Internetdienste vor DDoS-Angriffen schützen

Von überall her

Robert Fritzen, Norbert Pohlmann

Mit der Zahl vernetzter Geräte und dem Trend zu „always online“ wächst die Bedrohung durch Distributed-Denial-of-Service-Angriffe. Unternehmen und Organisationen sollten und können sich dagegen wappnen.

Angriffe auf die Verfügbarkeit von Internetdiensten finden laut BSI in Deutschland zurzeit über 32 000-mal pro Jahr statt – plus eine unbekannte Zahl undokumentierter Vorfälle. Die meisten finden in erpresserischer Absicht statt, hinzu kommen ideologisch motivierte Aktionen. Viele Opfer erfüllen die Forderungen, um die Verfügbarkeit sicherzustellen, andere nehmen einen Ausfall hin. Einen Schaden erleiden alle Betroffenen, egal ob und wie sie reagieren.

Relativ einfach und preiswert auszuführende DDoS-Angriffe bedrohen zunehmend die Verfügbarkeit der Internetdienste. Medienwirksame Angriffe wie auf das Playstation-Netzwerk Ende 2014 oder das von China aus über die Suchmaschine Baidu per Code-Injection initiierte DDoS-Feuer auf GitHub verdeutlichen den Aufwärtstrend. Das Risiko, Ziel eines Angriffs zu werden, gilt als gering, doch jeder kann einen DDoS-Angriff ab etwa 50 Euro bei kriminellen „Dienstleistern“ buchen. Die Schäden gehen schnell in die Millionen. Firewalls und Intrusion-Prevention-Systeme (IPS) bieten entgegen weitläufiger Meinung keinen ausreichenden Schutz gegen DDoS-Angriffe.

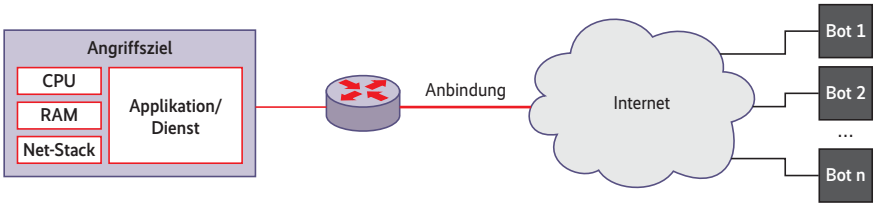
„DDoS“ steht für Distributed Denial of Service und deutet an, dass das angegriffene System zwar nicht abstürzt, den Dienst aber praktisch einstellt. Meist gehen solche Angriffe von zahlreichen kompromittierten Computersystemen („Bots“) aus. Die Täter legen die Zielsysteme koordiniert mit einer großen Last von Anfragen durch Erschöpfung von Ressourcen wie CPU, Arbeitsspeicher oder Übertragungskapazität lahm. Zum Teil sind Tausende oder sogar Millionen von Bots beteiligt. Wenn ein Täter 100 000 Bots missbraucht und jeder davon nur 100 KBit/s Upstream nutzen würde, stünden bereits 10 GBit/s für den DDoS-Angriff zur Verfügung.

Solche Überlastsituationen sind kaum zu handhaben und eine wachsende Herausforderung. Heutzutage sollte jeder IT-Verantwortliche rechtzeitig Sicherheitsvorkehrungen treffen, um die Schäden im Angriffsfall begrenzen zu können. Die Nichterreichbarkeit der Internetdienste kann durch Umsatzeinbußen, Gewährleistungsfälle, Kundenabwanderung oder Reputationsschäden enorme Schäden hervorrufen, und das gilt nicht nur für „Big Player“. Die finanziellen Schäden betreffen neben der IT- und Sicherheitsabteilung oft auch die Marketing-Abteilung, den Kundenservice sowie das Risikomanagement und können ein Unternehmen schlimmstenfalls zur Geschäftsaufgabe zwingen.

