Barrierefreie Version
CSBW-Factsheet: Cybersecurity-Wissen kompakt

Zum Thema: DoS- und DDoS-Attacken

Viele gleichzeitige Anfragen überlasten die Systeme und Server!

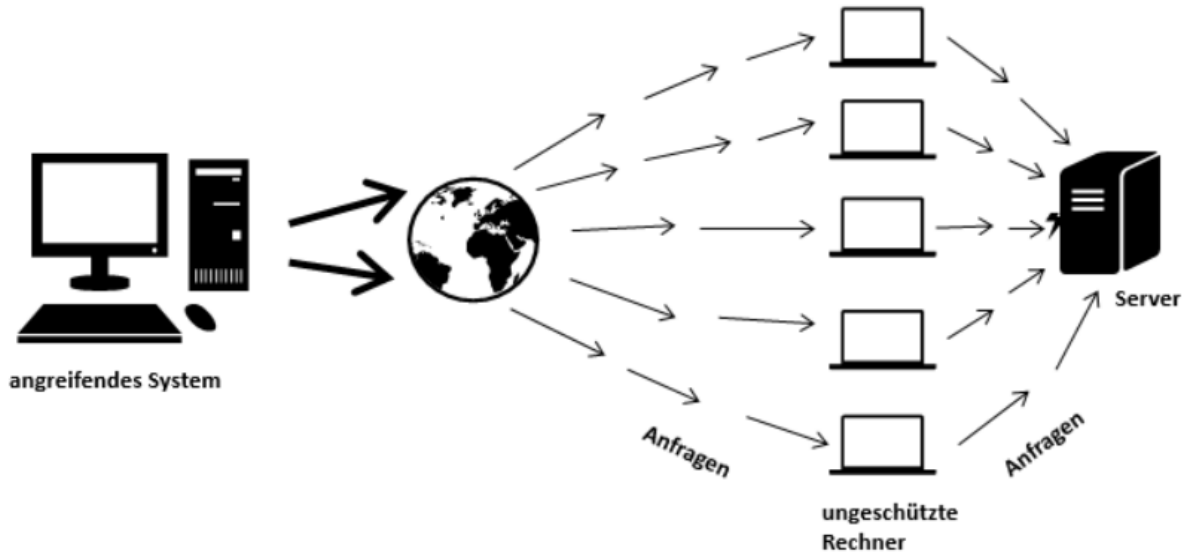
(Distributed) Denial-of-Service-Attacken zählen zu den effektivsten Angriffsmethoden auf Webseiten und Online-Dienste. Bei Erfolg sind die Seiten und Dienste nicht mehr verfügbar, was hohe wirtschaftliche Schäden verursachen kann. Mit den nachfolgenden Informationen lernen Sie die Hintergründe solcher Cyberattacken kennen.

DoS – Denial-Of-Service

auch „Verweigerung des Dienstes“, bedeutet im übertragenen Sinne, dass **etwas unzugänglich gemacht** oder **außer Betrieb** gesetzt wird.

