DDoS -HANDBUCH

HINTERGRÜNDE UND FAKTEN ZU **DDoS-ANGRIFFEN**

Inhalt

1 Einführung 4

2 Ein kurzer Blick zurück 5

3 Jüngste Vergangenheit: Denkwürdige Cyber-Attacken im Jahr 2014 8

4 Angriffstypen 10

5 Angriffstools 19

6 Unternehmenssicherheit: damals und heute 24

7 Die Zukunft: Prognosen für 2015 und die folgenden Jahre 29

8 Erwägungen zur DDoS-Abwehr 31

9 Checkliste: Bewertung der Fähigkeiten eines Anbieters bei der Abwehr von DDoS- und Cyber-Angriffen 35

10 DDoS-Glossar 37

1 Einführung

Seit dem ersten Denial of Service (DoS) im Jahr 1974 sind DDoS- (Distributed Denial of Service) und andere DoS-Angriffe ein fester Bestandteil der Cyber-Bedrohungslandschaft. In diesen Angriffen spiegelt sich nicht nur die frustrierende Beharrlichkeit von Hackern wider, sondern sie stellen auch alle für die Cyber-Sicherheit verantwortlichen Personen vor komplexe und sich ständig wandelnde Herausforderungen.

Dieser Leitfaden enthält einen Überblick darüber, wie Sie auch die raffiniertesten Cyber-Attacken erkennen und abwehren können. Inhalt des DDoS-Handbuchs von Radware:

- Geschichte der DDoS-Angriffe und die jüngsten Cyber-Attacken in aller Kürze
- Die wichtigsten Angriffstypen und -werkzeuge im Überblick
- Die kontinuierliche Weiterentwicklung der Anwendungssicherheit
- Praxisrelevante Tools und Tipps für Angriffserkennung und -abwehr
- Ausführliche Checkliste für die Bewertung eines Anbieters bei der Abwehr von DDoS- und Cyber-Angriffen
- DDoS-Glossar zur Erleichterung der Kommunikation und Beseitigung von Bedrohungen

An vielen Stellen in diesem Handbuch verweisen wir uns auf die Ergebnisse des Global Application & Network Security Reports 2014-2015 von Radware, einem der wichtigsten Forschungsberichte der Branche zum Thema DDoS- und Cyber-Angriffe.

2 Ein kurzer Blick zurück

2014 feierte der DoS-Angriff seinen 40. Geburtstag. Aus der Taufe gehoben wurden diese Angriffe von jugendlichen „Computerfreaks“. Seitdem haben sie sich wie ein Lauffeuer ausgebreitet und sind zudem wesentlich raffinierter geworden.

Die Anfänge

Der allererste DoS-Angriff wurde 1974 von einem 13-jährigen Schüler namens David Dennis lanciert. Dennis besuchte die University High School, die direkt gegenüber dem Forschungslabor für computergestütztes Lernen (CERL, Computer-Based Education Research Laboratory) der University of Illinois Urbana-Champaign lag. Dennis lernte einen Befehl kennen, der auf den PLATO-Terminals von CERL ausgeführt werden konnte. PLATO war eines der ersten computergestützten Lernsysteme und ein Vorläufer vieler künftiger Mehrplatzsysteme. Der Befehl „external“ oder „ext“ war dafür gedacht, die Kommunikation mit externen, an die Terminals angeschlossenen Geräten zu ermöglichen. Bei einem Terminal ohne Anschluss an externe Geräte bewirkte der Befehl aber eine Sperrung des Terminals. Das betroffene Terminal konnte erst wieder genutzt werden, nachdem es aus- und wieder eingeschaltet worden war.

Dennis fragte sich, wie es wohl wäre, wenn ein ganzer Raum voller Benutzer gleichzeitig ausgesperrt würde. Er schrieb ein Programm, das den Befehl „ext“ an viele PLATO-Terminals auf einmal sendete. Dennis ging hinüber zu CERL und testete sein Programm. Das Resultat war eindeutig: Alle 31 Benutzer mussten ihre Geräte gleichzeitig herunterfahren. Die Annahme des Befehls „ext“ wurde schließlich standardmäßig deaktiviert und das Problem hierdurch behoben.

In der zweiten Hälfte der 90er Jahre, als IRC (Internet Relay Chat) aufkam, kämpften einige Benutzer um die Kontrolle nicht registrierter Chat-Kanäle. Wenn ein Administrator sich abmeldete, verlor er seine Befugnisse. Dieses Verhalten inspirierte Hacker zu dem Versuch, sämtliche Benutzer eines Kanals zur Abmeldung zu zwingen, damit nur sie selbst Zugang zu diesem Kanal hatten und sich Administratorrechte aneignen konnten. Es kam zu regelrechten Schlachten, in denen Benutzer versuchten, die Kontrolle eines IRC-Kanals an sich zu reißen und gegenüber anderen Hackern zu verteidigen. Diese Kämpfe wurden mithilfe sehr einfacher, auf Bandbreiten basierender DoS-Angriffe und IRC-Chat-Floods ausgetragen.

Der Siegeszug der DDoS-Angriffe

Einer der ersten DDoS-Angriffe größeren Stils ereignete sich im August 1999. Ein Hacker legte mit einem Tool namens „Trinoo“ das Computernetzwerk der University of Minnesota mehr als zwei Tage lang lahm. Trinoo setzte sich aus einem Netzwerk kompromittierter Geräte namens „Masters“ und „Daemons“ zusammen. Ein Angreifer übermittelte eine DoS-Anweisung an einige der Masters, die diese Anweisungen wiederum an Hunderte von Daemons weiterleiteten. Hierdurch wurde bei der zum Opfer auserkorenen IP-Adresse eine UDP-Flood ausgelöst. Das Tool unternahm keinerlei Versuche, die IP-Adressen der Daemons zu verbergen. Die Eigentümer der angreifenden Systeme waren völlig überrascht, zu hören, dass jemand in ihre Systeme eingedrungen war und sie zu einem Angriff ausgenutzt hatte.

Zu den frühen Tools gehörten auch „Stacheldraht“, das per Fernzugriff aktualisiert werden konnte und IP-Spoofing unterstützte, sowie „Shaft“ und „Omega“, mit denen Angriffsstatistiken von Opfern erfasst wurden. Hackern war es also möglich, Daten über ihre Angriffe abzurufen. Dies wiederum gestattete es Ihnen, die Wirkung bestimmter Angriffstypen besser nachzuvollziehen und sich benachrichtigen zu lassen, wenn ein Angriff erkannt und gestoppt wurde.

Als Hacker auf DDoS-Angriffe umzusteigen begannen, gerieten DoS-Attacken erstmals in die Schlagzeilen. DDoS-Angriffe setzen an verteilten Punkten an und sind daher wesentlich wirkungsvoller. Ihre Identifizierung und die Blockierung ihrer Quelle gestalten sich zudem erheblich schwieriger. Hacker nutzten diese eindrucksvolle Waffe, um größere und prominentere Ziele ins Visier zu nehmen. Dabei bedienten sie sich besserer Tools und Methoden.

Um die Jahrtausendwende erregten DDoS-Angriffe öffentliche Aufmerksamkeit. Im Jahr 2000 wurden verschiedenen Unternehmen, Finanzinstitute und Behörden Opfer von DDoS-Attacken. Nur zwei Jahre später wurden DNS-Angriffe auf alle 13 Root-DNS-Server (Domain Name Service) ausgeführt. DNS ist ein wichtiger Internetdienst. Er übersetzt Hostnamen, die URL-Form (Uniform Resource Locator) vorliegen, in IP-Adressen. Im Prinzip ist DNS eine Art Telefonbuch mit einer Masterliste aller Internetadressen und der zugehörigen URLs. Ohne DNS wäre eine effiziente Internetnavigation nicht möglich, für den Besuch einer Website oder für die Kontaktaufnahme mit einem bestimmten Gerät die jeweilige IP-Adresse bekannt sein müsste.

Von Skriptkiddies bis hin zu geopolitischen Ereignissen

Im Zuge der technologischen Entwicklung haben sich auch die Beweggründe und die Akteure geändert. Heutzutage haben wir es nicht mehr nur mit jugendlichen „Computerfreaks“ oder „Skriptkiddies“ zu tun, die aus Neugier handeln. Es gibt noch andere. In den letzten Jahren ist die Anzahl der DDoS-Angriffe stetig gestiegen. Die Beweggründe für diese Angriffe ändern sich ständig und werden immer komplexer.

Zeitachse

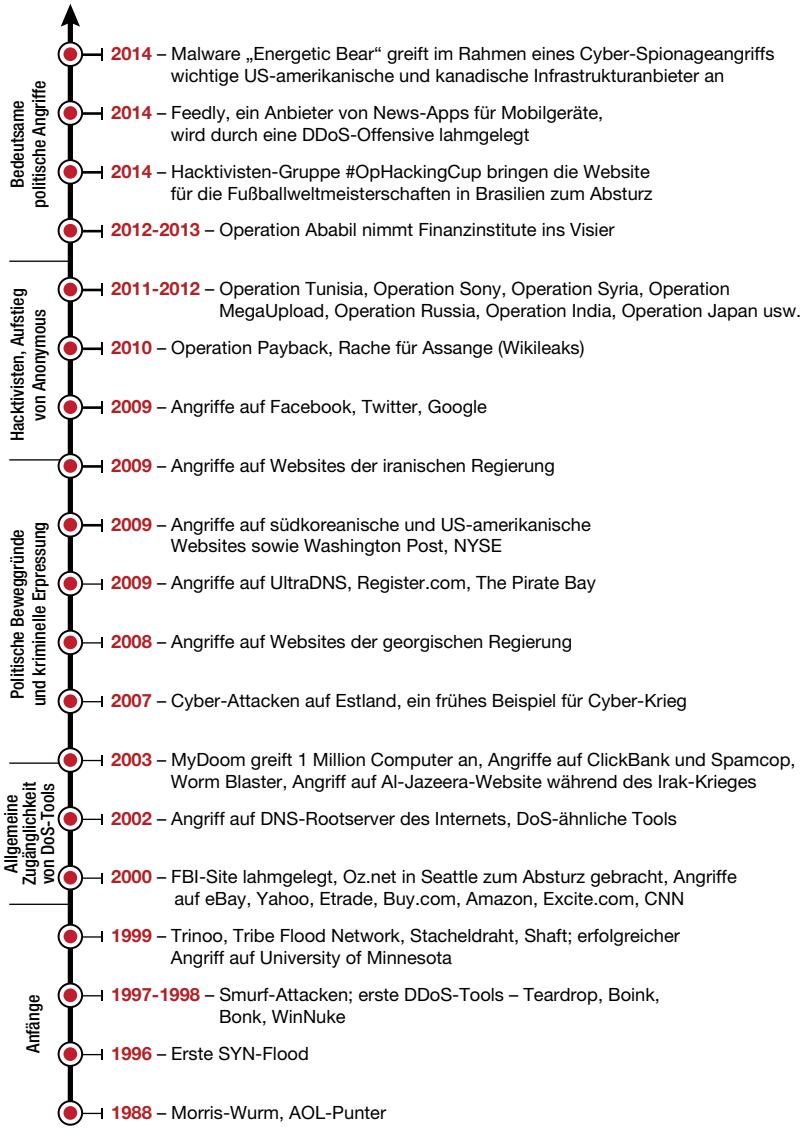


Abbildung 1

3 Jüngste Vergangenheit: Denkwürdige Cyber-Attacken im Jahr 2014

Dieser Abschnitt enthält einen Überblick über die jüngsten und denkwürdigen Angriffe, die sich 2014 ereignet haben. Sie sind in die Kategorien „Technisch“, „Ausfall“ und „Verstoß“ unterteilt.

Verstoß **Ausfall** **Technisch**

Januar bis März

- Der E-Mail-Service von Yahoo! mit 273 Millionen Benutzern ist Berichten zufolge Hackerangriffen ausgesetzt. Wie viele Konten betroffen sind, wird nicht bekannt gegeben.
- Bitcoin hat Code-Integritätsprobleme und fällt DDoS-Angriffen zum Opfer.
- Bei NTP werden neue DDoS-Schwachstellen aufgedeckt.
- Das britische Justizministerium und GCHQ (Government Communication Headquarters) sind DDoS-Angriffen ausgesetzt.
- Bei Neiman Marcus werden Kreditkartendetails von 350.000 Personen gestohlen. Mehr als 9.000 dieser Karten wurden seitdem für betrügerische Transaktionen verwendet. Hackern gelang es dank besonders raffiniertem Code, die Computer des Unternehmens monatelang unauffällig zu durchsuchen.

April bis Juni

- Neue Heartbleed-Schwachstelle wird bekannt gegeben.
- Fünf chinesische Staatsbürger werden wegen Computer-Hacking und Wirtschaftsspionage bei US-amerikanischen Firmen von 2006 bis 2014 angeklagt.
- Ukrainisch-russischer Cyber-Krieg lodert auf; die am Konflikt beteiligten Länder sind Angriffen ausgesetzt.
- Laut US-amerikanischem Ministerium für Innere Sicherheit (Department of Homeland Security, DHS) gelang es Hackern durch eine Brute-Force-Attacke, sich über die Login-Kennwörter der Mitarbeiter Zugang zum Kontrollsystem eines namentlich nicht genannten öffentlichen Versorgungsbetriebs zu verschaffen.
- Infolge zahlreicher DDoS-Attacken können 15 Millionen Benutzer die Feedly-Services nicht oder nur mit Einschränkungen nutzen.
- Evernote und seine 100 Millionen Benutzer sehen sich in der gleichen Woche, in der auch der Angriff auf Feedly stattfand, mit einem ähnlichen DoS-Angriff konfrontiert.
- Anonymous lanciert eine erfolgreiche DDoS-Kampagne gegen das Kinderkrankenhaus in Boston und bringt den Krankenhausbetrieb zum Erliegen.

