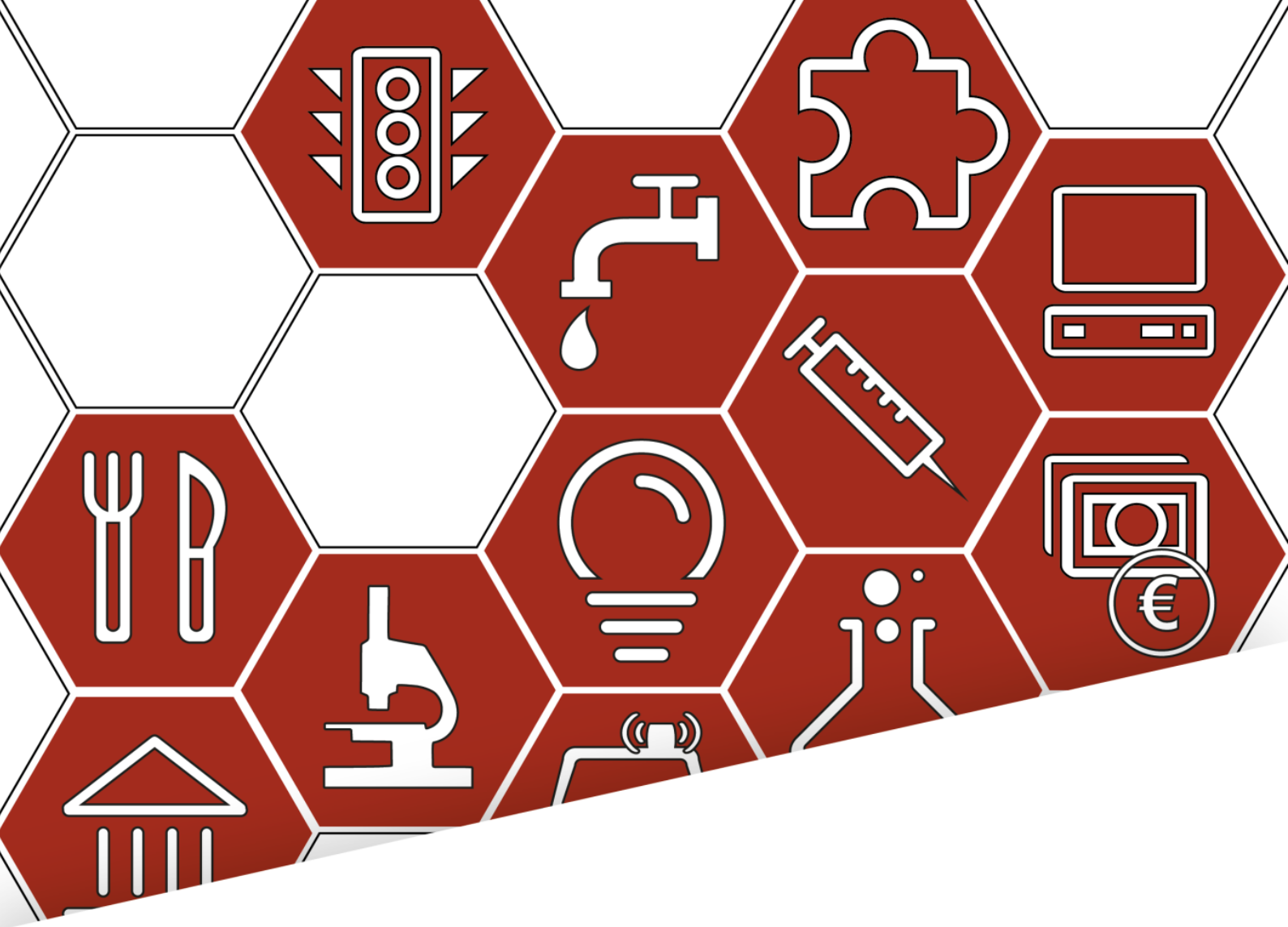


Dezember 2017

Distributed Denial of Service

Hintergründe, präventive Maßnahmen und Mitigationsmaßnahmen

BM.I
REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
BUNDESAMT FÜR VERFASSUNGSSCHUTZ UND TERRORISMUSBEKÄMPFUNG

IMPRESSUM

Medieninhaber/Herausgeber:
Bundesamt für Verfassungsschutz und Terrorismusbekämpfung,
Herrengasse 7, 1010 Wien

Herstellung:
Digitalprintcenter des BMI

CYBER SECURITY .BVT
Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert.

