

LU12c - Gegenmassnahmen DDoS

Glücklicherweise gibt es auch gegen DoS/DDoS-Attacken wirksame Gegenmassnahmen. Anders als bei einer SQLi reicht dabei ein einzelnes Mittel selten aus – wirksamer Schutz entsteht erst durch die *Kombination* mehrerer Massnahmen (*Defense in Depth*). Die hier vorliegende Liste ist daher nur ein Ausschnitt mit den prominentesten.

Rate Limiting

Beim *Rate Limiting* wird die Anzahl Anfragen begrenzt, die ein einzelner Client (meist erkannt an der IP-Adresse) innerhalb eines bestimmten Zeitfensters stellen darf. Wer die Grenze überschreitet, wird verlangsamt oder vorübergehend abgewiesen. Damit werden vor allem einfache Floods von einzelnen Quellen wirkungsvoll ausgebremst.

Wie funktioniert es?

1. Für jeden Client wird mitgezählt, wie viele Anfragen pro Sekunde eintreffen.
2. Bis zu einem definierten Schwellenwert werden die Anfragen normal beantwortet.
3. Übersteigt ein Client den Schwellenwert, werden weitere Anfragen verzögert oder mit einem Fehler (HTTP 429 «Too Many Requests») abgelehnt.

Beispiel mit nginx

```
# max. 10 Anfragen pro Sekunde je IP-Adresse zulassen
limit_req_zone $binary_remote_addr zone=schutz:10m rate=10r/s;

server {
    location / {
        limit_req zone=schutz burst=20 nodelay;
    }
}
```

Oder kurz: Lass niemanden so oft anklopfen, wie er will.

Traffic-Filterung & Blackholing

Nicht jeder Verkehr muss den eigentlichen Server überhaupt erreichen. Auf Netzwerkebene lässt sich bössartiger Verkehr bereits am Rand (*Edge*) verwerfen, bevor er Ressourcen bindet. Beim *Blackholing* (auch *Null-Routing*) wird der Verkehr zu einer angegriffenen Adresse gezielt ins «Nichts» geleitet.

```
# einzelne, bekannte Angreifer-IP verwerfen
iptables -A INPUT -s 203.0.113.42 -j DROP
```

- **Blacklisting:** Bekannte bössartige IP-Adressen oder Netze werden blockiert.
- **Geo-Blocking:** Verkehr aus Regionen, die für den Betrieb irrelevant sind, wird abgewiesen.

- **Blackholing:** Der gesamte Verkehr zur Zieladresse wird verworfen – wirksam, aber der Dienst ist damit für *alle* nicht mehr erreichbar (Notmassnahme).

Load Balancing & Skalierung

Ein *Load Balancer* verteilt eingehende Anfragen auf mehrere Server. Fällt ein einzelner Server unter der Last aus oder wird überlastet, übernehmen die übrigen. In Kombination mit *Autoscaling* (automatisches Hochfahren zusätzlicher Server bei Bedarf) und einer gewissen Überkapazität an Bandbreite lässt sich ein Angriff abfedern.

- Die Last verteilt sich auf viele Systeme statt einen einzigen Flaschenhals.
- Zusätzliche Kapazität wird bei Bedarf automatisch bereitgestellt.
- Ein einzelner überlasteter Server führt nicht mehr zum Totalausfall.

Wichtig: Reine Skalierung ist ein *Wettrüsten* – gegen sehr grosse DDoS-Angriffe stösst man damit an (teure) Grenzen. Sie wird deshalb meist mit den nachfolgenden Massnahmen kombiniert.

DDoS-Scrubbing / Cloud-Mitigation

Spezialisierte Anbieter (z. B. Cloudflare, Akamai) leiten den gesamten Verkehr durch sogenannte *Scrubbing Center*. Dort wird der Datenstrom in Echtzeit analysiert: Schädlicher Verkehr wird herausgefiltert, nur der «saubere» Verkehr wird an den eigentlichen Server weitergeleitet.

Wie Scrubbing grundsätzlich schützt

- Der Angriffsverkehr trifft die spezialisierte Infrastruktur des Anbieters, nicht den eigenen Server.
- Die Anbieter verfügen über enorme Kapazitäten, die einzelne Betriebe nie vorhalten könnten.
- Angriffsmuster aus vielen Kunden fließen zusammen und werden dadurch früher erkannt.

Kurz: Der Angriff läuft ins Filternetz des Anbieters, bevor er den eigenen Dienst überhaupt erreicht.

Web Application Firewall (WAF)

Gegen Angriffe auf der *Applikationsschicht* (Layer 7, z. B. HTTP-Flood oder Slowloris) hilft eine *Web Application Firewall*. Sie prüft die Anfragen inhaltlich und kann verdächtige Muster erkennen, die eine reine Netzwerk-Firewall nicht sieht.

- Erkennt automatisierte Bot-Anfragen anhand ihres Verhaltens.
- Kann verdächtige Clients mit einer *Challenge* (z. B. CAPTCHA) zu einem Nachweis zwingen, ein echter Mensch zu sein.
- Blockiert bekannte Angriffssignaturen gezielt auf HTTP-Ebene.

Kurz: Keine dieser Massnahmen ist für sich allein ein Freifahrtschein – erst ihre Kombination ergibt einen belastbaren Schutz.

✖ Volkan Demir

From:

<https://wiki.bzz.ch/> - **BZZ - Modulwiki**

Permanent link:

<https://wiki.bzz.ch/modul/m183/learningunits/lu12/03>

Last update: **2026/09/16 15:43**