- Hacker verschaffen sich bei 33 Restaurants der Kette P.F. Chang Zugang zu Kredit- und Debitkartendetails und verkaufen diese Berichten zufolge online.
- Sponsoren und Organisatoren der Fußballweltmeisterschaft 2014 sehen sich DDoS-Attacken ausgesetzt. Zahlreiche Übertragungen, News-Feeds und Marketing-Events werden beeinträchtigt.

Juli bis September

- Die Bash/Shellshock-Schwachstelle wird bekannt gegeben, die Millionen von Netzwerkgeräten weltweit betrifft.
- Bei U.S. Investigations Services, einem Subunternehmen, das Leumundsprüfungen für Bundesbedienstete durchführt, werden im August infolge eines Datenverstoßes Mitarbeiterdaten gestohlen.
- Neue DDoS-Schwachstelle Tsunami bietet Hackern neue volumetrische DDoS-Möglichkeiten.
- Erst im August wird ein Angriff auf J.P. Morgan Chase entdeckt, der sich bereits im Juni ereignete und bei dem Kontaktinformationen von 76 Millionen Haushalten und 7 Millionen Kleinunternehmen gestohlen wurden. Die Hacker stammten wahrscheinlich aus Russland und hatten möglicherweise Verbindungen zur russischen Regierung.
- Das FBI gibt den „Brobot Alert“ sowie eine Liste mit den URLs von 1492 Websites aus, die erwiesenermaßen infiziert wurden. Unternehmen werden gebeten, den Opfern bei der Entfernung der Malware zu helfen.
- Google entdeckt die SSLv3 „Poodle“-Schwachstelle, die später auf TLS (Transport Layer Security) erweitert wird.

Oktober bis Dezember

- Sony Pictures fällt kurz vor der Veröffentlichung des Films „Das Interview“ einem medienwirksamen Angriff zum Opfer. Die Folgen: Die Filmproduktion wird gestört, die Einspielergebnisse werden geschmälert und es entstehen Spannungen zwischen Mitarbeitern und Darstellern.
- Offene SSL-Schwachstelle bekannt gegeben, die Millionen von Softwareprodukten und Hardwaregeräten weltweit betrifft.
- Kredit- und Debitkartendetails werden bei den Läden 395 Dairy Queen und Orange Julius durch die Backoff-Malware gefährdet.
- Unbefugte verschafften sich Berichten zufolge Zugang zu Fotos von 200.000 Snapsave-Benutzern. Snapsave ist eine Drittanbieter-App zum Speichern von Fotos aus der Snapchat-App, die zum Instant-Verstand von Fotos dient.
- Über Weihnachten sind Sony PSN und Microsoft Xbox tagelang Angriffen ausgesetzt und für Millionen von Kunden weltweit nicht verfügbar.

4 Angriffstypen

Dieser Abschnitt enthält einen Überblick über die wichtigsten Angriffskategorien sowie über die einzelnen Angriffstypen.

Angriffe auf Netzwerkressourcen

Bei Angriffen auf Netzwerkressourcen wird versucht, die gesamte Bandbreite eines Opfers aufzubrauchen. Zu diesem Zweck wird der Internetzugang eines Unternehmens durch sehr umfangreichen, illegitimen Traffic überlastet. Diese als Flooding bezeichneten Angriffe sind einfach, aber wirkungsvoll.

In einem typischen Flood-Angriff führt eine aus Tausenden von freiwillig oder unfreiwillig eingezogenen Computern (ein Botnet) bestehende Armee eine Offensive aus. Durch die Übermittlung enormer Datenmengen wird das Netzwerk des beabsichtigten Opfers überwältigt.

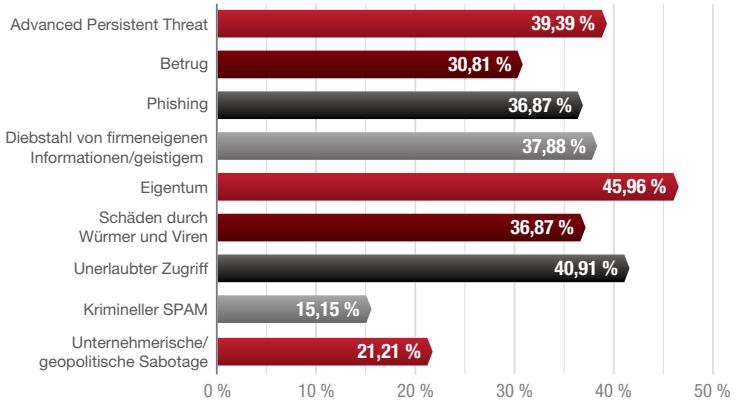


Abbildung 2: Die für Unternehmen schädlichsten Angriffe – Global Application & Network Security Report 2014-2015 von Radware

In kleineren Mengen mögen Anfragen dieser Art durchaus legitim wirken. In größeren Mengen können sie aber erheblichen Schaden anrichten. Während eines Flood-Angriffs ist die Nutzung der betroffenen Website nicht oder nur stark eingeschränkt möglich.

Flooding-Typen

UDP-Flood: User Datagram Protocol (UDP) ist ein verbindungsloses Protokoll, das für die Kommunikation in IP-Pakete eingebettete Datagramme verwendet. Zwischen zwei Geräten muss also keine Sitzung erstellt werden (d. h., es ist kein Handshake-Prozess erforderlich).

Ein UDP-Flood-Angriff setzt nicht bei einer bestimmten Schwachstelle an. Stattdessen nutzt er normale Verhaltensweisen in einem Maß aus, das zur Überlastung des betroffenen Netzwerks führt. Im Rahmen des Angriffs werden zahlreiche UDP-Datagramme von möglicherweise gefälschten IP-Adressen an willkürliche Ports eines Zielservers gesendet. Der Server ist nicht in der Lage, jede einzelne Anfrage zu bearbeiten. Bei dem Versuch, durch ICMP-Pakete („Ziel nicht erreichbar“) zu bestätigen, dass an den entsprechenden Ports keine Anwendungen lauschen, verbraucht er seine ganze Bandbreite. Eine UDP-Flood ist ein volumetrischer Angriff und wird in Mbit/s (Bandbreite) und PPS (Packets per Second) gemessen.

ICMP-Flood: Internet Control Message Protocol (ICMP) ist ein weiteres verbindungsloses Protokoll. Es wird für IP-Abläufe, Diagnosen und Fehler verwendet. Genau wie eine UDP-Flood kann auch eine ICMP-Flood (oder Ping-Flood) ein Denial of Service verursachen, ohne eine bestimmte Schwachstelle auszunutzen. Bei einer ICMP-Flood kann jede Art von ICMP-Nachricht verwendet werden, darunter eine Ping-Anfrage (Echoanforderung und -antwort). Wenn an einen Zielserver so viel ICMP-Traffic gesendet wird, dass er nicht mehr alle Anfragen verarbeiten kann, kommt es zum Denial of Service. Eine ICMP-Flood ist genau wie eine UDP-Flood ein volumetrischer Angriff und wird in Mbit/s (Bandbreite) und PPS (Packets per Second) gemessen.

IGMP-Flood: Internet Group Management Protocol (IGMP) ist ebenfalls ein verbindungsloses Protokoll. Es wird von IP-Hosts (Computern und Routern) verwendet, um Multicast-Gruppenmitgliedschaften für benachbarte Router zu melden oder zu verlassen. Bei einer IGMP-Flood wird keine Schwachstelle ausgenutzt, weil IGMP von der Konzeption her Multicast zulässt. Bei Floodings dieser Art werden zahlreiche IGMP-Nachrichten an ein Netzwerk oder an einen Router gesendet. Der legitime Datenverkehr über das Zielnetzwerk wird zunächst erheblich verlangsamt und schließlich zum Erliegen gebracht.

Amplification-Angriffe: Bei einem Amplification-Angriff (Amplification = Verstärkung) wird eine Disparität zwischen einer Anfrage und einer Antwort in einer technischen Kommunikation ausgenutzt. Beispielsweise kann ein Angreifer einen Router als Verstärker einsetzen. Über die Broadcast-IP-Adresse des Routers können dann Nachrichten an mehrere IP-Adressen gesendet werden, wobei als Absender die IP-Adresse des anzugreifenden Ziels angegeben wird. Bekannte Beispiele für diese Art von Angriffen sind Smurf-Angriffe (ICMP-Amplifier) und Fraggle-Angriffe (UDP-Amplifier). Ein weiteres Beispiel ist ein DNS-Amplification-Angriff. Hierbei wird zuerst ein zuvor kompromittierter, rekursiver DNS-Namensserver zur Speicherung einer großen Datei im Cache veranlasst. Dann wird eine Anfrage direkt oder über ein Botnet an diesen rekursiven DNS-Server gesendet. Der DNS-Server wiederum eröffnet eine Anfrage, mit der die große Datei im Cache gefordert wird. Die Antwortnachricht (die wesentlich größer als die ursprüngliche Anfrage ist) wird dann an die (gefälschte) IP-Adresse des Opfers gesendet; es kommt zum Denial of Service.

Verbindungsorientierte Angriffe:
Bei einem verbindungsorientierten Angriff muss der Angreifer zuerst eine Verbindung herstellen. Diese Art von Angriff wirkt sich in der Regel auf die Server- oder Anwendungsressourcen aus. TCP- oder HTTP-basierte Angriffe sind verbindungsorientierte DDoS-Angriffe.

Verbindungslose Angriffe:
Bei einem verbindungslosen Angriff hingegen ist der Angreifer nicht gezwungen, eine vollständige Verbindung zum Opfer herzustellen. Angriffe dieser Art lassen sich daher viel leichter lancieren. Verbindungslose Angriffe wirken sich auf Netzwerkressourcen aus und führen zu einem Denial of Service, ehe die böswilligen Pakete den Server erreichen. UDP-Floods und ICMP-Floods sind verbindungslose DDoS-Angriffe.

Reflection-Angriffe:
Bei dieser Angriffsart nutzt der Angreifer einen potenziell legitimen Dritten zum Senden seiner Angriffsdaten und verheimlicht hierdurch seine Identität.

Beweggründe für Angriffe
Richard Clarke, früherer Sonderberater für Cyber-Sicherheit im Weißen Haus, erfand das Akronym „C.H.E.W.“, um die Herkunft von Cyber-Angriffsrisiken zu klassifizieren und zu erläutern:

- **Cybercrime** (Cyber-Kriminalität)
  Angriffe mit dem Ziel, sich finanziell zu bereichern.

- **Hacktivisim** (Hacktivismus)
  Angriffe aufgrund ideologischer Meinungsverschiedenheiten. Hier geht es nicht darum, sich finanziell zu bereichern, sondern bestimmte Handlungen herbeizuführen oder zu vereiteln bzw. bestimmten „Stimmen“ Gehör zu verschaffen oder diese umzustimmen.

- **Espionage** (Spionage)
  Hier geht es einfach darum, Informationen über ein Unternehmen oder eine Einrichtung in Erfahrung zu bringen und diese zu politischen, finanziellen, kapitalistischen, marktpolitischen oder anderen Zwecken auszunutzen.

- **War (Cyber)** (Cyber-Krieg)
  Bei Angriffen dieser Art werden die Machtzentren eines Gegners durch einen Cyber-Angriff auf nationaler oder internationaler Ebene bedroht. Die Angriffe können sich gegen die zivile Infrastruktur oder Finanzdienstleister richten.

Angriffe auf Serverressourcen

Bei Angriffen auf Serverressourcen wird versucht, die Verarbeitungskapazitäten oder den Speicher eines Servers zu überlasten und hierdurch ein Denial of Service herbeizuführen. Dahinter steckt der Gedanke, dass ein Angreifer eine vorhandene Sicherheitslücke auf dem Zielserver (oder eine Schwäche in einem Kommunikationsprotokoll) ausnutzen und hierdurch bewirken kann, dass der Zielserver mit illegitimen Anfragen überlastet wird und keine Ressourcen für legitime Anfragen mehr hat. Bei diesem „Server" handelt es sich in der Regel um einen Website- oder Webanwendungsserver. DDoS-Angriffe dieser Art können sich aber auch gegen statusbehaftete Geräte wie Firewalls und Intrusion-Prevention-Systeme richten.

TCP/IP-Schwächen: Bei Angriffen dieser Art werden Schwächen im Design des TCP/IP-Protokolls ausgenutzt. Meist werden die sechs Kontrollbits (oder Flags) des TCP/IP-Protokolls (SYN, ACK, RST, PSH, FIN und URG) zur Behinderung des normalen TCP-Traffics eingesetzt. Im Gegensatz zu UDP und anderen verbindungslosen Protokollen ist TCP/IP verbindungsbasiert. Dies bedeutet, dass der Paketabsender erst Pakete absenden kann, nachdem er eine vollständige Verbindung zum beabsichtigten Empfänger hergestellt hat. TCP/IP beruht auf einem Drei-Wege-Handshake (SYN, SYN-ACK, ACK). Bei jeder Anfrage wird eine halb offene Verbindung (SYN), die Anforderung einer Antwort (SYN-ACK) und schließlich die Bestätigung der Antwort (ACK) erstellt. Bei Angriffen, die das TCP/IP-Protokoll ausnutzen, werden häufig TCP-Pakete in der falschen Reihenfolge gesendet. Bei dem Versuch, diesen ungewöhnlichen Traffic zu durchschauen, braucht der Zielserver seine gesamten Rechnerressourcen auf.

