonen erhalten bei den großen Anbietern gegen kleine Beträge ebenfalls einen Schutz, der technisch dem entspricht, was die größeren Kunden erhalten. Auch hier verursacht es also wenig Arbeit und kaum Kosten, eine solide Vorsorge vor DDoS-Angriffen zu treffen. Für Groß und Klein gilt: Wer möchte, kann seine Inhalte bei einem der großen Anbieter hosten lassen. Deren Load Balancer bieten bereits ein gewisses Maß an DDoS-Resistenz und können Angriffen mit mehreren GBit/s standhalten.

Die Angriffe auf Dyn haben das DNS erneut als entscheidenden Schwachpunkt

Kommentar: Aus Fehlern lernen?

Was haben IT und Autofahren gemeinsam? In beiden Fällen betreiben und nutzen wir die Technik in unangemessener – sprich unsicherer – Art und Weise. In beiden Fällen wundern wir uns, wenn doch etwas passiert. Und in beiden Fällen müssen wir Fehler mehrmals begehen, bis endlich ein Lerneffekt einsetzt.

In der IT wurde schon in den 1980er-Jahren deutlich, dass nicht alles einfach ans Netz sollte. Als der TCP/IP-Stack auch für die Host-Systeme verfügbar wurde, zeigte sich zwar schnell, dass mit der Integration in die mittlerweile vorherrschenden netzwerkbasierten Client-Server-Systeme erhebliche Vorteile verbunden waren. Auf der anderen Seite wurde aber – oft leider erst nach erfolgter Netzanbindung – auch klar, dass es bei Host-Systemen in der Regel bereits an den einfachsten Mechanismen – etwa SSL und SSH – fehlte, die für eine angemessene Absicherung von TCP/IP-Netzen unerlässlich sind.

Auch bei Smartphones hätte man sich eher überlegen können, welche Nachteile vor allem mit Mechanismen wie „always online“ und „Software aus unbekannten Quellen“ verknüpft sind. Denn Smartphones – und damit alle Daten, die sich auf ihnen befinden – sind nicht nur schnell geklaut. Viele sind aufgrund ausbleibender Betriebssystem-Updates zudem für Angreifer aus dem Netz von hohem Interesse. Und dabei geht es schon lange nicht mehr nur um die persönlichen Daten des Nutzers, sondern auch um Firmen- und Staatsgeheimnisse.

Anwender haften zu lassen, wäre weltfremd

Und nun kommen auch noch im Internet der Dinge Geräte ans Netz, die eigentlich nicht dafür gemacht oder unzureichend abgesichert sind und deren Ressourcen für einen besseren Schutz häufig nicht ausreichen. Während bei den Smartphones bisher aber meist „nur“ Daten betroffen waren, geht es jetzt auch um lebenswichtige – teilweise überlebenswichtige – Geräte und Steuereinheiten. Zudem lassen sich massenhaft übernommene IoT-Geräte vorzüglich als Angriffswerkzeuge einsetzen. Davon können kritische Infrastrukturen betroffen sein, beispielsweise das Domain Name System, ohne das im Internet nichts geht – wie die DDoS-Angriffe der jüngsten Vergangenheit auf eindrucksvolle Weise zeigen.

Anwender haften zu lassen, deren Gerätschaften Sicherheitslücken haben und als Angriffswerkzeuge dienen, wäre allerdings weltfremd: Sie haben in der Regel gar keine Möglichkeit, die Geräte zu patchen oder sicher zu betreiben. Mit seinem Urteil zur WLAN-Haftung hat so auch der Bundesgerichtshof argumentiert. Er stellte bereits 2010 klar, dass ein Anwender lediglich die zum Kaufzeitpunkt vom Gerät – im konkreten Fall dem WLAN-AP – bereitgestellten Sicherheitsmechanismen adäquat nutzen muss. Nachträgliche Verbesserungen forderte er gerade nicht vom Nutzer.

Bleibt die Frage, wer denn nun für etwaige Schäden durch unzureichende Sicherheitsmaßnahmen aufkommen soll. Denkbar wäre, die Hersteller stärker in die Pflicht zu nehmen – es muss ja keine ausufernde Produkthaftung wie in den USA sein. Ein wenig mehr Regulierung scheint jedenfalls angebracht, damit Hersteller Zwischenfälle nicht einfach aussitzen oder den Support nach häufig allzu kurzer Zeit einfach ganz einstellen. Ob das IT-Sicherheitsgesetz diesbezüglich ein Schritt in die richtige Richtung war, muss sich noch zeigen.

Aber all das interessiert ja eh niemanden – solange nichts Schlimmes passiert. Denn: Wir lernen erst dann, wenn wir selbst betroffen sind, und wir vergessen schnell. Und dies gilt für die Einführung und Nutzung unzureichend gesicherter IT offenbar genauso wie für den klassischen Auffahrunfall durch zu dichtes Auffahren. Es bleibt allerdings zu hoffen, dass wir in der IT auch die potenziellen Auswirkungen im Griff haben, wenn wirklich einmal ein gravierender Schaden eintritt.

