Bundesministerium
Inneres

Distributed Denial of Service (DDoS)

Hintergründe, präventive Maßnahmen und Mitigationsmaßnahmen

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Inneres
Herrengasse 7, 1010 Wien
bmi.gv.at
Autoren: Abteilung IV/S/2 – Netz- und Informationssystemsicherheit
Direktion Staatsschutz und Nachrichtendienst
Druck: Digitalprintcenter des BMI

Neuauflage
Wien, Februar 2022

Rückmeldungen: Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an praevention@nis.gv.at | csc@dsn.gv.at

Inhalt

1 Hintergründe 4
1.1 Was ist ein DoS/DDoS-Angriff? 4
1.2 Motivation hinter DDoS-Angriffen 5
Erpressung 5
Sabotage 6
Aktivismus 6
Ablenkung 7
1.3 DDoS-as-a-Service 7

2 Kategorisierung von DDoS-Angriffen 8
2.1 Quantitative Angriffe 8
Volume-Attacks 8
Reflection/Amplification-Attacks 9
2.2 Qualitative Angriffe 10
Application-Attacks (Angriff auf Programme) 11
Infrastructure-Attacks (Angriff auf Infrastruktur) 11

3 Präventive Maßnahmen 12
3.1 Aktives Monitoring 12
3.2 Härten der Peripherie 13
3.3 Organisatorische Maßnahmen 13
3.4 DDoS-Mitigations-Anbieter 14

4 Mitigationsmaßnahmen 17
4.1 Verstehen Sie den Angriff! 18
4.2 Ergreifen Sie Sofortmaßnahmen! 18
Sofortmaßnahmen bei quantitativen Angriffen 18
Sofortmaßnahmen bei qualitativen Angriffen 19
4.3 Seien Sie flexibel! 20
4.4 Suchen Sie Hilfe! 20

5 Weiterführende Literatur 21

Abbildungsverzeichnis 22

1 Hintergründe

1.1 Was ist ein DoS/DDoS-Angriff?

DoS/DDoS (Denial of Service/Distributed Denial of Service) sind Angriffe auf die Verfügbarkeit eines Dienstes, um vorübergehend die Erbringung dieses Dienstes für die dafür vorgesehenen Benutzer einzuschränken oder gänzlich zu unterbinden. Zu diesem Zweck wird das angegriffene System mit (teils sinnlosen) Anfragen überflutet, sodass die Ressourcen des angegriffenen Systems für die ordnungsgemäße Erbringung der vorgesehenen Funktion nicht mehr ausreichen.

Der Angriff kann entweder von einem einzelnen Ursprung (DoS) oder gleichzeitig von mehreren, verteilten Ursprüngen (DDoS) aus erfolgen. Die Systeme, mit denen der Angriff ausgeführt wird, befinden sich dabei in überwiegendem Ausmaß nicht im Besitz der Angreifer selbst. Stattdessen missbrauchen diese, meist ohne Kenntnis der eigentlichen Besitzer, Systeme von Dritten für den Angriff.

Dazu haben die Angreifer im Vorfeld durch eine Infektion mit Schadsoftware die Kontrolle über für den Angriff geeignete Systeme übernommen (Bots) oder sie nutzen Funktionalitäten von schlecht konfigurierten bzw. nicht ausreichend abgesicherten Servern (Reflection) für den Angriff. In diesem Zusammenhang muss daher stets bedacht werden, dass das oder die Angriffssysteme in aller Regel selbst unwissende Opfer sind. Die Tatsache, dass ein System für einen Angriff missbraucht wird oder wurde, bleibt von den rechtmäßigen Besitzern meist unbemerkt.

Solche Systeme werden dadurch „Teil des Problems“. Dass ein bestimmtes System nicht das Ziel eines DDoS-Angriffes ist, bedeutet nicht, dass es nicht gerade Teil eines DDoS-Angriffes sein kann.

In den folgenden Betrachtungen wird ausschließlich die Angriffsart DDoS behandelt, da Angriffe von einem einzelnen System (DoS) in der Praxis nahezu niemals zu beobachten sind.

1.2 Motivation hinter DDoS-Angriffen

Im Wesentlichen lässt sich die Motivation hinter DDoS-Angriffen auf vier grundsätzliche Motive reduzieren:

- Erpressung
- Sabotage
- Aktivismus
- Ablenkung

Selbstverständlich sind auch Kombinationen aus diesen Motiven denkbar.

Erpressung

In vielen Fällen können DDoS-Angriffe beobachtet werden, denen eine unmittelbare Bereicherungsabsicht zugrunde liegt. Diese richten sich vor allem gegen Unternehmen, die (mehr oder weniger) von der ordnungsgemäßen Funktion der von ihnen angebotenen digitalen Dienste abhängig sind.

