„Internet-Sicherheit“

„Wie man Type-1-DOS-Angriffe erkennt und abwehrt“

Ein Vortrag im Rahmen von nichts

„Schwerpunkt Thema: DOS-Angriff“

Nein, DOS steht nicht für ein altes M$-Betriebssystem.

„Schwerpunkt Thema: DOS-Angriff“

Denial Of Service Angriff

„Schwerpunkt Thema: DOS-Angriff“

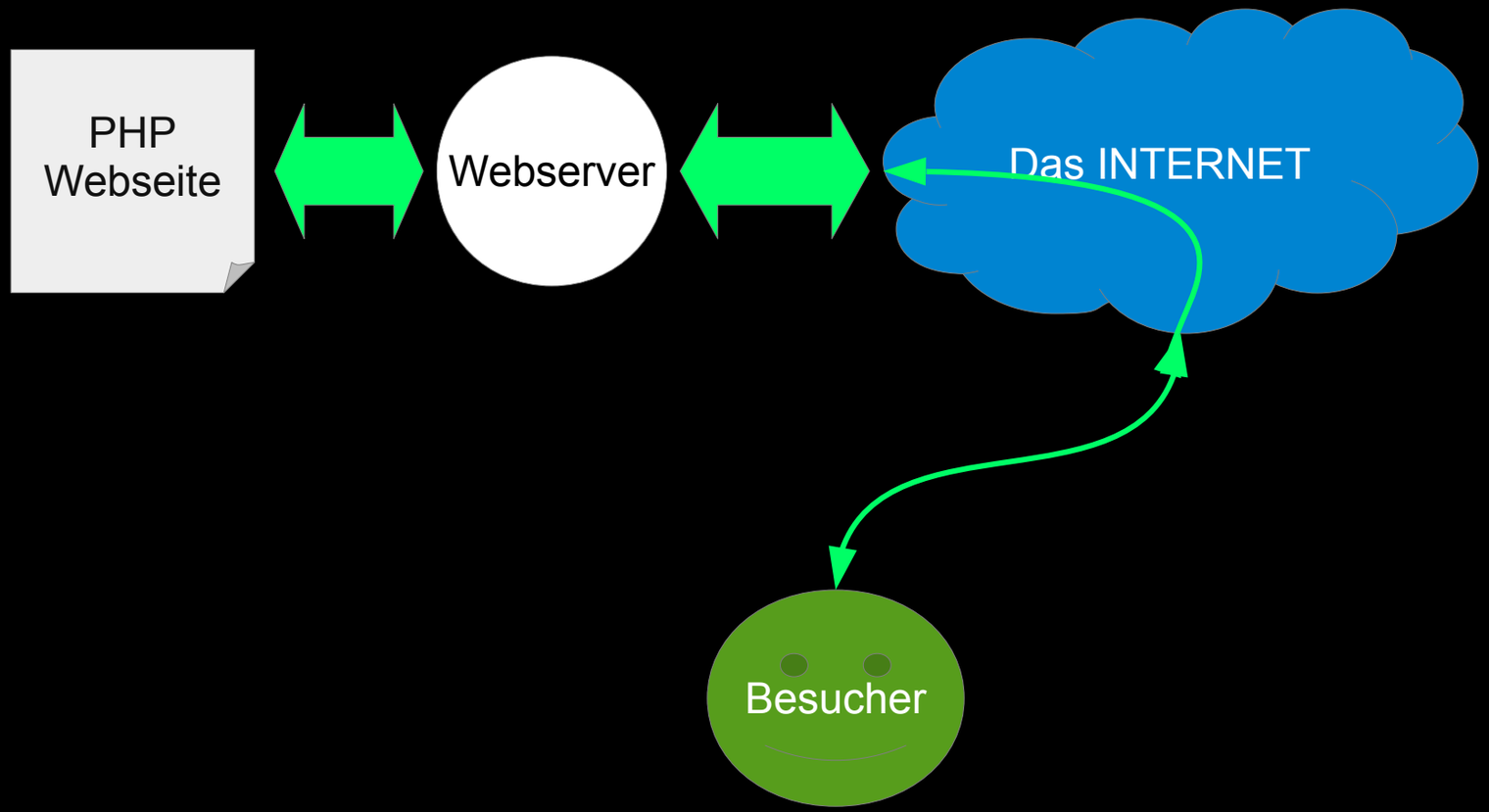
Denial Of Service Angriff

auf Deutsch „Dienstverweigerungsangriff“

„Schwerpunkt Thema: DOS-Angriff“

Der Normalzustand

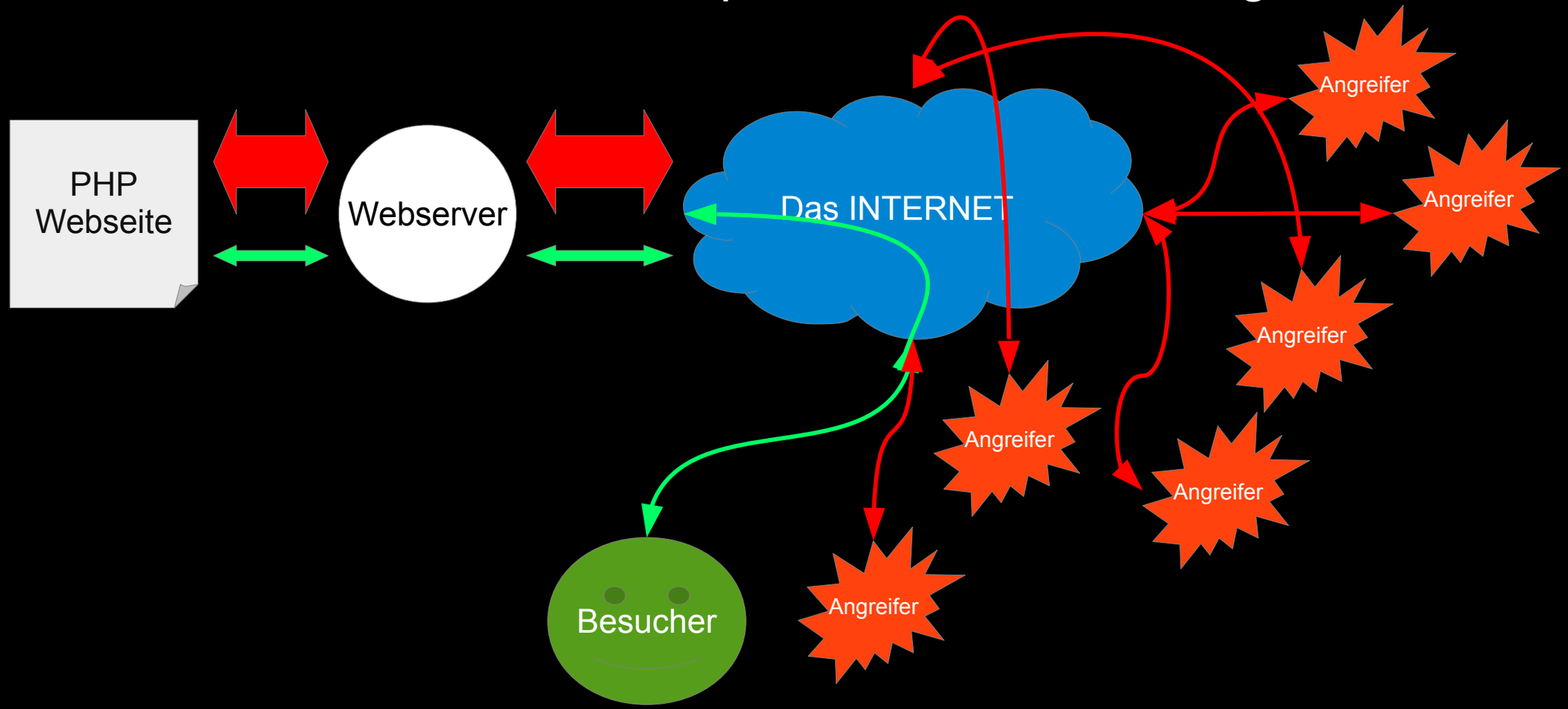
„Schwerpunkt Thema: DOS-Angriff“



„Schwerpunkt Thema: DOS-Angriff“

Wenige Angreifer können noch nichts ausrichten.

