Landesamt für Sicherheit in der Informationstechnik

# Leitfaden zur Abwehr von Distributed Denial of Service (DDoS) - Angriffen

Stand: 18.08.2023
Version: 1.0

Landesamt für Sicherheit in der Informationstechnik
Keßlerstraße 1
90489 Nürnberg
beratung-kritis@lsi.bayern.de
Telefon: 0911 21549-525

Denials of Service (DoS)-Angriffe zielen darauf ab, die Verfügbarkeit von Diensten, die über das Internet nutzbar sind, zu beeinträchtigen oder Dienste vollständig außer Betrieb zu setzen. Bei einem DDoS-Angriff (Distributed Denial of Service) handelt es sich um die verbreitetste Art der DoS-Angriffe.

Bei einem DoS-Angriff wird das den Dienst anbietende IT-System oder ein Netzwerk-Bereich mit teils schädlichem Datenverkehr so überlastet, dass dieser Dienst für einen längeren Zeitraum nicht mehr verfügbar ist.

Ein DDoS-Angriff erfolgt meistens gleichzeitig von vielen Geräten - oft automatisiert gesteuert, mit Hilfe sogenannter Bots. Diese Bots sind bereits im Vorfeld mit Malware infizierte Geräte, bei denen der Angreifer die Kontrolle über jedes einzelne betroffene System erlangt hat. Die Gefahr beim DDoS liegt in der schieren Masse an infizierten Geräten. Mittels simultaner Anfragen kann diese zahlenmäßige Stärke genutzt werden, um effektiv DDoS-Angriffe durchzuführen.

Durch DDoS-as-a-Service Angebote, können auch Angreifer, die nicht über die technische Expertise oder das Equipment verfügen, DDoS-Angriffe mit fast beliebigem Volumen und beliebiger Dauer bestellen. Um deren Wirksamkeit zu demonstrieren, werden von den Anbietern häufig Try-and-Buy Aktionen angeboten, z.B. 5 Minuten Angriffsdauer mit 10Gbps schädlichem Angriffsvolumen.

Es gibt verschiedene Arten von DDoS-Angriffsszenarien, die jeweils auf unterschiedliche Bestandteile eines Computernetzwerkverbundes abzielen. Konkret lassen sich diese Angriffe in drei Kategorien einteilen:

## Volumetrische Angriffe

Das Ziel von volumetrischen Angriffen ist es, die maximal verfügbare Bandbreite eines Netzwerkes zu erschöpfen, sodass dadurch die Zielanwendung oder der Service von legitimen Nutzern nicht mehr verwendet werden kann. Hierzu werden Botnetze und häufig auch Schwachstellen bei dritten Systemen (z.B. offene DNS-Server) genutzt, um massiv Datenverkehr zu erzeugen und so die verfügbare Bandbreite des Zielnetzwerks zu überlasten.

Beispielsweise können Verbindungsversuche mit gespoofter Absenderadresse (des Opfers) gestartet werden, die von Drittsystemen mit einem Vielfachen des ursprünglichen Datenvolumens beantwortet werden.

Volumetrische Angriffe sind schwer zurückzuverfolgen oder rechtzeitig zu erkennen, da der erzeugte Datenverkehr vom legitimen Datentraffic oft nicht zu unterscheiden ist.
Beispiele für volumetrische Angriffe: DNS-Amplifikation, UDP-Flooding, ICMP- oder Ping-Flooding, RST-FIN-Flood

## Protokoll-Angriffe

Protokoll-Angriffe zielen darauf ab, die Rechenkapazität verschiedener Netzwerkinfrastruktur-ressourcen wie zum Beispiel Server oder Firewalls zu erschöpfen. Hierzu werden die Ressourcen mit Protokollanfragen, die sehr große Antworten provozieren oder fehlerhaft sind, so überlastet, dass alle verfügbaren Ressourcen des Angriffsziels belegt sind. Dies kann unter anderem zu Abstürzen oder stark verlangsamtem Datenfluss führen.

Beispiele für Protokoll-Angriffe: Ping of Death, SYN-Flood, Tsunami-SYN-Flood, Connection Exhaustion, Smurf-Angriffe

## Angriffe auf der Anwendungsebene

Angriffe auf der Anwendungsebene sind darauf ausgelegt, die Anwendung selbst mithilfe von schädlichen Anfragen zur Ausnutzung von aktuell vorhandenen (noch ungepatchten) System-schwachstellen anzugreifen.

Im Gegensatz zu volumetrischen und Protokoll-Angriffen benötigt dieser Angriff weniger Ressourcen, um Funktionen oder Merkmale einer Anwendung zu stören. Wie bei den volumetrischen Angriffen wird auch hier legitimes Benutzerverhalten nachgeahmt, was diese Angriffsart teilweise schwer erkennbar macht.

Beispiel für Angriffe auf der Anwendungsebene: Angriffe auf HTTP/S

Die beste Verteidigung ist eine Mitigation d.h. der Versuch der Reduzierung des Angreifer-Verkehrs möglichst nah an seinem Ausgangspunkt und möglichst ohne Beeinträchtigung des anderen (legitimen) Verkehrs. In der Praxis kann die Mitigation nicht immer ganz ohne Beeinträchtigungen für legitime Nutzer erfolgen.