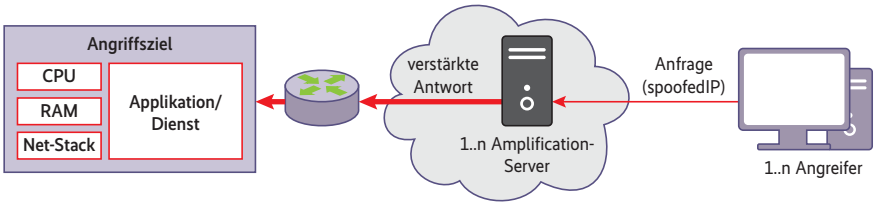
DDoS-Angriffe sind daher prinzipiell für missgünstige Konkurrenten interessant. Meist dienen DDoS-Angriffe jedoch dazu, Firmen und Organisationen zu erpressen oder auf politische Ziele aufmerksam zu machen. Zu beliebten Zielen gehören Onlinespiele-Server, Banking-Portale, politische und ideologische Webseiten, Nachrichtenportale, VoIP-Dienstleister und viele mehr. Technisch wenig bewanderte Täter können solche Angriffe für ihre Zwecke bei „Stresstest“-Dienstleistern und in einschlägigen Portalen einkaufen. Manche nutzen nicht nur die laufend zunehmende Übertragungskapazität der Netze, sondern zielen auch auf bestimmte Schwachstellen in Anwendungen, die im Rahmen einer adäquaten Abwehrstrategie zu beachten sind.

Gezielte Überlastung

Durch das Kombinieren mehrerer DDoS-Methoden kann ein Angreifer unterschiedliche Teile eines Internetdienstes gezielt überlasten sowie flexibel auf unzureichende Abwehrmaßnahmen und deren Schwachstellen reagieren [1].



Meist stehen Angreifern für einen DDoS-Angriff mehrere potenzielle Schwachstellen (hier rot umrahmt) zur Verfügung (Abb. 1).



Im Rahmen eines Amplification-Angriffs können Täter Ressourcen missbrauchen, ohne dass sie Kontrolle über die beteiligten Systeme benötigen (Abb. 2).

Folgende Teile der Dienst-Architektur können als Ziele von DDoS-Angriffen dienen:

– Netzanbindung: Der Angreifer produziert so viele unsinnige Datenpakete, dass die Bandbreite nicht ausreicht, sie zum Server zu transportieren. Bei hoher Last sinkt die Übertragungsqualität, und bei extremer Last muss der Router die meisten Datenpakete verwerfen, weil die Warteschlangen voll sind.

– Protokollstapel: Ein Crash oder ein Überlastungszustand lässt sich aufgrund von Fehlern in der Implementierung oder Eigenarten diverser Protokollfamilien hervorrufen, insbesondere auch der Verschlüsselungsverfahren. Zudem können Angreifer den Arbeitsspeicher durch sehr viele unvollständige Verbindungsanfragen komplett belegen, was die Verfügbarkeit eines Dienstes schnell stark einschränkt.

– Applikation: Mit maßgeschneiderten Anfragen können Täter auf fehlerhaft implementierte Teile bestimmter Anwendungen zielen. Dazu gehören harmlos anmutende Funktionen wie das Hashing oder Datenbank-intensive Suchanfragen, die sinnvollen Anfragen CPU-Ressourcen entziehen. Solche Angriffe heißen auch „Low and Slow“, wenn sich die Datenpakete hinsichtlich Frequenz und Payload kaum von gewöhnlichem Datenverkehr unterscheiden lassen.

Reflection und Amplification

Einen unheilvollen Aufwärtstrend verzeichnen Reflection- und Amplification-Angriffe, auch DrDoS genannt. Die Täter missbrauchen Server Dritter mittels UDP, die ein relativ kleines Anfragepaket mit viel größeren Paketen beantworten (Amplification) – und das mittels Address Spoofing an eine beliebige anzugreifende Ziel-IP-Adresse (Reflection). Der Angreifer muss dafür keine Kontrolle über den fremden Server gewinnen.

Prominentester Vertreter ist der eigentlich veraltete Befehl *monlist* im Network Time Protocol. Entsprechend vernachlässigte NTP-Server versenden die Adressen der letzten 600 Geräte, mit denen sie Kontakt hatten. Daraus ergibt sich ein für Angreifer sehr attraktiver Verstärkungsfaktor von über 200. Viele weitere Protokolle sind anfällig für derartigen Missbrauch, darunter DNS, SNMP und sogar die P2P-Protokolle einiger Botnetze.