„Schwerpunkt Thema: DOS-Angriff“

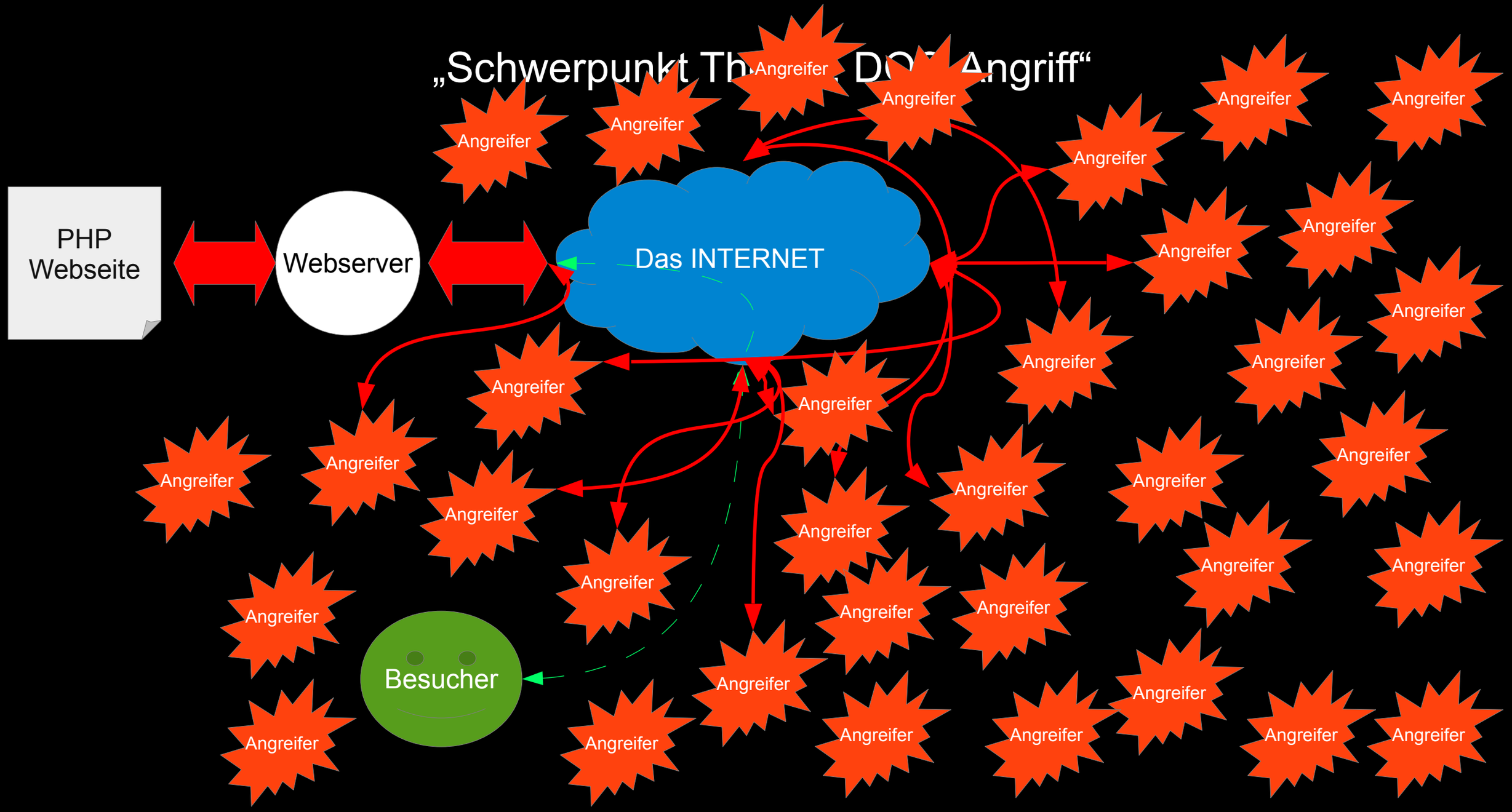


„Schwerpunkt Thema: DOS-Angriff“

Der von den Angreifern produzierte Datendurchsatz

blockiert den regulären Besucher.

„Schwerpunkt Th… DO… Angriff“



„Schwerpunkt Thema: DOS-Angriff“

Diese Art Angriff nennt man DDOS Angriff,

weil er von verschiedenen Orten aus durchgeführt wird.

