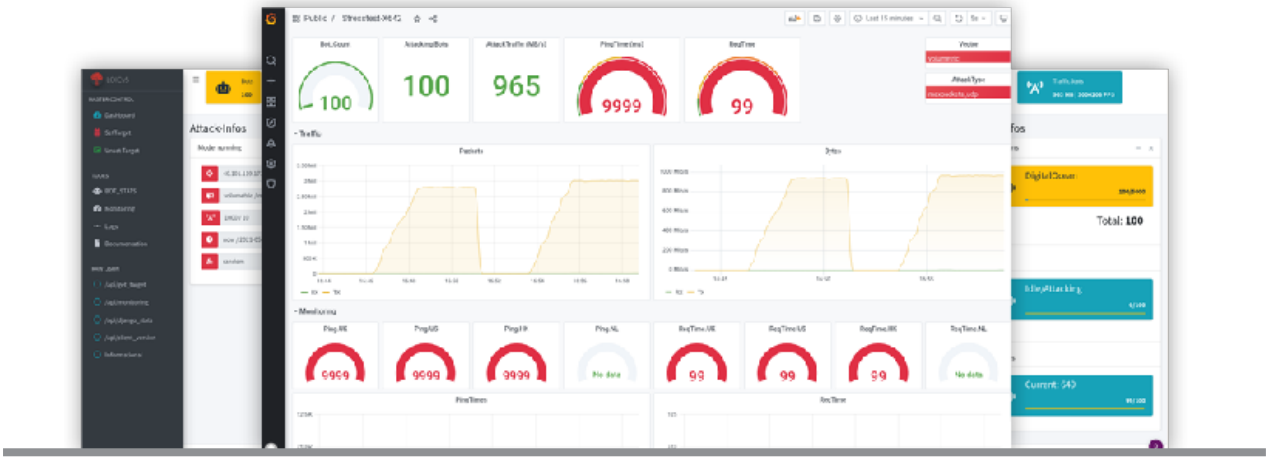


zeroBS DDoS-Stresstest

Für Admins und Operations – IT-Security made in Germany

zero.bs betreibt eine dedizierte, cloudbasierte Plattform zur Durchführung von DDoS-Belastungsangriffen auf Netze, Appliances und Applikationen, um die Wirksamkeit Ihrer DDoS-Abwehrmechanismen zu überprüfen.

Machen Sie sich die umfangreichen Funktionen unserer Bedrohungssimulationsplattform für Ihr Unternehmen und lassen Sie sich in sicherer Umgebung testen!

Vorteile DDoS-Stresstest

Nutzen Sie die Möglichkeit, anhand individueller, ausfallfreier DDoS-Stresstests Ihre vorhandene Infrastruktur realistisch einzuschätzen und pro-aktiv zu verbessern.

DDoS-TEST – Know How

Methodik zur Messbarkeit, Bewertung und Vergleichbarkeit während sowie nach einem Test

THREAT-LEVEL Bestimmung

Test des eigenen Schutzniveaus, Leistungsnachweis und Standortbestimmung

WORKFLOW optimieren

Workflow-Training bei Live-Monitoring unter realen Angriffsbedingungen in Echtzeit.

ANALYSE

Abschätzen von Auswirkungen und Kosten sowie eigenen Aufwänden nach einem erfolgreichen Angriff.

