

DoS/DDoS-Angriffe sind kein reines Netzwerkproblem. Sie gefährden die Verfügbarkeit geschäftskritischer Prozesse und können zeitgleich Webseiten, Portale, Mailserver, DNS, VPN-Zugänge sowie APIs lahmlegen. Um sowohl DDoS- als auch DoS-Angriffen wirksam zu begegnen, benötigen Unternehmen eine ganzheitliche und zukunftsorientierte Strategie, die technische und organisatorische Maßnahmen miteinander verbindet.

## Organisatorische Maßnahmen gegen DoS/DDoS-Angriffe

- Identifizierung von möglichen Zielen / Systemen
- Festlegung von internen Verantwortlichkeiten für die identifizierten Systeme
- Klärung der Kommunikationswege mit dem Provider (Erreichbarkeit, Ansprechpartner und Notfallnummern)
- Definition und Ausarbeitung von Checklisten und Prozessen für DDoS Angriffsfälle
- Schulung und Sensibilisierung der verantwortlichen Mitarbeiter

## Technische Maßnahmen gegen DoS/DDoS-Angriffe

- Bereitstellung von Analysetools, die direkt verfügbar sind
- Netzwerksegmentierung, um Auswirkungen auf die Gesamt-IT abmildern zu können
- Absicherung der Netzwerkinfrastruktur (z.B. Proxys oder Loadbalancer einsetzen, Traffic Shaping)
- Identifikation der Leistungsgrenzen im Vorfeld, dabei aktuelle und künftige Kapazitätsgrenzen berücksichtigen
- Konfiguration und Härtung der relevanten Systeme auf Dienst- und Serverebene
- Einsatz von DDoS-Abwehrmechanismen (Softwarelösungen, Apps)



## Prävention und Abmilderung

- Ein konsequentes **Patch- und Update-Management**
- **Regelmäßige Schwachstellenscans** und zeitnahe Behebung erkannter Sicherheitslücken
- Einsatz von **sicheren Passwort- und Zugriffskonzepten** und **Anti-Malware-Lösungen**
- **Web Application Firewalls** mit aktuellen Regelwerken und Zugriffskontrolllisten
- Kontinuierliches Monitoring des Datenverkehrs

### So finden Sie uns