Der folgende Abschnitt beschreibt, wie man sich und seine Organisation bestmöglich vor Angriffen schützen kann und enthält Tipps, welche Maßnahmen man treffen kann, bestmöglich auf einen DDoS-Angriff vorbereitet zu sein. Zu Beginn werden jene Maßnahmen erläutert, welche in der Organisation selbst, **mit eigenen Ressourcen** umgesetzt werden können. Im Anschluss werden Möglichkeiten aufgeführt, die eine **Unterstützung durch externe Dienstleister** erfordern. Hierfür ist entscheidend, wo und wie die Server betrieben werden (on-premise im eigenen Unternehmen oder extern gehostet bei einem Dienstleister).

# Eigene Schutzmaßnahmen

## Interne Verantwortlichkeiten festlegen

- Bestimmen Sie eine Person, die für die Absicherung gegen DDoS-Angriffe verantwortlich ist und diese Maßnahmen organisiert. Dies kann beispielsweise der IT-Sicherheitsbeauftragte (ISB) oder der IT-Leiter sein.
- Für die eigentliche Absicherung ist die Mithilfe von Systemadministratoren, Netzwerkspezialisten, etc. erforderlich.
- Auch Entscheidungsbefugte z.B. die Organisationsleitung, Abteilungsleitung müssen mit einbezogen werden.
  - Einerseits müssen Ressourcen wie Geld und Arbeitszeit bewilligt werden.
  - Andererseits müssen Entscheidungsbefugte Wissen über die Thematik besitzen, um im Falle eines Angriffes zügig Entscheidungen, beispielsweise über die Abschaltung von Systemen, treffen zu können.

## Potenzielle Angriffsziele identifizieren und Schutzbedarf festlegen

- Auf Basis bestehender Dokumentation müssen mögliche Angriffsziele identifiziert werden.
- Hierbei ist es wichtig, nicht nur on-premise Infrastruktur zu betrachten, sondern auch diejenigen Dienste mit einzubeziehen, welche bei externen Dienstleistern gehostet sind.
- Potenzielle Angriffsziele sind typischerweise Webserver. Aber auch Angriffe auf andere Dienste, wie beispielsweise Backend-Systeme oder VPN-Server, sind möglich.
- Zu jedem potenziellen Angriffsziel muss der Schutzbedarf festgelegt werden und inwieweit eine Beeinträchtigung der Verfügbarkeit akzeptiert werden kann.

## Ermittlung der Leistungsgrenzen

- Bei den identifizierten, potenziellen Angriffszielen sind die Leistungsgrenzen der Systeme zu ermitteln. Diese sind durch die verwendete Hardware begrenzt und ggf. zusätzlich durch Software weiter eingeschränkt. Hierbei sind unbedingt auch die Leistungsgrenzen der zugrunde liegenden Netzwerkinfrastruktur zu berücksichtigen.
- Anhand der so identifizierten Leistungsgrenzen müssen Schwellenwerte definiert werden, ab wann reaktive Maßnahmen eingeleitet werden sollen.

- Ein DDoS-Angriff stellt eine Ausnahmesituation dar, eine gute Vorbereitung ist daher unerlässlich, um diese Situation gut zu bewältigen. Hierbei empfiehlt es sich, Notfallprozesse zu erstellen und diese anschließend zu testen.

- Alternativen vorbereiten: abgespeckte (statische) Webseite bei einem externen Webhoster vorbereiten und eine Umleitung dorthin in die Notfallprozesse und Testszenarien einbeziehen.

## Anpassung der eigenen Infrastruktur an die Anforderungen

- Es ist zu prüfen, ob die eigene Infrastruktur den Anforderungen in Bezug auf DDoS-Angriffen gewachsen ist. Hier sollten unter anderem die Erkenntnisse aus Kapitel „Ermittlung der Leistungsgrenzen“ einfließen.

## Netzwerksegmentierung überprüfen/einrichten

- Die Segmentierung eines Netzwerks in verschiedene Zonen hilft, Kollateralschäden zu vermeiden: Im Falle einer noch nicht optimalen Netzwerksegmentierung kann ein Angriff auf einen Webserver zur Beeinträchtigung weiterer Systeme im selben Netzwerksegment führen.

  Es ist daher ratsam, eine Netzwerksegmentierung durchzuführen um den Ausfall möglichst einzugrenzen.

## Härtung und Konfiguration

- Bereits bei der Konfiguration des Servers sollte darauf geachtet werden, Angriffen möglichst wenig Angriffsfläche zu bieten.

- Unnötige Dienste sollten nicht installiert oder deaktiviert werden.

- Falls mehrere von extern, erreichbare Dienste zusammen auf einem Server laufen, können diese auf mehrere Server verteilt werden. Durch den Verteilungseffekt lässt sich ggf. auch der Schutzbedarf reduzieren.

- Bereits vorhandene produkteigene Funktionen können konfiguriert werden, um Angriffs- und Lastsituationen abzumildern oder zu vermeiden (z. B. durch Beschränken der Anzahl der IP-Verbindungen pro IP-Adresse).

