Maßnahmen gegen Distributed-Denial-of-Service-Angriffe

Von allen Seiten

Christoph Puppe, Jörn Maier

Verläuft ein DoS-Angriff erfolgreich, ist der Service, etwa eine Website oder ein Mailserver, nicht mehr erreichbar. Methoden für solche Attacken existieren viele, wirksame Gegenrezepte praktisch nicht. Zumindest aber lassen sich die Auswirkungen beschränken.

Die ersten in der Öffentlichkeit wahrgenommenen so genannten DDoS-Angriffe (Distributed Denial of Service) erfolgten auf die Webseiten von Yahoo, CCN, eBay, Amazon und andere. Am 9. Februar 2000 begann „Mafiaboy“ seine Angriffe und sorgte eine Woche lang für massive Störungen. Am 10. März 2000 brach das Vertrauen der Anleger in die Internet-Aktien zusammen und an der Börse wurden 2,7 Billionen US-Dollar vernichtet. Die zeitliche Nähe mag Zufall gewesen sein. Die Folge einer solchen Attacke ist jedenfalls immer ein Vertrauensverlust der Kunden und Anleger in das angegriffene Unternehmen. Wer mag schon in ein Geschäft investieren, dessen Lebensgrundlage, die globale Vertriebsniederlassung im Internet, von einem 15-jährigen ohne besondere Begabungen manipuliert werden kann? Heute, fast fünf Jahre später, sind DDoS-Angriffe immer noch die Achillesferse des Internet. Jugendliche nutzen sie, um ihre Ansprüche auf bestimmte Kanäle des Internet Relay Chats (IRC) durchzusetzten. Kriminelle bieten sie als Dienstleistung an, die wiederum von mafiaähnlichen Gruppierungen zur Erpressung von Unternehmen eingesetzt wird, und Regierungen entdecken sie als Waffe.

Dass ein bekanntes Problem noch nicht gelöst ist und der gesammelte Sachverstand der Sicherheitsberater und Produktstrategen nicht ausreicht, um dem Treiben ein Ende zu setzen, ist in den Wurzeln des Internet und seiner Geschichte begründet. Jedes im Internet verwendete Protokoll kann sich nur dann durchsetzten, wenn es so einfach ist, dass viele Programmierer es implementieren, robust genug, um Daten auch bei Störungen zu transportieren und flexibel für die Anpassung an neue Entwicklungen.

Nicht vorgesehen ist jedoch, jeden Kommunikationspartner eindeutig zu identifizieren, eine zentrale Verwaltung aller Datentransfers zu bieten oder jedem Teilnehmer einen Anteil an der vorhandenen Bandbreite zu garantieren. Das wären allerdings die erforderlichen Bedingungen, um DDoS an der Wurzel zu packen. Dazu müssten alle Teilnehmer am Internet ihre Privatsphäre aufgeben und sich einer Verwaltung unterwerfen – was wenig realistisch ist.

Weniger wirksam, aber zumindest praktikabel ist es, sich mit den Techniken des gezielten DoS-Angriffs vertraut zu machen. Gegenmaßnahmen können der private Anwender am heimischen PC, der Administrator eines Unternehmens sowie der Internet Service Provider ergreifen.

iX-TRACT

- Mit ausgeklügelten Angriffstechniken ist es Bösewichtern selbst mit wenigen Datenpaketen möglich, Dienste großer Anbieter lahm zu legen.
- Verhindern lassen sich solche Angriffe in absehbarer Zeit nicht. Gewisse Schutzmaßnahmen verringern aber wenigstens die Auswirkungen.
- Wenn jeder Teilnehmer am Internet dafür sorgt, dass seine Systeme nicht gekapert und missbraucht werden können, ist schon viel gewonnen. Insbesondere die Provider sollten unterbinden, dass ihre Kunden Datenpakete mit gefälschten Absenderadressen verschicken.

Die einfache Denial-of-Service-Attacke (DoS) wird von einem PC aus gestartet und ausgeführt. Sie kann Erfolg haben, wenn der Angreifer eine Methode kennt, mit der schon wenige verschickte Daten zum Zusammenbruch eines Dienstes führen. Ein Beispiel aus den 90er Jahren ist der Ping-of-Death. Ein einziges Ping-Paket konnte alle Windows-Systeme durch einen Pufferüberlauf sofort zum Stillstand bringen.