Inhalt

1. Hintergründe

1.1. Was ist ein DoS/DDoS Angriff?

DoS/DDos (Denial of Service/Distributed Denial of Service) ist ein **Angriff 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 Systemressourcen für die ordnungsgemäße Funktion nicht mehr ausreichen.

Der Angriff kann entweder von einem einzelnen Ursprung (DoS) oder gleichzeitig von mehreren, verteilten Ursprüngen (DDos) aus erfolgen. Die Angriffssysteme befinden sich dabei in überwiegendem Ausmaß nicht im Besitz der Angreifer, sondern werden von diesen, meist ohne Kenntnis der eigentlichen Besitzer, für den Angriff missbraucht.

Dazu hat der Angreifer im Vorfeld durch eine Infektion mit Schadsoftware die Kontrolle über die für den Angriff vorgesehenen Systeme übernommen (Bots) oder er nutzt für den Angriff Funktionalitäten von schlecht konfigurierten bzw. nicht ausreichend abgesicherten Servern (Reflection).

In diesem Zusammenhang muss stets bedacht werden, dass dabei das oder die **Angriffssysteme in aller Regel unwissende Opfer** sind, wobei selbst die Tatsache, dass ein System gerade für einen Angriff missbraucht wird, von den rechtmäßigen Besitzern meist unbemerkt bleibt. Allerdings werden diese Systeme dadurch „**Teil des Problems**“. Anders gesagt: nur weil ein bestimmtes System nicht selbst Ziel einer DDoS-Attacke ist, bedeutet nicht, dass es nicht gerade Teil eines DDoS-Angriffes ist.

In den folgenden Betrachtungen gehen wir nur auf DDoS ein, da in der Praxis beinahe ausschließlich diese Angriffsform zu beobachten ist.

1.2. Motivation hinter DDos-Angriffen

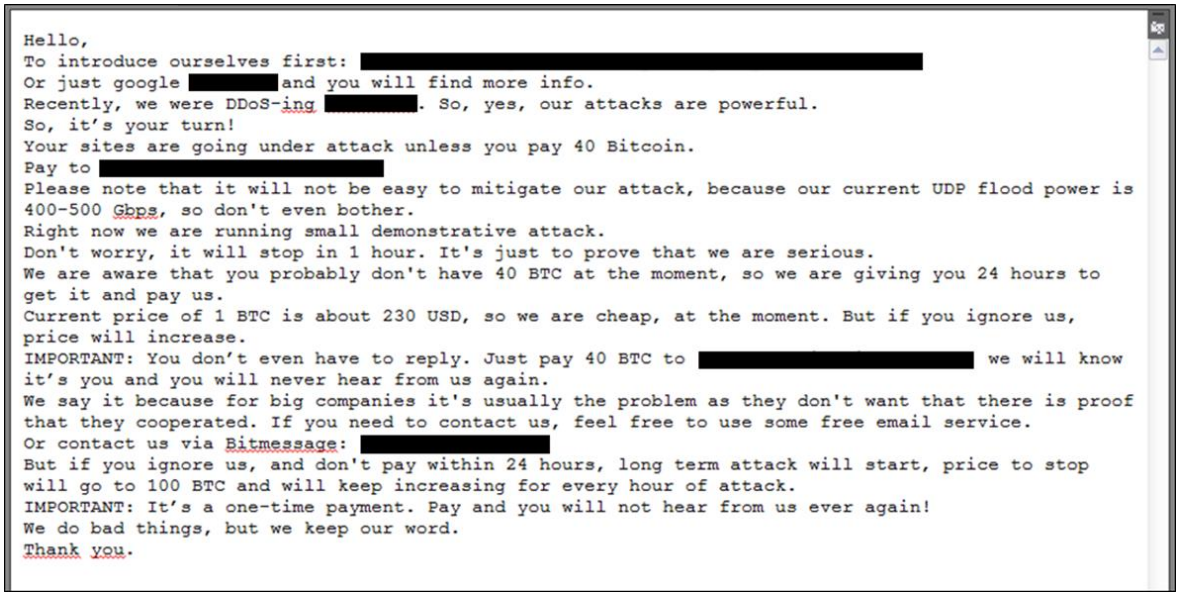
Im Wesentlichen lässt sich die Motivation hinter DDos-Angriffen auf **vier grundsätzliche Motive** reduzueren:

- Erpressung
- Sabotage
- Aktivismus
- Ablenkung

Selbstverständlich sind auch Kombinationen aus diesen Motiven denkbar.