## Patchmanagement

- Identifizierte DDoS-Schwachstellen müssen schnellstmöglich aktualisiert werden.
- Veraltete Komponenten, für die keine Sicherheitsupdates mehr bereitgestellt werden, können Schwachstellen enthalten, die nicht mehr behoben werden. Solche Systeme sollten nicht mehr in Betrieb und schon gar nicht aus dem Internet erreichbar sein. Ein Weiterbetrieb solcher Systeme ohne entsprechende Schutzmaßnahmen ist grob fahrlässig.

## Monitoring und Protokollierung

- Ein Monitoringsystem sollte eingeführt werden, um einen Überblick zu erhalten, wo bereits mögliche Überlastungen von Servern oder Netzwerkgeräten vorliegen.
- Aus dem Internet erreichbare Systeme müssen permanent überwacht werden, ob Dienste von außen erreichbar sind.
- Die Leistungsdaten sollten an einer zentralen Stelle protokolliert und ausgewertet werden.
- Dieses Monitoringsystem sollte insbesondere die Schwellenwerte überwachen (z. B. freie Kapazitäten von CPU, Arbeitsspeicher, Netzwerkbandbreite), um bei einer Überlastung schnell reagieren zu können. Diese Schwellwerte müssen vorab definiert werden.
- Bei einem DDoS-Angriff können die Details eines Angriffs oft erst im Nachgang analysiert werden. Hierzu sollten Logdaten und ggf. Mitschnitte kontinuierlich gesammelt und gesichert werden. Hierzu muss ausreichend Platz und Übertragungskapazität bereitstehen.

## Perimeter-Netzwerk-Schutz optimieren:

- Um die Auswirkungen des DDoS-Angriffs zu begrenzen, kann im Angriffsfall auf Basis von Access-Listen gefiltert werden nach:
  - Quelladressen
  - Zieladressen
  - Zielports
  - etc.

  Es ist zu beachten, dass bei oben beschriebenen Filterungen, potentiell auch legitime Aufrufe geblockt / verworfen werden können.

- Folgende Konfigurationen an der Firewall können helfen, den Angriff abzuschwächen und die Verfügbarkeit aufrecht zu erhalten:
  - DDoS-Prävention aktivieren
  - Verwendung einer strengeren Wartezeit für halboffene Verbindungen
  - Löschen falsch-formatierter und gefälschter Datenpakete
  - Festlegen niedrigerer Drop-Schwellenwerte für SYN, UDP und ICMP
  - Geo-IP-Blockierung

## Netzwerkinfrastruktur absichern:

Folgende Komponenten helfen die Netzwerkinfrastruktur zu sichern und diese somit robuster gegen (D)DoS-Angriffe zu machen:

- Reverse Proxy / Loadbalancer
  - Vorgeschaltet vor Zielserver, fängt Anfragen von Angreifern ab
  - Verteilt Traffic gleichmäßig auf Server, verhindert einzelne Überlastung
  - IP-Adressen der internen Server bleiben verborgen
  - mehrere Webserver mit abgespeckter Webseite anschalten (im Bedarfsfall)
- Web-Application-Firewall
  - Schützt auf Anwendungsebene vor bestimmten Arten von DDoS-Angriffen wie HTTP-REQUEST, HTTP GET- und HTTP POST-Floods
- DDoS-Mitigation-Appliance
  - Marktverfügbare Lösung mit entsprechenden DDoS-Erkennungs- und -Abwehrmaßnahmen
  - Basiert auf adaptiver, verhaltensbasierter Echtzeit-Signaturtechnologie
  - Lässt sich an eigene Bedürfnisse anpassen
  - Bietet trotzdem keinen vollständigen Schutz, z.B. vor massiven volumetrischen Angriffen

## Test der Schutzmaßnahmen:

Um im Ernstfall die Wirkung der Mitigations-Maßnahmen sicherzustellen bzw. deren Auswirkungen auf die legitimen Nutzer möglichst gering zu halten, sollten regelmäßige Tests der Schutzmaßnahmen durchgeführt werden. Dies gilt auch im Falle der Beauftragung eines Dienstleisters (z.B. externes Hosting oder „DDoS Mitigation Service“). Hier sind entsprechende Testszenarien abzustimmen.

# Unterstützung durch externe Dienstleister

Es gibt unterschiedliche Möglichkeiten, die Unterstützung durch externe Dienstleister zu nutzen. Dies hängt jedoch von der Art und Weise ab, wo und wie die Sever betrieben werden: **on-premise im eigenen Unternehmen** oder **extern gehostet bei einem Dienstleister**.

## Internes Hosting

Wenn die Server on-premise, d.h. im eigenen Unternehmen betrieben werden, kann der **DDoS-Mitigation-Service** des **Internet Service Provider (ISP)** genutzt werden.

- Bei einer Überlastung der Bandbreite des Unternehmens ist das Mitwirken des ISP für eine Umleitung des DDoS-Angriffs-Traffics essentiell.