Nicht nur rudimentäre Internet-Protokolle lassen sich für eine Amplification missbrauchen, sondern auch ausgewachsene Programmpakete wie die CMS- und Blogging-Software WordPress, genauer gesagt deren Pingback-Funktion, die eigentlich Querverweise zwischen Blogs generieren soll. Mittlerweile lässt sie sich mithilfe eines Plug-in bändigen (siehe „Alle Links“). Ohne diese Gegenmaßnahme können Angreifer Pingback-Requests mit der anzugreifenden Webseite als Ziel an beliebig viele WordPress-Seiten senden, die daraufhin allesamt das anzugreifende System kontaktieren.

Als Nebeneffekt stehen Angreifern auf diese Weise nahezu beliebig viele Source-IP-Adressen für einen DrDoS-Angriff zur Verfügung. Besonders kritisch wird ein derartiger Angriff, wenn ein Botnetz-Betreiber mehrere Amplification-Server von verschiedenen Teilen seines Botnetzes aus parallel ansteuert. Laut Akamais Sicherheitsreport „State of the Internet“ lag der Anteil von Reflection-Angriffen im Vergleich zu allen DDoS-Angriffen im vierten Quartal 2014 bereits bei etwa 40 Prozent.

Abwehrstrategien gegen DDoS-Angriffe

Auf DDoS-Angriffe sollten vor allem solche Unternehmen vorbereitet sein, deren Geschäft aus Internetdiensten besteht. Aber auch interne Abläufe kann ein DDoS-Angriff stark beeinträchtigen, beispielsweise wenn die komplette eigene Internetanbindung oder der Mailserver nicht mehr funktioniert. Als Rahmen einer Abwehrstrategie empfehlen sich drei grundlegende Kategorien: Sicherheitsrichtlinien, eine robuste Auslegung der eigenen Infrastruktur und das Hinzuziehen externer Unterstützung.

Ein Unternehmen sollte zuerst analysieren, welche Risiken den eigenen Internetdiensten drohen und welche Folgeschäden Ausfälle verursachen können. Daraus ergibt sich das Budget für die Schutzmaßnahmen. Es folgt ein Ablaufplan mit Richtlinien für die Vorgehensweise im Ernstfall. Er legt spezielle Handlungsrollen für das IT-Personal, andere Geschäftsabteilungen und eingebundene Dienstleister fest. Den Abschluss der

X-TRACT

- Erpresserische DDoS-Angriffe auf Firmen finden alltäglich statt und bilden eine kräftig sprudelnde Einnahmequelle für die Täter.
- Die lokale Infrastruktur einer Organisation lässt sich praktisch nicht präventiv gegen heftige Denial-of-Service-Angriffe schützen.
- Unternehmen können wichtige Online-Services zu bekannten Cloud-Anbietern oder auch spezialisierten Anti-DDos-Dienstleistern auslagern, um die Robustheit zu steigern.

Konzeptionierung bilden Tests mit simulierten Angriffsszenarien. Auch später im laufenden Betrieb ist die Abwehrstrategie regelmäßig zu überprüfen und zu testen. So lässt sich feststellen, ob die Maßnahmen aktuellen Angriffsvarianten noch standhalten, und ob das Personal im Falle eines Angriffs planmäßig handeln könnte.

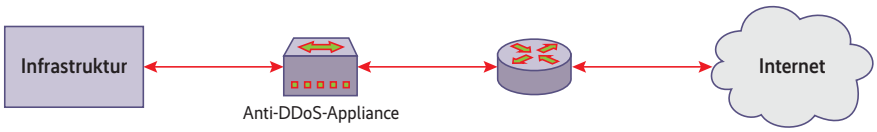
Infrastruktur schützen statt ausbauen

DDoS-Angriffe lassen sich durch rein präventive Maßnahmen kaum vollständig abwehren, aber ihre Auswirkungen lassen sich zumindest begrenzen. Ein beliebtes, aber zugleich besonders teures und dabei wenig wirksames Vorgehen besteht darin, einfach sämtliche bedrohten Ressourcen nach dem Motto „viel hilft viel“ aufzustocken. Dafür kommen mehr Übertragungskapazität sowie mehr und leistungsstärkere Server infrage. Gezielte Angriffe hebeln diese Art „Schutz“ jedoch mit Leichtigkeit aus. Ein wirksamer Schutz muss daher zum Ziel haben, die Infrastruktur für den Täter praktisch aus dem Netz auszublenden, sobald er seinen Angriff in Gang setzt.

