# LU12a - DoS/DDoS Grundlagen

## Lernziele

1. Erklären können was eine DoS- bzw. DDoS-Attacke ist und welches grundlegende Ziel diese Attacke hat.
2. Ursachen nennen können, warum DoS/DDoS auch in der Gegenwart ernstgenommen werden muss.

## Einleitung

Die *Denial-of-Service*-Attacke (DoS) gehört zu den ältesten und zugleich wirkungsvollsten Angriffsarten im Internet. Im Gegensatz zu einer SQL-Injection wird dabei nicht versucht, an Daten zu gelangen, sondern einen Dienst schlicht *unerreichbar* zu machen.

*Denial of Service* bedeutet wörtlich *Dienstverweigerung*. Ziel einer DoS-Attacke ist es also, einen Server, einen Dienst oder ein ganzes Netzwerk mit so vielen Anfragen oder gezielt schädlichen Paketen zu überlasten, dass er für legitime Benutzer nicht mehr verfügbar ist.

Wird ein solcher Angriff nicht von einem einzelnen Rechner, sondern *verteilt* von tausenden gekaperten Geräten – einem sogenannten *Botnet* – gleichzeitig ausgeführt, spricht man von einer *Distributed-Denial-of-Service*-Attacke (DDoS). Diese verteilte Form ist deutlich schwerer abzuwehren, da der Datenverkehr von unzähligen echten IP-Adressen stammt.

## Bekannte Attacken

Die nachfolgenden Beispiele zeigen, dass selbst grösste und professionell betriebene Infrastrukturen anfällig für DDoS-Attacken sind.

- Im Oktober 2016 legte das *Mirai*-Botnet den DNS-Anbieter *Dyn* lahm. Da unzählige schlecht gesicherte IoT-Geräte (Kameras, Router) missbraucht wurden, waren zeitweise Dienste wie Twitter, Netflix und Reddit nicht mehr erreichbar.
- Im Februar 2018 wurde *GitHub* mit einer sogenannten *Memcached-Amplification* getroffen. Mit 1.35 Tbit/s war dies zu diesem Zeitpunkt der grösste je gemessene Angriff – die Plattform war dank Schutzmassnahmen jedoch nach wenigen Minuten wieder erreichbar.
- Im Jahr 2023 nutzten Angreifer die *HTTP/2 Rapid Reset*-Schwachstelle aus und erzeugten bei *Google* und *Cloudflare* über 200 Millionen Anfragen pro Sekunde – ein neuer Rekord.

Die eben aufgeführten Beispiele sind nur einige aus einer langen Liste. Man kann also daraus folgern, dass die DoS/DDoS-Bedrohung auch in der Gegenwart ernstgenommen werden muss.

# Ursachensuche für DoS/DDoS-Verwundbarkeit

Obwohl das Grundprinzip dieser Angriffe seit Jahrzehnten bekannt ist, muss man sich fragen warum unsere heutigen Systeme nicht per Default gegen diese Attacken geschützt sind bzw. diese verunmöglichen. Nachfolgend finden Sie die wichtigsten Gründe.

### Offenheit des Internets

Das Internet wurde auf *Erreichbarkeit* und nicht auf *Abschottung* ausgelegt. Ein öffentlich erreichbarer Dienst muss Anfragen von jedem beliebigen Absender entgegennehmen können. Genau diese grundlegende Offenheit macht es so schwierig, bösartige von legitimen Anfragen zuverlässig zu unterscheiden.

## Awareness

Der Mensch ist in seinem Wesen *notwendigkeitsorientiert*. Solange ein Dienst reibungslos läuft, wird die Gefahr eines Angriffs oft unterschätzt («das trifft nur die Grossen»). Schutzmassnahmen werden dadurch häufig erst nach einem ersten Vorfall ernsthaft in Betracht gezogen – sehr bitter, aber wahr.

## Risiken

Im Gegensatz zu einer einzelnen Sicherheitslücke lässt sich ein DoS-Angriff nicht einfach «wegprogrammieren». Aggressive Schutzmassnahmen wie strenge Filter oder Rate-Limits bergen das Risiko, auch legitime Benutzer auszusperren (sogenannte *False Positives*).

Je nachdem wie vital (lebenswichtig) die Verfügbarkeit der Applikation für das eigene Business ist, muss zwischen maximalem Schutz und ungehindertem Zugang für echte Kunden abgewogen werden.

## Kosten

Wirksamer DDoS-Schutz verteuert den Betrieb. Massnahmen wie Cloud-basierte *Scrubbing*-Dienste oder das Vorhalten von überschüssiger Bandbreite kosten laufend Geld. Bei knappen Budgets wird darauf teilweise verzichtet, solange kein unmittelbarer Schaden sichtbar ist. Eine nachträgliche Absicherung während eines laufenden Angriffs wird jedoch meist deutlich teurer.

## Varianten

Das nachfolgende Schaubild zeigt die verschiedenen Varianten/Hauptarten von DoS/DDoS-Angriffen.

Man unterscheidet dabei mehrere Ansätze:

- **Volumetrische Angriffe:** Hierbei wird die verfügbare *Bandbreite* des Ziels mit einer riesigen Datenmenge geflutet (z. B. UDP-Flood oder DNS-Amplification). Die Stärke wird in Bit pro Sekunde (Bit/s) gemessen.
- **Protokoll-Angriffe:** Diese Angriffe zielen auf Schwächen in Netzwerkprotokollen ab, um die Ressourcen von Servern und Firewalls zu erschöpfen (z. B. SYN-Flood oder Ping of Death). Die Stärke wird in Paketen pro Sekunde (Pakete/s) gemessen.
- **Angriffe auf die Applikationsschicht (Layer 7):** Wenn nicht die Leitung, sondern die Anwendung selbst überlastet werden soll, setzen Angreifer auf scheinbar legitime Anfragen. Dabei gibt es zwei typische Vertreter:
  - **HTTP-Flood:** Es werden massenhaft echt wirkende Seitenaufrufe erzeugt, welche den Webserver zwingen, aufwändige Antworten zu berechnen.
  - **Slowloris:** Hier werden viele Verbindungen absichtlich möglichst *langsam* offen gehalten, bis der Server keine neuen Verbindungen mehr annehmen kann.

# Quellennachweis


- Cloudflare - What is a DDoS attack?


---

olkan Demir

---

Volkan Demir