- Folgende Daten des ISP sollten bekannt und an zentraler Stelle hinterlegt sein:
  - Ansprechpartner
  - Notfallnummern
  - Erreichbarkeiten
  - Kundennummer, bei Bedarf Sicherheitskennwort

- Folgende Serviceangebote sind zu prüfen und ggf. vertraglich zu vereinbaren;
  - Erhöhung der Bandbreite
  - Umleitung des Datenverkehrs
  - DDoS-Mitigation-Services des ISP
  - Reaktionszeit des ISP

## Externes Hosting

Wenn die Server (komplett oder teilweise) bei einem **Cloudanbieter** ausgelagert sind, können bei diesem in der Regel zusätzliche **DDoS-Mitigation-Services** zugebucht werden (Bild 1).

- Cloudanbieter verfügen in der Regel über eine große Gesamtkapazität und somit eine gewisse Resistenz gegenüber DDoS-Angriffen.
- Die Services und SLA des Cloud-Anbieters sind hoch standardisiert und enthalten in der Regel auch zubuchbare Angebote zur Abwehr von DDoS-Angriffen.

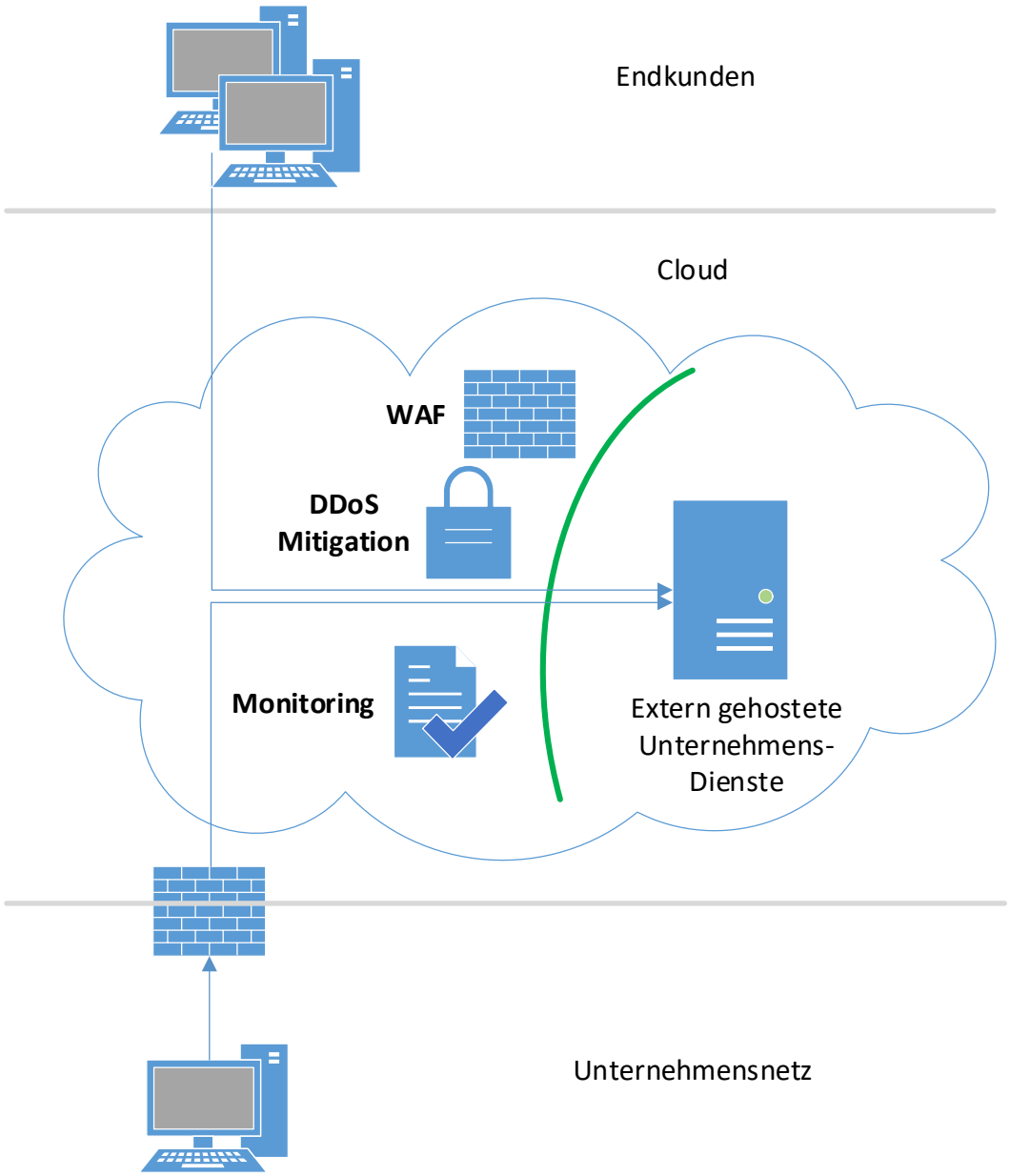


Bild 1 - DDoS-Mitigation-Services bei externem Hosting

## DDoS-Mitigation-Services

### Content Delivery Network (CDN)

- Bei einem CDN handelt es sich oft um ein über mehrere Standorte und oft über mehrere Backbones verteiltes Netzwerk des CDN-Anbieters.
- Die abrufbaren Inhalte werden auf mehreren Replica-Servern gespiegelt. Durch die Regionalisierung der Client-Anfragen ergibt sich eine geringere Last und schnellere Zugriffszeiten pro Instanz (Bild 2).
- Beim Betriebsmodell „Externes CDN in der hybriden Cloud“ (Bild 3) werden Server weiterhin im eigenen Netzwerk lokal (on-premise) betrieben und gleichzeitig werden im externen CDN gespiegelte und gecachte Informationen bereitgehalten. Bei Nicht-Verfügbarkeit des lokalen Ursprungsservers aufgrund eines laufenden DDoS-Angriffs werden über den „read only Cache“ im CDN die Lese-Verfügbarkeit der Inhalte sichergestellt.

