# Was kann man gegen DDoS Attacken tun?

## Intention

Dieses Pattern erläutert Maßnahmen zur Prävention und Umgang mit *DoS und DDoS* Attacken.

## Problemstellung

DoS sowie DDoS Attacken treten in den letzten Jahren vermehrt auf. Zwar richten sich die meisten dieser Attacken auf Finanzdienstleister oder Plattformen die Onlinedienste bereitstellen (z.B. *PayPal*, *GitHub*), doch auch Privatanwender, kleinere Websites oder Webshops können Ziele solcher Attacken werden.

## Szenario

Die eigene Website ist nicht mehr aufrufbar, sie reagiert nicht und gibt im Browser die *Fehlermeldung 503*.

## Lösung

Eines muss von vornherein gesagt werden: **Man kann einkommende Attacken nicht direkt stoppen**. Aber man kann diese **Attacken frühzeitig erkennen** um daraufhin Maßnahmen einzuleiten, wie zum Beispiel den Datentransfer des Angreifers zu ignorieren und damit die **Situation zu deeskalieren**. **Sollte man mit der Situation überfordert sein, ist es immer empfehlenswert einen Experten zu Rate zu ziehen!** Man unterscheidet generell unter DoS sowie DDoS Attacken. Bei einer DoS Attacke geschieht der Angriff von nur einem System mit einer direkten Verbindung zum Internet, somit also nur mit einer *IP-Adresse*. Dementsprechend ist es auch einfacher Gegenmaßnahmen zu ergreifen.

- Die IP-Adresse des Angreifers direkt in der Firewall, des Systems zu blockieren oder vom Provider blockieren lassen und damit jegliche Datenpakete von dieser Adresse zu ignorieren.
- Verwenden von Sicherheitstools, welche *ICMP*-Attacken (permanente *PING*-Anfragen auf eine Seite) erkennen und diese blockieren.

Sofern der Angriff von mehreren Quellen (Systemen sowie Internetverbindungen) aus erfolgt, nennt man diese dann DDoS Attacke. In diesem Fall reicht es daher nicht nur eine IP-Adresse zu blockieren, da der Angriff von mehreren Quellen stammt. Das Problem hierbei ist es, dass man nicht differenzieren kann ob es eine normale Seitenanfrage von Websitebesuchern ist, oder es sich aber um einen gezielten Angriff auf die Seite handelt. Folgende Maßnahmen kann man während oder vor einem DDoS Angriff ergreifen, wenn man die Seite nicht selbst hostet:

- Darauf achten oder in Erfahrung bringen, ob der Webhoster DDoS Angriffen standhält und welche Maßnahmen er anbieten kann um die Seite zu schützen.
- Es gibt auch Hoster die eine DDoS-Protection anbieten: https://www.cloudflare.com/de-de/
- Während eines Angriffs sollte der Internetdienstanbieter oder Hoster sofort benachrichtigt werden. Diese werden dann selbst Schritte gegen diese Angriffe einleiten.
- Einen DDoS-Spezialisten (z.B. https://www.akamai.com ) beauftragen die Seite im Fall eines Angriffs weiterhin online zu halten. Diese Anbieter haben eine große Infrastruktur und eigens entwickelte Systeme um den Schaden bei einem DDoS-Angriff so gering wie möglich zu halten.
- Die Seite temporär vom Netz nehmen.

Sofern man seine Seite selbst hostet:

- IPs, Länder oder Orte blockieren oder filtern, die bekannt für DDoS-Angriffe sind.
- Halboffene Verbindungen schneller Serverseitig kappen.
- *SYN*,*ICMP*– und *UDP*– Limits reduzieren um nicht mit Anfragepaketen überflutet zu werden.
- Beschränkung der Seitenzugriffe die zur selben Zeit stattfinden dürfen.
- Die Seite temporär vom Netz nehmen.

# Beispiele

**DDoS Schutz durch den Webhoster**
Üblicherweise reicht es sich die Angebote der Webhoster durchzusehen. Meist bieten diese einen DDoS-Schutz an. Da DDoS-Attacken jedoch unberechenbar sind, können Hoster nicht zu 100% garantieren, dass die Website immer erreichbar ist. Daher findet man oft die Auskunft, dass die eigenen Server 99,9% der Zeit online verfügbar sind.

**XML RPC in WordPress deaktivieren**
Hierzu wird die .htaccess Datei, welche üblicherweise im Hauptverzeichnis des Webservers liegt, geöffnet und folgende Codezeilen eingefügt.

```
# START XML RPC BLOCKING



<Files xmlrpc.php>Order Deny,Allow

Deny from all

</Files>

# FINISH XML RPC BLOCKING
```

Mehr hierzu unter: https://www.greengeeks.com/tutorials/article/how-to-enable-and-disable-xmlrpc-php-in-wordpress-and-why/

**Seite Offline schalten**
Folgenden Codezeilen in die .htaccess Datei im Hauptverzeichnis des Servers einfügen um die Seite Offline zu schalten:

```
<IfModule mod_rewrite.c> RewriteEngine On RewriteBase / Redirect 503
</IfModule>
```

**WordPress Seite Offline schalten**
Um eine WordPress Seite offline zu schalten sollte man am besten ein Plugin für den Wartungsmodus nutzen. Denn eine komplette Offline-Schaltung kann Auswirkungen auf das Suchmaschinen-Ranking haben. Hier ein Plugin, welches dafür benutzt werden kann: https://de.wordpress.org/plugins/wp-maintenance-mode/.

**Apache Webserver gegen DDoS Angriffe absichern**

- https://securityintelligence.com/defending-against-apache-web-server-ddos-attacks/

**Verwenden eines Intrusion Prävention System**
Ein Intrusion Prävention System (IPS) ist ein Framework zur Vorbeugung gegen Einbrüche. Ein gutes Tool für Server Admins ist beispielsweise Fail2Ban

- https://www.fail2ban.org/wiki/index.php/Main_Page

**DDoS Prävention mit NGINX**

- https://www.nginx.com/blog/mitigating-ddos-attacks-with-nginx-and-nginx-plus/

# Referenzen

https://www.heise.de/newsticker/meldung/DDoS-Attacke-kostet-Paypal-3-5-Millionen-Pfund-1755660.html
https://www.computerweekly.com/news/4500272230/DDoS-is-most-common-cyber-attack-on-financial-institutions
https://www.esecurityplanet.com/network-security/how-to-prevent-dos-attacks.html
https://www.incapsula.com/ddos/attack-glossary/ping-icmp-flood.html

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6389https://wpcerber.com/how-to-protect-wordpress-against-cve-2018-6389/

## Keywords

DDoS, DoS, Sicherheit, Absicherung, Prävention