DoS – wenige Daten genügen

Kurze Zeit später gab es weitere Ein-Paket-Angriffe wie Teardrop, bei dem fehlerhafte, fragmentierte Pakete verschickt werden, die viele Systeme zum Absturz brachten. Zahlreiche Betriebssysteme und bekannte Firewalls verabschiedeten sich für immer nach einem Land-Angriff mit einem Paket, bei dem Absender und Empfänger identisch waren. Der Code zur Analyse des Pakets ließ sich durch diesen einfachen Trick in eine Endlosschleife versetzen, die alle CPU-Ressourcen aufbrauchte und das System unbenutzbar hinterließ.

Eine weitere Methode, mit wenigen Daten einen DoS auszulösen, besteht darin, auf einem Server eine Anwendung aufzurufen, von der der Angreifer weiß, dass sie viele Ressourcen benötigt. Das kann etwa eine Seite mit einer komplexen Datenbankanfrage sein. Wenn die Aufrufe schnell genug aufeinander folgen, kann der Rechner so beschäftigt werden, dass er keine anderen Anfragen mehr bearbeiten kann. Die Beispiele ließen sich beliebig weiterführen, denn alle paar Tage entdecken Sicherheitsexperten und Computerbegeisterte neue Schwachstellen in Betriebssystemen und Anwendungen.

Wenig überraschend ist die ungleich größere Effektivität einer Distributed-DoS-Attacke. Wenn sich mehrere zehntausend PCs zusammenschließen, haben sie eine gewaltige Stimme, die das Internet zum Wackeln bringen kann wie einst die Trompeten die Mauern von Jericho. „Viel hilft viel“ ist folglich das Credo des geübten DDoS-Angreifers, der dazu sehr viele Daten zum Ziel leiten muss. Da er diese Datenmengen nicht von einem PC aus verschicken kann, muss er die Aufgabe an mehrere Systeme verteilen und die kumulierte Bandbreite nutzen – Grid-Computing einmal anders. Diese Verteilung hat der Distributed-Denial-of-Service-Attacke ihren Namen verliehen.

Eine alte Methode, an viele unfreiwillige Helfer zu kommen, ist die Smurf-Attacke (siehe Abb. 1). Mit Schlümpfen hat sie allerdings nur den Namen gemein. Dem Angreifer reicht ein PC aus, um auch sehr große Provider lahm zu legen. Er benutzt dafür fremde Systeme als Verstärker, die seine wenigen Pakete vervielfältigen. Der Angreifer schickt beispielsweise zehntausend Pakete an die Broadcast-Adresse eines großen Netzwerkes. Alle Rechner antworten auf jedes dieser Pakete an den Absender. Da der Absender jedoch gefälscht ist und anstelle der IP-Adresse des Angreifers die des Opfers enthält, kommen alle Antworten beim Opfer an. Wenn das Netz groß genug ist und über ausreichend Bandbreite verfügt, können so aus zehntausend Paketen schnell Millionen werden. Typischerweise wird dafür ein Ping genutzt, da die Antwort darauf immer so viele Daten enthält wie der Ping selbst.

Für diesen Angriff gibt es eine einfache Gegenmaßnahme. Alle Netze, die Bestandteil des Internet sind, können an ihrem Border-Router verhindern, dass ein Paket an eine Broadcast-Adresse ins Intranet eindringt. Es hat ein paar Jahre gedauert, aber heute schützen die meisten Admins ihre Netze dagegen und die Smurf-Attacke ist nicht mehr so einfach wie früher. Eine Liste mit anfälligen Netzen findet sich im Web (www.powertech.no/smurf/). Überdies reagieren viele Betriebssysteme nicht mehr auf Broadcast-Pings.