## Content Delivery Network (CDN)

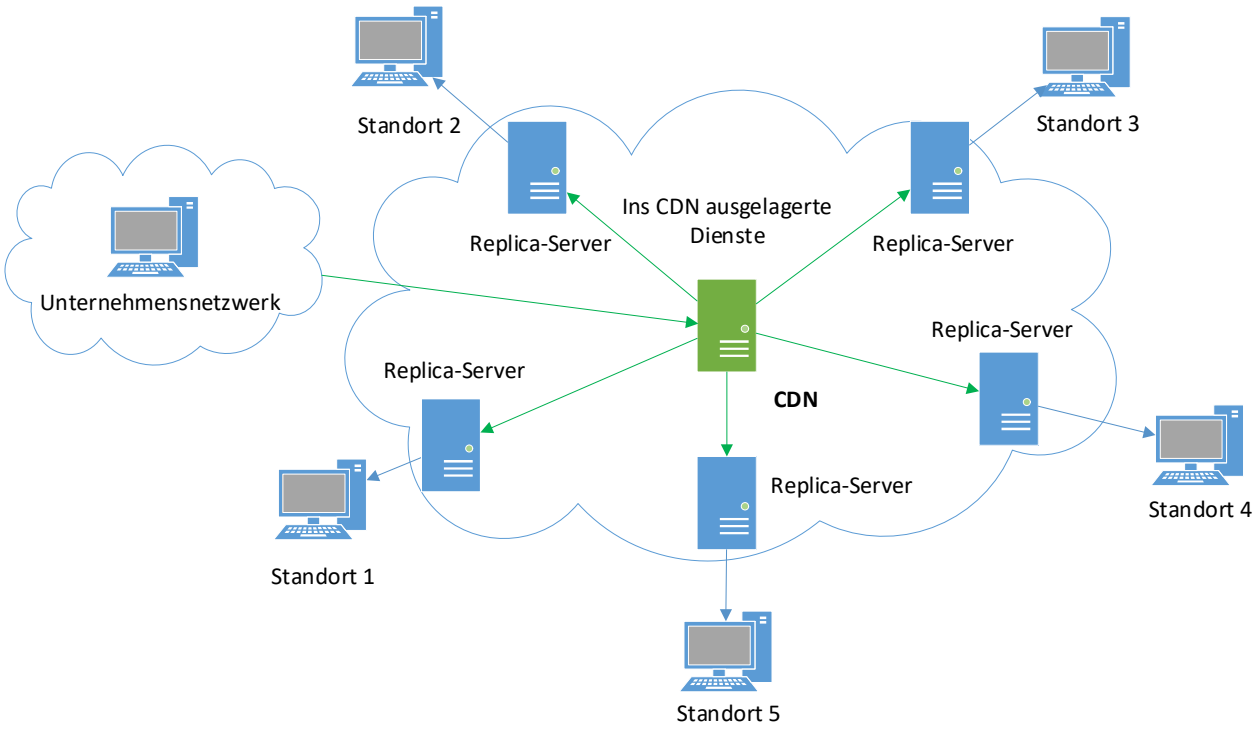


Bild 2 – Nutzung eines externen CDNs in einer Public-Cloud Umgebung, Unternehmen hat eigene Dienste an Server im CDN ausgelagert