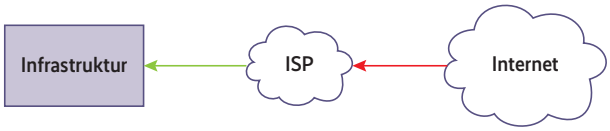
Da DDoS-Angriffe meist von vielen verschiedenen IP-Adressen ausgehen, kommt zum Beispiel ein beizeiten vorbereitetes Whitelisting für besonders wichtige, zugriffsberechtigte Nutzer oder Kunden infrage. Bei Webdiensten hingegen, auf die viele normalerweise anonyme Benutzer Zugriff haben, können eine Login-Seite, Captchas oder eine Überprüfung der Browser-Echtheit den Dienst auf Anwendungsebene schützen. Nur einem relativ simplen und nicht besonders intensiven Angriff auf essenzielle Dienste können die Systemverantwortlichen mithilfe von Sicherheitsausrüstung begegnen, ohne sich zugleich vor einem Großteil der erwünschten Zugriffe abzuschotten.

Wenn die globale Verfügbarkeit des Dienstes keine Priorität hat, können die Administratoren kurzerhand ganze IP-Adressbereiche anhand von Geolocation-Kriterien blockieren, um die Traffic-Flut einzugrenzen. Auf derlei Sofortmaßnahmen darf sich allerdings niemand ausruhen, da deren Effekt schnell zu verpuffen droht. Angreifer können ihre Taktik laufend ändern sowie ihre Angriffsressourcen aufrüsten.

Ebenso wichtig wie das Einleiten technischer Gegenmaßnahmen ist der richtige Umgang mit der Öffentlichkeit [2]. Es empfiehlt sich, die Hintergründe der Angriffe sowie das weitere Vorgehen transparent zu dokumentieren. Wer erläutert, dass Kriminelle den Ausfall verursachen und dass die Zuständigen intensiv an einer schnellen Lösung arbeiten, kann den Frust über den Ausfall auf die Angreifer lenken und den Image-Schaden begrenzen.



Anti-DDoS-Appliances sind leider kein Allheilmittel gegen Angriffe auf die eigene Infrastruktur (Abb. 3).



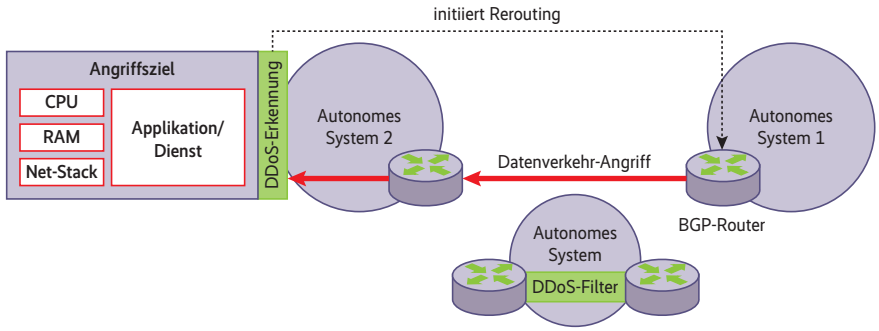
Der eigene Internetprovider kann DDoS-Angriffen mit Filtermaßnahmen außerhalb des Zielnetzes die Wucht nehmen (Abb. 4).