TCP-SYN-Flood: TCP-Handshakes funktionieren nur, wenn beide Parteien der Herstellung einer Verbindung zustimmen. Wenn der TCP-Client nicht vorhanden oder ein nicht anfragender Client mit einer gefälschten IP-Adresse ist, ist dies nicht möglich. In einem TCP-SYN- bzw. einem einfachen SYN-Flood-Angriff verleiten die angreifenden Clients den Server zu der Annahme, dass sie legitime Verbindungen anfordern. Dazu wird eine Reihe von TCP-Anfragen mit den TCP-Flags "SYN" von gefälschten IP-Adressen gesendet. Zur Abwicklung dieser SYN-Anfragen öffnet der Zielserver Threads und weist Puffer zu, um sich auf eine Verbindung vorzubereiten. Anschließend versucht er, eine SYN-ACK-Antwort an die anfragenden Clients zurückzusenden, um deren Verbindungsanfragen zu bestätigen. Da die IP-Adressen dieser Clients aber gefälscht sind, können die Clients nicht antworten. Der Server erhält kein Bestätigungspaket (ACK-Paket). Der Server ist gezwungen, weiterhin Threads und Puffer für jede der ursprünglichen Verbindungsanfragen bereitzuhalten. Er versucht, seine SYN-ACK-Anfragebestätigungspakete zu senden und fordert schließlich ein Timeout an. Weil Serverressourcen begrenzt sind und eine SYN-Flood häufig mit einer enormen Anzahl von Verbindungsanfragen einhergeht, ist es dem Server nicht möglich, für offene Anfragen ein Timeout anzufordern, bevor neue Anfragen eintreffen. Dies führt schließlich zu einem Denial of Service.

TCP-RST-Angriff: Mit einem TCP-RST-Flag wird Server aufgefordert, seine TCP-Verbindung sofort zurückzusetzen. Bei einem TCP-RST-Angriff stört der Angreifer eine aktive TCP-Verbindung zwischen zwei Einheiten. Hierzu errät er die aktuelle Sequenznummer und fälscht ein TCP-RST-Paket, um die Quell-IP-Adresse des Clients zu nutzen (die dann an den Server gesendet wird). Normalerweise werden Tausende solcher Pakete mit unterschiedlichen Sequenznummern über ein Botnet an den Server gesendet. Es ist relativ einfach, die richtige Nummer zu erraten. An diesem Punkt bestätigt der Server das vom Angreifer gesendete RST-Paket. Die Verbindung mit dem Client unter der gefälschten IP-Adresse wird beendet.

TCP PSH+ACK-Flood: Wenn ein TCP-Absender ein Paket mit dem PUSH-Flag 1 sendet, werden die TCP-Daten umgehend an den TCP-Empfänger gesendet oder „gepusht“. Hierdurch wird der empfangende Server gezwungen, seinen TCP-Stack-Puffer zu leeren und anschließend eine Bestätigung zu senden. Ein Angreifer – in der Regel ein Botnet – kann einen Zielserver mithilfe zahlreicher Anfragen dieser Art überschwemmen. Der TCP-Stack-Puffer auf dem Zielserver wird hierdurch so überlastet, dass er keine Anfragen mehr verarbeiten oder bestätigen kann. Das Ergebnis ist ein Denial of Service.

„Low & Slow“-Angriffe

Im Gegensatz zu Floodings benötigen langsame DDoS-Angriffe mit geringer Leistung, so genannte „Low & Slow“-Angriffe, nicht viel Datenverkehr. Sie setzen bei bestimmten Designschwächen oder Sicherheitslücken auf einem Zielserver an und bringen den Server durch relativ wenig Traffic zum Absturz. „Low & Slow“-Angriffe richten sich meist gegen Anwendungsressourcen (und gelegentlich auch Serverressourcen). Sie lassen sich nur sehr schwer erkennen, weil Verbindungen und der Datenverkehr normal erscheinen.

Sockstress: Sockstress ist eine Angriffsmethode, die Schwachstellen im TCP-Stack ausnutzt und mit der ein Angreifer auf einem Zielserver ein Denial of Service herbeiführen kann. Im normalen Drei-Wege-Handshake des TCP-Protokolls sendet ein Client ein SYN-Paket an den Server, der Server gibt ein SYN-ACK-Paket zurück und der Client bestätigt dies (ACK). Die Verbindung ist damit hergestellt. Angreifer stellen mithilfe von Sockstress zunächst eine normale TCP-Verbindung mit dem Zielserver her. Im letzten ACK-Paket senden sie jedoch das Paket „Window Size 0", das den Server anweist, dem TCP-Window eine Größe von 0 Byte zuzuweisen. Das TCP-Window ist ein Puffer, in dem die empfangenen Daten vor dem Hochladen in die Anwendungsschicht gespeichert werden. Das Feld „Window Size“ (Fenstergröße) gibt an, wie viel Platz im Puffer jeweils noch bereitsteht. Die Größe 0 bedeutet, dass keinerlei Platz vorhanden ist. Die Gegenseite wird angewiesen, vorerst keine weiteren Daten mehr zu senden.

Der Server sendet in diesem Fall wiederholt Testpakete an den Client, um festzustellen, wann Platz für neue Daten bereitsteht. Der Angreifer ändert die Fenstergröße aber nicht, und die Verbindung wird unbegrenzt lange offen gehalten. Durch Öffnen vieler Verbindungen dieser Art auf einem Server nimmt der Angreifer den gesamten Platz in der TCP-Verbindungstabelle des Servers (sowie anderer Tabellen) in Anspruch und hält legitime Benutzer davon ab, Verbindungen herzustellen. Alternativ kann ein Angreifer viele Verbindungen mit einer geringen Fenstergröße (ca. 4 Byte) öffnen. Hierdurch wird der Server gezwungen, Daten in eine extrem hohe Anzahl winziger 4-Byte-Stücke zu zerlegen. Viele Verbindungen dieser Art brauchen den verfügbaren Serverspeicher auf und führen zu einem Denial of Service.

SSL-basierte Angriffe

Secure Socket Layer (SSL): eine von vielen anderen Netzwerkkommunikationsprotokollen verwendete Verschlüsselungsmethode. Weil SSL immer beliebter wird, ist es in das Visier von Angreifern geraten. Von der Konzeption her ist SSL oberhalb von TCP/IP angesiedelt. Es bietet Benutzern, die über andere Protokolle kommunizieren, Sicherheit, indem es die Kommunikation verschlüsselt und die an der Kommunikation teilnehmenden Parteien authentifiziert. SSL-basierte DoS-Angriffe können vielerlei Gestalt annehmen. Einige setzen beim SSL-Handshake-Mechanismus an, einige senden Datenmüll an den SSL-Server und andere nutzen bestimmte Funktionen im Zusammenhang mit der Aushandlung des SSL-Verschlüsselungsschlüssels aus.
Bei manchen SSL-basierten Angriffen wird ein DoS-Angriff einfach über SSL-verschlüsselten Datenverkehr lanciert und ist dann äußerst schwer zu erkennen. Angriffe dieser Art werden oft als „asymmetrisch“ bezeichnet, weil für die Abwehr eines SSL-basierten Angriffs wesentlich mehr Serverressourcen erforderlich sind als für die Lancierung eines solchen Angriffs.

Verschlüsselungsbasierte HTTP-Attacken (HTTPS-Flooding): Viele Online-Unternehmen stützen sich immer stärker auf SSL/TLS (Transport Layer Security) in Anwendungen, um den Datenverkehr zu verschlüsseln und eine durchgängige Sicherheit bei der Datenübertragung zu gewährleisten. DoS-Attacken auf verschlüsselten Datenverkehr erfreuen sich zunehmender Beliebtheit. Die Abwehr derartiger Angriffe ist unerwartet schwierig. Die meisten Technologien zur Eindämmung von DoS-Angriffen nehmen den SSL-Traffic nicht genauer unter die Lupe, weil dies die Entschlüsselung des verschlüsselten Datenverkehrs voraussetzt. HTTPS-Floods – verschlüsselter HTTP-Traffic in extrem hohem Umfang (siehe nachstehende Erläuterung) –, spielen bei Offensiven gegen mehrere Schwachstellen immer häufiger eine Rolle. Verschlüsselte HTTP-Attacken verstärken die Wirkung „normaler" HTTP-Floods und bringen neue Herausforderungen mit sich, darunter die Notwendigkeit, Verschlüsselungs- und Entschlüsselungsmechanismen zu verwenden.

THC-SSL-DoS: Die Hackergruppe „The Hacker's Choice" (THC) entwickelte dieses Tool für Proof-of-Concept-Zwecke und um Anbieter zur Beseitigung von SSL-Schwachstellen zu animieren. Ähnlich wie andere Angriffe der Kategorie „Low & Slow" kann THC-SSL-DoS mit nur wenigen Paketen selbst auf einem recht großen Server ein Denial of Service verursachen. Das Tool setzt einen normalen SSL-Handshake in Gang und fordert dann sofort die Neuaushandlung des Verschlüsselungsschlüssels. Es wiederholt diese Forderung, bis alle Serverressourcen erschöpft sind. SSL-basierte Attacken sind bei Angreifern überaus beliebt, weil jeder SSL-Sitzungs-Handshake auf der Serverseite fünfzehnmal so viele Ressourcen verschlingt wie auf der Clientseite. Ein einzelner, ganz normaler Heimcomputer kann einen ganzen SSL-basierten Webserver zum Absturz bringen. Eine Gruppe von Computern kann sogar eine Serverfarm mit umfangreichen, abgesicherten Onlinediensten zum Erliegen bringen.

Angriffe auf Anwendungsressourcen

In den letzten Jahren haben DoS-Angriffe gegen Anwendungen zugenommen. Sie richten sich nicht nur gegen das bekannte HTTP (Hypertext Transfer Protocol), sondern auch gegen HTTPS, DNS, SMTP, FTP, VOIP und andere Anwendungsprotokolle, die für DoS-Attacken anfällig sind. Genau wie Angriffe auf Netzwerkressourcen gibt es auch bei Angriffen auf Anwendungsressourcen eine Reihe von Varianten, darunter Flooding und „Low & Slow"-Attacken. „Low & Slow"-Attacken sind besonders beliebt und nutzen meist Schwachstellen im HTTP-Protokoll aus. Das HTTP-Protokoll ist das meistgenutzte Anwendungsprotokoll im Internet und stellt ein attraktives Ziel für Angreifer dar.

HTTP-Flood: der gängigste DDoS-Angriff auf Anwendungsressourcen. Hierbei werden legitime, sitzungsbasierte HTTP-, GET- oder POST-Anfragen an den Webserver des Opfers gesendet. Angriffe dieser Art sind daher schwer erkennbar. HTTP-Flood-Angriffe werden in der Regel

von mehreren Computern (freiwillig bereitgestellten Geräten oder Bots) gleichzeitig ausgeführt. Diese Bots fordern kontinuierlich und wiederholt den Download der Seiten der Zielwebsite an (HTTP-GET-Flood), bis die Anwendungsressourcen erschöpft sind. Das Resultat ist ein Denial of Service. Viele moderne DDoS-Angriffstools, darunter High Orbit Ion Cannon (HOIC), erleichtern HTTP-Flood-Angriffe mit mehreren Threads.

DNS-Flood: leicht zu lancieren, schwer zu erkennen. DNS-Floods beruhen auf dem gleichen Prinzip wie andere Flooding-Angriffe. Angriffsziel ist hier das DNS-Anwendungsprotokoll, das durch eine große Anzahl von DNS-Anfragen überwältigt wird. Domain Name System (DNS) ist das Protokoll, mit dem Domänennamen in IP-Adressen aufgelöst werden. Ihm liegt das UDP-Protokoll zugrunde, das kurze Anfrage- und Antwortzeiten unterstützt, ohne Verbindungen herstellen zu müssen (wie bei TCP nötig). Bei einer DNS-Flood sendet ein Angreifer mehrere DNS-Anfragen entweder direkt oder über ein Botnet an den DNS-Server des Opfers. Der DNS-Server wird überlastet und ist nicht fähig, alle eingehenden Anfragen zu verarbeiten. Schließlich stürzt er ab.

„Low & Slow"-Angriffe: Im Mittelpunkt dieses Abschnitts stehen „Low & Slow"-Angriffe auf Anwendungsressourcen. Diese unterscheiden sich von „Low & Slow"-Angriffen auf Serverressourcen, die weiter oben erörtert wurden. „Low & Slow"-Angriffe auf Anwendungsressourcen richten sich gegen bestimmte Schwachstellen in Anwendungen und ermöglichen es einem Angreifer, unbemerkt ein Denial of Service zu verursachen. Angriffe dieser Art sind nicht volumetrisch und können häufig von einem einzelnen Gerät ausgelöst werden. Weil diese Angriffe in der Anwendungsschicht stattfinden, ist bereits ein TCP-Handshake vorhanden. Der böswillige Datenverkehr wirkt hierdurch wie normaler, über eine legitime Verbindung ablaufender Datenverkehr.

Langsame HTTP-GET-Anfrage: Bei einer langsamen HTTP-GET-Anfrage geht es darum, die Ressourcen einer Anwendung ganz oder zum Teil in Beschlag zu nehmen. Hierzu werden viele offene Verbindungen verwendet. Die Anwendung wird davon abgehalten, für legitime Benutzer legitime Verbindungen zu öffnen. Bei dieser Angriffsvariante erstellt und sendet ein Angreifer unvollständige HTTP-GET-Anfragen an den Server. Der Server öffnet für jede dieser Anfragen einen separaten Thread und wartet dann auf den Rest der Daten. Der Angreifer sendet weiterhin in bestimmten, aber relativ langen Zeitabständen HTTP-Header-Daten, damit die Verbindung offen bleibt und es nicht zu einem Timeout kommt. Weil die noch erforderlichen Daten so langsam hereinkommen, ist der Server gezwungen, zu warten. Wenn der begrenzte Platz in der Verbindungstabelle aufgebraucht ist, entsteht ein Denial of Service.

