# Reaktion auf DoS/DDoS-Angriffe

| | | | | |
|---|---|---|---|---|
| *Dok: Richtlinie* | *Kat: D* | *Version: 1.1* | *Status: Release* | *Stand: 23.01.2026* |
| *Revision fällig am* | *23.01.2027* | | *Durchgeführt am* | *23.01.2026* |
| *Freigabe erteilt am* | *23.01.2026* | | *Erteilt von* | *Andrea Schilling* |

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet.
Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter

## Allgemeines

Diese Richtlinie beschreibt die Regeln der intersaar GmbH zum Umgang mit DoS/DDoS-Angriffe.
Sie richtet sich an Administratoren der intersaar GmbH.

Wird das Auftreten von DoS-/DDoS-Angriffen durch die Erkennung von ungewöhnlichen Verkehrsmustern oder instabilen Betriebszuständen von Telekommunikationseinrichtungen erkannt, werden geeignete Gegenmaßnahmen ergriffen, um den fortlaufenden stabilen Betrieb von Telekommunikationseinrichtungen sicherzustellen.

### Maßnahmen:

Abhängig von der Art der DoS-/DDoS-Angriffe werden die nachfolgenden Maßnahmen ergriffen:

- Filtern von Paketen, die für den angegriffenen Standort bestimmt sind;

- Einschränkung des für DoS-/DDoS-Angriffe verwendeten Kommunikations-Ports;

- Reduzierung oder Aussetzung des Betriebs der anvisierten Telekommunikationseinrichtungen.

Handelt sich bei dem DoS-/DDoS-Angriff um einen Angriff aus dem Netz oder Server eines eigenen Kunden, behält sich die intersaar GmbH das Aussetzen von Telekommunikationsdienstleistungen für den betreffenden Kunden vor, um die DoS-/DDoS-Angriffe auf Telekommunikationseinrichtungen zu unterbinden.

Werden DoS-/DDoS-Angriffe aus dem Netz anderer Telekommunikationsorganisationen heraus durchgeführt, werden diese über den Angriff informiert und aufgefordert, entsprechende Maßnahmen zur Unterbindung zu ergreifen.

Zum eigenen Schutz wird Blackholing eingesetzt.
Ein Blackhole ist ein Präfix, für das der gesamte Zielverkehr verworfen wird.
Blackholing ist eine Sicherheitsmaßnahme, um ein Netzwerk vor einem Distributed Denial of Service (DDoS)-Angriff zu schützen. Mit dieser Methode können Datenpakete an ein bestimmtes Netzwerk fallen gelassen werden, damit sie den Empfänger gar nicht erst erreichen und dessen Ressourcen nicht überlasten. Das angegriffene Netzwerk kann die betroffenen Präfixe als Blackholes ankündigen, indem es die BGP BLACKHOLE Community verwendet. Der Blackhole-Service wird im eigenen Netz und auch in Upstreams verwendet

Zum Schutz vor DDoS Attacken werden Honey-Pots (Honigtöpfe) eingesetzt.
Honey-Pots gaukeln Schwachstellen in Services vor, die von Angreifern ausgenutzt werden können. IP-Adressen der Angreifer werden in einer Honey-Pot Datenbank geführt und vom Datenverkehr ausgeschlossen.

Zum Schutz von Servern und Diensten der Hosting-Umgebung wird das Fail2ban System verwendet. Fail2ban ist ein Sicherungssystem, das Brute-Force-Angriffe erkennt und abwehrt.
In der den Servern vorgeschalteten Firewall werden nur benötigte Ports freigegeben und ein GEO-IP Filter eingesetzt, um Angriffs-Pattern auf benötigte geographische Regionen zu begrenzen.
Als vorbeugende Maßnahme werden weltweit verteilte CDN-Proxyserver verwendet.
Angriffe erfolgen dann auf den geographisch nächsten Proxy anstatt des Ziel-Systems des Angriffs.

Die zu verwendenden Maßnahmen werden vom zuständigen Administrator bestimmt und durchgeführt. Kann er den Vorfall nicht allein beheben wird der ISB hinzugezogen.

Der Angriff ist als Informationssicherheitsvorfall zu dokumentieren.
Die getroffenen Maßnahmen sind zu dokumentieren und an den ISB zu berichten.