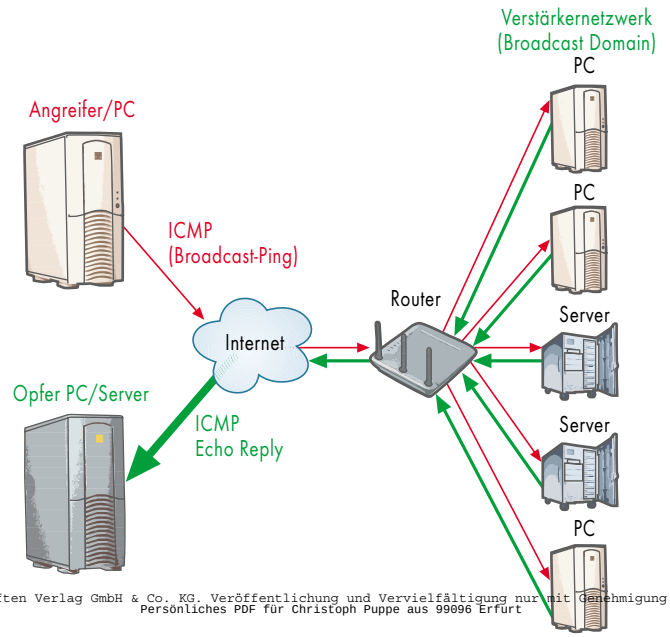
Handles, Handler und Händler

Die heute übliche Methode, sich Helfer zu besorgen, nutzt die zahlreichen Schwachstellen in Windows-Betriebssystemen und das Unwissen der meisten Benutzer. Bösewichter infizieren normale PCs der nichtsahnenden Internet-Nutzer mit einer Schadsoftware, die eine Fernsteuerung des PC erlaubt. Diese im Fachjargon Zombies genannten Rechner werden zu Bot-Nets zusammengeschaltet, die ein oder mehrere über ihre Spitznamen (Handle) identifizierbaren so genannten Handler kontrollieren (siehe Abb. 2).

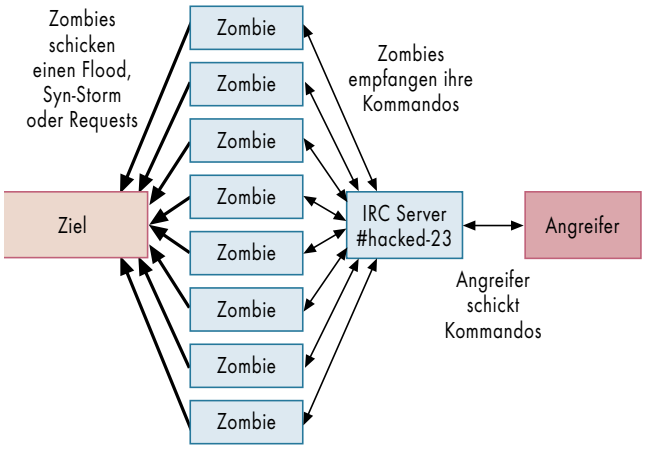
Ein solches Bot-Net kann schnell mehrere zehntausend PCs umfassen. Dem Angreifer ermöglicht es, von allen Seiten gleichzeitig auf das Opfer loszugehen. Eine Chance zur Verteidigung besteht kaum, da die Pakete aus allen Teilen des Internet gleichzeitig auf das Opfersystem einprasseln und die Absenderangaben innerhalb der Pakete in der Regel gefälscht sind. Dass diese Bot-Netze von Kriminellen für viel Geld an Spammer vermietet werden, fand unsere Schwesterzeitschrift c’t heraus (siehe Artikel „Ferngesteuerte Spam-Armeen“, c’t 5/2004, S. 18).

In Bezug auf die Verantwortung des privaten Anwenders, dessen PC für einen DDoS-Angriff missbraucht wurde, steckt die Rechtsprechung noch in den Kinderschuhen, die Gerichte neigen derzeit noch zu Freisprüchen. Eine Mitschuld ist aber sicherlich technisch vertretbar, ähnlich der versicherungsrechtlichen Behandlung eines Einbruchs bei unverschlossener Wohnungstür.

Eine Möglichkeit, das angegriffene System lahm zu legen, ist der Syn-Storm, bei dem immer nur das erste Paket eines TCP-Verbindungsaufbaus verschickt wird (Abb. 3). Das Ziel reagiert darauf, indem es für die erwartete Verbindung Speicher reserviert und eine Antwort schickt. Kommt von der Gegenseite keine Antwort mehr, wartet es eine Zeit lang und gibt erst dann den Speicher wieder frei. Die Zahl dieser halboffenen Verbindungen ist



Sendet ein Angreifer einen Ping an die Broadcast-Adresse eines großen Netzes, vervielfältigt sich die Datenmenge durch die Antwort jedes einzelnen Systems. Der Opferrechner bricht unter der Datenlast des an ihn umgeleiteten Ping-Request zusammen (Abb. 1).



Der Handler kontrolliert die übernommenen Zombie-Rechner und kann mit ihnen eine verteilte DoS-Attacke starten (Abb. 2).