1.2.1 Erpressung

Gerade in der jüngeren Vergangenheit ist eine starke Häufung von DDos-Angriffen zu beobachten, denen eine unmittelbare Bereicherungsabsicht zugrunde liegt. Diese richten sich vor allem Unternehmen, die (mehr oder weniger) von der ordnungsgemäßen Funktion der von ihnen angebotenen Dienste abhängig sind.



Hello,
To introduce ourselves first: [redacted]
Or just google [redacted] and you will find more info.
Recently, we were DDoS-ing [redacted]. So, yes, our attacks are powerful.
So, it's your turn!
Your sites are going under attack unless you pay 40 Bitcoin.
Pay to [redacted]
Please note that it will not be easy to mitigate our attack, because our current UDP flood power is 400-500 Gbps, so don't even bother.
Right now we are running small demonstrative attack.
Don't worry, it will stop in 1 hour. It's just to prove that we are serious.
We are aware that you probably don't have 40 BTC at the moment, so we are giving you 24 hours to get it and pay us.
Current price of 1 BTC is about 230 USD, so we are cheap, at the moment. But if you ignore us, price will increase.
IMPORTANT: You don't even have to reply. Just pay 40 BTC to [redacted] we will know it's you and you will never hear from us again.
We say it because for big companies it's usually the problem as they don't want that there is proof that they cooperated. If you need to contact us, feel free to use some free email service.
Or contact us via Bitmessage: [redacted]
But if you ignore us, and don't pay within 24 hours, long term attack will start, price to stop will go to 100 BTC and will keep increasing for every hour of attack.
IMPORTANT: It's a one-time payment. Pay and you will not hear from us ever again!
We do bad things, but we keep our word.
Thank you.

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 Cryptowährung Bitcoin oder mit „prepaid-Karten“). 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 Bundesamt für Verfassungsschutz und Terrorismusbekämpfung 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.

1.2.2 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 Mitbewerb erhoffen. Beispiele sind:

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

1.2.3 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/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 diesem Bereich liegt in der Regel **keine Bereicherungsabsicht** vor.

1.2.4 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 DDoS-Angriff bindet**. Während aller 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 die Entwicklung zu beobachten, dass **DDos-Angriffe im Internet „eingekauft“** werden können. So bieten im „Darknet“ zahlreiche Institutionen gegen vergleichsweise geringes Entgelt die Möglichkeit, Angriffe nach Dauer und Volumen preislich gestaffelt, zu ordern. Die Bezahlung erfolgt in den meisten Fällen auf Basis der Cryptowährung Bitcoin.

Besonders unangenehm ist diese Entwicklung vor allem aus dem Grund, dass nun jedermann (unabhängig von seinen technischen Fähigkeiten) einen DDos-Angriff durchführen kann.