Was wir machen

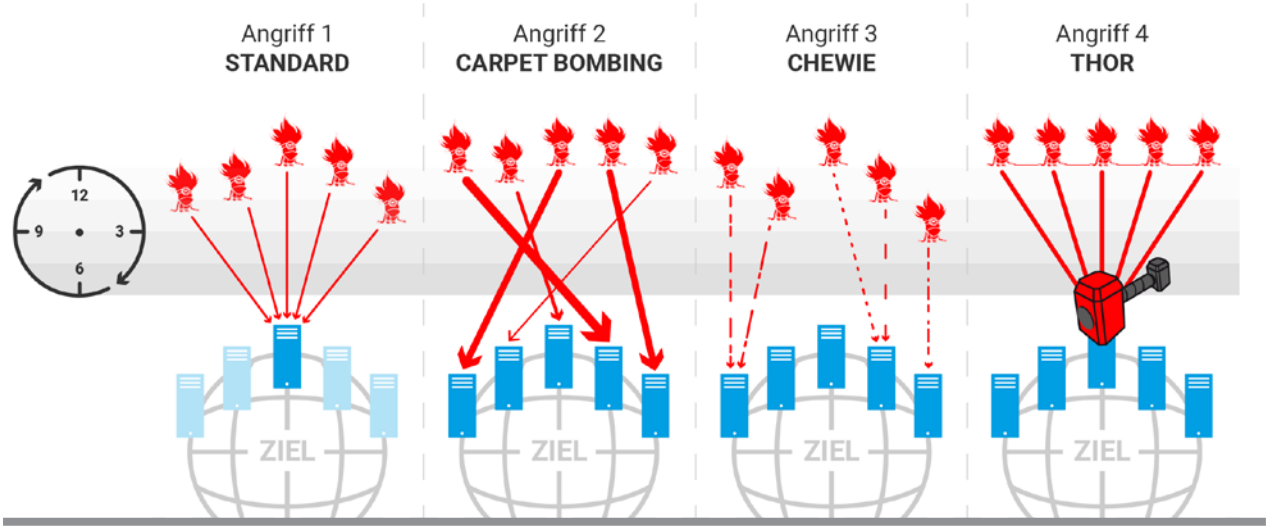
Neben Teamtrainings und Prüfen der Anti-DDoS-Maßnahmen rückt immer mehr die Durchführung von Leistungsnachweisen in den Fokus unserer Stresstests.

Das Team der zeroBS GmbH hat inzwischen umfangreiche Erfahrungen gesammelt, um alle einzelnen Punkte der gesamten Kette – vom BGP-seitigen Entrypoint über Anti-DDoS-Appliances, Firewalls, Loadbalancer bis hin zu Application-Servern – gezielt zu testen.

Erfolgreich getestet

Nachfolgend finden Sie eine Auswahl an Herstellern, Technologien und Providern, welche bereits von uns analysiert wurden.

Neben umfangreichen Analysen im Vorfeld ist ein integriertes Monitoring der angegriffenen Ziele Teil eines Tests, um qualitative, messbare Aussagen zu Performance und Limits treffen zu können.



AttackModes

- **Angriff 1 – STANDARD**
  Angriff auf einzelne IPs, ideal für Leistungsnachweise und Nachtests
- **Angriff 2 – CarpetBombing**
  Angriff auf ganze Netze, notwendig für fortgeschrittene Leistungsnachweise und erhöhte Bedrohungslevel
- **Angriff 3 – ChewyAttack (CarpetBombing v 2.0)**
  jede AngreiferIP sendet nur für max 30 Sekunden Traffic, geht dann in Standby und sucht sich nach 2 Minuten ein neues Ziel
- **Angriff 4 – ThorsHammer**
  auf die Millisekunde abgestimmter Angriff (Thors Hammer); eine Eigenentwicklung mit durchschlagendem Erfolg.

Features

- Volumenangriffe bis 100 GB/s oder 100 Mio pps via TCP, UDP oder ICMP
- Layer-7-Angriffe mit FullStack-Browsern, bis zu 10 Mio RPS
- 50 Locations, bis zu 100.000 IPs möglich
- IPv4 und IPv6
- Automatisiertes Setup und Orchestration der Infrastruktur
- Dashboard und Monitoring
- Exports und Logs für einfache Nachverfolgung und Analyse
- Simulation von echten Botnetzen (Server, IoT, Mirai etc)
- Komplett anpassbare Angriffe
- Interaktives Dashboard: jeder Angriff wird aufgezeichnet und ist Replay-fähig zur späteren Analyse