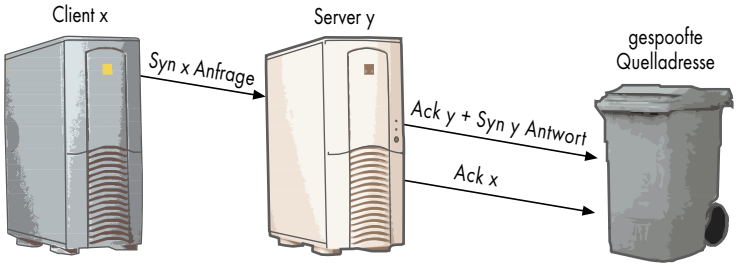
begrenzt, da nicht beliebig Speicher zur Verfügung steht.

Zahllose Verbindungsanfragen

Wenn der Angreifer nun sehr viele Verbindungsanfragen schickt, wird das Ziel bald keine neuen Verbindungen annehmen können, da es ja bereits auf die maximale Zahl von Verbindungen wartet. Üblicherweise sind circa 100 bis 200 halboffene Verbindungen erlaubt, die Wartezeit bis zum vollständigen Verbindungsaufbau beträgt zwischen 60 und 300 Sekunden. Ein Angreifer kann also schon mit wenigen hundert Paketen pro Sekunde einen Server oder mit deutlich mehr selbst einen großen Load-Balancer vollständig auslasten und verhindern, dass der Dienst für andere zugänglich ist. Ein solcher Angriff zwang vor kurzem auch den Load-Balancer für die Heise-Webangebote in die Knie.

Der Name lässt es schon anklingen: Beim Flooding geht es um das (Über-)Fluten einer Leitung, indem die gesamte Bandbreite ausgenutzt wird – zum Beispiel mit Antworten auf Pings bei einer Smurf-Attacke. Fluten lässt sich die Internet-Verbindung von Unternehmen oder Providern mit allen erdenklichen Pakettypen. Neben den Kosten für den Ausfall kommen für den solchermaßen Angegriffenen auch noch die Kosten für den Datenverkehr hinzu, zumindest wenn er mit seinem Provider nach Volumen abrechnet. Mehrere IRC-Server-Betreiber haben bereits ihre Server abgeschaltet, da die Kosten durch die ständigen DDoS-Attacken zu hoch wurden. Ein Flood war auch das Mittel der Wahl bei den eingangs erwähnten Angriffen auf Yahoo und Co. Eingesetzt wurde ein damals aktuelles Tool, das sich Tribal Flood Network (TFN) nennt, sowie die Programme Stacheldraht und Trinoo. Da moderne Backdoors diese Funktionen bereits oft mitbringen, sind heute keine spezialisierten Werkzeuge mehr notwendig.

Schwieriger durchzuführen sind die Angriffe gegen Schwächen in Protokollen. Ein Beispiel ist die TCP-Connection-Reset-Verwundbarkeit. Im IP-Protokoll ist vorgesehen, dass das Paket zur Bestätigung eine Ack-Nummer enthält, die mindestens um eins höher ist als die empfangene Sequence-Nummer. Die Ack-Nummer kann aber auch sehr viel höher sein, je nachdem, ob alle Pakete bestätigt werden oder nicht. Ein Angreifer hat so eine größere Chance, ein Reset-Paket in die Verbindung einzuschleusen und sie damit zu beenden. Wenn nun ein Router mit anderen Routern Informationen über das Routen und BGP-Updates (Border Gateway Protocol) austauscht, kann der plötzliche Abbruch dieser Unter-



TCP-Syn-Flood-Angriff: Anders als beim üblichen 3-Wege-Handshake bestürmt der angreifende PC das attackierte System mit Syn-Paketen zum TCP-Verbindungsaufbau, bis dessen Speicher für weitere, reguläre Verbindungen keine Kapazität mehr hat (Abb. 3).

haltung zu gravierenden Problemen beim Routing führen.

Prinzipiell lassen sich die DoS-Angriffe also in folgende Gruppen unterteilen:
– Flooding-Angriffe;
– Schwächen in der Architektur eines Protokolls;
– fehlerhafter Programmcode

Ein vollständiger Schutz vor DoS-Angriffen ist lediglich gegen das Ausnutzen fehlerhaften Programmcodes möglich. Die für einzelne Angriffe anfälligen Systeme sind mit den entsprechenden Patches zu versehen, um die bekannt gewordene Schwachstelle zu schließen. Ein gut funktionierendes Patchmanagement ist daher die Voraussetzung, sich zumindest vor einem Teil der Angriffe zu schützen.