Zumeist läuft ein derartiger Angriff zwei- oder auch mehrstufig ab:

- In einem ersten Schritt wird das betroffene Unternehmen von den Erpressern mittels E-Mail (oft auch an eine ganze Reihe von Adressaten gleichzeitig) angeschrieben. Dieses Schreiben kann dabei individuell auf das Opfer abgestimmte technische Details (z. B. angegriffene IP-Adresse) enthalten. Im Schreiben wird ein DDoS-Testangriff mit einer vergleichsweise geringen Bandbreite und einer beschränkten Dauer angekündigt, der entweder bereits angelaufen ist oder unmittelbar bevorsteht. Diese Angriffe finden in der Folge tatsächlich wie angekündigt statt.
- In der Folge wird das Unternehmen unter Fristsetzung erpresst, einen gewissen Betrag an die Erpresser zu übermitteln (z. B. mittels der Kryptowährung Bitcoin). Widrigenfalls wird ein weiterer DDoS-Angriff mit weitaus höherer Bandbreite und/oder Dauer angedroht. Manche Angreifer drohen sogar damit, dass dieser zweite Angriff dann bis zur vollständigen Zahlung der (progressiv mit der Zeit ansteigenden) Lösegeldforderung anhält. Für den Fall einer Zahlung wird oftmals zugesichert, dass dies der einzige Erpressungsversuch bleiben wird. Eine Kontaktaufnahme mit den Erpressern ist im Regelfall nicht möglich.

Für den Fall einer Erpressung ersucht das Bundesministerium für Inneres dringend, **das geforderte Lösegeld nicht zu bezahlen**; Sie signalisieren den Kriminellen dadurch, dass dieses Geschäftsmodell funktioniert. Die finanziellen Mittel, die die Erpresser durch Ihre Zahlung erhalten, fließen in der Regel unmittelbar in die Finanzierung weiterer Angriffe (z. B. Zukauf von BOT-Netzen und anderer Ressourcen). Sie tragen dadurch also direkt zur Aufrechterhaltung derartiger Angriffe bei.

Sabotage

Beschränkt man sich bei den Betrachtungen auf ein „ziviles“ Umfeld, so sind DDoS-Angriffe mit dem Motiv Sabotage zumeist in einem geschäftlichen Umfeld mit ausgeprägtem Wettbewerb zu beobachten. Diesen Angriffen ist gemein, dass sich die Angreifer einen (zumindest mittelbaren) Wettbewerbsvorteil gegenüber dem angegriffenen Mitbewerber erhoffen.

Beispiele sind:

- Reputation (Zuverlässigkeit) des Mitbewerbers untergraben
- Lahmlegen von Online-Shops des Mitbewerbers
- Werbekampagnen des Mitbewerbers stören
- Binden von personellen und finanziellen Ressourcen des Mitbewerbers

Aktivismus

Derartigen DDoS-Angriffen ist gemein, dass in der Regel Missmut gegenüber dem Betreiber des Zielsystems die Motivation für den Angriff liefert. Das Ziel der Angreifer ist es, auf ein (behauptetes oder tatsächliches) Fehlverhalten von Unternehmen oder Institutionen hinzuweisen. Durch die Angriffe erhoffen sich die Akteure erhöhte Aufmerksamkeit der Medien und der Öffentlichkeit, um die eigene Message breiter streuen zu können. Ein weiteres mögliches Ziel kann sein, den Ruf oder die Reputation des angegriffenen Unternehmens nachhaltig zu schädigen.

Die Bereiche, in denen diese Ausprägung auftritt, sind vielfältig. Beispiele sind:

- Firmenpolitik (Umweltverschmutzung, Waffenhandel)
- Tierschutz (z. B. Tierversuche, Pelzhandel)
- Tagespolitik (menschenverachtende Politik, Verhetzung)

In Bereich des Aktivismus liegt in der Regel keine mittelbare oder unmittelbare Bereicherungsabsicht vor.

Ablenkung

Eine besonders perfide Ausprägung eines DDoS-Angriffs ist der Ablenkungs-Angriff. Diese Strategie geht davon aus, dass man einen eigentlich beabsichtigten Angriff auf ein Unternehmen (z. B. den Diebstahl von Daten) am besten dadurch unterstützen kann, indem man die Betriebsmannschaften dieses Unternehmens durch einen unmittelbar zuvor angesetzten DDoS-Angriff bindet. Weil alle Augen auf den DDoS-Angriff gerichtet sind, wird der eigentliche Angriff maßgeblich erleichtert.

1.3 DDoS-as-a-Service

Gegenwärtig ist in immer stärkerem Ausmaß eine Entwicklung zu beobachten, dass DDoS-Angriffe im Internet eingekauft werden. So bieten zahlreiche Institutionen im Darknet, aber mitunter auch im allgemein zugänglichen Internet, gegen vergleichsweise geringes Entgelt die Möglichkeit, Angriffe nach Dauer und Volumen, preislich gestaffelt, zu bestellen. Die Bezahlung erfolgt in den meisten Fällen auf Basis der Kryptowährung Bitcoin.

Besonders unangenehm ist diese Entwicklung vor allem aus dem Grund, dass nun praktisch jede Person (unabhängig von ihren technischen Fähigkeiten) einen DDoS-Angriff durchführen kann und sich dadurch der potenzielle Täterkreis maßgeblich erweitert.

