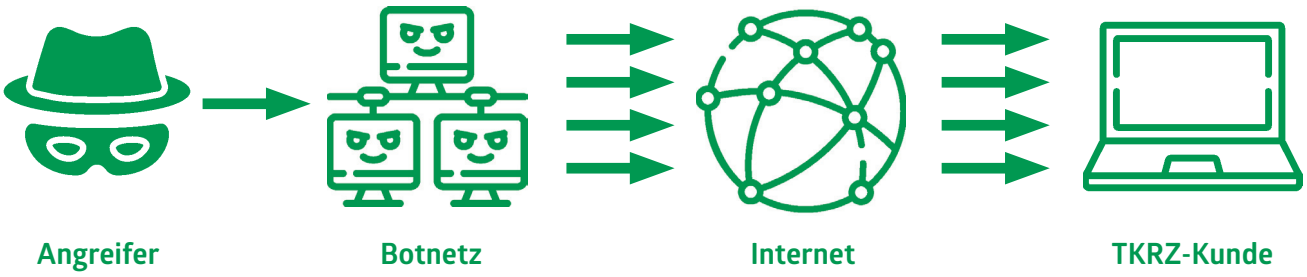
TKRZ DDOS-PROTECTION
Produktinformationen

DDOS-ANGRIFFE (Distributed Denial of Service)

Unternehmen und öffentliche Einrichtungen sind in letzter Zeit immer häufiger Ziel sogenannter DDoS-Angriffe. Dabei spielt es keine Rolle, ob die Betroffenen eine komplexe eigene IT-Infrastruktur betreiben oder die Dienste eines Rechenzentrums nutzen. Durch DDoS-Attacken versuchen Angreifer, die Anschlüsse ihre Opfer offline zu nehmen und so einen (wirtschaftlichen) Schaden zu erzeugen.

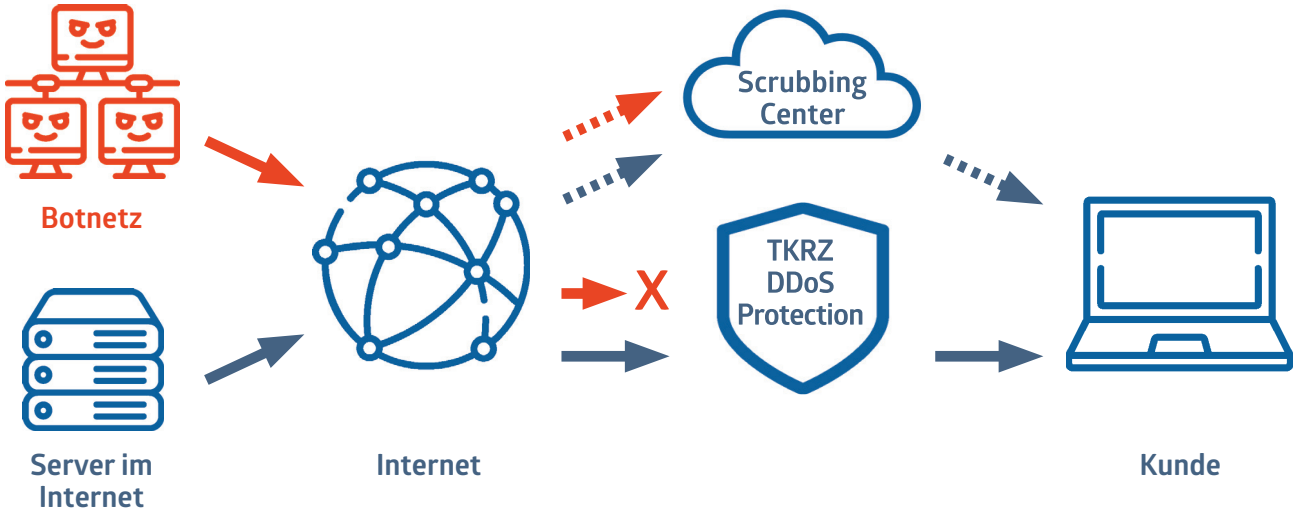
Über Botnetze werden sehr große Mengen an gefälschten / illegitimen Anfragen an die IP-Adressen des Opfers gesendet und so eine gezielte Überlastung der Anschluss-Bandbreite oder der dahinterliegenden Geräte wie Router oder Firewalls verursacht.

Dies hat zur Folge, dass der reguläre, legitime Datenverkehr nicht mehr zugestellt werden kann und der Anschluss somit nicht mehr nutzbar ist.



TKRZ DDOS-PROTECTION

Die Abwehr von DDoS-Angriffen erfolgt bereits an den Grenzen des TKRZ-eigenen Backbone-Netzes. Durch ein mehrstufiges Verfahren von Erkennungs- und Mitigationssystemen können sowohl einfache Angriffe wie z.B. DNS / NTP Amplification als auch komplexe Attacken mit sich schnell verändernden Vektoren abgewehrt werden.



TKRZ DDOS-PROTECTION
Produktinformationen

SCHUTZ IHRES INTERNET-ACCESS GEGEN DDOS-ANGRIFFE MIT HILFE FOLGENDER VERFAHREN

- Nutzung der von BSI und BNetzA emfohlenen Systeme der Hersteller Netscout/Arbor und F5 Networks
- Erkennung von DDoS-Angriffen durch permanente Analyse von Traffic-Samples im Backbone der TKRZ
- Implementierung von individuellen Filterlisten an den TKRZ-Edge-Routern
- Umleitung und Mitigation des Traffics über die Systeme der F5 Networks (bei Bedarf)
- Blackholing von einzelnen IP-Adressen oder Netzen (bei Bedarf)
- Alle Maßnahmen erfolgen in direkter Kundenabsprache mit unseren Network-Engineers
- 24/7 Support bei DDoS-Angriffen
- Reporting

Bei Eintritt eines DDoS-Angriffes wird die TKRZ Maßnahmen zur Abwehr einleiten. Hierbei kann es zu Beeinträchtigungen wie z.B. False-Positives, Paktetverlusten oder höheren Latenzen kommen. Solche Beeinträchtigungen sind Folge eines durch externe Angreifer verursachten DDoS und daher nicht als durch die TKRZ verursachte Störung des Internet-Access zu verstehen. TKRZ wird in solchen Fällen zusammen mit dem Kunden die bestmöglichen Einstellungen vornehmen.

VORAUSSETZUNGEN

- Internet-Access über einen Zugang der TKRZ. Anbindungen über andere Anbieter können nicht geschützt werden.
- Mindest-Bandbreite: 100 Mbit/s symmetrisch
- Definition der zu schützenden IP-Adressen

Das Produkt kann als Option zu allen Glasfaser-Anbindungen mit Internet-Access sowie für die IP-Transit-Produkte in unseren Rechenzentren gebucht werden.

Die Bereitstellung erfolgt in der Regel innerhalb von fünf Arbeitstagen. In einem gemeinsamen Workshop mit dem Kunden werden die initialen Filterregeln und Schwellwerte bestimmt und eingestellt. Auf Anforderung des Kunden können während der Vertragslaufzeit Anpassungen vorgenommen werden.

Die Regelungen des TKRZ SLA+ (insbesondere für Reaktionszeit, Verfügbarkeit, Störungen, Wartungsarbeiten) gelten auch für das Produkt „TKRZ DDoS-Protection“. Durch die Buchung eines DDoS-Protection Produktes erhalten Sie automatisch das SLA+ Level für das geschützte Internet-Access-Produkt.