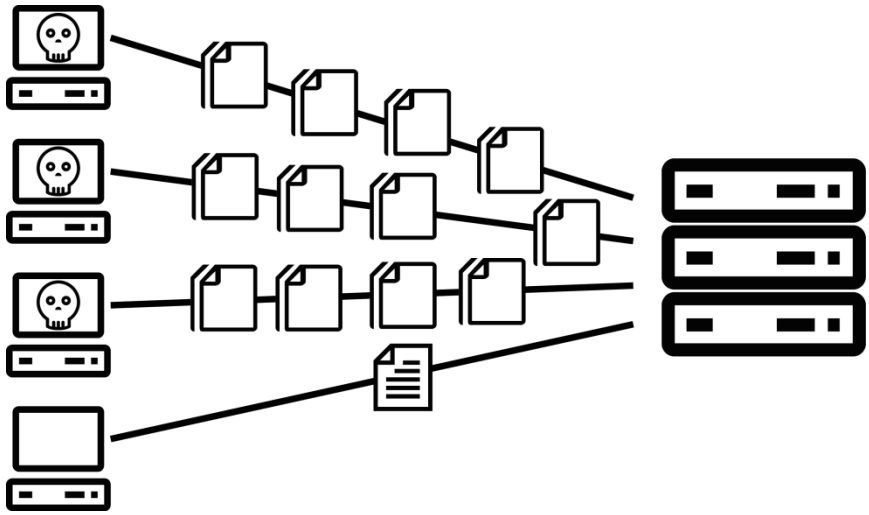
1.4. Kategorisierung von DDoS Angriffen

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

- Quantitative Angriffe
- Qualitative Angriffe
- Kombinationen der genannten Angriffe

1.4.1 Quantitative Angriffe

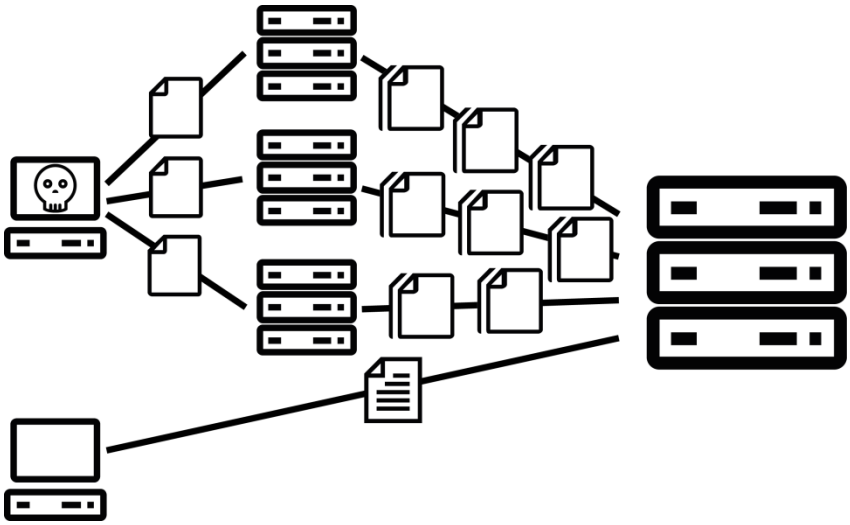
Allen Arten von quantitativen Angriffen ist gemein, dass sie versuchen, das **Zielsystem (Opfer) durch den Angriff zu überlasten**. Dabei kommen in der Regel keine hochspezialisierten Angriffsvektoren zum Einsatz, sondern der gewünschte Effekt wird durch die schiere Menge an Verkehr erzielt, mit dem 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 Verstärkung) in der Regel nicht eine ausreichende Verkehrsmenge generieren kann, um ein Zielsystem zu überlasten.

  Für diese Art des Angriffs wurden 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**

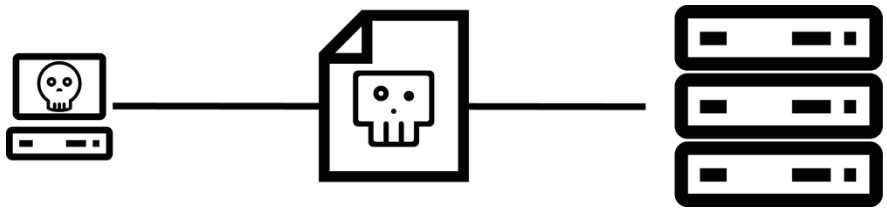
  Bei Reflection- oder Amplification Attacken handelt es sich im Grunde ebenfalls um Volume-Attacken, die jedoch spezielle Funktionalitäten von schlecht konfigurierten bzw. nicht ausreichend abgesicherten Servern benutzen, um den Effekt zu verstärken.

  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 in diesem Beispiel er seine Angriffskapazität um den Faktor 50 (gegenüber einem direkten Angriff) verstärken.