Grenzen der Anti-DDoS-Appliances

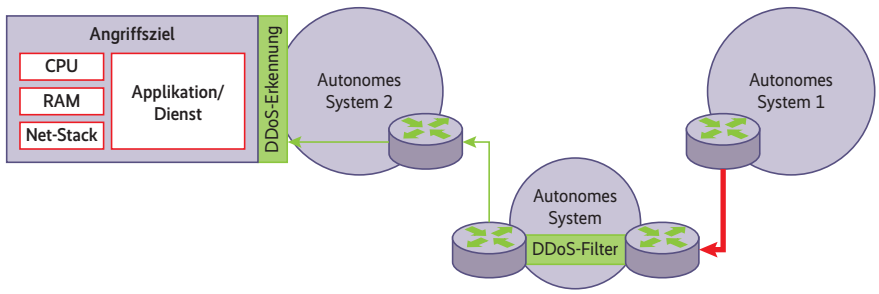
Als schnell installierter Basisschutz für die eigenen Dienste stehen spezielle Anti-DDoS-Appliances zur Verfügung. Auch viele Firewalls enthalten inzwischen Schutzfunktionen gegen verteilte Angriffe.

Solche Appliances filtern den Datenstrom und wirken vielen Angriffsmustern im Rahmen der verfügbaren Anbindungsbandbreite entgegen. Sie bieten, je nach Ausführung, neben Filterung altbekannter DoS-Muster inzwischen auch heuristische Filter gegen bis dato unbekannte Angriffe auf Applikationsebene, „Low and Slow“- sowie Multivektor-Angriffe.

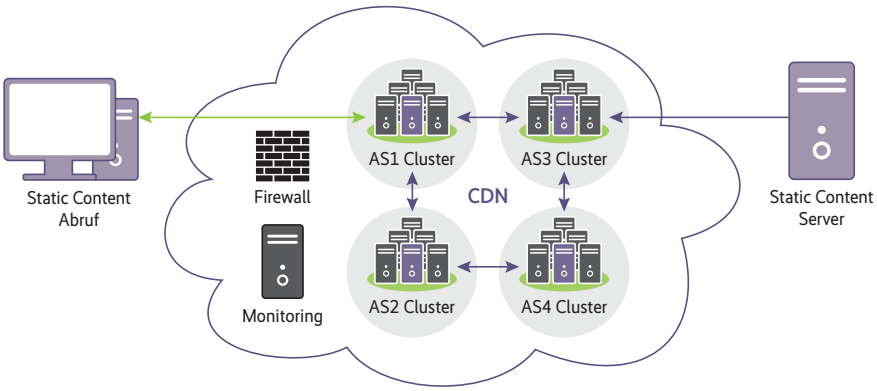
Lastet das Angriffsvolumen allerdings die verfügbare Bandbreite aus – und das ist leider meist der Fall –, kann die Appliance kaum helfen. Die Leitung wird dann bereits am Gateway zur Infrastruktur „verstopft“. Zudem wirken die Filter oft nicht gegen alle Angriffe, insbesondere wenn die Täter Verschlüsselung und Amplification nutzen. Eine schnelle Rundum-sorglos-Lösung bieten diese Appliances folglich nicht. Angriffe mit großem



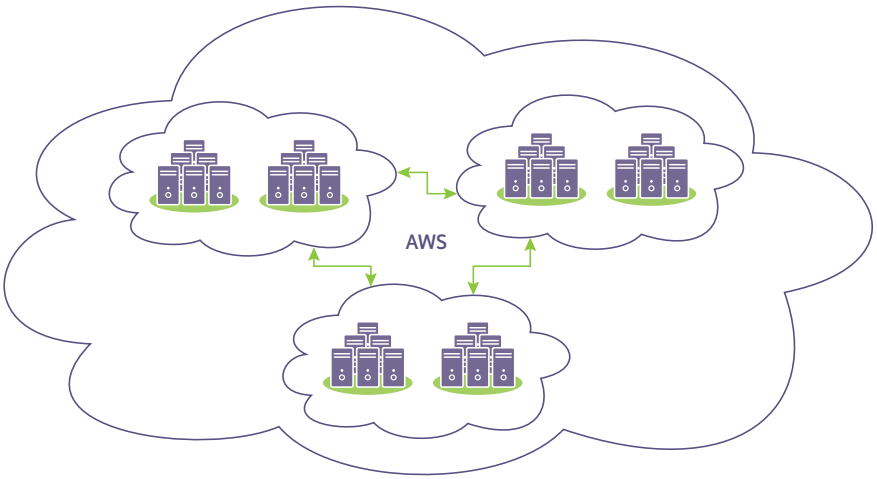
Das Monitoring erkennt einen DDoS-Angriff, während sich das filternde Netz im Hot-Standby befindet (Abb. 5).