2 Kategorisierung von DDoS-Angriffen

DDoS-Angriffe lassen sich technisch im Wesentlichen in drei große Gruppen (und einige Subgruppen) kategorisieren:

- Quantitative Angriffe
- Qualitative Angriffe
- Kombinationen der beiden Angriffe

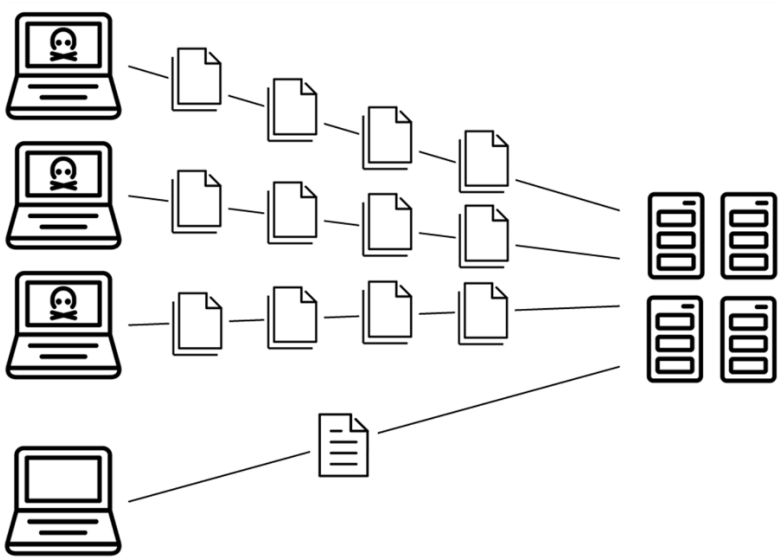
2.1 Quantitative Angriffe

Allen Arten von quantitativen Angriffen ist gemein, dass sie versuchen, das Zielsystem (Opfer) durch den Angriff zu überlasten. Dabei kommen in der Regel keine hochspezialisierten Angriffsvektoren zum Einsatz, sondern der gewünschte Effekt wird durch die schiere Menge an Verkehr erzielt, mit dem die Angreifer das Opfer überschwemmen.

Volume-Attacks

Bei Volume-Attacks handelt es sich zumeist um klassische DDoS-Angriffe mit einer hohen Zahl von gleichzeitig angreifenden Systemen. Dies ist notwendig, da ein einzelnes Angriffssystem (ohne Amplification) in der Regel keine ausreichende Verkehrsmenge generieren kann, um ein Zielsystem zu überlasten.

Abbildung 1 Volume Attacks

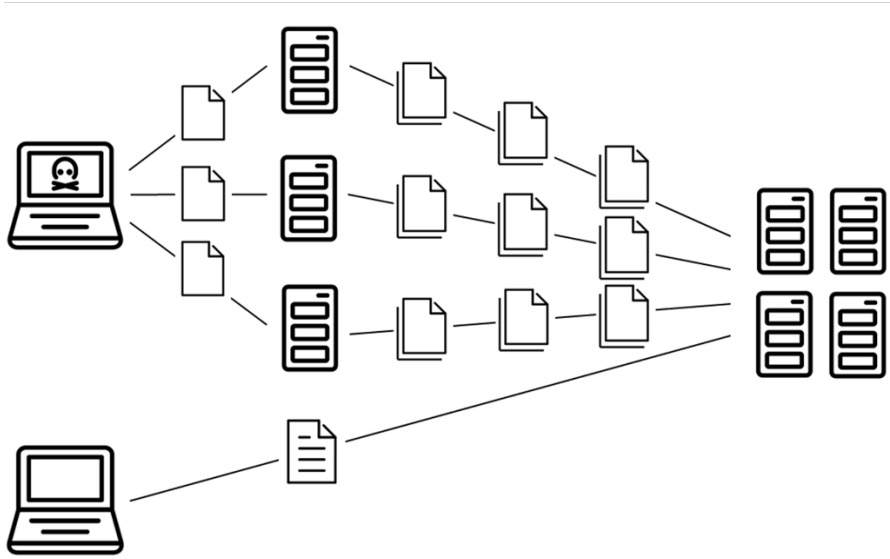


Für diese Art des Angriffs werden in der Regel bereits im Vorfeld eine große Anzahl (Tausende bis hin zu Millionen) von ahnungslosen Systemen gezielt mit Schadsoftware infiziert (Bots), sodass der Angreifer auf Knopfdruck sämtlichen gekaperten Systemen gleichzeitig (Bot-Netz) befehlen kann, das Zielsystem parallel mit (zumeist sinnlosen) Anfragen zu überfluten, bis dieses unter dem Verkehrsvolumen zusammenbricht.

Reflection/Amplification-Attacks

Bei Reflection- oder Amplification-Attacks handelt es sich im Grunde ebenfalls um volumensbasierte Angriffe, die jedoch spezielle Funktionalitäten von schlecht konfigurierten bzw. nicht ausreichend abgesicherten Servern benutzen, um den Effekt zu verstärken.

Abbildung 2 Reflection/Amplification-Attacks



Viele im Internet angebotene Dienste sind (bewusst oder unbewusst) so konfiguriert, dass vergleichsweise kleine Anfrage-Pakete zu vergleichsweise großen Antwort-Paketen führen. So kann es beispielsweise beim Domain-Name-System (DNS) in bestimmten Fällen dazu kommen, dass ein Name-Server auf eine etwa 60 Byte große Anfrage mit einer bis zu 3.000 Byte großen Antwort reagiert.