Langsame HTTP-POST-Anfrage: Bei dieser Angriffsart sucht der Angreifer auf der Zielwebsite Formulare und sendet über diese HTTP-POST-Anfragen an den Webserver. Die POST-Anfragen werden aber nicht normal übermittelt, sondern Byte für Byte. Genau wie bei langsamen HTTP-GET-Anfragen stellt der Angreifer auch hier sicher, dass seine böswillige Verbindung offen bleibt, indem er regelmäßig ein weiteres Byte der POST-Daten sendet. Der Server kennt die Länge der HTTP-POST-Anfragen und ist gezwungen, zu warten, bis die POST-Anfrage vollständig eingegangen ist (hier werden legitime Benutzer mit langsamer Internetverbindung nachgeahmt). Der Angreifer wiederholt diesen Vorgang viele Male und lässt alle Verbindungen stets offen. Wenn die Zahl der offenen Verbindungen mehrere Hundert beträgt, ist der Zielserver nicht mehr fähig, neue Anfragen abzuwickeln. Das Resultat ist ein Denial of Service.

RegEx DoS-Angriffe: RegEx DoS-Angriffe (auch ReDoS-Angriffe) sind eine Sonderform der „Low & Slow"-Angriffe (RegEx ist kurz für „Regular Expression" – regulärer Ausdruck). Hierbei sendet ein Angreifer eine speziell erstellte Nachricht (so genannte bösartige oder „evil" RegExes), die eine Sicherheitslücke in einer auf dem Server bereitgestellten Bibliothek ausnutzt. Dies ist in diesem Fall eine Softwarebibliothek für regelmäßige Ausdrücke. Der Server wird veranlasst, einen regelmäßigen Ausdruck über die vom Benutzer bereitgestellte Eingabe zu berechnen und dabei extrem viele Ressourcen zu verbrauchen oder aber die Verarbeitung eines vom Angreifer vorgegebenen, komplexen und ressourcenintensiven regelmäßigen Ausdrucks auszuführen.

Hashkonflikt-DoS-Angriffe: Angriffe dieser Art richten sich gegen gängige Sicherheitslücken in Webanwendungs-Frameworks. Die meisten Anwendungsserver erstellen Hashtabellen, die zur Indizierung der POST-Sitzungsparameter dienen. Anwendungsserver müssen gelegentlich Hashkonflikte lösen, wenn ähnliche Hashwerte zurückgegeben werden. Die Lösung von Konflikten ist ein ressourcen-intensiver Vorgang, weil für die Verarbeitung der Anfragen das CPU stärker belastet wird. Bei einem Hashkonflikt-DoS-Angriff sendet ein Angreifer eine speziell erstellte POST-Nachricht mit zahlreichen Parametern. Die Parameter sind so aufgebaut, dass sie auf dem Server Hashkonflikte verursachen und die Verarbeitung der Antworten erheblich verlangsamen. Angriffe dieser Art sind überaus wirkungsvoll und können von einem einzelnen Computer aus ausgeführt werden. Sie bewirken eine langsame, aber stetige Erschöpfung der auf dem Anwendungsserver verfügbaren Ressourcen.

5 Angriffstools

Die Hartnäckigkeit und Kreativität der Angreifer spiegelt sich in der Vielfalt der Angriffstools wider, die sie eigens entwickelt haben. Nachstehend finden Sie eine Übersicht über die am häufigsten verwendeten und gefährlichsten dieser Tools.

Viele DDoS-Angriffstypen können zwar manuell ausgeführt werden, aber es wurden zahlreiche spezielle Tools entwickelt, die die Ausführung von Angriffen bequemer und effizienter gestalten. Die ersten DDoS-Tools entstanden um die Jahrhundertwende, darunter Trinoo und Stacheldraht. Diese Tools waren jedoch recht kompliziert und funktionierten nur auf den Betriebssystemen Linux und Solaris. Inzwischen gibt es DDoS-Tools, die mehrere Plattformen angreifen können. Die heutigen Tools sind nicht nur moderner, sondern auch einfacher. DDoS-Angriffe lassen sich somit wesentlich einfacher ausführen und sind für die Opfer wesentlich gefährlicher.

Wie lange haben Sicherheitsbedrohungen bei Ihnen bisher im Schnitt gedauert?

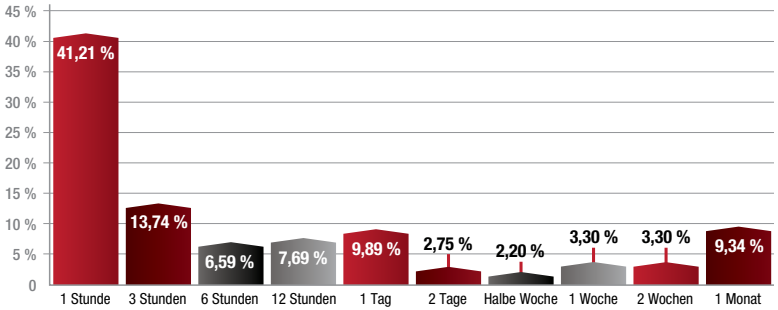


Abbildung 3: Durchschnittliche Dauer von Sicherheitsbedrohungen – Global Application & Network Security Report 2014-2015 von Radware

Einige dieser neueren DDoS-Tools, wie beispielsweise Low Orbit Ion Cannon (LOIC), wurden ursprünglich zur Durchführung von Belastungstests in Netzwerken entwickelt, später aber für böswillige Zwecke umgeschrieben. Andere Tools wie Slowloris wurden von „Gray Hat"-Hackern entwickelt, um die Aufmerksamkeit der Öffentlichkeit auf eine bestimmte Sicherheitslücke in Software zu lenken. Durch die Veröffentlichung derartiger Tools werden die Hersteller anfälliger Software gezwungen, Patches bereitzustellen und die Gefahr spektakulärer Offensiven abzuwenden.

Die zur Ausführung von DDoS-Attacken verwendeten Tools unterliegen genau wie die Netzwerksicherheit und die Welt der Hacker einem stetigen Wandel. Angriffstools werden immer kompakter und unauffälliger und können Denial-of-Service-Zustände immer effektiver auslösen.

Low Orbit Ion Cannon (LOIC)

LOIC (Low Orbit Ion Cannon) ist das Lieblingstool der Hacktivistengruppe Anonymous. Es ist ein einfaches Flooding-Tool, das eine enorme Menge von TCP-, UDP- oder HTTP-Traffic erzeugen und so einen Server in die Knie zwingen kann. Ursprünglich entwickelt wurde das Tool von Praetox Technologies. Es sollte es Entwicklern ermöglichen, ihre eigenen Server Belastungstests zu unterziehen. Anonymous erkannte das böswillige Potenzial dieses Open-Source-Tools und setzte es für die Lancierung koordinierter DDoS-Angriffe ein. Kurze Zeit später wurde LOIC modifiziert und mit der Funktion „Hivemind “ ausgestattet. Ein LOIC-Benutzer kann nun eine LOIC-Kopie auf einen IRC-Server verweisen und die Kontrolle des Servers auf einen Masterbenutzer übertragen. Dieser Masterbenutzer wiederum kann über IRC Befehle an alle verbundenen LOIC-Clients gleichzeitig senden. In dieser Konfiguration können Benutzer DDoS-Angriffe lancieren, die wesentlich effektiver sind als die Angriffe weniger gut koordinierter und nicht simultan arbeitender LOIC-Benutzergruppen. Ende 2011 ließ Anonymous LOIC als DDoS-Haupttool fallen, weil es keinen Versuch unternimmt, die IP-Adressen seiner Benutzer zu verbergen. Dieser Mangel an Anonymität führte weltweit zur Verhaftung verschiedener Personen, die an LOIC-Attacken teilgenommen hatten. Anonymous teilte daraufhin auf allen IRC-Kanälen mit, dass LOIC fortan nicht mehr genutzt werden solle.

Wie lange dauerte die längste Sicherheitsbedrohung, die sich in Ihrem Unternehmen ereignet hat?

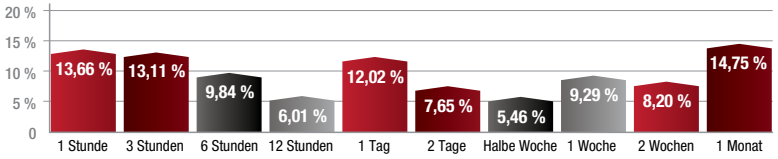


Abbildung 4: Längste Sicherheitsbedrohungen –
Global Application & Network Security Report 2014-2015 von Radware

Wie lange können Sie einer 24-stündigen Offensive effizient standhalten?

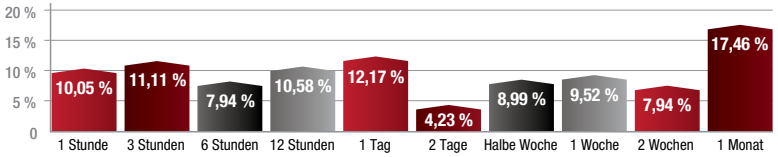


Abbildung 5: Längste Sicherheitsbedrohungen –
Global Application & Network Security Report 2014-2015 von Radware

High Orbit Ion Cannon (HOIC)

High Orbit Ion Cannon (HOIC) erregte erstmals Aufmerksamkeit, als es für einen Angriff auf das US-amerikanische Justizministerium eingesetzt wurde. Der Anlass war die Entscheidung des Ministeriums, die Website Megaupload.com abzuschalten. HOIC ist im Kern eine einfache Anwendung. Über ein plattformübergreifendes einfaches Skript werden HTTP-POST und -GET-Anfragen in einem bedienfreundlichen GUI gesendet. Seine Wirksamkeit beruht aber auf ergänzenden „Booster"-Skripts. Dabei handelt es sich um Textdateien mit einem zusätzlichen Basiscode, der zu Beginn eines Angriffs von der Hauptanwendung interpretiert wird. Obwohl HOIC die Anonymität nicht direkt schützt, können Benutzer mithilfe der Booster-Skripts Listen mit Ziel-URLs und Kennungen zusammenstellen, die HOIC dann bei der Generierung des schädlichen Datenverkehrs durchläuft. Hierdurch wiederum wird die Blockierung von HOIC-Angriffen erschwert. HOIC wird auch heute noch von Anonymous überall auf der Welt für DDoS-Attacken eingesetzt. Allerdings ist HOIC nicht die einzige Waffe im Anonymous-Arsenal.

hping

Anonymous und andere Hackergruppen bedienen sich bei ihren DDoS-Angriffen vieler anderer Tools. Einer der Gründe hierfür ist, dass weder LOIC noch HOIC genügend Anonymität bieten. Zu diesen Tools gehört unter anderem hping, ein recht einfaches Befehlszeilenprogramm, das viel Ähnlichkeit mit dem Ping-Dienstprogramm hat. Es ist aber vielseitiger als Ping, das traditionell zum Versenden von ICMP-Echoanfragen dient. Mit hping kann umfangreicher TCP-Traffic an ein Ziel gesendet werden, wobei die Quell-IP-Adressen gefälscht werden. Dadurch entsteht der Eindruck, dass der Datenverkehr willkürlich ist oder gar aus einer bestimmten benutzerdefinierten Quelle stammt. hping ist ein leistungsstarkes, vielseitiges Tool (mit einigen Fälschungsfunktionen), das sich bei Anonymous weiterhin großer Beliebtheit erfreut.

Slowloris

Einmal abgesehen von direkten Brute-Force-Flood-Attacken werden viele der komplizierteren „Low & Slow"-Angriffstypen in bedienfreundliche Tools verpackt, die gut versteckte Denial-of-Service-Angriffe erzeugen. Slowloris, ein von einem Gray-Hat-Hacker mit dem Aliasnamen RSnake entwickeltes Tool, kann mithilfe einer sehr langsamen HTTP-Anfrage ein Denial of Service auf einem Server verursachen. HTTP-Header werden in winzigen Stücken und so langsam wie möglich an die Zielsite gesendet. Die Übermittlung des nächsten winzigen Stücks erfolgt erst kurz vor dem Timeout der Anfrage. Der Server wird hierdurch gezwungen, weiter auf die Header zu warten. Sobald mit dem Server genügend Verbindungen dieser Art geöffnet wurden, verliert der Server schnell die Fähigkeit, legitime Anfragen abzuwickeln.

R U Dead Yet? (R.U.D.Y.)

R U Dead Yet? (R.U.D.Y.) ist ein weiteres, langsam arbeitendes DoS-Tool, das Slowloris ähnelt. R.U.D.Y. ist nach einem Album der finnischen Band „Children of Bodom“ benannt. Dieses Tool verwendet anders als Slowloris keine HTTP-Header, sondern langsame HTTP-POST-Feldeingaben.

Die größten Sorgen

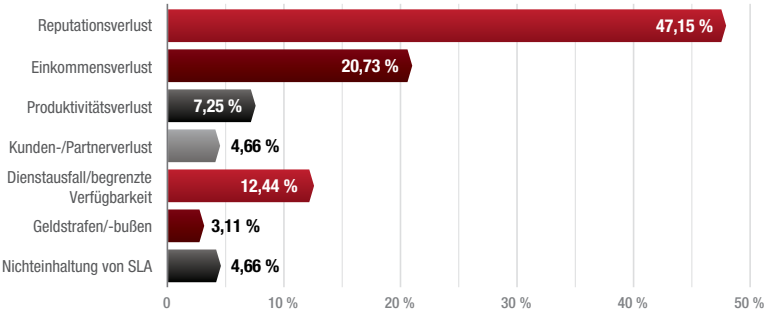


Abbildung 6: Sorgen von Unternehmen im Zusammenhang mit Cyber-Attacken – Global Application & Network Security Report 2014-2015 von Radware

Es gibt jeweils ein Byte Daten in das POST-Feld einer Anwendung ein und wartet dann. Anwendungsthreads werden hierdurch von R.U.D.Y. gezwungen, mit der Verarbeitung zu warten, bis das Ende niemals endender Posts erreicht ist. (Dieses Verhalten ist notwendig, damit Webserver auch Benutzer mit langsameren Verbindungen unterstützen können.) Weil R.U.D.Y. den Zielwebserver dazu veranlasst, zu „hängen“ und auf den Rest einer HTTP-POST-Anfrage zu warten, kann ein Benutzer viele gleichzeitige Verbindungen zum Server herstellen. Die Verbindungstabelle des Servers ist irgendwann erschöpft, und es entsteht ein Denial of Service.