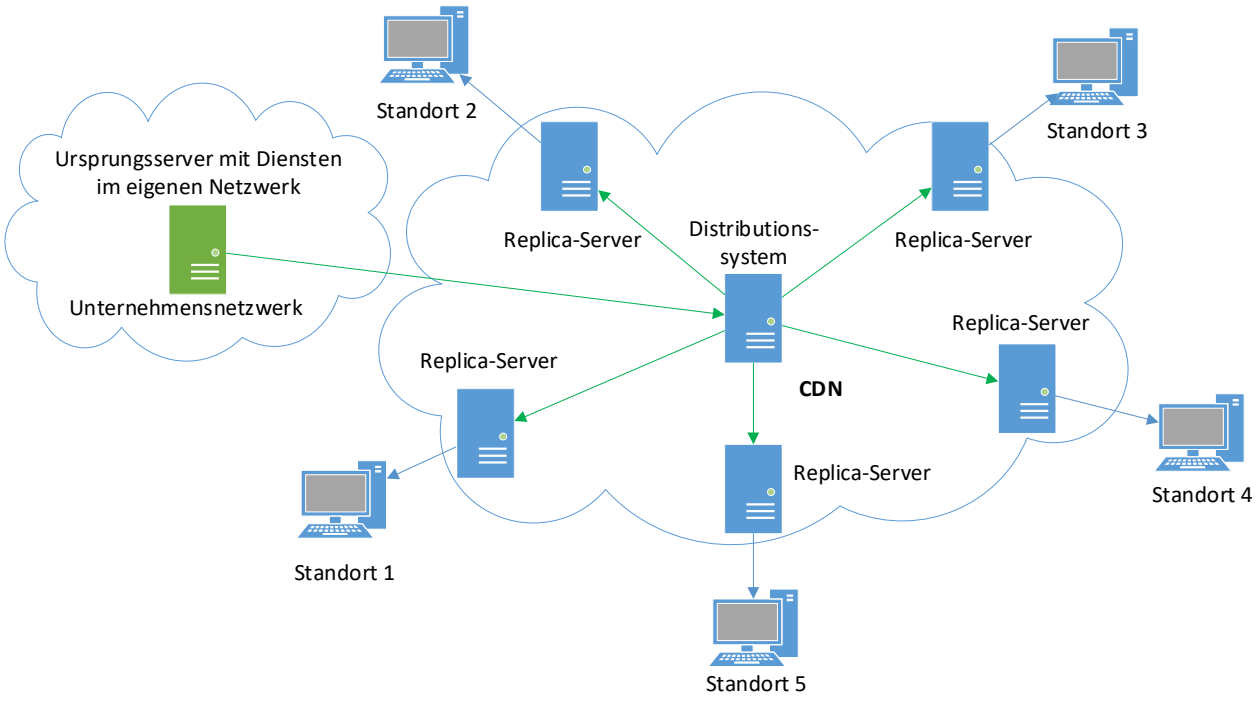


Bild 3 – Nutzung eines externen CDNs in einer hybriden Cloud-Umgebung

## Scrubbing Center

Der „Scrubbing Center“ kann als Dienstleistung vom ISP, dem Cloudanbieter oder einem DDoS-Mitigation-Dienstleister bereitgestellt werden und bietet Schutz für alle Anwendungen, Ports und Protokolle, einschließlich Web- und IP-basierter Services im Rechenzentrum.

- Unternehmen leiten ihren Netzwerktraffic an die Scrubbing-Infrastruktur des Abwehranbieters. Der Traffic wird überwacht, auf schädliche Aktivitäten gefiltert und der gesäuberte Verkehr wird an den Server weitergeleitet (Bild 4 und Bild5).
- Die Umschaltung des Datenverkehrs ins Scrubbing-Center kann sowohl manuell als auch automatisiert erfolgen.