Christoph Wegener, wecon.it-consulting

Dienste gegen DDoS-Angriffe

Beim Thema DDoS-Abwehr empfiehlt es sich, einen möglichst großen Partner zu wählen, der über die notwendigen Kapazitäten verfügt. Die Aufzählung erhebt keinen Anspruch auf Vollständigkeit.

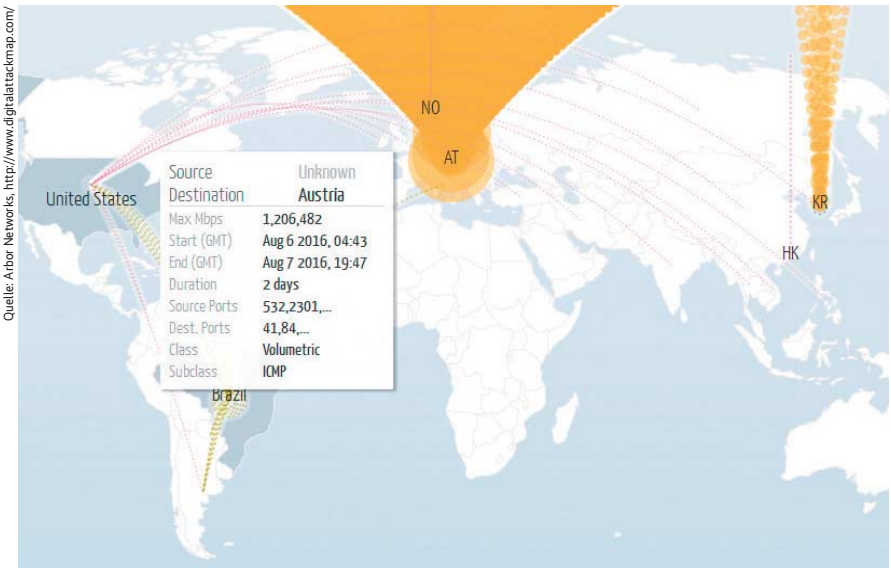
Content Delivery Networks:

- Arbor Networks
- Imperva
- Cloudflare
- Akamai Technologies
- Google

Clean Pipe:

- Level3 Communications
- Deutsche Telekom

Quelle: Arbor Networks, http://www.digitalattackmap.com/



Bei etlichen heftigen Angriffen lässt sich nicht feststellen, welchen Ausgangspunkt die unzähligen Datenpakete genommen haben (Abb. 3).

des Internets ins Blickfeld gerückt. Seit Jahren ist bekannt, dass ein Ausfall von DNS-Servern gravierende Auswirkungen hat. Ohne die zu den Hostnamen im DNS hinterlegten IP-Adressen funktioniert das Internet nicht. Ein lang anhaltender Angriff auf sämtliche Root-Server, die in der DNS-Hierarchie am höchsten stehen, wäre der schlimmste denkbare Fall: Sobald die Lebensdauer der zwischengespeicherten DNS-Daten abläuft, wäre das Internet fast vollständig unbenutzbar.

Das Domain Name System schützen

Einen Vorgeschmack auf dieses Worst-Case-Szenario gab der DDoS-Angriff auf die Server der Firma Dyn am 20. Oktober 2016. Dyn stellt nicht nur DNS-Dienste für Heim-Router, sondern auch für viele große Internetunternehmen bereit. Mit Kunden wie Twitter, Netflix, PayPal und Spotify bildet Dyn ein so zentrales wie verlockendes Angriffsziel. Im Dezember 2015 hatte es bereits einen Angriff auf die Top-Level-Domain der Türkei gegeben. Um alle .tr-Domains aus dem Netz zu nehmen, reichten 40 GBit/s. Beim besagten Angriff auf Dyn wurden bis dahin unglaubliche 1,2 Terabit pro Sekunde gemessen [f].

Verwunderlich, dass die vom Dyn-Ausfall Betroffenen nicht besser vorgesorgt hatten. Das DNS bietet einfache Mittel der Lastverteilung: Wer nicht von einem einzelnen DNS-Server oder Anbieter abhängig sein möchte, muss lediglich mehrere DNS-Server bei unterschiedlichen Anbietern in der Domain-Konfiguration eintragen – natürlich erst, sobald es einen Account bei den Anbietern gibt und die Daten der Domain vorliegen.

Einen alternativen Weg, eine gewisse Redundanz herzustellen, gehen manche Provider schon seit Jahren zum Leidwesen der DNS-Administratoren: Sie speichern die Domain-Daten (DNS Resource Records) länger als vorgegeben auf ihren DNS-Servern. Das ungefragte Verlängern der Gültigkeitsdauer entlastet zwar die Netze der Provider, kann allerdings dazu führen, dass Domain-Änderungen die Endkunden mit einigen Tagen Verspätung erreichen.

Das bewusste Hinauszögern des Ablaufzeitpunkts kann sich, etwas geschickter ausgeführt, aber auch als Vorteil erweisen. Normalerweise holt der DNS-Server eines Providers die benötigten Einträge vom zuständigen (authoritative) DNS-Server der Domain. Wenn der nicht antwortet, beispielsweise weil ein Angriff auf ihn stattfindet, dann antwortet auch der DNS-Server des Providers nicht – die gesuchte Domain wird für den anfragenden Kunden praktisch ausgeblendet, selbst wenn sämtliche Dienste unter dieser Domain eigentlich online sind.