Bei Reflection-Angriffen fälscht der Angreifer seine Absende-IP-Adresse. Statt seiner eigenen Adresse verwendet er als Absende-IP-Adresse die IP-Adresse des anzugreifenden Systems. Wenn nun im obigen Beispiel der Angreifer mit der gefälschten Absende-IP-Adresse eine Anfrage mit 60 Byte an einen Name-Server sendet, so erzeugt er damit eine 3.000 Byte lange Antwort an das anzugreifende System. Auf diese Art kann er in diesem Beispiel seine Angriffskapazität um den Faktor 50 (gegenüber einem direkten Angriff) verstärken.

2.2 Qualitative Angriffe

Qualitative Angriffe setzen bei ihrer Angriffsstrategie nicht (oder nicht ausschließlich) auf hohes Angriffsvolumen. Vielmehr versuchen sie primär, Schwachstellen in Systemen gezielt auszunutzen, um so die Erbringung dieses Dienstes für die dafür vorgesehenen Benutzer einzuschränken oder gänzlich zu unterbinden. Solche Angriffe setzen zumeist ein höheres technisches Niveau der Angreifer voraus.

Application-Attacks (Angriff auf Programme)

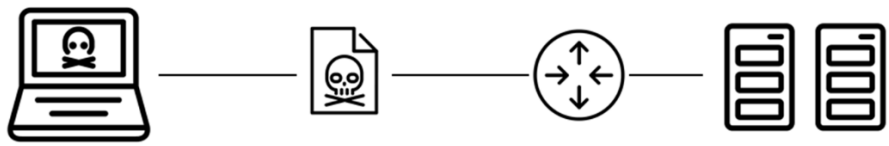
Bei einem Angriff auf Applikationsebene nutzen die Angreifer gezielt Schwachstellen in Software-Anwendungen (Applikationen) beim Ziel aus, um diese außer Gefecht zu setzen. Dies kann, muss jedoch nicht zwingend, mit einem hohen Angriffsvolumen zusammenhängen.

Abbildung 3 Application-Attacks

Infrastructure-Attacks (Angriff auf Infrastruktur)

Bei einem Angriff auf Infrastrukturen werden gezielt Angriffsstrategien entwickelt, um gewisse Hardwarekomponenten beim Ziel (z. B. vorgeschaltete Router) außer Gefecht zu setzen. Dies muss ebenfalls nicht zwingend mit einem hohen Angriffsvolumen zusammenhängen.

Abbildung 4 Infrastructure-Attacks



3 Präventive Maßnahmen

Keine Maßnahme kann Ihnen vollständigen Schutz vor DDoS-Angriffen bieten. Im Folgenden ist jedoch eine Reihe von präventiven Maßnahmen zusammengefasst, die zumindest die Auswirkungen eines solchen Angriffs minimieren können.

Es ist wichtig zu verstehen, dass erste Schutzmaßnahmen gegen DDoS-Angriffe bereits im Regelbetrieb erfolgen müssen, also zu einem Zeitpunkt, an dem noch kein Angriff stattfindet.

3.1 Aktives Monitoring

Ein grundlegendes Erfordernis für eine umfassende Schutzstrategie ist, dass Sie Ihr Unternehmen, Ihre Infrastruktur, Ihre Dienste und alle Schwachstellen in diesen Bereichen genau kennen. Dabei ist entscheidend, dass Sie im Falle eines Angriffes sofort verstehen, welche Systeme angegriffen werden und welche Folgen eine Beeinträchtigung bzw. ein Ausfall genau dieser Systeme für Ihr Unternehmen haben kann (Einbeziehung eines möglichen DDoS-Angriffs in die Risikoanalyse). Dieser Schritt ist nicht einfach und erfordert erhebliche Aufwände; ohne diesen Schritt ist jedoch die Implementierung eines nachhaltigen Schutzkonzepts nicht sinnvoll möglich.

Weiterhin ist es unerlässlich, dass alle wichtigen Infrastrukturelemente und Dienste von Ihrem Monitoring-System bzw. einer permanenten, zentralen Logauswertung erfasst und abgedeckt werden. Es muss sichergestellt sein, dass Ihre Mitarbeiterinnen und Mitarbeiter die Auslastung von kritischen Netzwerkkomponenten und Geschäftsanwendungen zu allen Zeiten im Blick haben, um so Anomalien frühzeitig erkennen zu können.

In Ihrem eigenen Interesse sollten Sie in der Lage sein, einen DDoS-Angriff festzustellen, bevor Ihre Kunden mögliche Auswirkungen des Angriffs bemerken.

Außerdem sollte es Ihnen im Falle eines Angriffs schnell und einfach möglich sein, eine Zuordnung des Angriffs einerseits zu den betroffenen Systemen und andererseits zur Herkunft zu treffen. Nur so ist es im weiteren Verlauf möglich, adäquate Gegenmaßnahmen zu ergreifen.