#RefRef

Keines der bisher genannten Tools nutzt Schwachstellen aus. #RefRef hingegen, eine weitere Waffe im Anonymous-Arsenal, basiert auf einer Sicherheitslücke in der weit verbreiteten SQL-Datenbanksoftware, die Angriff durch Einschleusung zulässt. Mit einer SQL-Injection (Einschleusung) ermöglicht es #RefRef einem Angreifer, auf einem Zielserver ein Denial of Service hervorzurufen. Der Server wird zur Verwendung einer bestimmten SQL-Funktion gezwungen (die wiederum die wiederholte Ausführung eines anderen SQL-Ausdrucks ermöglicht). Durch die ständige Ausführung einiger weniger Codezeilen werden die Ressourcen des Zielservers aufgebraucht, bis ein Denial of Service erreicht ist.

Im Gegensatz zu LOIC oder HOIC benötigt #RefRef kein Heer von Maschinen, um einen Server zum Absturz zu bringen. Wenn das Back-End des Servers SQL verwendet und anfällig ist, lässt sich ein bedeutsamer Ausfall mit nur wenigen Geräten erzielen. Anonymous probierte das #RefRef-Tool bereits während der Entwicklungsphase an mehreren Sites aus. Für minutenlange Site-Ausfälle brauchte eine einzige Maschine nur 10 oder 20 Sekunden. Bei einer dieser Attacken (auf Pastebin) genügte eine 17-Sekunden-Salve von einem einzelnen Gerät, um die gesamte Site 42 Minuten lang lahmzulegen.

Botnets als DDoS-Tool

Unabhängig vom verwendeten Tool stehen die Erfolgsaussichten eines Angriffs wesentlich besser, wenn Hunderte, Tausende oder Millionen von Computern daran beteiligt sind. Nicht selten stehen Angreifern so genannte Botnets zur Verfügung. Botnets sind große Gruppen von kompromittierten Computern („Zombies“), die mit Malware infiziert sind und von einem Angreifer gesteuert werden können. Die Eigentümer oder „Herder“ von Botnets können die Botnet-Geräte über einen verdeckten Kanal wie beispielsweise IRC steuern und durch entsprechende Befehle zu böswilligen Aktivitäten veranlassen. Diese Aktivitäten reichen von DDoS-Attacken (Distributed Denial of Service) über Spam-Mails bis hin zum Datendiebstahl.

Im Jahr 2006 gehörten einem Botnet im Schnitt 20.000 Geräte an, und Botnet-Eigentümer bemühten sich, ihre Netzwerke zu verkleinern, um weiterhin verdeckt arbeiten zu können. Einige größere und komplexere Botnets, darunter BredoLab, Conficker, TDL-4 und Zeus, umfassen Berechnungen zufolge Millionen von Geräten. Gegen eine geringe Gebühr – oft nur 100 US-Dollar pro Tag – können etliche große Botnets von Zahlungswilligen gemietet werden. (Eine Werbeanzeige in einem Onlineforum bot die Nutzung eines Botnets mit 80.000 bis 120.000 infizierten Geräten zu einem Tagessatz von 200 US-Dollar an.) Bei derartigen Spottpreisen kann praktisch jeder, der technisch einigermaßen versiert ist und über die richtigen Tools verfügt, einen vernichtenden Angriff ausführen. Es ist wichtig, sich über die neuesten Angriffstools auf dem Laufenden zu halten, auf allen Servern und Netzwerkgeräten aktuelle Software zu verwenden und eine interne DDoS-Abwehrlösung zu verwenden. Nur so können Sie sich vor gegenwärtigen und künftigen Angriffen schützen.

6 Unternehmenssicherheit: damals und heute

Bis vor Kurzem noch befanden sich alle Assets, die ein Unternehmen schützen muss – Rechenzentren, Anwendungen, Datenbanken – innerhalb des Perimeters. Wie lautet die Grundregel? Ein abgesicherter Perimeter bedeutet sichere Assets.

Heutzutage ist der Perimeter bedeutungslos, weil Unternehmensanwendungen nach und nach in die Cloud ausgelagert werden. Kurz: Assets befinden sich überall. Wie kann ein Unternehmen seine Assets unabhängig von deren Standort schützen?

In vielen Unternehmen sieht die IT-Infrastruktur wie in Abbildung 7 dargestellt aus. Rechenzentren sind über mehrere Standorte verteilt, und ein immer größerer Teil der Infrastruktur befindet sich in der Cloud. Die Verteilung der IT-Infrastruktur birgt viele Vorteile, aber auch viele Herausforderungen in sich. Wenn die Assets eines Unternehmens nicht mehr durch die physische Absicherung des Perimeters geschützt werden können, müssen die vorhandenen Sicherheitsmaßnahmen geprüft werden.

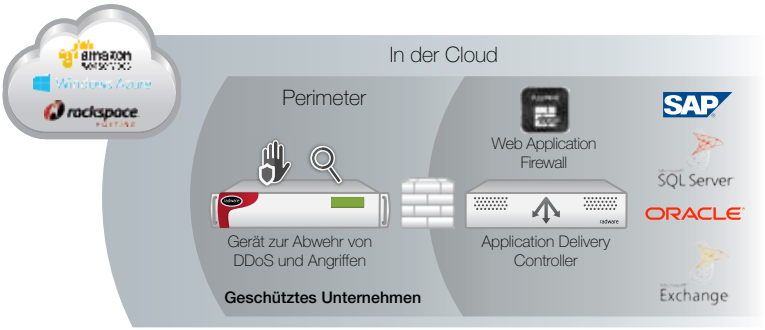


Abbildung 7: IT-Infrastruktur

Die Sicherheitsmaßnahmen von Unternehmen werden kontinuierlich weiterentwickelt, und auch Cyber-Kriminelle bemühen sich, ihre Angriffe zu vervollkommnen. Die Angreifer und ihre Taktiken werden immer raffinierter. Jeder weiß heute, dass Angriffe sich nicht verhindern lassen. Es ist aber wichtig, sich dagegen zu wehren.

Wenn die Sicherheitsstrategie eines Unternehmens nicht all diese Punkte berücksichtigt, sind das Unternehmen und dessen Benutzer Risiken ausgesetzt.

In diesem Kapitel werden die mit dem Schutz einer verteilten Infrastruktur einhergehenden Herausforderungen unter der Prämisse beleuchtet, dass unbekannt ist, wo Angriffe zu erwarten sind und

wie diese Angriffe sich auf verschiedene Assets auswirken. Anhand einiger wichtiger Überlegungen wird deutlich gemacht, wann eine Sicherheitsstrategie überarbeitet und an die gegenwärtigen Realitäten angepasst werden muss.

Neue Gegebenheiten, neue Herausforderungen

Die jüngsten Entwicklungen im IT-Bereich und im Bereich der Benutzermobilität haben die IT-Infrastruktur in einen Motor für Geschäftsagilität und -effizienz verwandelt. Gleichzeitig stellen sie IT-Manager/Sicherheitsbeauftragte und Unternehmen, die das Internet zur Umsatzgenerierung und zur Unterstützung ihrer Produktivität benötigen, vor neue Herausforderungen:

- **Der Perimeter des Netzwerks löst sich auf.** Viele Unternehmen haben ihre IT-Infrastruktur auf die öffentliche Cloud ausgedehnt, stellen neue Anwendungen in der Cloud bereit oder nutzen die Cloud für ihre Disaster-Recovery. Dies bedeutet aber, dass sie ihre Anwendungen sowohl in der Cloud als auch in privaten Rechenzentren schützen müssen. Herkömmliche Sicherheitstechnologien sind hier überfordert. Unternehmen müssen Fachwissen in verschiedenen Bereichen aufbauen und fördern und gleichzeitig neue Verwaltungstools in Betrieb nehmen.

- **Der CDN-Markt dehnt sich aus.** CDN-Lösungen (Content Delivery Network) bergen neue Sicherheitslücken in sich. Hacker benutzen dynamische Inhalte, um den leistungsstarken Cache-Offloading-Mechanismus zu umgehen, der den CDN-Lösungen zugrunde liegt. Mit dieser Methode können raffinierte Hacker Tools erstellen, die CDN nicht auffallen und die Anwendungsserver im Rechenzentrum überlasten.

- **Die Virtualisierung von Rechenzentren bedeutet eine höhere Anfälligkeit gegenüber Angriffen, die die Verfügbarkeit betreffen.** Es stimmt zwar, dass private Cloudtechnologien die Vertraulichkeit und Integrität von Anwendungsdaten schützen. Sie sind aber nicht in der Lage, die physische Infrastruktur vor Angriffen zu schützen, die die Verfügbarkeit betreffen. Gegen externe Anwendungen gerichtete Angriffe wirken sich auch auf die Verfügbarkeit kritischer interner Anwendungen aus. Ein Angriff auf eine einzige Anwendung kann eine Gefahr für andere Anwendungen in einer gemeinsamen Infrastruktur bedeuten.

Mehrschichtige IT-Infrastruktur erfordert eine mehrschichtige Sicherheitsstrategie

Herkömmliche Netzwerk- und Sicherheitslösungen verbinden in der Regel Erkennung und Abwehr im gleichen System. Der Systembediener legt Regeln (Richtlinien oder Profile) fest, und das System blockiert (oder gestattet) Traffic, der mit den vordefinierten Regeln übereinstimmt. In einigen Fällen, beispielsweise bei Intrusion-Detection-Systemen, gibt das System nur bei verdächtigem Traffic eine Warnung

aus, und die zuständige Bedienkraft muss die Daten manuell auswerten. Herkömmliche Sicherheitslösungen werden als punktuelle Sicherheitslösungen bezeichnet, weil sie Angriffe verhindern, die am physischen Ort ihres Auftretens untersucht werden. Bei ausgefeilten Angriffen, zu deren Abwehr der gesamte Netzwerkkontext berücksichtigt werden muss, stoßen diese Lösungen daher schnell an ihre Grenzen.

Laut Gartner[1] stützen sich Unternehmen zu stark auf Blockierungs- und Vorbeugungsmaßnahmen, die gegen moderne Angriffe immer weniger ausrichten können. Angreifer haben längst erkannt, dass Sicherheitstools meist „Inseln des Wissens“ sind, und nutzen diese mangelnde Integration in komplexen Offensiven aus. Selbst für Unternehmen, die in SIEM-Lösungen (Security Informationen and Event Management) investieren, ist der Umfang der von den einzelnen Tools erzeugten Daten häufig erdrückend. Die Auswertung dieser Daten ist zeitaufwändig, was wiederum die Abwehr von Angriffen verzögern kann.

Unternehmen stellen auch fest, dass die Fähigkeit, vorbeugende Maßnahmen anzuwenden, durch die zunehmende Komplexität von Sicherheitslösungen eingeschränkt wird. Häufig kennen sie ein Produkt nicht gut genug, um neue Regeln mit dem richtigen Tool und an der richtigen Stelle anzuwenden.

Das Zeitalter der integrierten Hybridlösung

Es mag zwar wie ein Widerspruch klingen, aber die einzige ganzheitliche Lösung ist eine verteilte Lösung. Die wirksame Bekämpfung komplexer Offensiven und neuer Bedrohungen setzt voraus, dass sich das Design der Sicherheitsarchitektur primär an der verteilten Natur der gegenwärtigen IT-Infrastruktur orientiert.

Anders ausgedrückt, wenn Assets über mehrere Standorte und Geräte verteilt sind und dort abgerufen werden, müssen auch die Tools zur Erkennung und Abwehr von Angriffen verteilt sein. Die Reichweite der Erkennungstools muss auf alle Unternehmensressourcen ausgeweitet werden. Wenn die Zahl der Endpunkte steigt, müssen verschiedenartige Erkennungstools von unterschiedlichen Anbietern an unterschiedlichen Orten eingesetzt werden. Für die Verwaltung und Wartung der verschiedenen Erkennungstools wird weiterhin Personal benötigt, das darüber entscheidet, wann, wo und wie die erkannten Angriffe abgewehrt werden.

Sicherheitsszenarios

Im Folgenden werden Szenarios erörtert, in denen einige der neuen Herausforderungen eine Rolle spielen, die Unternehmen bei der Entwicklung einer Sicherheitsstrategie berücksichtigen müssen.

1. Ein internes Gerät zum Schutz gegen DoS/DDoS-Angriffe erkennt volumetrische Flood-Angriffe am Perimeter. Die Abwehrmaßnahmen

[1] Designing an Adaptive Security Architecture for Protection From Advanced Attacks, Gartner, Februar 2014

werden sofort in Gang gesetzt. Die Stärke der Offensive droht jedoch, den Internetzugang zu überlasten. Nach kurzer Zeit ist der Internetzugang überlastet, und das Unternehmen verliert Aufträge.