„Schwerpunkt Thema: DOS-Angriff“

Merke:

Wenn genug große Datenpakete an den Server gesendet werden,

ist die Leitungskapazität überlastet.

„Schwerpunkt Thema: DOS-Angriff“

Eine schöne Analogie ist ein Verkehrsstau,

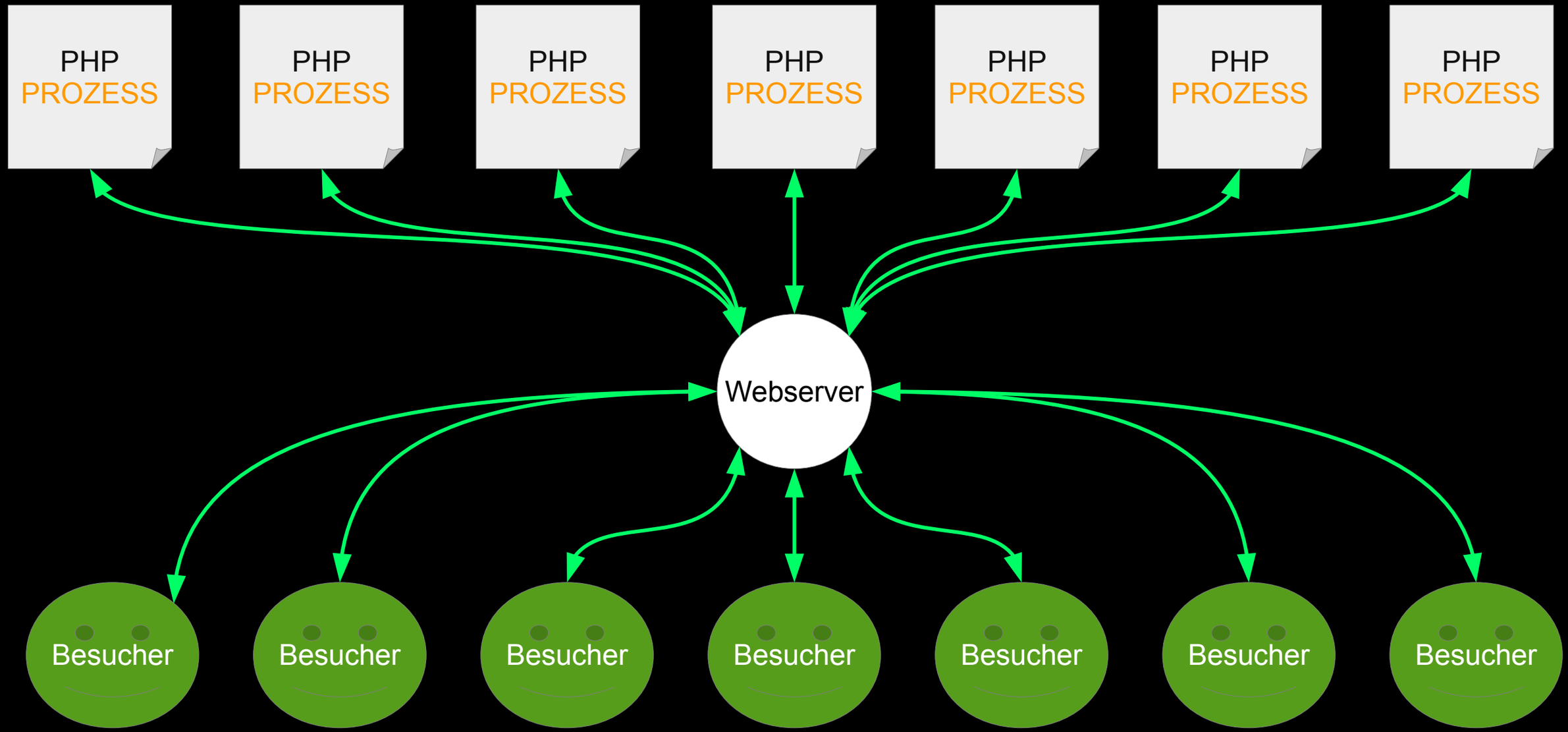
da möchten auch mehr Autos eine Stelle passieren,

als möglich ist.

„Schwerpunkt Thema: DOS-Angriff“

Es geht aber auch anders...