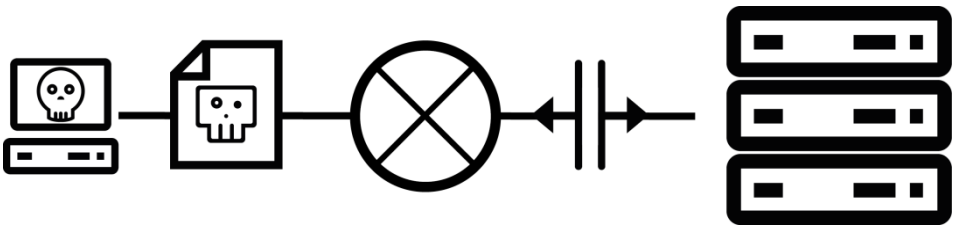
1.4.2 Qualitative Angriffe

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 Softwareanwendungen (Applikationen) aus, um diese außer Gefecht zu setzen. Dies muss nicht zwingend, kann jedoch mit einem hohen Angriffsvolumen zusammenhängen.



- **Infrastructure-Attacks (Angriff auf Infrastruktur)**

  Bei einem Angriff auf Infrastrukturen werden gezielt Angriffsstrategien entwickelt, um gewisse Hardwarekomponenten außer Gefecht zu setzen. Dies muss ebenfalls nicht zwingend mit einem hohen Angriffsvolumen zusammenhängen.

2. Präventive Maßnahmen

Keine Maßnahme kann Ihnen vollständigen Schutz vor DDos-Angriffen bieten. Im Folgenden sind 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 in „Friedenszeiten“** erfolgen müssen, also zu einem Zeitpunkt, an dem noch kein Angriff stattfindet.

2.1. Aktives Monitoring

Das grundlegendste Erfordernis für eine umfassende Schutzstrategie ist, dass Sie Ihr Unternehmen, Ihre Infrastrukturen, 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/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 Infrastrukturen und Dienste von Ihrem Monitoring-System bzw. einer permanenten, zentralen Logauswertung erfasst und abgedeckt werden. Es muss sichergestellt sein, dass 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.

2.2. 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 in Falle eines erhöhen 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.

2.3. 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 Ereignisses wissen, was zu tun ist. Finden diese Überlegungen erst im Ernstfall statt, ist es zu spät.

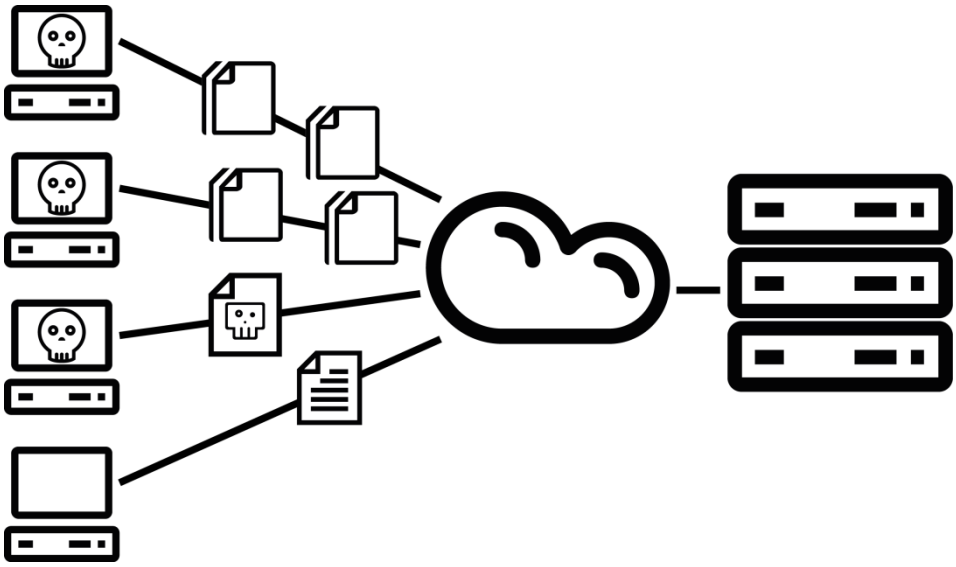
Planen Sie bereits in „Friedenszeiten“ gemeinsam mit Ihren Notfallkontakten - dazu zählen interne Ansprechpartner (v.a. IT, Network Operations, Security Operations) und externe Ansprechpartner (v.a. Upstream-Service-Provider) - die im Falle eines Angriffes notwendigen Maßnahmen. Halten Sie diese **Notfallkontakte 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 in „Friedenszeiten" 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. Unternehmenswebsite) 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 Basis-Informationen** sinnvoll sein, die bei einem anderen Provider bereit steht und die Sie mit einer einfachen Änderung im DNS aktivieren können.