Kurz nach dem Beginn des DDoS-Angriffs wird der Datenverkehr über das spezielle autonome System umgeleitet und dort gefiltert (Abb. 6).



Ein über mehrere autonome Systeme verteilter CDN-Cluster speichert statische Inhalte redundant zum schnellen Abrufen (Abb. 7).



Ein Auslagern der eigenen Dienste in die Cloud kann deren Robustheit gegenüber Angriffen dank hoher Redundanz und auf viele Standorte verteilter Ressourcen erhöhen (Abb. 8).

Datenvolumen lassen sich wirksamer in Zusammenarbeit mit einem externen Dienstleister für Monitoring und DDoS-Abwehr in den Griff bekommen.

Gegenmaßnahmen nach außen verlagern

Erster Ansprechpartner auf dem Weg zu externer Unterstützung im Notfall ist der eigene Internetprovider. Der kann eigene Filter einrichten und bestimmte Adressbereiche vorübergehend blockieren.

Aber nicht jeder Provider sieht sich in der Lage oder Verantwortung, bei einem DDoS-Angriff Maßnahmen zu ergreifen, die über das Sicherstellen des eigenen Geschäfts hinausgehen. In den meisten Fällen ist es deutlich wirkungsvoller, auf DDoS-Abwehr spezialisierte Dienstleister mit eigenen Filternetzwerken in Anspruch zu nehmen. Diese bieten eine Reihe von Schutzkonzepten mit verschiedenen Vor- und Nachteilen und Wirkungsgraden an.

Einige Anbieter betreiben spezielle autonome Systeme (AS), die DDoS-Traffic mittels BGP-Rerouting ausfiltern können. Quell- und Ziel-Adressen der Datenpakete bleiben dabei unverändert, und die Umleitung durch das Filternetz kostet kaum Zeit. Alternativ steht meist eine DNS-Umleitung speziell für Webserver zur Verfügung. Die Filtertechnik läuft ständig im Hot-Standby. Sobald das Monitoring einen Angriff feststellt, leiten die Router den Datenverkehr per Netz-Announcement über das Filternetz (Abb. 5 und 6).

Traffic-Scrubbing-Netze

Diese Schutzmaßnahme erfordert – in IPv4-Maßstäben – mindestens ein eigenes /24-Subnetz. Der deutsche Anbieter Link11 etwa verfügt über Rechenzentren mit 500-Gbps-Anbindung an verschiedene Carrier und setzt auf eigene Filter zum Erkennen und Abwehren von Angriffen. Als Kriterium für die Filterung von DDoS-Verkehr dient neben bekannten Mustern ein Scoring-Modell zum Erkennen von Anomalien im Netzwerkverkehr.

Ein Content Delivery Network (CDN) verteilt statische Inhalte redundant auf Server, die an vielen Standorten über verschiedene AS angebunden sind (Abb. 7). CDNs bieten durch die kombinierten Übertragungskapazitäten der AS einiges an Robustheit. Die Inhalte kann der jeweils physisch nächstgelegene oder am besten verfügbare Server-Cluster rasch ausliefern. Zieht ein Angriff einen Server in Mitleidenschaft, kann ein anderer Server oder Cluster die Inhalte liefern. Ein Angreifer müsste also gegen mehrere AS vorgehen. Dynamische Inhalte lassen sich allerdings nicht zwischenspeichern. Daher eignet sich ein CDN in diesem Fall weniger gut als Schutzmaßnahme.