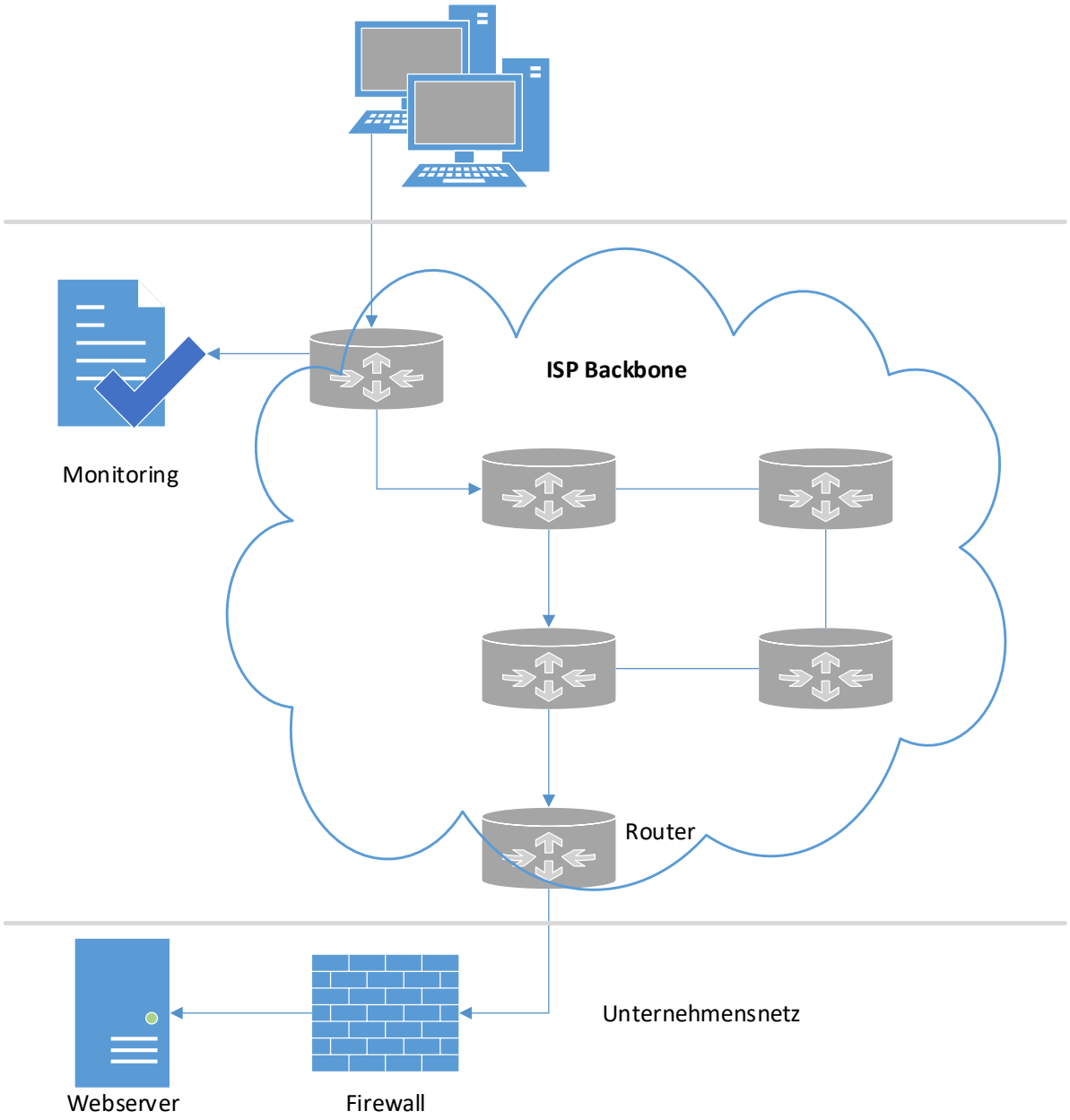


Bild 4 – Der Traffic wird vom ISP überwacht.

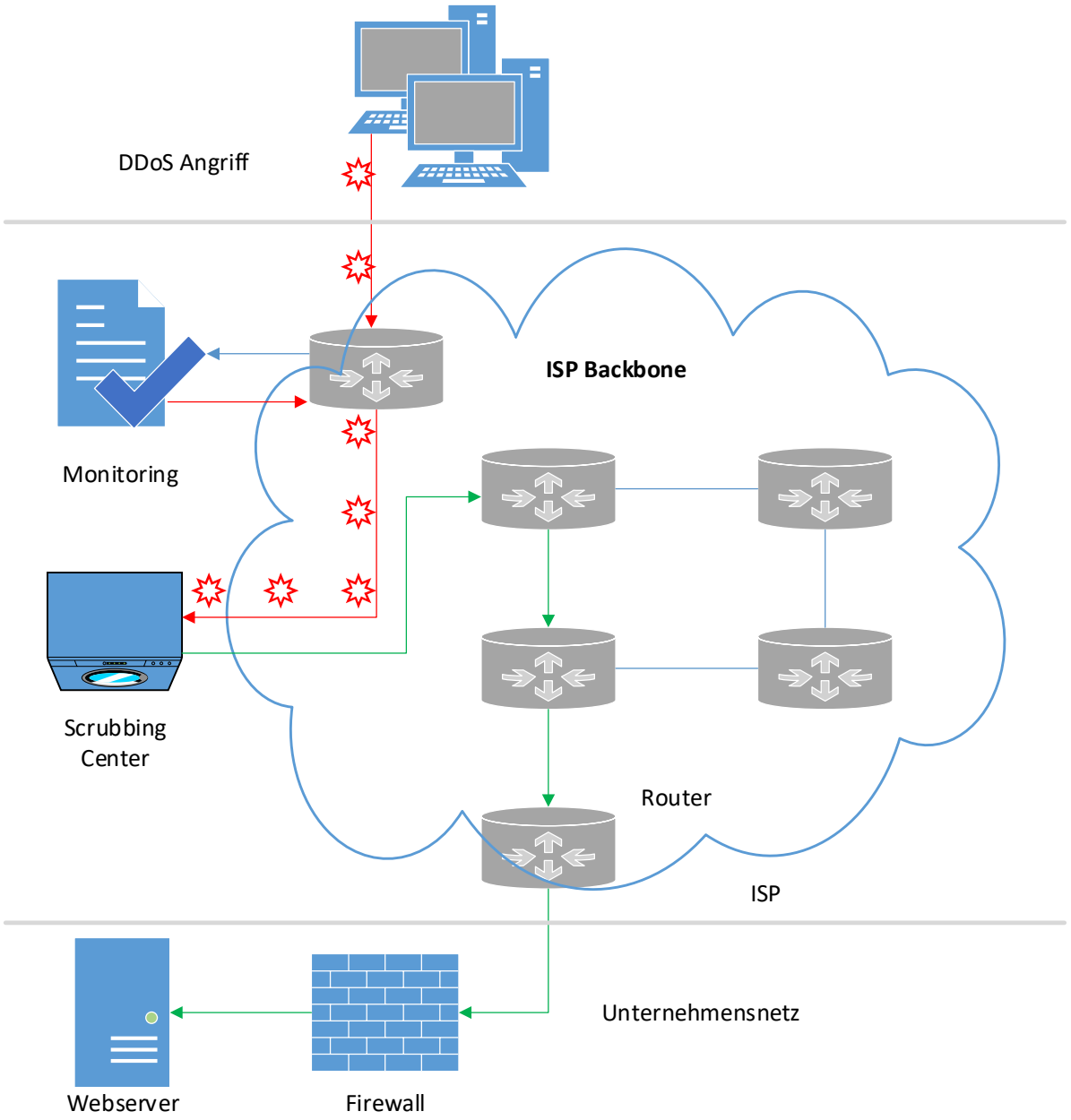


Bild 5 – Bei einem DDoS Angriff wird der Traffic ins Scrubbing-Center umgeleitet.