Gibt es eine Alternative? Immer mehr DDoS-Abwehrlösungen bieten eine Hybridlösung. Sie wehren einen Angriff vor Ort ab, solange keine Überlastung des Internetzugangs droht. Beim ersten Anzeichen dieser Gefahr wird der Datenverkehr in ein cloudbasiertes Scrubbing-Center umgeleitet, und nur „sauberer" Verkehr wird an das Unternehmen zurückgeleitet. Der Vorgang ist vollkommen transparent, und die Benutzer bemerken keine Leistungseinbußen. (Warnung: Wenn Erkennungs- und Abwehrtools von unterschiedlichen Anbietern stammen, läuft der Vorgang möglicherweise nicht automatisch ab. Er kann sich daher als zeitaufwändig erweisen, und es können sich Fehler durch menschliches Versagen einschleichen.)

2. Angriffe, die sich echter IP-Adressen bedienen und von einem CDN verdeckt werden, werden von der WAF (Web Application Firewall) des Unternehmens beseitigt. Weil der Angriff aber in der Nähe der Anwendung (nicht am Perimeter) abgewehrt wird, kann nicht garantiert werden, dass er nicht möglicherweise andere Assets erreicht hat, die nicht unter den Schutz der WAF fallen. Bei einer intensiveren Offensive kapituliert die WAF, und das Unternehmen ist gefährdet. Die Lösung muss skalierbar sein und ist daher möglicherweise problematisch, wenn zu viele WAFs inline implementiert sind.

Nach den Erkenntnissen von Radware gibt es zwei erfolgversprechende Lösungsansätze. Beim ersten Ansatz erfolgt die WAF-Implementierung „Out-of-Path", wodurch die Lösung skalierbar wird. Beim zweiten Ansatz wird ein WAF zur Datenauswertung befähigt. Dieser Ansatz eignet sich für einen Netzwerkkontext und setzt die Konfiguration einer Blockierungsregel auf dem internen DoS-Schutzgerät oder – bei zunehmender Intensität der Angriffe – in der Cloud voraus. Das Resultat ist ein agileres Netzwerk, das Angriffslasten von Anwendungsgeräten wie beispielsweise der WAF in den Perimeter oder die Cloud verschiebt.

Die Verwendung mehrerer Erkennungs- und Abwehrtools an unterschiedlichen Standort ist unvermeidlich. Der Betrieb, die Verwaltung, die Instandhaltung und die Korrelation sämtlicher Tools mögen IT-Mitarbeitern sowohl zu Friedenszeiten als auch während Angriffen schier unmöglich erscheinen.

In einem kontinuierlichen Katz-und-Maus-Spiel trachten Angreifer und die Anbieter von Sicherheitslösungen gleichermaßen nach dem Sieg. Es wurde bereits auf den Markttrend hin zu Hybridlösungen hingewiesen, die Erkennung und Abwehr vor Ort mit Abwehrmaßnahmen in cloudbasierten Scrubbing-Centern verbinden. Die Verwendung mehrerer Erkennungstools, die über verschiedene Standorte verteilt sind und häufig von unterschiedlichen Anbietern stammen, birgt aber Zündstoff in sich.

Wir gehen davon aus, dass Erkennungs- und Abwehrlösungen künftig schneller, genauer und stärker automatisiert sein werden. Die Notwendigkeit, diese Lösungen zu verwalten und auf dem aktuellen Stand zu halten, dürfte aber weiterhin bestehen. Es ist daher wichtig, dass Unternehmen die Prozesse besser verstehen und einen besseren Einblick in Angriffe nehmen können – und zwar vor, während und nach ihrem Auftreten.

Vom Standort zur Kommunikation

Was ist der Schlüssel zu einer erfolgreichen Sicherheitsstrategie, die wirklich von den Vorteilen der in einem Unternehmen implementierten modernen Erkennungs- und Abwehrlösungen profitieren kann? Die Antwort scheint zu sein, dass nicht mehr der Standort, sondern die Kommunikation entscheidend ist. Erkennungs- und Abwehrtools werden an immer mehr Standorten eingesetzt, und es wird immer dringlicher, diese Tools manuell oder maschinell zu koordinieren.

Die Verteilung der Erkennungs- und Abwehrschichten über die gesamte Anwendungsinfrastruktur eines Unternehmens kann einen umfassenden Einblick in das Netzwerkverhalten und den Angriffsstatus geben. Die von den einzelnen Erkennungstools erfassten Daten müssen miteinander in Beziehung gebracht und analysiert werden, um festzustellen, welche Abwehrprozesse am besten geeignet sind.

Was gebraucht wird, ist ein automatisches, zentrales Befehls- und Kontrollsystem, das kontinuierlich Daten von allen Erkennungstools erfasst und hierdurch nicht nur alle Tools verwalten, sondern auch den Abwehrprozess automatisch steuern kann. Ein derartiges System würde für eine vollständige Transparenz sorgen und ausgefeilte Berichtfunktionen bereitstellen. Ein zentrales Befehls- und Kontrollzentrum, das Daten von allen Erkennungstools erhält (zu Friedenszeiten und bei Angriffen), wählt automatisch den besten Abwehrprozess aus. Dieses allwissende Befehls- und Kontrollzentrum wird ständig und in Echtzeit über die Normalwerte des legitimen Datenverkehrs und über Angriffsdaten auf dem Laufenden gehalten und damit synchronisiert.

Warum würde ein solches System im Kampf gegen aktuelle und neue Bedrohungen die ideale Lösung darstellen?

- Es dehnt die Erkennung auf alle Unternehmensressourcen vor Ort und in remoten Rechenzentren aus (Disaster-Recovery-Sites, private Clouds und zum Teil auch öffentliche Clouds).
- Es automatisiert die Abwehr, indem es die wirkungsvollsten Tools und Stellen auswählt – im Rechenzentrum, am Perimeter, in einem Scrubbing-Center oder in der Cloud.
- Es bietet einen beispiellosen Schutz an allen Fronten vor aktuellen und künftigen Bedrohungen, die auf der Verfügbarkeit basieren.

Die gegenwärtigen Offensiven sind komplex. Ein Unternehmen kann sich nur vor den Gefahren schützen, die es erkennen kann. „Erkennen wo möglich, abwehren wo nötig“ lautet die neue Mantra. Wer Angreifern in diesem ewigen Katz-und-Maus-Spiel einen Schritt voraus bleiben möchte, sollte sich diese Mantra zu eigen machen.

7 Die Zukunft: Prognosen für 2015 und die folgenden Jahre

Sicherheitsexperten sprechen leidenschaftlich gern über Angriffsvektoren, Cyber-Vorfälle oder Trends im Bereich der Datensicherheit. Häufig werden wir um unsere Meinung oder um Prognosen gebeten. Ausgehend von den Ereignissen des letzten Jahres möchten wir für 2015 fünf Prognosen abgeben.

Prognose 1

Cyber-Attacken können Menschenleben kosten.
Seit Jahren mehren sich die Anzeichen dafür, dass Angriffe auf verschiedene Dinge – Herzschrittmacher, Züge, Autos und sogar Flugzeugsysteme – irgendwann Menschenleben kosten könnten. Es besteht heute kein Zweifel darüber, dass Cyber-Angriffe einen tödlichen Ausgang haben können und werden. Es ist lediglich eine Frage der Zeit.

Prognose 2

Geiselnahmen und die Erpressung von Lösegeldern in der Cyber-Welt werden zunehmen.
Die Erpressung von Lösegeldern ist in der Cyber-Welt nichts Neues, aber seit 2014 sind Angriffe mit kriminellem Hintergrund gefährlicher geworden. Bösartige Gruppen nehmen neuerdings Geiseln in Form von digitalen Assets oder Services, das heißt, sie beschlagnahmen diese Ressourcen, bis bestimmte Forderungen finanzieller oder anderer Art erfüllt sind. In mindestens einem Fall hat eine solche Geiselnahme zum Konkurs eines Unternehmens geführt.

Prognose 3

Kritische Infrastrukturausfälle nehmen zu.
Man braucht nicht viel Fantasie, um sich auszumalen, wie breit angelegte Cyber-Offensiven die kritischen Infrastrukturdienste eines Landes lahmlegen könnten, darunter Stromerzeugung, Wasserversorgung, Mobilfunk-, Telefon- und Fernsehnetze sowie Netzwerke von Polizei und Rettungsdiensten. Selbst die am weitesten entwickelten Länder sind hiergegen nicht gefeit.

Prognose 4

Zahlreiche Gesetze gegen Cyber-Kriminalität werden verabschiedet, darunter nationalistische Regeln.

Als Reaktion auf die sich in der Wählerschaft ausbreitende Unzufriedenheit und Frustration – und die zunehmende Bedrohung durch staatlich sanktionierte Spionage – werden Regierungen versuchen, Cyber-Angriffen durch neue Gesetze Einhalt zu gebieten. Derartige Gesetze werden wahrscheinlich versuchen, den Fluss des Netzwerkdatenverkehrs, Sicherheitsstufen in kritischen Infrastrukturunternehmen und akzeptable Standorte für die Datenverarbeitung vorzuschreiben. Sie dürften auch Richtlinien zu akzeptablen Verhaltensweisen im Internet umfassen.

Prognose 5

Unternehmensmanager verlieren ihren Kampfgeist.

Obwohl die Medien und die Öffentlichkeit heute wachsamer denn je sind, scheint sich unter den für die Sicherheit zuständigen Entscheidungsträgern eine gewisse Apathie oder Müdigkeit ausgebreitet zu haben. Möglicherweise haben viele von ihnen einfach den Mut verloren oder sie sind abgestumpft. Vielleicht glauben sie auch, dass sie gegen hartnäckige Angreifer langfristig nichts ausrichten können. Wir befürchten, dass immer mehr Unternehmensleiter die intensive Suche nach Lösungen zur effektiveren Absicherung von Endpunkten und anderen Punkte aufgeben. Vermutlich sind sie davon überzeugt, dass sie irgendwann – sofern nicht bereits geschehen – ohnehin einem Angriff zum Opfer fallen werden.

8 Erwägungen zur DDoS-Abwehr

In diesem Abschnitt werden aktuelle Trends in Unternehmen und bei Angriffen erörtert. Außerdem werden Best Practices vorgestellt, die Unternehmen bei ihren Plänen für Cyber-Angriffe berücksichtigen sollten.

Auswahl eines Anbieters. Es ist wichtig, die Erfahrungen und den Ruf des Anbieters zu überprüfen. Ist seine Technologie markterprobt? Wer sind seine Kunden, und gehören dazu auch MSSPs? Sind seine Kunden Angriffen zum Opfer gefallen und deshalb in die Schlagzeilen geraten? Es empfiehlt sich außerdem, sich einen Anbieter näher anzusehen, der eine umfassende Erkennungs- und Abwehrlösung bereitstellen kann.

Umfang der Schutzmaßnahmen. Neue Bedrohungen gehen mit neuen Angriffsvektoren einher. Vergewissern Sie sich unbedingt, ob die angebotene Lösung die bekannten Angriffsvektoren abwehren kann und auch Schutz vor SSL-Verschlüsselungsangriffen und verschiedenen webbasierten, verdeckten Angriffsvarianten bietet. Prüfen Sie zudem, ob die Lösung eine Hybridlösung ist, die Sie vor einer Überlastung des Internetzugangs schützt, ohne dass die Benutzer Performance-Einbußen hinnehmen müssen. Achten Sie darauf, dass die Lösung einen mehrschichtigen Schutz vor Angriffen gegen Netzwerke, Server und Anwendungen bietet.

Analyse in Echtzeit und nach Attacken. In einer mehrschichtigen Sicherheitsarchitektur ist Transparenz unverzichtbar. Ein in die DDoS-Schutzlösung integriertes

Erwägungen hinsichtlich Compliance

Cyber-Angriffe machen weder vor Finanzinstituten noch vor Kraftwerken halt und bedrohen die Redlichkeit und Integrität zahlreicher Branchen. Weil sie sich in vielen Ländern zu einer existenziellen Bedrohung entwickelt haben, sehen viele Behörden sich zum Eingreifen gezwungen. Es gibt unter anderem die folgenden Initiativen:

- Cybersecurity Framework des National Institute of Standards and Technology (NIST) (US)
- DDoS Memorandum des Office of the Superintendent of Financial Institutions (OFSI) (Kanada)
- FFIEC Joint Statement Distributed Denial-of-Service (DDoS) Cyber-Attacks, Risk Mitigation, and Additional Resources (US)
- Securities and Exchange Commission Cyber Exams (US)
- Office of the Comptroller of the Currency Guidance (US)
- National Credit Union Administration Risk Alert (US)

SIEM-System (Security Information and Event Management) ist äußerst wichtig. Es ist wichtig, dass IT-Mitarbeiter sich einen vollständigen Überblick verschaffen und Informationen von allen zum Schutz der Assets eingesetzten Erkennungstools in Echtzeit erhalten. Erweiterte Anti-DDoS-Lösungen müssen in SIEM-Systeme integriert sein, die Daten aus mehreren Quellen aggregieren, normalisieren und korrelieren können. Informationen, Berichte, automatische Analysen und Prozesse in Echtzeit sorgen während Angriffen für Transparenz und Klarheit und erleichtern nach einem Angriff die Analyse und Forensik.

Unterstützung während eines Angriffs. Es ist wichtig, im Voraus zu prüfen, welche Hilfsleistungen der Anbieter im Angriffsfall bereitstellt. Einige Anbieter stellen ihren Kunden in einem solchen Fall ein Expertenteam zur Seite. Vergewissern Sie sich, dass die Hilfe während der gesamten Offensive zur Verfügung steht und dass das Team in Anschluss an den Angriff eine Analyse durchführt. Bei einigen Anbietern gibt es spezielle Forschungsteams, die in regelmäßigen Abständen Informationen zum Markt und zu den neuen Bedrohungen bereitstellen.