3.2 Härten der Peripherie

Ab einem gewissen Angriffsvolumen sind zur Abwehr von DDoS-Angriffen die technischen Möglichkeiten im eigenen Bereich begrenzt. Trotzdem ist es erforderlich, diejenigen Komponenten des Unternehmensnetzwerks, die eine Angriffsfläche für eine mögliche Attacke aufweisen, bestmöglich vorzubereiten. Man spricht hier von „Härten“.

Vorgelagerte Systeme, wie Router, Load-Balancer, Firewalls, Web Application Firewalls (WAF) oder Intrusion Detection Systeme (IDS) sollten jedenfalls über ausreichende Systemressourcen verfügen, um auch im Falle eines erhöhten Datenaufkommens Ihre Funktion zu gewährleisten.

Darüber hinaus sollten diese Systeme anwendungsspezifisch gehärtet sein. Allgemein ist zu empfehlen, dass immer die neuesten Patches installiert und ungenutzte Services nach außen blockiert sind sowie eine restriktive Rechtevergabe sichergestellt ist. Insbesondere sollte darauf geachtet werden, dass SYN-Cookies aktiviert sind.

In der Praxis hat es sich zudem bewährt, dass Systeme, bei denen eine hohe Wahrscheinlichkeit für einen DDoS-Angriff vorliegt (z. B. Unternehmenswebsite oder Online-Shop), über einen eigenen Internet-Uplink verfügen, also hinsichtlich des Internet-Uplinks von den anderen Systemen Ihres Unternehmens getrennt sind. Dies erleichtert es, die betroffenen Systeme im Falle eines Angriffs durch einen kommerziellen DDoS-Mitigations-Anbieter betreuen zu lassen.

3.3 Organisatorische Maßnahmen

Die wichtigste präventive Maßnahme ist, dass für den Fall eines Angriffs eine Strategie vorhanden ist. Jede involvierte Person muss bereits vor dem Auftreten eines solchen Vorfalls wissen, was zu tun ist. Finden diese Überlegungen erst im Ernstfall statt, ist es zu spät.

Planen Sie bereits im Regelbetrieb gemeinsam mit Ihren Notfallkontakten – dazu zählen interne Ansprechpartner (v. a. IT, Network Operations, Security Operations) und externe Ansprechpartner (v. a. Upstream-Service-Provider) – die im Falle eines Angriffes notwendigen Maßnahmen. Halten Sie diese Notfallkontakte stets am aktuellen Stand, sodass Sie im Krisenfall nicht mit nicht mehr erreichbaren Telefonnummern oder falschen E-Mail-Adressen konfrontiert sind.

Eine wesentliche Voraussetzung dafür, dass die festgelegten Prozesse und Maßnahmen im Anlassfall auch funktionieren, ist, sie in regelmäßigen Abständen zu überprüfen und zu trainieren.

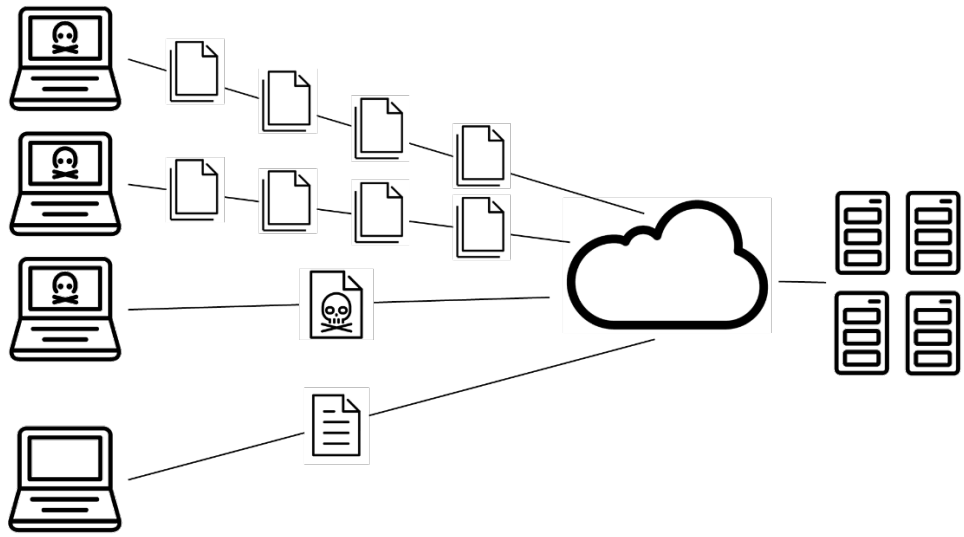
Wie bereits ausgeführt, sind die technischen Möglichkeiten im eigenen Bereich zur Abwehr von DDoS-Angriffen ab einem gewissen Angriffsvolumen begrenzt. Wenn auch für derartige Angriffe Vorsorge getroffen werden soll, ist die rechtzeitige Einbeziehung eines kommerziellen Anbieters von DDoS-Mitigationslösungen unumgänglich. Erfolgt der Erstkontakt erst im Krisenfall, erschwert dies eine schnelle und erfolgreiche Abwehr des Angriffs erheblich. Es ist daher ratsam, diesen Erstkontakt bereits im Regelbetrieb durchzuführen und mit dem Anbieter Ihrer Wahl für Ihren Anwendungsfall optimierte Strategien zu entwickeln und vorzubereiten.