„Schwerpunkt Thema: DOS-Angriff“



„Schwerpunkt Thema: DOS-Angriff“

Jeder PHP Prozess braucht:

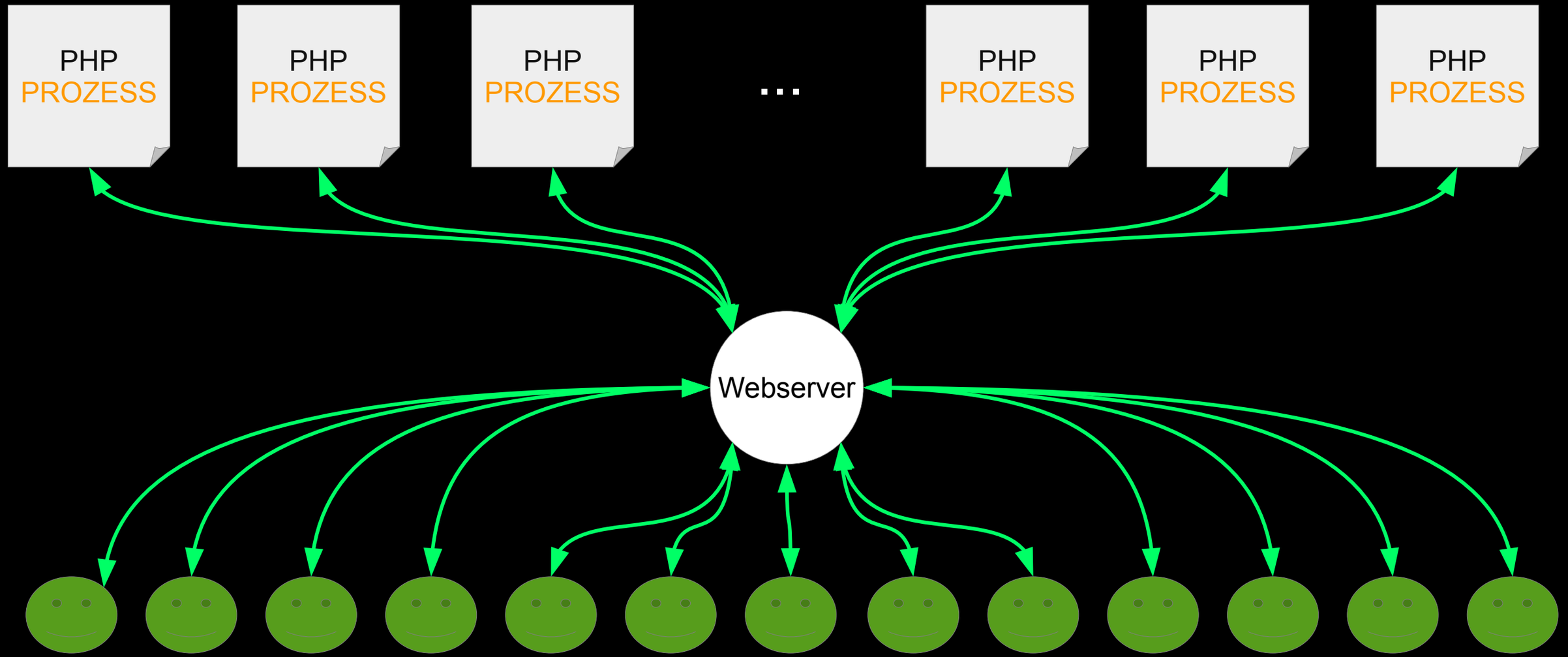
Rechenleistung
Hauptspeicher
DISK-IO

„Schwerpunkt Thema: DOS-Angriff“

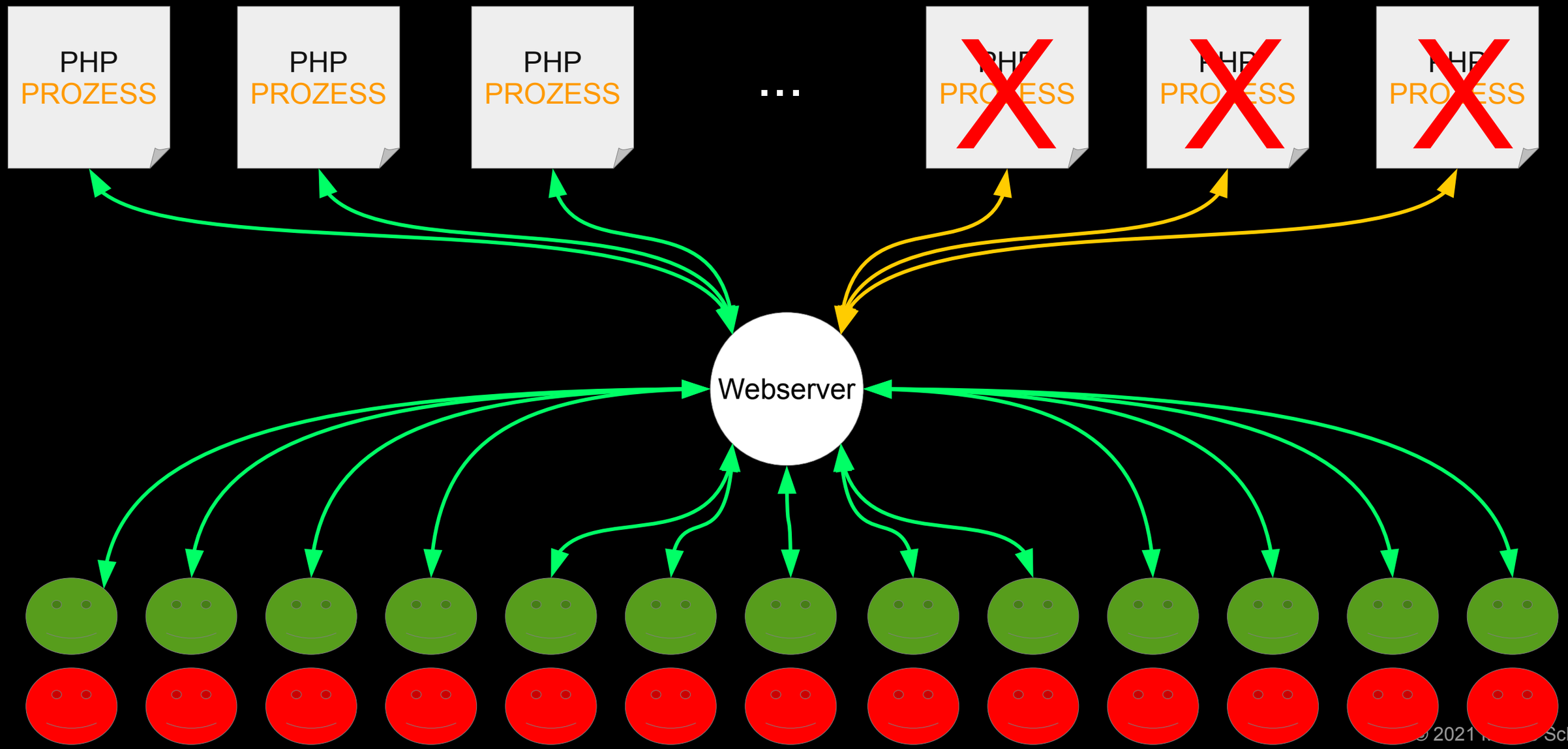
Das geht solange gut, bis mehr Anfragen reinkommen,

als der Server verarbeiten kann.

„Schwerpunkt Thema: DOS-Angriff“



„Schwerpunkt Thema: DOS-Angriff“



„Schwerpunkt Thema: DOS-Angriff“

Merke:

Eine kleine Anzahl an Verbindungen kann einen Server in die Knie zwingen,

wenn dessen Ressourcen erschöpft sind.

„Schwerpunkt Thema: DOS-Angriff“

Klar kann man sich wehren.

„Schwerpunkt Thema: DOS-Angriff“

GEGENMAßNAHMEN

„Schwerpunkt Thema: DOS-Angriff“

Für einen DOS auf Basis der Serverressourcen braucht man valide Verbindungen.

Es reicht nicht, einfach nur irgendwelche Datenpakete zu senden.

„Schwerpunkt Thema: DOS-Angriff“

Das Logfile ansehen...