DDoS-Angriffe – Was Sie tun oder lassen sollten

Vor einem Angriff – Kriterien für die Auswahl einer DDoS-Schutzlösung

To Do's	Zu vermeiden
1. Finden Sie sich damit ab, dass kein Unternehmen sicher ist. Die Frage ist nicht, ob Sie angegriffen werden, sondern wann. 2. Sorgen Sie dafür, dass Erkennungstools sich an der rechten Stelle befinden. Denken Sie daran, dass Sie sich nur vor den Gefahren schützen können, die Sie erkennen können. 3. Stellen Sie sicher, dass Ihre Sicherheitsstrategie in Richtlinien und Verfahren einfließt. Bereiten Sie Ihre Mitarbeiter vor, und weisen Sie ihnen klare Rollen und Pflichten zu. 4. Testen und bewerten Sie die bei Ihnen vorhandenen Systeme sowie die im Markt neu verfügbaren Technologien regelmäßig. Beispiel: a. Prüfen Sie, ob eine Out-of-Path-Implementierung einiger Ihrer Erkennungstools für das Unternehmen vorteilhafter wäre. b. Bewerten Sie die Implementierung einer Hybridlösung, um Ihr Unternehmen vor Angriffen zu schützen, die den Internetzugang überlasten. 5. Sorgen Sie dafür, dass Ihre Mitarbeiter wissen, was sie im Fall eines DDoS-Angriffs tun und lassen sollen. Im Notfall	1. Lassen Sie sich bei der Implementierung einer Lösung nicht rein von Compliance-Erwägungen leiten. Sie müssen Ihre Sicherheitsrisiken und -anforderungen verstehen. 2. Implementieren Sie keine Erkennungstools von unterschiedlichen Anbietern, es sei denn, diese Tools können miteinander kommunizieren und relevante Informationen austauschen.

muss eine Liste der zu verständigenden Person(en) griffbereit liegen. Wenn bei Ihnen das Risiko besteht, dass eine öffentliche Website zum Absturz gebracht wird, verfassen Sie bereits im Vorfall eine Erklärung und Entschuldigung.

Während eines Angriffs – Schadensbegrenzung

To Do's	Zu vermeiden
1. Setzen Sie sich mit dem internen Emergency Response Team (ERT, Notfallteam) bzw. mit dem ERT der Anbieters in Verbindung, um sicherzustellen, dass die besten Entscheidungen getroffen und umgesetzt werden. Wenn Sie von einem ISP-Anbieter abhängig sind, setzen Sie sich jetzt mit ihm in Verbindung. 2. Bestimmen Sie den Erkennungspunkt, den Angriffstyp und das Angriffstool, und entscheiden Sie, welcher Abwehrprozess am besten geeignet ist. 3. Achten Sie darauf, den Angriff Schritt für Schritt zu dokumentieren. 4. Sorgen Sie dafür, dass ein Sprecher bereitsteht, der Ihre Kunden über den Angriff auf dem Laufenden hält (Blog, Twitter, Berichterstattung).	1. Verfallen Sie nicht in Panik. Bewahren Sie einen kühlen Kopf. 2. Treffen Sie keine Entscheidungen, ohne sich mit dem internen ERT bzw. mit dem ERT des Anbieters abzusprechen. 3. Leiten Sie keinen Datenverkehr an das Scrubbing-Center in der Cloud weiter, es sei denn, der Internetzugang ist fast überlastet. 4. Ignorieren Sie keinesfalls Ihre Kunden, und sorgen Sie dafür, dass jemand sie auch während des Angriffs beruhigt.

Nach einem Angriff – Lektionen und Vermeidung einer Wiederholung

To Do's	Zu vermeiden
1. Führen Sie eine Schadensbegrenzungsanalyse durch und lesen Sie die Berichte und die Ergebnisse der forensischen Untersuchungen. Finden Sie heraus, was schiefgelaufen ist, damit Sie diese Fehler künftig nicht wiederholen. Untersuchen Sie alles. 2. Optimieren Sie Ihre Sicherheitsarchitektur. Unterziehen Sie sämtliche Aspekte des Angriffs einer Analyse und Bewertung. Passen Sie Technologien, Richtlinien und Lösungsstrategien entsprechend an. 3. Leiten Sie relevante Details an Ihre Kunden bzw. die Presse weiter. Bei Online-Unternehmen empfiehlt sich eine Marketingkampagne, um die Loyalität der enttäuschten Kunden zurückzugewinnen. 4. Sorgen Sie dafür, dass Ihre Berichte und die Ergebnisse der forensischen Untersuchungen griffbereit sind für den Fall, dass eine polizeiliche Untersuchung eingeleitet werden muss.	1. Bleiben Sie auch am Ende eines Angriffs weiterhin wachsam. 2. Ignorieren Sie weder die Fragen Ihrer Kunden noch Anfragen von der Presse. Sprechen Sie mit Ihnen, und zeigen Sie, dass Sie Herr der Lage sind. 3. Zögern Sie die Umsetzung der Untersuchungsergebnisse nicht hinaus, sei es im Bereich der Sicherheitsstrategie, Technologielösungen, Richtlinien, Rollen, Pflichten usw.

Best Practices in aller Kürze

Denken Sie bei der Planung Ihre Defensivstrategie an die C.H.E.W.-Bedrohungen, stellen Sie hohe Ansprüche an Ihre Anbieter und lassen Sie die folgenden Grundsätze niemals außer Acht:

Timing ist alles.
Unternehmen müssen die für die Abwehr benötigte Zeit als wichtigen Erfolgsfaktor betrachten. Achten Sie in diesem Sinne darauf, dass die implementierte Lösung eine schnellstmögliche Abwehr bietet.

Schließen Sie alle Lücken.
Anti-DDoS-Lösungen müssen eine große Reichweite haben. Es genügt nicht, wenn sie nur einen einzelnen Angriffsvektor erkennen. Sie müssen auch Attacken mit mehreren Angriffsvektoren erkennen, die bei unterschiedlichen Schichten der Infrastruktur ansetzen.

Nutzen Sie eine mehrschichtige Architektur.
Beseitigen Sie die mit punktuellen Lösungen verbundenen Probleme. Blockieren Sie volumetrische Angriffe mit einer cloudbasierten Lösung und alle nicht volumetrischen Angriffe mit einer lokalen Lösung.

Wehren Sie SSL-Angriffe ab.
SSL-Angriffe stellen weiterhin eine große Bedrohung dar. Suchen Sie nach SSL-basierten DoS/DDoS-Abwehrlösungen, deren Implementierung den legitimen Datenverkehr nicht behindert.

Ein zentraler Ansprechpartner muss bereitstehen.
Bei einem Angriff ist ein zentraler Ansprechpartner wichtig, der bei der Umleitung des Internet-Traffics und bei der Implementierung von Abwehrmaßnahmen behilflich sein kann.

9 Checkliste: Bewertung der Fähigkeiten eines Anbieters bei der Abwehr von DDoS- und Cyber-Angriffen

Bei der Bewertung der Fähigkeiten eines Anbieters bei der Abwehr von DDoS- und Cyber-Angriffen stehen zwei Kernkompetenzen im Vordergrund: Erkennung und Abwehr. Bewerten Sie jeden Anbieter anhand der nachstehenden Kriterien. Je mehr Fähigkeiten ein Anbieter in den einzelnen Bereichen nachweisen kann, desto besser.

Wie gut ist der Anbieter bei der Erkennung?

Qualität – Hier geht es um die Fähigkeit des Herstellers, eine hochwertige Erkennung bereitzustellen:

Verfügbare(r) Erkennungstyp(en)
- Netflow
- Layer-7-Pakete ohne Header
- Openflow
- Abdeckung von OWASP-Schwachstellen
- Layer-3-/Layer-4-Pakete
- Eingabe/Signale von anderen Abwehrtools
- Header für Layer-7-Paket erforderlich

Bereitstellungsmodelle
- Inline
- Scrubbing-Center in der Cloud – Asynchron
- OOP – Synchron
- Software Defined Networking (SDN)
- Hybride Cloud-Optionen
- Optionale virtuelle Bereitstellung
- Internes Scrubbing-Center – Asynchron
- Feeds von Partnern/Nutzt Signale anderer Anbieter

Zeit – Her werden die für die moderne Angriffserkennung erforderlichen Kompetenzen bewertet:
- Echtzeitoptionen
- Signal-/automatische Optionen (für erweiterte Anwendungsangriffe)
- Signal-/automatische Optionen (für Cloud-Umleitung)

Berichterstellung und Reaktion – Hier werden die für die Steuerung der modernen Angriffserkennung und der zugehörigen Berichterstattung erforderlichen Kompetenzen bewertet:
- Echtzeit
- Support-Reaktion bei Erkennung – Echtzeit
- Historisch

- Support-Reaktion bei Erkennung – Optionen vor Ort
- Forensik
- Integrierte Berichterstattung mit Cloud-Portal
- Spähberichte
- Fähigkeit, legitimen Datenverkehr von illegitimem Datenverkehr in Echtzeit zu unterscheiden

Wie gut ist der Anbieter bei der Abwehr?

Qualität – Ist der Anbieter bei der Abwehr von Bedrohungen übervorsichtig oder nicht vorsichtig genug? Auf wie viele Technologien stützt er sich dabei?

- Nur ratenbezogen
- HTTP-Server-basierte Schutzmechanismen
- Routing-Techniken
- HTTP-OWASP-basierte Schutzmechanismen
- Nur ratenbezogene Verhaltensweise
- Koordinierung hybrider Signale/Scrubbing-Center in der Cloud
- Nicht ratenbezogene Verhaltensweise
- SSL-Schutzmaßnahmen
- Heuristische Verhaltensweise
- HTTP-Umleitungen
- Statistische Verhaltensweise
- JavaScript-Challenge-Response
- Signaturen – Statisch mit Updatedienst
- Cloud-Challenge-Response
- Signaturen – Benutzerdefiniert, Echtzeit

Zeit – Wie schnell kann der Hersteller die Abwehr einleiten?

- Echtzeitoptionen
- Automatische Optionen

Berichterstattung und Reaktion – Wie detailliert sind die Berichte? Kann ein Benutzer feststellen, ob legitimer Datenverkehr durch die Abwehrmaßnahmen behindert wird?

- Echtzeit-Displays
- Detaillierte Anzeige aller Angriffsvektoren
- Messwerte für die Wirksamkeit historischer Abwehrmaßnahmen
- Optionen für Abwehr, Reaktion und Gegenangriff
- Forensische und detaillierte Berichte
- Support-Reaktion bei Abwehr – Echtzeit
- Notfalloptionen
- Support-Reaktion bei Abwehr – Optionen vor Ort
- Anzeige von legitimem und illegitimem Datenverkehr
- Integrierte Berichterstattung mit Cloud-Portal

10 DDoS-Glossar

In diesem Glossar finden Sie Begriffe rund um die Netzwerk- und Anwendungssicherheit. Auch etliche DDoS-Begriffe sind erläutert.

Advanced Persistent Threats (APT)
Kategorie von Cyber-Bedrohungen, die versuchen, in ein Netzwerk einzudringen und nach und nach vertrauliche oder sensible Daten herauszuschmuggeln. Angriffe dieser Art haben in der Regel einen Spionagehintergrund und sind oft staatlich sanktioniert.

Always-On
Modell für die Bereitstellung von Sicherheitsdiensten, bei dem der gesamte Traffic einer ständigen Sicherheitskontrolle unterzogen wird. Beim DDoS-Schutz bedeutet „Always-On" im Allgemeinen, dass der gesamte Traffic auf DDoS-Angriffe untersucht wird. Zu diesem Zweck werden interne Inline-Geräte oder lokale Out-of-Path-Lösungen verwendet, oder der Traffic wird kontinuierlich über cloudbasierte Scrubbing-Dienste weitergeleitet.

Angriffe auf die Verfügbarkeit
Angriffe gegen einen Dienst, mit denen die Nichtverfügbarkeit dieses Dienstes bewirkt werden soll. Die meisten Angriffe dieser Art sind volumetrische Angriffe. Jeder Angriff, durch den ein Dienst nicht mehr verfügbar wird, wird als Angriff auf die Verfügbarkeit betrachtet. In diese Kategorie fallen Brute-Force-Attacken auf Login-Seiten, SSL-Verschlüsselungsangriffe und andere verdeckte Methoden, die letztlich zu erheblichen Performance-Einbußen oder zu einem Totalausfall eines Dienstes führen. Wie die Verfügbarkeit auch während eines Angriffs aufrechterhalten werden kann, ist eine der wichtigsten Herausforderungen, denen Unternehmen und Serviceanbieter sich stellen müssen.

Angriffe auf Layer 3 und Layer 4
Umfangreiche Kategorie von Angriffen, die gegen die Netzwerk- (Layer 3) und die Transportschicht (Layer 4) des OSI-Modells gerichtet sind. Zu den gängigen Angriffsvektoren gehören dabei TCP-SYN-Floods, UDP-Floods und ICMP-Angriffe.

Angriffe auf Layer 7
Umfangreiche Kategorie von Angriffen, die gegen die Anwendungsschicht (Layer 7) des OSI-Modells gerichtet sind. Zu den gängigen Angriffsvektoren gehören dabei SMTP-Angriffe, DNS-Floods und HTTP/HTTPS-Angriffe.

Bot/Botnet
Eine aus vielen (oft Tausenden) freiwillig oder unfreiwillig bereitgestellten Computern bestehende Gruppe, die Datenverkehr in erheblichem Umfang an ein Opfer sendet, um dessen Netzwerk zu überwältigen.

Denial of Service (DoS)
Ein DoS-Angriff ist der Versuch, legitimen Benutzern die Verwendung eines Geräts oder einer Netzwerkressource unmöglich zu machen. Bei Angriffen dieser Art kann ein Computer oder Netzwerk minuten- oder gar tagelang unbrauchbar gemacht werden. Je nach Angreifer oder Angriffsziel kann ein solcher Angriff im Prinzip ein ganzes Unternehmen außerstand setzen.