Mehr Robustheit durch verteiltes Liefern

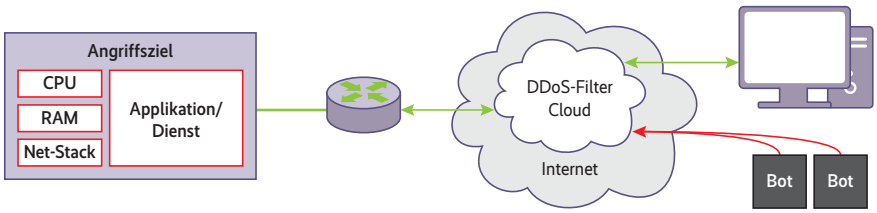
Die Robustheit der eigenen Internetangebote lässt sich mit Cloud-Diensten wie Amazons Web Services (AWS) steigern. Anwendungen, Datenbanken, Webseiten und Inhalte sind in die Cloud ausgelagert, die viele redundante Ressourcen in einer weltweit verteilten Umgebung bietet. Dank schneller Anbindung kombiniert mit Skalierbarkeit und Replikation können Anbieter hier Webservices besser vor DDoS-Angriffen geschützt unterbringen als in den eigenen Räumen. Ein Umzug in die Cloud bedeutet manchmal jedoch viel Aufwand und kommt nicht für alle Teile der eigenen Infrastruktur infrage, insbesondere wenn es um sensible Daten geht. Für einen verbesserten Datenschutz stellt Amazon seinen CloudHSM-Service bereit.

Spezialisierte Cloud-Filternetze vereinen alle oben erwähnten Konzepte unter einem Dach, mit unterschiedlichen Abstufungen für einzelne Webserver oder auch ganze Infrastrukturen. Die Anbieter agieren hier als Reverse-Proxy über einem weltweiten Content Delivery Network (CDN) mit DNS-Servern, Caching, Blocklisten, BGP Origin Protection, Web Application Firewall (WAF), Malware-Scanner sowie Spam- und DDoS-Filtern. Mittels ihrer redundant und großzügig dimensionierten Infrastruktur erreichen solche Cloud-Filternetze einen starken Schutz mit vielen einfach nutzbaren Zusatz-Services speziell für Webanwendungen.

Je nach Schutzbedarf, SLA und Support können sich die Kunden zwischen einem kostenlosen Basis-Schutz und Verträgen für über 5000 US-Dollar monatlich entscheiden. Die eigenen Server sind

durch die Cloud-Infrastruktur vor Angriffen abgeschirmt. Dafür muss der Nutzer lediglich einen DNS-Server seines Dienstleisters als verantwortlichen Nameserver der eigenen Domain(s) eintragen. Alles Weitere findet über die Webseite des Anbieters statt. Webserver lassen sich mit relativ wenig Aufwand und geringem Budget schützen. Zu den Cloud-Filter-Anbietern gehören die Firmen Cloudflare, Akamai und Incapsula.

Trotz derlei Maßnahmen gibt es bereits gelegentlich Angriffswellen, die sogar die Kapazitäten solcher Anbieter überschreiten. Derartig heftige Störungen sind allerdings noch die Ausnahme, bestätigen aber: Hundertprozentigen Schutz vor DDoS-Angriffen gibt es ebenso wenig wie absolute Sicherheit. Ziel solcher Strategien und Sicherheitsmaßnahmen ist immer, das Schutzniveau und somit die Hürden für Angreifer möglichst hoch zu setzen. Der letzte große Angriff auf das Playstation-Netzwerk mit berichteten 1,2 Tbps Volumen ist ein gutes Beispiel dafür. Bei gezieltem Ausnutzen mehrerer Schwachpunkte zugleich (Multivektor- oder auch „hybride“ Angriffe) kann ein eigenständiges Filtersystem meist nicht mehr alle „Low and Slow“-Varianten erkennen und unterbinden.



Spezialisierte Anbieter bauen ihre Cloud eigens zum Schutz ihrer Kunden gegen Angriffe auf (Abb. 9).