Weitaus schwieriger sieht es bei den beiden anderen Angriffsursachen aus. Theoretisch würde es ausreichen, die folgenden Schritte umzusetzen:
– der Systemverantwortliche erkennt, dass ein Angriff stattfindet;
– es werden Unterscheidungskriterien zwischen dem Datenstrom des Angreifers und dem „normalen“ Datenstrom erarbeitet;
– die durch den Angriff verursachten Daten werden anhand der zuvor erstellten Unterscheidungsmerkmale gefiltert und verworfen.

In der Praxis ist diese Vorgehensweise jedoch alles andere als trivial. Bereits die Unterscheidung, ob es sich um einen DoS-Angriff oder eine durch Benutzer verursachte Lastspitze handelt, ist nicht einfach – dafür sorgen Angriffe, die mit „normalen“ oder rechenintensiven Benutzeranfragen versuchen, ein System in die Knie zu zwingen.

Was jeder tun kann

Bei Flooding-Angriffen gibt es noch ein weiteres Problem: Übersteigt die Masse der Angriffsdaten die Bandbreite des Netzanschlusses, hilft auch das Filtern des Datenstroms nichts. Es reicht nicht aus, wenn ein Serverbetreiber alleine Schutzmaßnahmen ergreift, da die ihm zur Verfügung gestellte Bandbreite immer endlich ist. Sinnvoll ist es daher, wenn sowohl Endanwender als auch ISPs und Server- beziehungsweise Netzadministratoren präventive Schutzmaßnahmen gegen DoS-Angriffe umsetzen.

Systeme von Endanwendern bieten oft ein einfaches Ziel zur Installation von Agenten, da sie meist ein sehr niedriges Sicherheitsniveau haben. Damit sie nicht selbst Verursacher eines DoS-Angriffs werden, sollten PC-Besitzer sowohl einen Virenscanner (der die meisten DoS-Agenten erkennt) als auch eine Personal Firewall (zum Schutz des Rechners vor Schwachstellen und um den ausgehenden Datenverkehr zu kontrollieren) installieren. Darüber hinaus sind die Systeme mit aktuellen Patches zu versehen, bei Windows-Betriebssystemen am einfachsten via automatischer Updatefunktion. Der Anwender sollte außerdem auf unvorhergesehenen Traffic von seinem Rechner achten und gegebenenfalls nach der Ursache suchen. Bei der Suche nach unerlaubt installierten DoS-Angriffstools können auch Mal- oder Spyware-Scanner (Spybot, Pestpatrol et cetera) helfen.

Deutlich mehr können ISPs zur Prävention von DoS-Angriffen beitragen. Das gilt insbesondere für die Lokalisierung der Angriffsquellen. In vielen Fällen versuchen Angreifer, durch Fälschen der Absender-IP-Adresse den Ursprung der Angriffe zu vertuschen. Dieses als IP-Spoofing bekannte Verfahren ist eines der Hauptprobleme bei der Bekämpfung von DoS-Angriffen. Der Einsatz von Ingress- und Egress-Filtern verhindert IP-Spoofing oder schränkt es zumindest ein.

Ingress-Filter (RFC 2267) prüfen Datenpakete, die von einem Unternehmen oder einer Organisation ins Internet beziehungsweise ins Netz des ISP übertragen werden sollen, auf die korrekte Absenderadresse. Da jede Organisation, die an einen Netzbetreiber angeschlossen ist, über einen bestimmten IP-Adressbereich verfügt, kann man IP-Pakete, deren Quell-Adresse nicht aus diesem Bereich stammt, als gespoofte Pakete identifizieren und damit herausgefiltern. Das Fälschen von IP-Paketen bleibt somit auf den Adressbereich der jeweiligen Organisation reduziert.

Egress-Filter (RFC 3013) prüfen Datenpakete, die vom Internet in das Netzwerk einer Organisation gelangen. Pakete an Broadcast-Adressen des eigenen Netzes sollten genauso wenig hinein gelangen dürfen wie Pakete mit IP-Adressen, die im Moment nicht von der IANA vergeben sind oder nach RFC 1918 nicht über das Internet geroutet werden dürfen. Unter www.cymru.com/Documents/bogon-list.html finden Administratoren Templates für verschiedene Systeme, die die Webseitenbetreiber zyklisch aktualisieren. Diese Empfehlung gilt für alle ISPs, egal ob sie Hosting oder Dialup anbieten, sowie für alle Organisationen wie Universitäten, Firmen oder Behörden.