Gründe für einen Stresstest

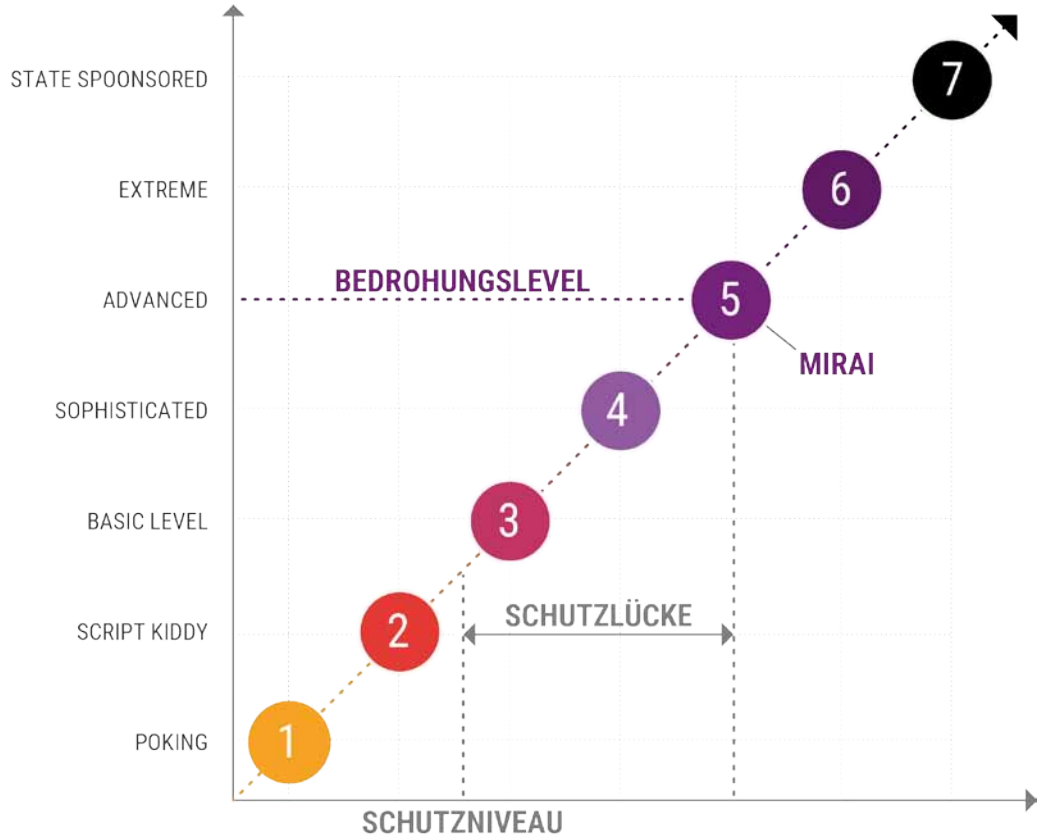
- Leistungsnachweis für die einzelnen Netz-Komponenten
- Prüfen der DDoS-Schutzmaßnahmen (Funktionsnachweis)
- Messen des eigenen Schutzniveaus im Vergleich zur Bedrohungslage gem. DDoS Resiliency Score*
- Testen, ob Administratoren für einen DDoS-Angriff ausreichend geschult sind
- Optimieren des Workflow für den Fall eines DoS-Angriffs
- Abschätzen der Auswirkungen sowie Kosten (Aufwände) eines erfolgreichen Angriffs

Folgende Ziele stehen u.a. im Fokus

- Netzwerke
- BGP-Router
- Firewalls und VPN-Gateways
- Webserver/Web-Infrastruktur
- APIs
- SSL Offloader
- Loadbalancer
- DNS-Infrastruktur
- beliebige TCP-Services
- DDoS-Appliances
- WebApplicationFirewalls
- IDS/IPS
- CDNs
- cloudbasierter DDoS-Schutz (Akamai, CloudFront, CloudFlare)
- Inhouse DDoS-Protection