2.4. DDoS-Mitigations-Anbieter



Die meisten Anbieter von DDoS-Mitigations-Lösungen 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 automatisch erkannt und blockiert werden können.

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 hochredundaten Verteinetz alternativ zuzustellen.

Ausgewählte österreichische Internet Service Providers schützen bereits seit einigen Jahren die größten und komplexesten Netzwerke Österreichs vor DDoS-Angriffen. Sie setzen auf ein Konzept, in dem Ressourcen durch eine **mehrstufige Implementierung** von **DDoS-Angriffsabwehrmechanismen** geschützt werden können.

Hochvolumige Angriffe die 300 Gbps überschreiten erfordern einen Cloud-basierten Schutz (s.o.) des ISPs, welcher auch lokal (in österreichischen Rechenzentren) den in ihren Netzen angeschlossenen Kunden zur Verfügung gestellt werden kann. Somit wird auch hinsichtlich Datenschutzaspekten ein Augenmerk darauf gelegt, dass der zu säubernde Datenverkehr, der über die sogenannte „Mitigationsplattform" läuft, nicht das Land verlassen muss („Anti-DDOS - made in Austria").

Idealerweise arbeitet der **Vor-Ort-Schutz** (Firewalls, IPS, ADCs etc.) mit der **Cloud-basierten** Lösung des **ISPs** „**Zahn-in-Zahn**" zusammen, indem mit der gemeinsamen Sprache namens „Cloud-Signaling" kommuniziert wird. So wird eine Internetanbindung effektiv sauber gehalten, die ursprünglich von DDOS-Angriffen lahmgelegt hätten werden sollen – das Ergebnis nennt man „Clean pipe" und die Erreichbarkeit des Kunden dahinter ist sichergestellt.

Eine zweckmäßige und effiziente Nutzung eines DDoS-Mitigations-Anbieters ist daher praktisch nur für dem Fall gegeben, in dem bereits **präventiv** die Dienste dieses Anbieters genutzt werden.

3. Mitigationsmaßnahmen

Sehen Sie sich trotz der ergriffenen präventiven Maßnahmen mit einem Angriff konfrontiert, ist es essentiell, **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 mitgedacht 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 dies von außen zumindest so aussieht), besteht eine gute Chance, dass der Angeifer 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 anderer Ressourcen). Wenn vermutet wird, dass die Attacke nicht zum gewünschten Ziel führt, wird auch der Angreifer danach trachten, unnötige Kosten zu vermeiden.

3.1. 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.

3.2. Ergreifen Sie Sofortmaßnahmen!

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

3.2.1 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 einerseits auf Basis der geografischen Zuordnung (GeoIP-Blocking) oder andererseits 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 state-less 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.

3.2.2 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.

3.3. Weiterführende Literatur

Hier finden sie sehr gute und auch detailierte Dokumente unserer deutschen, schweizer und niederländischen Kollegen, die sich ebenfalls mit dem Thema DDoS auseinandersetzen:

https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/factsheets/factsheet-technical-measures-for-the-continuity-of-online-services/1/FS%2BDDoS%2Btechnical%2Bmeasures%2Bv1.0_EN.pdf

https://www.ncsc.nl/binaries/content/documents/ncsc-en/current-topics/factsheets/factsheet-protect-you-online-services-against-ddos-atta-cks/1/Factsheet%2Bprotect%2Byour%2Bonline%2Bservices%2Bagainst%2BDDoS%2Battacks.pdf

https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_025.pdf?__blob=publicationFile&v=4

https://www.melani.admin.ch/dam/melani/de/dokumente/2015/04/Massnahmen_gegen_DDoS_Attacken.pdf.download.pdf/Massnahmen_gegen_DDoS_Attacken.pdf

3.4. 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.

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

3.5. Suchen Sie Hilfe!

Wie bereits mehrfach angeführt, reduzieren sich die Möglichkeiten von effektiven Abwehrmaßnahmen im eigenen Bereich mit Anstieg des Angriffsvolumen 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.

Cyber Security Center