Durch permanente Überwachung ihrer Systeme könnten ISPs überdies plötzlich auftretende Spitzenwerte erkennen und die dafür verantwortlichen Netzwerke ausfindig machen. Das schützt jedoch nur bedingt vor DDoS-Angriffen, deren einzelne Zombie-Systeme sich in verschiedenen Netzwerken befinden.

Vorsicht Mittäterschaft

Schlecht gewartete Server-Systeme sind dank ihrer meist sehr guten Netzanbindung ein besonders lohnenswertes Ziel für die Installation von DDoS-Agenten. Eine adäquate Absicherung dieser Systeme sollte die Pflicht eines jeden Administrators sein. Hierzu gehören nicht nur die Installation aktueller Patches sowie die „sichere“ Konfiguration von Systemen nach anerkannten Standards, sondern auch der Einsatz von Viren- und Malware-Scannern sowie eine Überwachung der an das Internet angebundenen Systeme. Letzteres ist notwendig, um auf Anomalien wie das plötzliche Senden großer Datenströme adäquat reagieren zu können und so zu verhindern, dass man Teil eines Angriffs auf einen fremden Server wird.

Neben diesen präventiven Maßnahmen, die sämtliche Teilnehmer des Internet befolgen sollten, existieren für die Administratoren der angegriffenen Systeme weitere Möglichkeiten, sich zumindest teilweise vor Angriffen zu schützen. Zwar bietet keine der im Folgenden genannten Strategien einen 100%igen Schutz, zumindest aber erschweren sie die erfolgreiche Durchführung eines DoS-Angriffs.

Eine Möglichkeit des Behinderns ist etwa das so genannte Overprovisioning. Dazu ist das Gesamtsystem mit zusätzlicher Hardware (redundante Server, Round-Robin-Verfahren, redundantes Load-Balancing, hohe Bandbreite der Zugangsleitungen, leistungsstarke Server und Router et cetera) so auszubauen, dass es die durch einen DDoS-Angriff verursachten Spitzenlasten selbst abfangen kann. Außerdem kann man die redundanten Systeme bei mehreren Providern unterbringen oder den Service eines auf verteilte Auslieferung spezialisierten Anbieters in Anspruch nehmen. Dabei werden die DNS-Anfragen – ähnlich wie bei Round Robin – mit der IP-Nummer eines dem Client nahe gelegenen Proxies beantwortet. Der Client schickt seine Anfrage nun an den Proxy und erhält von diesem die Daten. Der bekannteste Anbieter Akamai betreibt 15 000 Server in 69 Ländern. Es wären schon extrem viele Zombies erforderlich, um einen erfolgreichen Angriff durchzuführen.

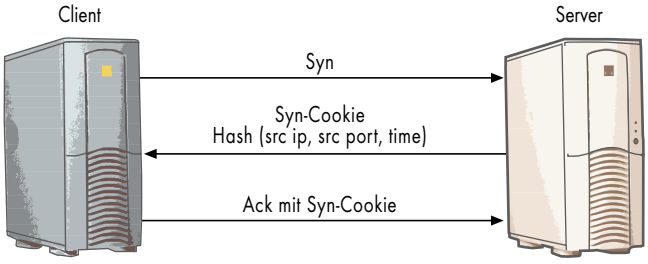
Selbst solche recht kostspieligen Varianten bieten jedoch keinen vollständigen Schutz. Das wird umso deutlicher angesichts der Tatsache, dass auch sehr große und gut angebundene Anbieter wie Yahoo oder Amazon durch DDoS-Angriffe zum Erliegen gebracht wurden. Ein Angreifer muss lediglich über genügend Zombie-Systeme mit ausreichend Bandbreite verfügen.

Manche Hersteller bieten gegen DDoS-Angriffe eigene Produkte an oder integrieren zusätzliche Features in bestehende Intrusion-Prevention-Systeme. Die meisten Systeme arbeiten sowohl mit Signaturen als auch mit heuristischen Verfahren. Signaturen eignen sich besonders zum Abfangen von bekannten Angriffen wie Land- oder Smurf-Attacken oder von solchen, die auf fehlerhaftem Programm-Code basieren.