Der auf DDoS-Abwehr spezialisierte Anbieter Cloudflare hat daher als Reaktion auf den Angriff auf Dyn seine DNS-Server modifiziert. Falls der zuständige Nameserver ausfällt, geben sie nun die zuletzt von ihm gelieferte Antwort nochmals weiter – so lange, bis er seinen Dienst wieder aufnimmt. Auf diese Weise bleiben Dienste wie WWW oder E-Mail selbst in solchen Domains erreichbar, deren DNS ausgefallen ist.

Wie bei jedem inoffiziellen Eingriff in ein bewährtes Internetprotokoll muss sich nun zeigen, ob es dieser in weitverbreitete DNS-Serversoftware – etwa BIND –

Onlinequellen

[a] Arbor Digital Attack Map
http://www.digitalattackmap.com/

[b] Rio Olympics Take the Gold for 540gb/sec Sustained DDoS Attacks!
https://www.arbornetworks.com/blog/asert/rio-olympics-take-gold-540gbsec-sustained-ddos-attacks/

[c] BGP-Updates als animierte Grafik
https://twitter.com/IamStan/status/789492066208415746

[d] Die Polizei, dein Freund und Hacker
http://www.zeit.de/digital/internet/2016-10/ddos-attacken-internet-der-dinge-fbi-hacker

[e] Learning how to take down the internet
https://www.schneier.com/blog/archives/2016/09/someone_is_lear.html

[f] Details emerging on Dyn DNS DDoS attack, Mirai IoT botnet
http://searchsecurity.techtarget.com/news/450401962/Details-emerging-on-Dyn-DNS-DDoS-attack-Mirai-IoT-botnet

schafft und sich als Standard durchsetzt. Zu wünschen wäre es, denn selbst längere DDoS-Angriffe gegen DNS-Server verlören damit etwas von ihrem Schrecken.

Nicht selbst zum Mittäter werden

Wer selbst Internetinfrastruktur betreibt, geht nicht nur das Risiko ein, einem Onlineangriff zum Opfer zu fallen. Die eigenen Dienste können umgekehrt zu Tatwerkzeugen werden. Besonders der DNS-Dienst ist gefährdet, wenn er Anfragen nicht nur für die eigenen Systeme weiterleitet. Er ist dann Teil eines DNS-Amplifier-Netzwerkes, das Messungen zufolge derzeit etwa 9 Millionen Server umfasst. Hier kann jeder leicht selbst Abhilfe schaffen und das Weiterleiten von Anfragen nur für die eigenen Systeme erlauben. Außerdem sollten anfällige Dienste wie Chargen, NTP und ähnliche entweder gar nicht laufen oder nur von den eigenen Systemen aus erreichbar sein.

Für Provider und Firmen mit zahlreichen Endgeräten empfiehlt es sich, am Übergang zum Internet nur Daten passieren zu lassen, die dort einen berechtigten Zweck erfüllen – anders als beispielsweise aus dem Internet eingehende Anfragen zu Domains, die nicht der Organisation gehören. Zudem sollten alle Datenpakete, die das eigene Netzwerk verlassen, eine plausible Absenderadresse haben, die zum eigenen Netzwerk gehört. Das verhindert bereits viele Amplify-Angriffe – genauer gesagt die Einbeziehung der eigenen Systeme in solche Angriffe.

Fazit

Auch wenn zurzeit Ideen die Runde machen, wie sich das Risiko von DDoS-Angriffen verringern lassen könnte, steht zu befürchten, dass der Trend zu häufigeren, stärkeren und längeren Datenbombardements anhält. Mehr IoT, mehr Leitungskapazität zwischen den Kontinenten und immer schnellere Anschlüsse in den Haushalten liefern einen guten Nährboden für verteilte Angriffe. Jeder, der die Verfügbarkeit seiner Internetangebote schützen möchte, hat selbst dafür Sorge zu tragen. Technik und Angebote sind verfügbar, und wer ausreichend Vorsorge trifft, kann vielen DDoS-Angriffen mit Aussicht auf Erfolg begegnen. Wie die jüngste Vergangenheit zeigt, sollten die Gegenmaßnahmen jedoch nicht nur die Inhalte schützen, sondern auch das DNS, das seit Jahrzehnten unverzichtbare Internetadressbuch. (un)

Christoph Puppe

ist seit 1989 in der IT-Sicherheit aktiv, Cybersecurity Strategy Principal Consultant bei der HiSolutions AG in Berlin, Lead Auditor ISO 27001 nach Grundschutz, BSI-zertifizierter Penetrationstester, IS-Revisor und verantwortete 12 Jahre lang die technischen Audits der HiSolutions AG.

Literatur

[1] Jörn Maier, Volker Tanger; Unter Beschuss; Was man gegen Distributed-Denial-of-Service-Attacken tun kann; *iX* 5/2014, S. 40

Alle Links: www.ix.de/ix1612088