„Schwerpunkt Thema: DOS-Angriff“

```
20.43.24.148 - - [24/Mar/2021:19:37:11 +0100] "GET / HTTP/2.0" 200 - "-" "curl"
138.186.140.200 - - [24/Mar/2021:19:37:20 +0100] "GET / HTTP/2.0" 200 75974 "-" "curl"
172.97.102.37 - - [24/Mar/2021:19:37:21 +0100] "GET / HTTP/2.0" 200 75974 "-" "curl"
12.18.196.100 - - [24/Mar/2021:19:37:25 +0100] "GET / HTTP/2.0" 200 75974 "-" "curl"
66.155.58.127 - - [24/Mar/2021:19:37:27 +0100] "GET / HTTP/2.0" 200 75974 "-" "curl"
12.180.180.39 - - [24/Mar/2021:19:37:43 +0100] "GET / HTTP/2.0" 200 75974 "-" "curl"
63.98.212.38 - - [24/Mar/2021:19:37:52 +0100] "GET / HTTP/2.0" 200 75974 "-" "curl"
63.64.110.241 - - [24/Mar/2021:19:37:55 +0100] "GET / HTTP/2.0" 200 75974 "-" "curl"
52.78.200.19 - - [24/Mar/2021:19:37:57 +0100] "GET / HTTP/2.0" 200 75974 "-" "curl"
52.78.200.19 - - [24/Mar/2021:19:38:01 +0100] "GET / HTTP/2.0" 301 - "-" "curl"
12.18.196.100 - - [24/Mar/2021:19:38:00 +0100] "GET / HTTP/2.0" 200 - "-" "curl"
12.180.180.39 - - [24/Mar/2021:19:38:00 +0100] "GET / HTTP/2.0" 200 - "-" "curl"
63.98.212.38 - - [24/Mar/2021:19:38:00 +0100] "GET / HTTP/2.0" 200 - "-" "curl"
20.43.24.148 - - [24/Mar/2021:19:38:00 +0100] "GET / HTTP/2.0" 200 - "-" "curl"
172.97.102.37 - - [24/Mar/2021:19:38:00 +0100] "GET / HTTP/2.0" 200 - "-" "curl"
66.155.58.127 - - [24/Mar/2021:19:38:00 +0100] "GET / HTTP/2.0" 200 - "-" "curl"
138.186.140.200 - - [24/Mar/2021:19:38:00 +0100] "GET / HTTP/2.0" 200 - "-" "curl"
63.64.110.241 - - [24/Mar/2021:19:38:00 +0100] "GET / HTTP/2.0" 200 - "-" "curl"
52.78.200.19 - - [24/Mar/2021:19:38:01 +0100] "GET / HTTP/2.0" 200 - "-" "curl"
52.78.200.19 - - [24/Mar/2021:19:38:04 +0100] "GET / HTTP/2.0" 301 - "-" "curl"
74.113.248.119 - - [24/Mar/2021:19:38:02 +0100] "GET / HTTP/2.0" 200 - "-" "curl"
52.231.70.133 - - [24/Mar/2021:19:38:05 +0100] "GET / HTTP/2.0" 200 - "-" "curl"
52.232.111.57 - - [24/Mar/2021:19:38:08 +0100] "GET / HTTP/2.0" 200 - "-" "curl"
63.64.110.249 - - [24/Mar/2021:19:38:14 +0100] "GET / HTTP/2.0" 301 - "-" "curl"
207.198.106.43 - - [24/Mar/2021:19:38:15 +0100] "GET / HTTP/2.0" 301 - "-" "curl"
172.97.102.38 - - [24/Mar/2021:19:38:19 +0100] "GET / HTTP/2.0" 301 - "-" "curl"
63.98.212.38 - - [24/Mar/2021:19:38:23 +0100] "GET / HTTP/2.0" 301 - "-" "curl"
4.28.133.108 - - [24/Mar/2021:19:38:21 +0100] "GET / HTTP/2.0" 200 - "-" "curl"
74.113.248.112 - - [24/Mar/2021:19:38:26 +0100] "GET / HTTP/2.0" 301 - "-" "curl"
201.168.210.70 - - [24/Mar/2021:19:38:23 +0100] "GET / HTTP/2.0" 200 - "-" "curl"
40.74.63.146 - - [24/Mar/2021:19:38:39 +0100] "GET / HTTP/2.0" 301 - "-" "curl"
40.74.63.146 - - [24/Mar/2021:19:38:42 +0100] "GET / HTTP/2.0" 200 75974 "-" "curl"
4.28.133.107 - - [24/Mar/2021:19:38:51 +0100] "GET / HTTP/2.0" 301 - "-" "curl"
138.186.140.217 - - [24/Mar/2021:19:38:53 +0100] "GET / HTTP/2.0" 301 - "-" "curl"
```

„Schwerpunkt Thema: DOS-Angriff“

Alle Verbindungen der Angreifer im Beispiel geben sich als CURL aus.