IPS- und DoS-Mitigation-Appliances

Um unerwünschte Pakete aus dem Datenstrom filtern und somit DoS-Angriffe effektiv verhindern zu können, müssen die eingesetzten Systeme „inline“, also ähnlich einer Firewall, in das Netzwerk eingebunden sein. Es existiert auch eine Reihe von Firewall-Systemen, die eine Prüfung auf bestimmte DoS-Angriffe anhand von Signaturen durchführen und die entsprechenden Pakete blocken.

Der deutlich interessantere Ansatz besteht in der heuristischen Überprüfung des gesamten Netzverkehrs. In diesem Fall muss man dem System zuerst beibringen, wie der „übliche“ Datenfluss beschaffen ist. Übersteigen bestimmte Datenpakete einen gewissen Schwellwert, treten also deutlich häufiger auf als der zuvor definierte Normalwert, schlägt das System Alarm und kann unter Umständen die entsprechenden Datenpakete aus dem „normalen“ Datenstrom herausfiltern. Beim Einsatz solcher Systeme ist zu bedenken, dass auch durch normalen



Die normalerweise auf dem angefragten System gespeicherten Daten werden kryptographisch gesichert im Antwort-Paket untergebracht (Abb. 4).

QUELLEN IM INTERNET

DDoS gegen CNN & Co	www.heise.de/tp/r4/artikel/5/5766/1.html
DDoS als Waffe	www.heise.de/tp/r4/artikel/7/7332/1.html
Käufliche Bot-Netze	www.heise.de/tp/r4/artikel/17/17637/1.html
Schuldfrage Trojaner	www.heise.de/tp/r4/artikel/15/15889/1.html
GMD-IRC abgeschaltet	www.heise.de/newsticker/meldung/8766
Powertech	www.powertech.no/smurf/
Bogon-Liste	www.cymru.com/Documents/bogon-list.html

Netzverkehr hervorgerufene „Anomalien“ (etwa wenn sehr viele Anwender auf einen Webserver zugreifen) unter Umständen als DoS-Angriff bewertet werden könnten, was zum Ausschluss regulärer Anwender führen würde.

Kekse zur Syn-Flood-Abwehr

Zur Abwehr der beschriebenen Syn-Flooding-Angriffe sind verschiedene Verfahren denkbar. BSD und Linux lösen dieses Problem sehr elegant durch die von Dan Bernstein vorgeschlagenen Syn-Cookies: Der angesprochene Server reserviert für eine halboffene Verbindung keinen Speicher mehr, sondern quetscht alles, was er sich über die Verbindung merken muss, in die Sequence-Nummer der Antwort auf die Verbindungsanfrage. Wenn nun jemand wirklich eine Verbindung aufbauen möchte, verwendet er gemäß Standard die um eins erhöhte Sequence-Nummer als Ack-Nummer seines nächsten Paketes (Abb. 4). So kann der Kernel die in der Sequence-Nummer festgehaltenen Daten wieder auslesen und nutzen. Da er keinen Hauptspeicher oder Plätze in einer begrenzten Liste dafür benötigt, kann diese Ressource nicht überlastet werden. Andere Betriebssysteme verlängern einfach die Liste für halboffene Verbindungen oder verkürzen die Wartezeit für das nächste Paket des Gegenübers – was bei langsamen Leitungen oder einem gerade stattfindenden DDoS dazu führt, dass keine Verbindungen zu Stande kommen.

Heute existiert eine Reihe von Produkten (Firewalls, Router, Load-Balancer et cetera), die versuchen, Server-Systeme vor Syn-Flood-Angriffen zu schützen. In den meisten Fällen fungiert die eingesetzte Appliance entweder als Gateway oder als Relay.

Als Relay nimmt die Appliance das eingehende Syn-Paket des Clients anstelle des Servers an und versendet an seiner Stelle (mit der IP-Adresse des Servers) das zweite Paket eines Verbindungsaufbaus, ein Syn-Ack-Paket. Erhält die Appliance ein Ack-Paket zur Bestätigung durch den Client, wird eine zweite Verbindung zwischen Appliance (mit der IP-Adresse des Client) und Server aufgebaut, und die Kommunikation zwischen den beiden Systemen kann stattfinden. Ein Nachteil dieses Verfahrens ist, dass beim Aufbau der beiden Kommunikationsverbindungen unterschiedliche Initiale Sequenznummern (ISN) vergeben werden. Diese Sequenznummern muss die Appliance während der Kommunikation zwischen Client und Server anpassen.