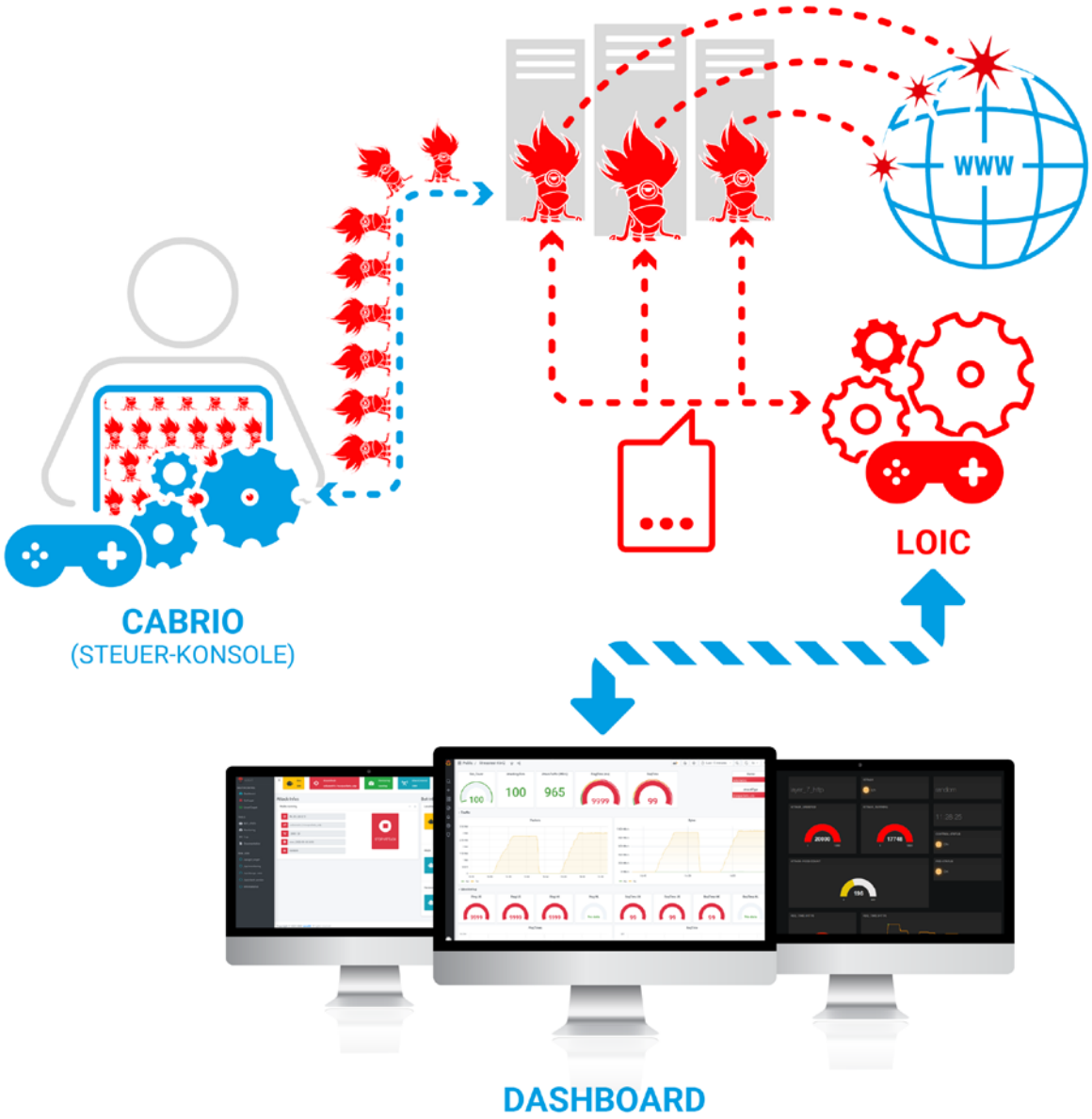
Angriffsvektoren

- Layer 3/4 (Volumenangriffe)
- Layer 7 (Angriffe auf Applikationen)
- IPv4 oder IPv6
- Angriffe gegen Firewalls
- Angriffe gegen Loadbalancer
- DNS-Waterboarding
- CDN-Reflections
- insgesamt über 50 verschiedene Angriffsarten
- individuell gestaltete Angriffe
- Real-World-Botnet-Simulationen (10.000 IPs)
- Paperworks und Trockenübungen für Notfall-Workflows



DRS – DDoS-Resiliency-Score

Unsere Bewertungen finden auf Grundlage des „DDoS-Resiliency-Score“ (DRS) statt und sind damit jederzeit nachzuvollziehen und vergleichbar.



Plattform – Aufbau / Ablauf

- Cabrio: Planung, Provisionierung der benötigten Pods (Auf/Abbau, Anzahl und Regionen)
- LOIC: Fernsteuerung für tatsächliche Angriffsaktivitäten während eines Assessments
- Dashboard: Live-Dashboard und Monitoring für Kunden und Reports