Dienstausfall/Totalausfall
Der Begriff „Downtime“ (Ausfall) bezeichnet Phasen, in denen ein System nicht verfügbar ist und folglich seine Hauptfunktion nicht erfüllen kann. Ein DDoS-Angriff kann zum Totalausfall eines Dienstes führen, sodass der Dienst nicht mehr verfügbar ist. Der Ausfall eines Dienstes kann schwere finanzielle Konsequenzen haben und gelegentlich sogar ein Unternehmen in die Knie zwingen. (Beispielsweise wurde 2013 gemeldet, dass ein fünfminütiger Ausfall bei Google Einnahmeverluste in Höhe von 545.000 US-Dollar verursachte.)

Dienstbeeinträchtigung
Eine DoS/DDoS-Angriffsvariante, die die Geschwindigkeit und Reaktionszeit eines Netzwerks oder einer Website verlangsamt und hierdurch einen Dienst beeinträchtigt. Manche Angriffe lassen es hierbei bewenden; bei anderen Angriffen ist dies lediglich der Auftakt zu einem Totalausfall des Dienstes. Einige Hacker setzen Angriffe dieser Art ein, um die Widerstandskraft des anvisierten Ziels zu beurteilen, ehe sie den eigentlichen Angriff starten.

Distributed Denial of Service (DDoS)
Bei einem DDoS-Angriff nehmen eine oder mehrere Personen, Bots oder andere kompromittierte Systeme ein einzelnes Ziel ins Visier. Dies führt zu Performance-Einbußen oder einem Totalausfall, und den Benutzern wird die Nutzung des betroffenen Systems erschwert oder verweigert. Bei DDoS-Angriffen kann ein Onlinedienst mit Datenverkehr aus mehreren Quellen überschwemmt und letztendlich lahmgelegt werden. Aus Untersuchungen von Radware geht hervor, dass derartige Angriffe sich meist gegen Behörden, ISPs, Anbieter von Hosting-Services, Finanzinstitute und die Gaming-Branche richten.

DNS-Flood
Angriff, der sich gegen das DNS-Anwendungsprotokoll richtet und bei dem extrem viele DNS-Anfragen gesendet werden. Domain Name System (DNS) ist das Protokoll, mit dem Domänennamen in IP-Adressen aufgelöst werden. Ihm liegt das UDP-Protokoll zugrunde, das kurze Anfrage- und Antwortzeiten unterstützt, ohne Verbindungen herstellen zu müssen (wie bei TCP nötig).

Forensik
DDoS-Datenforensik und Analysen nach Angriffen sind aus verschiedenen Gründen wichtig. Während eines Angriffs ermöglichen forensische Analysen die Identifizierung des Angreifers und die Unterscheidung des legitimen Datenverkehrs von illegitimem Datenverkehr. Sie erleichtern auch die Auswahl geeigneter Abwehrmaßnahmen.

Wenn ein Angriff erfolgreich abgewehrt wurde, bietet die Forensik Aufschluss über Herkunft, Beweggründe, Typen und Tools des Angriffs. Die hier gewonnenen Erkenntnisse können für juristische Zwecke genutzt werden und in die Vorkehrungen für künftige Angriffe einfließen. Die Forensik eignet sich auch als Forschungstool, weil sie zu einem besseren Verständnis der DDoS-Trends führen kann.

HOIC
Ein häufig für DDoS-Angriffe eingesetztes Tool, das HTTP-Post und -GET-Anfragen in einem bedienfreundlichen GUI senden kann. Seine Wirksamkeit beruht auf ergänzenden „Booster"-Skripts. Dabei handelt es sich um Textdateien mit einem zusätzlichen Basiscode, der zu Beginn eines Angriffs von der Hauptanwendung interpretiert wird.

HTTP-Flood
Gängige Angriffsvariante, bei der legitime, sitzungsbasierte HTTP-, GET- oder POST-Anfragen an den Webserver des Opfers gesendet werden. Angriffe dieser Art sind schwer erkennbar. HTTP-Flood-Angriffe werden in der Regel von mehreren Computern (freiwillig bereitgestellten Geräten oder Bots) gleichzeitig ausgeführt.

Hybride Abwehr
Eine Kombination aus internen und cloudbasierten Abwehrtechnologien, die eine sofortige Abwehr nicht volumetrischer Angriffe ermöglicht. Falls ein Angriff den Internetzugang des Opfers zu überlasten droht, können zusätzliche Abwehrressourcen genutzt werden.

IP-Spoofing
Eine Taktik, bei der IP-Pakete (Internet Protocol) mit einer falschen Quell-IP-Adresse erstellt werden. Hierdurch wird die Identität des Absenders verborgen. Gleichzeitig werden die Blockierung IP-basierter Angriffe und die Identifizierung des Angreifers erschwert.

LOIC
Tool, das häufig für DDoS-Angriffe verwendet wird. Es kann einen extrem starken TCP-, UDP- oder HTTP-Datenverkehr mit dem Ziel erzeugen, einen Server einer hohen Netzwerkbelastung auszusetzen. Ursprünglich sollte es Entwicklern ermöglichen, ihre eigenen Server zu Belastungstests zu unterziehen.

„Low & Slow“-Angriffe
Angriffe, die bei bestimmten Designschwächen oder Sicherheitslücken auf einem Zielserver ansetzen und den Server durch relativ wenig Traffic zum Absturz bringen. „Low & Slow“-Angriffe richten sich meist gegen Anwendungsressourcen (gelegentlich auch gegen Serverressourcen). Sie sind schwer zu erkennen, weil sie Verbindungen und den Datenverkehr normal erscheinen lassen.

On-Demand
Bezieht sich generell auf die bedarfsgerechte Verfügbarkeit von DDoS-Scrubbing-Services, insbesondere wenn volumetrische Angriffe die Kapazität des Inbound-Links zu überlasten drohen.

Out-of-Path
Architektur von Sicherheitsdiensten, bei der die Sicherheitsgeräte oder -dienste nicht in den konstanten Datenverkehrsfluss eingebunden sind. In Out-of-Path-Architekturen ist das Sicherheitsgerät bzw. der Sicherheitsdienst mit einem anderen Gerät oder Dienst im Datenpfad verbunden, das bzw. der Datenverkehr anhand bestimmter Verkehrsprofile oder -muster an das Out-of-Path-Gerät umleitet. Out-of-Path-Bereitstellungen tragen zur Reduzierung der potenziellen Fehlerstellen im normalen Netzwerk-Traffic bei, aber schränken auch die Fähigkeit des Sicherheitsgeräts oder -dienstes ein, einen optimalen Dienst bereitzustellen.

Scrubbing-Center
Eine zentrale Datenbereinigungsstelle, an der der Traffic analysiert und böswilliger Traffic entfernt wird. Scrubbing-Center werden häufig von Großunternehmen wie ISP- und Cloud-Anbietern verwendet, weil sie es vorziehen, den Traffic an eine zentrale Out-of-Path-Datenbereinigungsstelle auszulagern.

Während eines Angriffs wird der Datenverkehr (meist über DNS oder BGP) an das Scrubbing-Center umgeleitet. Dort wird der böswillige Traffic herausgefiltert, und unbedenklicher Traffic wird an das Netzwerk übergeben.

Ein Scrubbing-Center muss in der Lage sein, volumetrischen Floodings in der Netzwerk- und Anwendungsschicht, „Low & Slow“-Angriffen, RFC Compliance-Prüfungen, bekannten Sicherheitslücken und Zero-Day-Attacken Stand zu halten.

Security Operations Center (SOC)/Notfallschutz
Eine Art Kommandozentrale eines Unternehmens für den IT-Bereich. Hier werden unter anderem die Rechenzentren, Server, Anwendungen, Netzwerke, Websites und Endpunkte des Unternehmens ständig von einem Expertenteam überwacht, überprüft und abgesichert.

DDoS-Angriffe können einige Stunden oder gar Tage oder Wochen dauern. In derartig langen, aufreibenden Phasen benötigen Unternehmen

einen zentralen Ansprechpartner, der den Abwehrprozess von Anfang bis Ende begleitet – von der Erkennung des Angriffs über die Anwendung der richtigen Tools zum richtigen Zeitpunkt bis hin zur Umleitung des attackierten Traffics in ein cloudbasiertes Scrubbing-Center.

Ein Unternehmen muss über einen Sicherheitsdienst verfügen, der rund um die Uhr verfügbar ist und im Bedarfsfall einen aktiven Beitrag zur Abwehr von Angriffen und somit zur Verteidigung des Netzwerks gegen Cyber-Angriffe leisten kann. Bei diesem Dienst kann es sich um ein internes SOC-Team oder um das Notfallteam eines externen Sicherheitsanbieters handeln. Diese Experten verfügen über das Fachwissen, das zur Bekämpfung lang anhaltender Angriffe an mehreren Fronten notwendig ist.

SSL-basierte Angriffe
Angriffe, die böswilligen Datenverkehr verschlüsseln, um seinen Inhalt zu verschleiern und bestimmte Erkennungsmethoden zu umgehen. SSL-Angriffe verbrauchen auch mehr Rechnerkapazität, weil ihre Inhalte entschlüsselt und verschlüsselt werden müssen.

Time to Mitigate (TTM)
Je langer ein Unternehmen oder eine Einrichtung angegriffen wird, desto länger müssen Benutzer die Nichtverfügbarkeit von Diensten und langsame Reaktionen hinnehmen. Frustration und Unzufriedenheit breiten sich aus, und die Produktivität wird in Mitleidenschaft gezogen. Wie lange es dauert, einen Angriff zu erkennen und vor allem abzuwehren, ist wichtig. Die „Time to Mitigate“ (Zeit bis zur Abwehr) ist ein wichtiger Faktor bei der Entscheidung für oder gegen eine DoS/DDoS-Abwehrlösung. Je früher die Abwehrmaßnahmen beginnen, desto früher sind die Dienste des Unternehmens wieder funktionstüchtig.

Überlastung des Internetzugangs
Kann während Angriffen auftreten, die volumetrische Floodings verursachen und versuchen, ein Ziel durch eine übermäßige Bandbreite zu überlasten. Am beliebtesten sind UDP-Floods, weil sie sich leicht fälschen und nur mit Mühe abwehren lassen. SYN-Floods und falsch formatierte Pakete treten ebenfalls häufig auch. Die Absicht vieler Angriffe besteht zwar darin, eine Überlastung der Inbound-Bandbreite zu erzielen, aber es kommt auch vor, dass eine Überlastung der Outbound-Bandbreite angestrebt wird. Hierzu identifizieren Angreifer große Dateien auf Websites oder freigegebenen FTP-Sites und laden sie herunter.

Volumetrische Angriffe
Umfangreiche Kategorie von Angriffen, die versuchen, den Internetzugang oder andere Bereiche mit begrenzter Kapazität des Ziels zu überlasten. Der Schutz vor volumetrischen Angriffen ist nicht unproblematisch. Der Empfang des Traffics vor der Datenbereinigung setzt ein hohes Maß an Bandbreite voraus, und häufig sind cloudbasierte Scrubbing-Ressourcen erforderlich.

Web Application Firewall (WAF)
Sicherheitsprodukt oder -dienst, das bzw. der auf die Transaktionen auf einer Website statische oder dynamische Sicherheitsrichtlinien anwendet. WAFs werden in der Regel für Webangriffe wie Cross-Site-Scripting (CSS) und SQL-Injection (Einschleusung) eingesetzt.

Web-Stealth-Angriffe/Smokescreens
Web-Stealth-Angriffe sind Vektoren, zu denen unter anderem Brute-Force-Angriffe (beispielsweise auf eine Login-Seite), Verstöße gegen Datei-Uploads und mit SSL verschlüsselte Angriffe gegen Anwendungen gehören. Diese Angriffsvektoren bauen auf HTTP-Pakete auf, die den relevanten Spezifikationen für Web-Traffic entsprechen. Sie werden daher nicht von Netzwerksicherheitstools wie IPS, Firewalls und auf Schwellenwerten basierenden DoS/DDoS-Tools erkannt.

Angreifer machen sich die Beweglichkeit von HTTPS und anderen SSL-verschlüsselten Mechanismen sowie die asymmetrische Natur dieser Angriffe zunutze, um die Sicherheitsmechanismen zu umgehen und Server tief in der Netzwerktopologie anzugreifen. Genau hier sind diese besonders anfällig für eine Überlastung der Ressourcen.

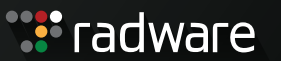
Weitere Informationen

Unter www.radware.com finden Sie weitere Ressourcen und Informationen. Besuchen Sie auch unser Sicherheitscenter unter DDoSWarriors.com. Hier finden Sie umfassende Analysen zu Strategien, Trends und Bedrohungen bei DDoS-Angriffen.

Schließen Sie sich der Radware-Community an und folgen Sie uns auf Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect (App für iPhone®).

Über die Autoren

Radware (NASDAQ: RDWR) ist ein weltweit führender Anbieter von Lösungen im Bereich Application Delivery und Application Security für virtuelle, cloud- und softwarebasierte Rechenzentren. Sein vielfach ausgezeichnetes Portfolio sorgt für eine optimale Quality of Service bei geschäftskritischen Anwendungen und gleichzeitig für eine maximale IT-Effizienz. Mehr als 10.000 Enterprise- und Carrier-Kunden weltweit profitieren von den Lösungen von Radware – zur schnellen Anpassung an Marktentwicklungen, Aufrechterhaltung der Geschäftskontinuität (Business Continuity) und Maximierung der Produktivität bei geringen Kosten. Weitere Informationen finden Sie unter www.radware.com.


radware