### ☐ Krisenreaktionsteam bilden

Um schnellstmöglich auf einen DDoS-Angriff reagieren zu können, sollte ein Krisenreaktionsteam, bestehend aus Organisationsleitung, dem IT-Sicherheitsbeauftragten, dem IT-Sicherheitsteam, erfahrenen IT-Mitarbeitern und Vertretern der Presse- und Öffentlichkeitsarbeit, gebildet werden. Das Krisenreaktionsteam leitet und koordiniert alle notwendigen Maßnahmen zur Behandlung des DDoS-Angriffs.

### ☐ Management/Geschäftsführung über DDoS-Angriff informieren

Das Management bzw. die Geschäftsführung ist, entsprechend Ihrer internen Richtlinien zur Behandlung und Eskalation von IT-Sicherheitsvorfällen, über den DDoS-Angriff zu informieren.

### ☐ Internet-Service-Provider (ISP) einbinden

Ihr ISP bzw. Hosting-Provider sollte frühzeitig eingebunden werden. Dieser kann Ihnen unterstützend zur Seite stehen. Informationen, wie Ihr ISP Sie bereits im Vorfeld zum Schutz vor einem DDoS-Angriff unterstützen kann, finden Sie unter dem Punkt „Unterstützung durch externe Dienstleister".

### ☐ Protokollierung

Bei einem DDoS-Angriff können die Details eines Angriffs oft erst im Nachgang analysiert werden. Hierzu sollten Logdaten und ggf. Mitschnitte zeitnah gesammelt und gesichert werden.

### ☐ Mitigation aktiv halten

Die Angriffe verlaufen oft in mehreren Wellen, wobei Angreifer die benutzten Angriffsvektoren unter Umständen ändern oder ergänzen. Deshalb ist es meist sinnvoll aktivierte Mitigationen noch einige Zeit nach einem erfolgten Angriff präventiv aktiviert zu halten.

### ☐ Aufmerksamkeit

DDoS-Angriffe dienen manchmal auch nur dazu die Aufmerksamkeit abzulenken. Dadurch fallen andere Hacker-Aktivitäten (z.B. kurz vorher begonnene Phishing- oder Ransomware-Angriffe) manchmal weniger oder erst verzögert auf.

### ☐ Nachbereitung

Nach einem DDoS Angriff sollten die Auswirkungen stets analysiert und bei Bedarf die vorbereiteten Gegenmaßnahmen geschärft werden, um den nächsten Angriff robuster zu überstehen.

**Als Behörde, Kommune, öffentliches Unternehmen im Bereich kritischer Infrastrukturen oder Unternehmen mit mehrheitlicher Beteiligung des Freistaats Bayern kann Sie das Bayern-CERT im LSI unterstützen (cert@bayern.de, 0911 21549 999).**

## Checkliste: Was tun bei einem DDoS-Angriff?

☐ **Strafanzeige bei der Polizei stellen**

Das LSI empfiehlt generell die **Anzeige** eines Cyberangriffs bei der Polizei.

Sollten Sie eine Strafanzeige gegen die Angreifer in Erwägung ziehen, entstehen besondere Anforderungen an eine angemessene Beweismittelsicherung.

Hierzu unterstützt sie die **Zentrale Ansprechstelle Cybercrime (ZAC)** der bayerischen Polizei.

- ➔ Telefon: 089/1212-3300
  (Bürozeiten:
  Mo-Do 08:00 – 16:00 Uhr und
  Fr 08:00 – 14:00 Uhr)
- ➔ Telefon außerhalb der Bürozeiten: Polizeinotruf 110
- ➔ Webauftritt: https://www.polizei.bayern.de/kriminalitaet/internetkriminalitaet/002464/index.html

Informieren Sie Ihren zuständigen Datenschutzbeauftragten über den Vorfall, falls der Verdacht besteht, dass personenbezogene Daten entwendet wurden.

☐ **Pressemitteilung vorbereiten**

Für mögliche Presseanfragen sollte eine Pressemitteilung mit Informationen zum DDoS-Angriff bereits im Vorfeld vorbereitet werden, um so Pressevertreter schnell informieren zu können, dass bereits Maßnahmen getroffen werden. Im **IT-Notfallmanagement-Paket** des LSI finden Sie diese und weitere Arbeitshilfen. zur IT-Notfallvorsorge und -bewältigung.

☐ **Kunden/Öffentlichkeit informieren**

Informieren Sie zeitnah Ihre Kunden, Vertragspartner und, falls für Sie sinnvoll, die Öffentlichkeit über mögliche Einschränkungen der Verfügbarkeit. Hierzu sollten die Informationskanäle bereits im Vorfeld klar definiert und Kontaktlisten aktuell gehalten werden.

**Für weitere Informationen steht Ihnen das Beratungsteam des LSI für Kritische Infrastrukturen gerne zur Verfügung.**

- ➔ **E-Mail: beratung-kritis@lsi.bayern.de**
- ➔ **Telefon: 0911 21549-525**

**Die Beratung für Kommunen erreichen Sie über:**

- ➔ **E-Mail: beratung-kommunen@lsi.bayern.de**
- ➔ **Telefon: 0911 21549-523**