Zuletzt ist es empfehlenswert, für den Fall der Fälle zumindest für wesentliche Funktionen mit Außenwirkung (z. B. Unternehmens-Website) eine Ausweichlösung bereitzustellen, um auch bei einem vorübergehenden Ausfall Ihrer Infrastruktur grundlegende Informationen kommunizieren zu können. Für diese Aufgabe kann beispielsweise eine statische Website mit Basisinformationen sinnvoll sein, die bei einem anderen Provider bereitsteht und die Sie mit einer einfachen Änderung im DNS aktivieren können.

3.4 DDoS-Mitigations-Anbieter

Die meisten Anbieter von DDoS-Mitigations-Lösungen für Webauftritte funktionieren nach einem einheitlichen Prinzip. Der Anbieter stellt dabei für seine Kunden ein sogenanntes „Content Delivery Network“ zur Verfügung. Dabei handelt es sich um einen weltweit verteilten Rechenverbund, der die Netzwerklast international verteilt und sie im Bedarfsfall ausgleichen kann. Zusätzlich sind darin Regeln definiert, mit deren Hilfe DDoS-Angriffe oft auch automatisch erkannt und blockiert werden können.

Abbildung 5 DDoS-Mitigations-Anbieter



Das Prinzip beruht darauf, dass im Domain Name System (DNS) beispielsweise nicht die IP-Adresse Ihres Webservers, sondern die IP-Adresse des DDoS-Mitigations-Anbieters eingetragen wird. Hinter dieser IP-Adresse des Anbieters spannt sich dessen weltweites, gemanagtes, hochredundantes Verteilnetz auf. Ihre Kunden besuchen also im genannten Beispiel zu keinem Zeitpunkt direkt Ihren Webserver, sondern stattdessen Server im „Content Delivery Network“ Ihres Anbieters. Diese Server wiederum laden den eigentlichen Inhalt des Webangebots von Ihrem Webserver herunter und speichern diesen zwischen („caching“).

Wird Ihr Webangebot angegriffen, richtet sich der Angriff folgerichtig nicht gegen Ihren Webserver, sondern gegen einen Server im Verteilnetz des DDoS-Mitigations-Anbieters. Dieser hat sowohl die Ressourcen, als auch die technischen Möglichkeiten, den Angriffs-Verkehr auszufiltern und den eigentlichen Nutzverkehr im hochredundanten Verteilnetz alternativ zuzustellen.

Ist nicht ausschließlich das Webangebot, sondern auch die dahinterliegende Unternehmensinfrastruktur von einem hohen volumensbasierten DDoS-Angriff betroffen, ist eine Zusammenarbeit mit einem Internet Service Provider erforderlich, der eine Vorfilterung („white washing“) der eingehenden Datenpakete vornimmt. Ausgewählte österreichische Anbieter schützen in diesem Zusammenhang bereits seit einigen Jahren die größten und komplexesten Netzwerke Österreichs vor DDoS-Angriffen. Sie setzen auf ein Konzept, bei dem Ressourcen durch eine mehrstufige Implementierung von Abwehrmechanismen geschützt werden.

Idealerweise arbeitet der Vor-Ort-Schutz (z. B. Firewalls, IPS, ADCs) mit der cloudbasierten Lösung des ISPs verzahnt zusammen, indem in einer gemeinsamen Sprache namens „Cloud-Signaling“ kommuniziert wird. So wird eine Internetanbindung effektiv sauber gehalten, die ursprünglich von DDoS-Angriffen lahmgelegt hätte werden sollen – das Ergebnis wird auch „Clean Pipe“ genannt und die Erreichbarkeit des dahinterliegenden Netzes ist sichergestellt.

Eine zweckmäßige und effiziente Nutzung eines DDoS-Mitigations-Anbieters ist in der Praxis allerdings nur für den Fall gegeben, in dem bereits präventiv die Dienste eines entsprechenden Anbieters genutzt oder zumindest entsprechende Vorabkommen getroffen wurden.

Bei der Wahl des Anbieters bzw. der Mitigationsplattform sind gegebenenfalls auch datenschutzrechtliche Aspekte zu berücksichtigen, insbesondere dort, wo personenbezogene Daten an Drittanbieter weitergegeben werden.

4 Mitigationsmaßnahmen

Sehen Sie sich trotz der ergriffenen präventiven Maßnahmen mit einem Angriff konfrontiert, ist es entscheidend, rasch aber überlegt zu handeln. Wenn die im Vorfeld geplanten bzw. festgelegten Maßnahmen und Prozesse allen relevanten Personen bekannt sind und auch entsprechend trainiert wurden, besteht eine gute Chance, die Auswirkungen des Angriffs in einem Bereich zu halten, der Ihrem Unternehmen geringen Schaden zufügt. Als Grundregel können folgende Schritte empfohlen werden:

- Verstehen Sie den Angriff!
- Ergreifen Sie Sofortmaßnahmen!
- Seien Sie flexibel!
- Suchen Sie Hilfe!