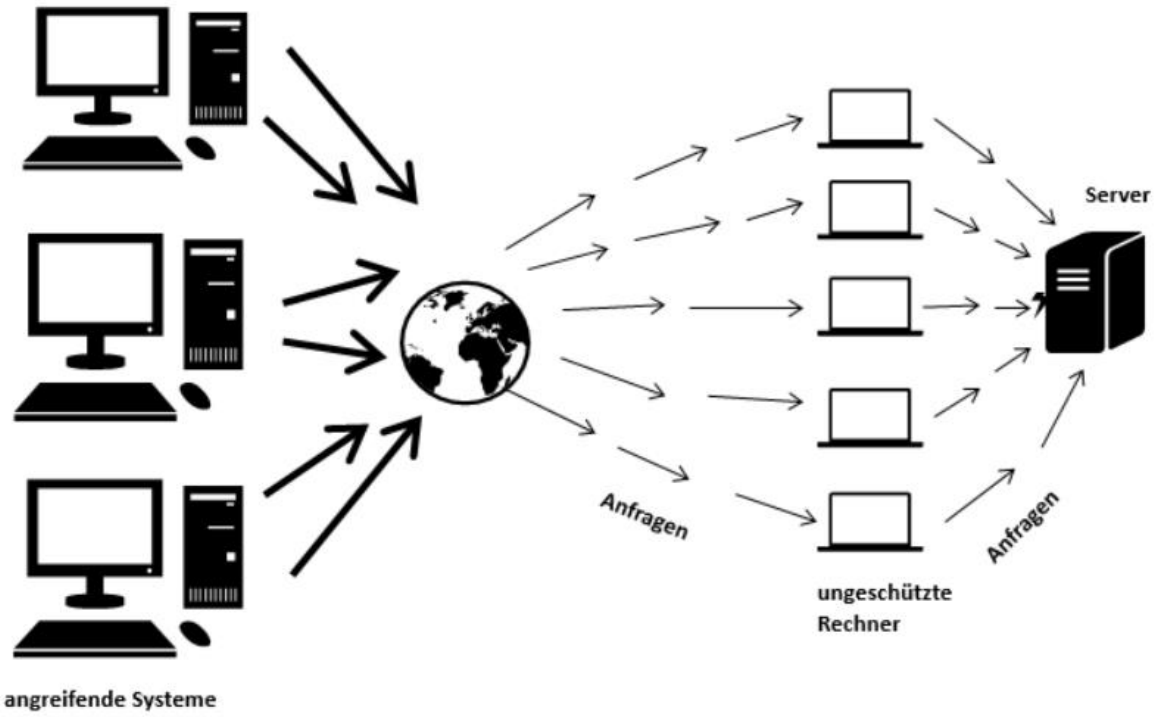
Bei DoS-Attacken werden so viele Anfragen gleichzeitig an die jeweiligen Server geschickt, dass das System mit der Menge an Anfragen überfordert ist und aufgrund dessen zusammenbricht.[1]

Darstellung eines DoS – Denial-of-Service



DDoS – Distributed-Denial-of-Service
werden auch als sogenannte „**verteilte DoS-Attacken**“ bezeichnet. Hierbei kommt anstelle eines einzelnen angreifenden Systems eine Vielzahl von unterschiedlichen angreifenden Systemen zum Einsatz.[1] Dieser Umstand macht DDoS-Attacken besonders effektiv. Als Angriffswerkzeuge werden beispielsweise ungeschützte Rechner genutzt. Diese überhäufen ein bestimmtes Ziel mit so vielen gefälschten Anfragen, dass das angegriffene Zielobjekt überlastet ist und abstürzt.

Darstellung eines DDoS – Distributed-Denial-of-Service



Darstellungen in Anlehnung an BSI [2]

Verfügbarkeit
bezieht sich darauf, dass Webseiten, Daten und Online-Dienste wie vorgesehen zur Verfügung stehen und von den Anwendern genutzt werden können.

Arten von Denial-of-Service-Angriffen:

1. **Syn Flooding:**
   Mit Hilfe einer gefälschten IP-Adresse werden Tausende Anfragen an das Zielsystem geschickt. Dieses versucht alle Anfragen zu beantworten, ist dadurch jedoch überfordert und somit nicht mehr für andere Anfragen zu erreichen.
2. **Ping Flooding:**
   Über Pings kann festgestellt werden, ob ein Rechner im Netz erreichbar ist. Werden an den Zielrechner große Mengen an Pings gesendet, ist dieser durch den Versuch der Beantwortung innerhalb kürzester Zeit überlastet und stürzt ab.
3. **Mailbombing:**
   Versenden einer enorm großen Nachricht in Form einer E-Mail oder das

Überhäufen einer Zieladresse mit Tausenden von Nachrichten bis der Mail-Server abstürzt.

Laut einer repräsentativen Studie des Bitkom e.V. zählen DDoS-Angriffe hinter Malware zu den Hauptangriffsarten, die einen Schaden verursachen.

Quellen:
[1] vgl. BSI - Denial-of-Service (DoS) und Distributed Denial-of-Service (DDoS) (bund.de)
[2] https://www.bsi.bund.de/dok/6599510

Weitere Factsheets und Informationen unter: www.cybersicherheit-bw.de

CSBW – Abteilung 1: Prävention – Stand 05.2023
Kontakt: schulungen@cybersicherheit.bwl.de