Um dieses Anpassen zu vermeiden, fungieren viele Appliances auch als Gateway. In diesem Fall leitet die Appliance eingehende Anfragen direkt an den Server weiter. Der versendet ein Syn-Ack-Paket an den Client. Die Appliance sendet daraufhin anstelle des Clients sofort ein Ack-Paket. Die Verbindung gilt auf dem Server somit als „established“, und es können weitere Verbindungsanfragen entgegengenommen werden. Bleibt das eigentliche Ack-Paket des Clients aus, versendet die Appliance ein Reset-Paket an den Server, das die Verbindung beendet. Kommt das eingehende Ack-Paket des Client verspätet an, verwirft der Server es, da er ja bereits ein solches Paket erhalten hat.

Speichergröße und Leistung der CPU bestimmen die Anzahl der halboffenen Verbindungen, die eine solche Appliance oder Software verarbeiten kann, sodass bei einer großen Anzahl an Zombie-Systemen selbst mit diesen Abwehrversuchen ein DoS-Angriff erfolgreich sein kann.

Die bisher beschriebenen Verfahren sollen DoS-Angriffe erschweren oder verhindern. Finden dennoch weiterhin erfolgreiche Angriffe statt, bleibt insbesondere bei Flooding-Angriffen nur die Zusammenarbeit mit dem ISP. Für diesen Fall sollte ein Notfallkonzept existieren, in dem die notwendigen Schritte beschrieben sind. Ist der Netzzugang des Opfers durch Anfragen der Zombie-Systeme überlastet, kann der ISP die Daten in ein so genanntes Sinkhole umleiten. Der Nachteil dieses Verfahrens ist, dass der gesamte Datenstrom für ein angegriffenes System (also auch reguläre Anfragen) auf einen speziell aufgesetzten Server oder ins „Nirwana“ umgelenkt wird. Ein Sniffer oder der eingesetzte Server können den Datenstrom zur weiteren Analyse speichern.

Router und Serversysteme, die man für das Sinkholing einsetzt, sollten so konfiguriert sein, dass kein „backscatter-traffic“ (System-Nachrichten wie ICMP unreachable und so weiter) erzeugt wird beziehungsweise dieser das eigene Netzwerk nicht verlässt, um weitere Systeme durch den zusätzlichen Traffic nicht zu gefährden. Sinkholing ist vor allem dann sinnvoll, wenn andere Services durch den DoS-Angriff – zum Beispiel durch Überlastung der angemieteten Datenleitung – gefährdet sind. So stehen durch Umleiten des Datenstroms wenigstens diese Dienste weiter zur Verfügung. Die gewonnenen Daten können darüber hinaus zur Analyse des Angriffs und zum Einleiten weiterer investigativer Maßnahmen dienen. Führen den Angriff nur einige wenige Systeme aus, kann der ISP sie blockieren.

Fazit

Je mehr Teilnehmer des Internet ihre eigenen Systeme absichern und je mehr Provider ihre Netze nach dem neuesten Stand der Technik schützen, desto kleiner wird das Problem DDoS-Attacken werden. Microsoft hat mit eigenen Tools den Kampf gegen Backdoors aufgenommen, wird aber voraussichtlich in Zukunft keine Updates mehr an nichtlizenzierte Windows-Installationen ausliefern. Dadurch würde die Zahl der verwundbaren und damit die mit einem Wurm infizierten Systeme stark steigen. Das Phänomen Bot-Net und damit die Angreifbarkeit über Verwundbarkeiten in den Serverbetriebssystemen bleibt der Internetwelt damit weiterhin erhalten.

Retten kann sich nur, wer mit hohem Aufwand Gegenmaßnahmen ergreift, die entweder darauf basieren, dass mehr Bandbreite zur Verfügung steht als der Angreifer lahm legen kann, oder auf der schnellen Erkennung von Angriffen und Filterung dieser Daten. Wer sein Recht auf Privatsphäre und unzensierte Meinungsfreiheit schätzt, wird dennoch ein Internet mit DDoS-Angriffen einem vollständig überwachten und kontrollierten Netz vorziehen. (ur)

CHRISTOPH PUPPE
UND JÖRN MAIER

sind Security Consultants bei der Hisolutions AG in Berlin.