Darüber hinaus sollten weitere Bereiche wie Presse- und Öffentlichkeitsarbeit oder Beweissicherung nicht außer Acht gelassen werden. Sorgen Sie dafür, dass Mitarbeiterinnen und Mitarbeiter Ihres Unternehmens bereits frühzeitig damit beginnen, sich auf Anfragen von Kunden oder der Presse entsprechend vorzubereiten. Informieren Sie (abhängig von der konkreten Situation und Ihrer Kommunikationsstrategie) gegebenenfalls Kunden, Presse und Öffentlichkeit aktiv. Gleichzeitig sollte bei einem Ausfall Ihres öffentlichen Auftritts nicht darauf vergessen werden, eine etwaige im Vorfeld vorbereitete statische Website mit Basis-Informationen auch zu aktivieren. Achten Sie im Verlauf des Angriffs darauf, dass alle relevanten Informationen zu der Attacke (z. B. Logfiles, Erpressungsschreiben) erhalten bleiben. Diese können für eine spätere Analyse oder polizeiliche Ermittlungen eine wichtige Rolle spielen.

Bei allen Mitigationsmaßnahmen sollte auch stets mitbedacht werden, dass es bei der Abwehr in erster Linie darum geht, dem Angreifer zu vermitteln, dass er sein Ziel nicht erreichen wird. Wenn es Ihnen gelingt, die Funktionsfähigkeit Ihrer Systeme lange genug aufrecht zu erhalten (oder dass dies zumindest von außen so aussieht), besteht eine gute Chance, dass der Angreifer die Attacke einstellt. In der Regel ist die Aufrechterhaltung von Angriffen für den Angreifer mit laufenden Kosten verbunden (z. B. Zukauf von BOT-Netzen und anderen Ressourcen). Wenn vermutet wird, dass die Attacke nicht zum gewünschten Ziel führt, wird auch der Angreifer danach trachten, unnötige Kosten zu vermeiden.

Achten Sie gleichzeitig darauf, überlegt und schonend mit Ihren eigenen Personalressourcen umzugehen. Insbesondere bei schweren Vorfällen kann die Versuchung groß sein, sofort alle verfügbaren Mitarbeiterinnen und Mitarbeiter des Sicherheitsteams zur Bewältigung einzusetzen. Dies hat bei Angriffen, die sich über einen längeren Zeitraum erstrecken (z. B. mehrere Tage) den Effekt, dass Ihre Durchhaltefähigkeit nicht mehr gegeben ist.

4.1 Verstehen Sie den Angriff!

Geeignete und angemessene Gegenmaßnahmen können nur ergriffen werden, wenn Ihnen klar ist,

- dass sie angegriffen werden,
- was konkret angegriffen wird,
- welche Bedeutung die angegriffenen Systeme für das Unternehmen haben und
- um welche Art von Angriff (Kategorie) es sich handelt.

Sollte ein Angriff erkannt werden, eskalieren Sie diesen umgehend!

Versuchen sie schnellstmöglich, durch Analyse des eingehenden Datenverkehrs zu erkennen, um welche Kategorie von Angriff es sich handelt (quantitativ oder qualitativ bzw. welche Subkategorien davon) und ergreifen Sie in Abhängigkeit davon geeignete Sofortmaßnahmen.

4.2 Ergreifen Sie Sofortmaßnahmen!

Hinsichtlich der zu ergreifenden Sofortmaßnahmen gibt es kein Patentrezept. Im Folgenden findet sich jedoch eine Zusammenstellung von Maßnahmen, die entscheidenden Einfluss auf die erfolgreiche Abwehr eines Angriffs haben können.

Sofortmaßnahmen bei quantitativen Angriffen

Quantitative Angriffe (DDoS) gehen in der Regel von vielen Ursprüngen (tausende bis hin zu Millionen) aus, da von einzelnen Ursprüngen normalerweise nicht das erforderliche Volumen generiert werden kann, um nennenswerte Angriffe durchzuführen (dies gilt im Wesentlichen auch für Amplification-Attacks).

Grundsätzlich müssen alle diejenigen Datenpakete, die sich eindeutig dem Angriff zuordnen lassen, (nieder-)priorisiert, gefiltert oder blockiert werden. Dies kann entweder auf Basis der geografischen Zuordnung (GeoIP-Blocking) oder basierend auf technischen Informationen über die Art des Angriffs (SYN- oder UDP-Flooding) geschehen.

Wird ein Einsatz von GeoIP-Blocking angedacht, ist es entscheidend zu wissen, aus welchen geographischen Regionen Ihre extern angebotenen Dienste vorwiegend genutzt werden. Können diese Regionen auf einen überschaubaren Bereich eingegrenzt werden (d. h. dass sie also nicht weltweit gleichmäßig verteilt sind), können Sie die IP-Adressen aus dem vorgesehenen Zielgebiet priorisieren bzw. die restlichen IP-Adressen blockieren. Größtmögliche Effizienz kann hier erreicht werden, wenn dies bereits im Vorfeld (z. B. innerhalb eines vorgefertigten Profils) festgelegt wird.