Nicht zum Mittäter werden

Schlecht konfigurierte IT-Endgeräte und Server sind potenzielle Tatwerkzeuge, da sie die Basis für Botnetze und Amplification-Angriffe bilden. Administratoren müssen verhindern, dass vom eigenen Netzwerk DDoS-Aktivitäten ausgehen. Die eigenen öffentlich erreichbaren Server sind auf Missbrauchspotenzial für Amplification-Angriffe zu prüfen. Zu den wichtigen Maßnahmen gehört das Abschalten offener Rekursion auf DNS-Servern. Es sollten nur rekursive DNS-Anfragen aus vertrauenswürdigen Quellen erlaubt sein. NTP-Server laufen häufig auf älteren, schlecht gewarteten Servern. Dabei müssen gerade diese unbedingt auf dem aktuellen Stand sein. Grundlegende IT-Sicherheitsmaßnahmen wie Awareness-Kampagnen und Endpoint-Protection dämmen das Infektionsrisiko für Botnetz-Malware weiter ein. Darüber hinaus sollte IP-Spoofing mittels Filtern des ausgehenden Datenverkehrs (Egress Filtering) unterbunden sein. Wer keine ausreichenden Vorkehrungen gegen den Missbrauch der eigenen Infrastruktur als „Waffe“ trifft, kann möglicherweise schadenersatzpflichtig gegenüber dem Angegriffenen werden.

Der Angegriffene wiederum muss umgehend Beweise für ein rechtliches Vorgehen und eine technische Analyse sichern. Dazu zählt die Kommunikation der Erpresser ebenso wie protokollierbare IP-Adressen. Zudem sollten die Betroffenen Dauer, Intensität und Angriffsvektoren erfassen – sich aber nicht auf erpresserische Forderungen einlassen. Einerseits würde ein Nachgeben das kriminelle Geschäftsmodell bestätigen und stärken, andererseits kann sich niemand auf das Abstellen der Angriffe nach einer getätigten Zahlung verlassen. Wer zahlt, provoziert zumeist weitere Forderungen seitens der Erpresser. Stattdessen sind umgehend Abwehrmaßnahmen einzuleiten sowie die Polizei einzuschalten und Anzeige zu erstatten.

Einen weiteren Aspekt sollte jeder zu seiner DDoS-Abwehrstrategie im Hinterkopf behalten: Die Angriffe dienen gerne als strategisches Ablenkungsmanöver, um IT-Mitarbeiter zu beschäftigen und vom übrigen Sicherheits-Monitoring abzulenken. Auf diese Weise können anderweitige Schwachstellen unbemerkt ausgenutzt und dabei Zugangsdaten, geistiges Eigentum, Geld oder sonstige Daten beispielsweise durch eingeschleuste Malware entwendet werden.

Ausblick

Die Zeiten des „Internet of Everything“ kommen. Ganze Zombie-Armeen aus vielen schlecht gesicherten Embedded-Devices werden DDoS-Angriffen zusätzlichen Aufschwung verleihen. Schon heute kommen die Überfälle schnell und meist unvorhergesehen. Verantwortliche in Firmen und Organisationen, deren Umsatz und Geschäftsbetrieb von Internetdiensten abhängt, sollten sich so bald wie möglich um eine passende Abwehrstrategie kümmern. (un)

Robert Fritzen (B.Sc.)

ist wissenschaftlicher Mitarbeiter im Bereich Botnetzerkennung am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule Gelsenkirchen.

Norbert Pohlmann

arbeitet als Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie Leiter des Instituts für Internet-Sicherheit – if(is) an der Westfälischen Hochschule Gelsenkirchen. Außerdem ist er Studienbeauftragter für den Master Internet-Sicherheit.

Onlinequellen

[a] BSI; Die Lage der IT-Sicherheit in Deutschland 2014
https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html

[b] Allianz für Cyber-Sicherheit; Thema Q1/2015: DDoS-Angriffe im Cyber-Raum
https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Informationspool/Themen/DDoS/ddos.html

[c] Seminararbeit „Distributed-Denial-of-Service-DDoS-Angriffe
https://www.internet-sicherheit.de/fileadmin/docs/publikationen/2015/Seminararbeit_Distributed-Denial-of-Service-DDoS-Angriffe.pdf

[d] WordPress.org: Disable XML-RPC Pingback
https://wordpress.org/plugins/disable-xml-rpc-pingback/

Literatur:

[1] Robert Fritzen, Norbert Pohlmann; Distributed Denial of Service Attacks (DDoS) – Wie robust sind Dienste im Internet?; IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 2/2015

[2] Marcel Knop; Schadensbegrenzung; Management von Cyberkrisen; *iX* 7/2015, S. 78

Alle Links: www.ix.de/ix1509087