„Schwerpunkt Thema: DOS-Angriff“

Alle Verbindungen der Angreifer im Beispiel geben sich als CURL aus.

Dümmer geht’s echt nicht mehr ;)

„Schwerpunkt Thema: DOS-Angriff“

Innovative Umleitung der Angreifer direkt im Webserver an die zuständige Stelle ;)

```
<IfModule mod_rewrite.c>
RewriteEngine On

RewriteCond %{HTTP_USER_AGENT} "curl"
RewriteRule  (.*)  https://www.fbi.gov/tips   [R=301,L]

</IfModule>
```

„Schwerpunkt Thema: DOS-Angriff“

Die IP-Firewall einsetzen

um den Webserver zu entlasten.

„Schwerpunkt Thema: DOS-Angriff“

Wir extrahieren aus dem Logfile mit allen „CURL“-Verbindungen die IPs:

```
# cat /tmp/log | sed -e "s/ .*$//g"  | sort -u | awk '{print "iptables -A wordpress -j DROP -s "$1;}'
```

„Schwerpunkt Thema: DOS-Angriff“

```
# cat /tmp/log | sed -e "s/ .*$//g"  | sort -u | awk '{print "iptables -A wordpress -j DROP -s "$1;}'
iptables -A wordpress -j DROP -s 12.180.180.39
iptables -A wordpress -j DROP -s 12.180.180.43
iptables -A wordpress -j DROP -s 12.18.196.100
iptables -A wordpress -j DROP -s 12.18.196.91
iptables -A wordpress -j DROP -s 13.71.190.54
iptables -A wordpress -j DROP -s 138.186.140.200
iptables -A wordpress -j DROP -s 138.186.140.217
iptables -A wordpress -j DROP -s 172.97.102.37
iptables -A wordpress -j DROP -s 172.97.102.38
iptables -A wordpress -j DROP -s 201.168.210.70
iptables -A wordpress -j DROP -s 201.168.210.84
iptables -A wordpress -j DROP -s 20.43.24.148
iptables -A wordpress -j DROP -s 207.198.106.43
iptables -A wordpress -j DROP -s 40.74.63.146
iptables -A wordpress -j DROP -s 4.28.133.107
iptables -A wordpress -j DROP -s 4.28.133.108
iptables -A wordpress -j DROP -s 45.9.150.27
iptables -A wordpress -j DROP -s 52.231.26.62
iptables -A wordpress -j DROP -s 52.231.70.133
iptables -A wordpress -j DROP -s 52.232.111.57
iptables -A wordpress -j DROP -s 52.78.200.19
iptables -A wordpress -j DROP -s 63.64.110.241
iptables -A wordpress -j DROP -s 63.64.110.249
iptables -A wordpress -j DROP -s 63.98.212.38
iptables -A wordpress -j DROP -s 66.155.58.127
iptables -A wordpress -j DROP -s 74.113.248.112
iptables -A wordpress -j DROP -s 74.113.248.119
```

„Schwerpunkt Thema: DOS-Angriff“

Die Anweisungen führt man dann einfach noch aus,

oder macht es gleich in einem Schritt:

```
cat /tmp/log | sed -e "s/ .*$//g"  | sort -u | awk '{print "iptables -A wordpress -j DROP -s "$1;}' | bash
```

„Schwerpunkt Thema: DOS-Angriff“

Angriffe, welche die Datenleitung dicht machen,

kann man so nicht abwehren.

„Schwerpunkt Thema: DOS-Angriff“

Hier hilft nur die Quellen anzugreifen

oder

den Zufluss an Datenpaketen durch den Provider zu stoppen:

„DDOS Abwehr“