Richtet sich der Angriff ausschließlich auf öffentliche Auftritte Ihres Unternehmens, können im Normalfall Stateless-Protokolle (z. B. UDP) ausgefiltert werden, ohne mit nennenswerten Einschränkungen rechnen zu müssen, da für diese Systeme zumeist nur TCP-basierte Protokolle (z. B. HTTP, HTTPS, SMTP) benötigt werden.

Ist zu befürchten bzw. zu erwarten, dass die bei dem Angriff verwendeten Absende-IP-Adressen gefälscht sind (was oftmals bei SYN-, UDP-, BGP- und SNMP-Flooding-Angriffen der Fall sein kann), ist eine Filterlösung auf Basis der Absende-IP-Adressen im eigenen Bereich nicht sinnvoll.

Bei Angriffen auf Nameserver bestehen grundsätzlich verschiedene Mitigationsstrategien:

- Bei kurzen Ausfällen kann durch Erhöhung der Time-To-Live (TTL) die Zeit der eingeschränkten Verfügbarkeit des Nameservers überbrückt werden. Allerdings wird es mit zunehmender Höhe der TTL schwieriger, kurzfristige Abwehrmaßnahmen zu setzen.
- Eine andere Maßnahme wäre das Betreiben eines externen Nameservers außerhalb der eigenen Peripherie (z. B. direkt bei einem auf DDoS-Angriffe spezialisierten Anbieter), um eine dauerhafte Verfügbarkeit zu gewährleisten zu können.

Sofortmaßnahmen bei qualitativen Angriffen

Wenn Sie sich in Ihrem Unternehmen mit einem qualitativen Angriff konfrontiert sehen, besteht eine gute Chance, dass der Angriff lediglich von einer begrenzten Anzahl von IP-

Absende-Adressen aus erfolgt. Wenn Sie den Angriff rechtzeitig erkannt haben, besteht somit eine vergleichsweise gute Chance, diese Adressen an Ihrem Router oder Ihrer Firewall zu filtern (Blackholing).

Im Bereich von Applikationen (Software) ist zum einen ein Einsatz von Web-Application-Firewalls (WAF) anzudenken; zum anderen nutzen entsprechende Angriffe in der Regel TCP als Netzwerk-Protokoll. Die Absende-IP-Adresse ist also nur schwer fälschbar und kann daher nach verschiedenen Kriterien gefiltert werden.

4.3 Seien Sie flexibel!

Die Methoden der Angreifer können sich im Verlauf eines Angriffs ändern. „Professionell" agierende Angreifer verfolgen Ihre Abwehrmaßnahmen genau und versuchen oftmals, die Angriffsstrategie daran anzupassen. Wenn im Gegenzug Sie Ihre Abwehrmaßnahmen nicht anpassen, wird dies den Erfolg Ihrer Bemühungen erheblich reduzieren. So folgt zum Beispiel auf einen quantitativen, volumensbasierten Angriff, der sich in vielen Fällen noch von Ihrem (Mitigation)-Provider alleine in den Griff bekommen lässt, oft ein qualitativer Angriff auf Applikationsebene, bei dem eine aktive Zusammenarbeit zwischen dem angegriffenen Unternehmen und dem Provider erforderlich ist.

Es ist daher unabdingbar, dass Sie im Verlauf Ihrer Abwehrmaßnahmen wiederholt zum Punkt „Verstehen Sie den Angriff!" zurückspringen müssen.

4.4 Suchen Sie Hilfe!

Wie bereits mehrfach angeführt, reduzieren sich die Möglichkeiten von effektiven Abwehrmaßnahmen im eigenen Bereich mit Anstieg des Angriffsvolumens kontinuierlich. Bei Angriffen, die einen gewissen Schwellwert, der primär von Ihren technischen Ressourcen abhängig ist, überschreiten, benötigen Sie Hilfe von externen Partnern. Primär werden dies Ihr Service-Provider und/oder kommerzielle Anbieter von DDoS-Mitigationslösungen sein.

5 Weiterführende Literatur

Hier finden sie gute und auch detaillierte Dokumente unserer deutschen, schweizerischen und niederländischen Kollegen, die sich ebenfalls mit dem Thema DDoS auseinandersetzen (Stand: Februar 2022):

Prävention von DDoS-Angriffen v2.0, Allianz für Cybersicherheit (BSI), DE
[https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_025.pdf?__blob=publicationFile&v=1]

Massnahmen zum Schutz vor DDoS-Angriffen, Melde- und Analysestelle Informationssicherung (MELANI), CH
[https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-unternehmen/aktuelle-themen/massnahmen-schutz-ddos.html]

Continuity of online services - Protect your organisation against (D)DoS attacks, Factsheet June 1, 2019, National Cyber Security Centre, NL
[https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-continuity-of-online-services]

Abbildungsverzeichnis

Abbildung 1 Volume Attacks 9
Abbildung 2 Reflection/Amplification-Attacks 10
Abbildung 3 Application-Attacks 11
Abbildung 4 Infrastructure-Attacks 11
Abbildung 5 DDoS-Mitigations-Anbieter 15

Bundesministerium für Inneres
Herrengasse 7, 1010 Wien
praevention@nis.gv.at | csc@dsn.gv.at
bmi.gv.at