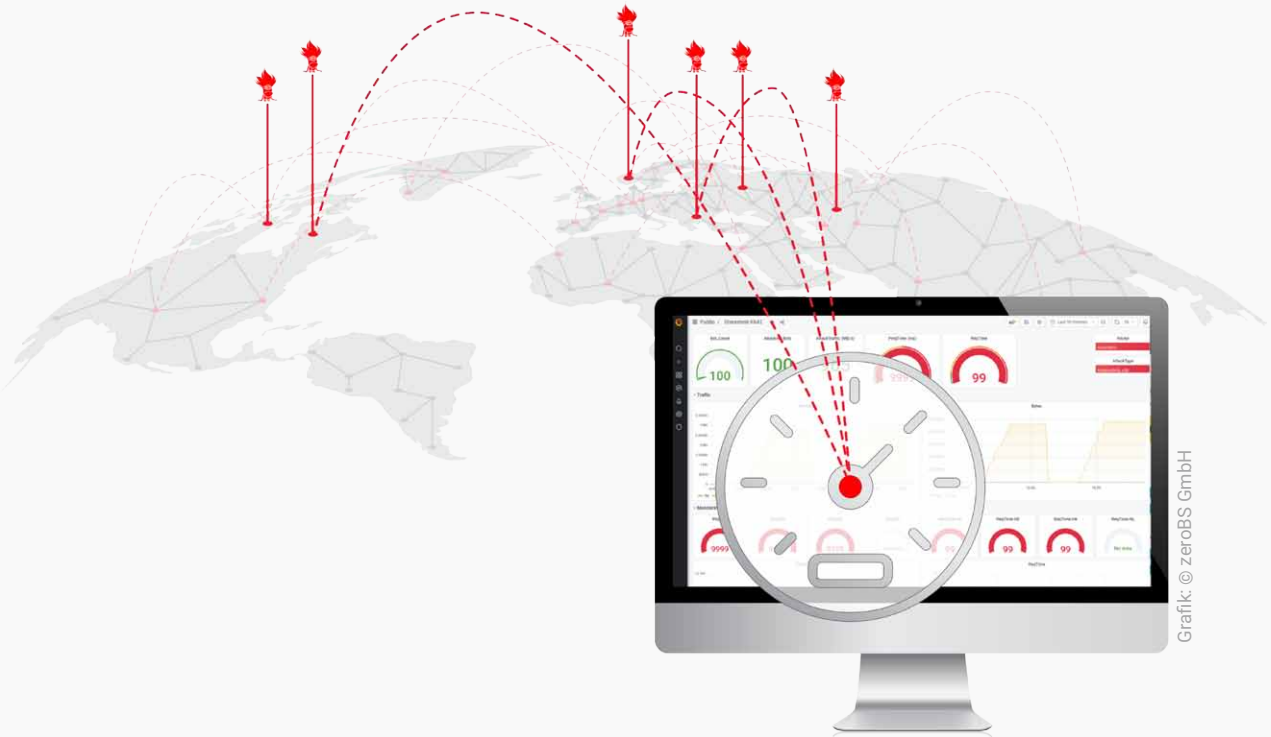
zeroBS

DDoS-Stresstest

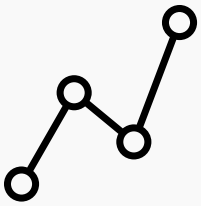
Für Admins und Operations

Gewährleisten Sie die Availability Ihres Geschäftsbetriebs und testen Ihre Infrastruktur mit unserer hochmodernen, cloud-basierten Threat Simulations-Plattform.



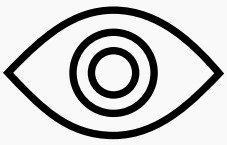
Vorteile DDoS-Stresstest

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



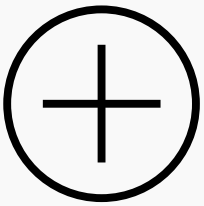
DDoS-TEST – Know How

Methoden zur Messbarkeit, Bewertung und Vergleichbarkeit während / nach einem Test.



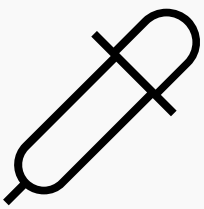
THREAT-LEVEL Bestimmung

Test eigenes Schutzniveau / Leistungsnachweis + Standortbestimmung.



WORKFLOW optimieren

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



ANALYSE

Abschätzen von Auswirkungen und Kosten sowie Aufwänden bei erfolgreichem Angriff.

Einführung

zeroBS ist Vorreiter im Bereich IT-Security und bietet eine dedizierte, cloudbasierte Plattform, die speziell für die Durchführung von DDoS-Stresstests entwickelt wurde.

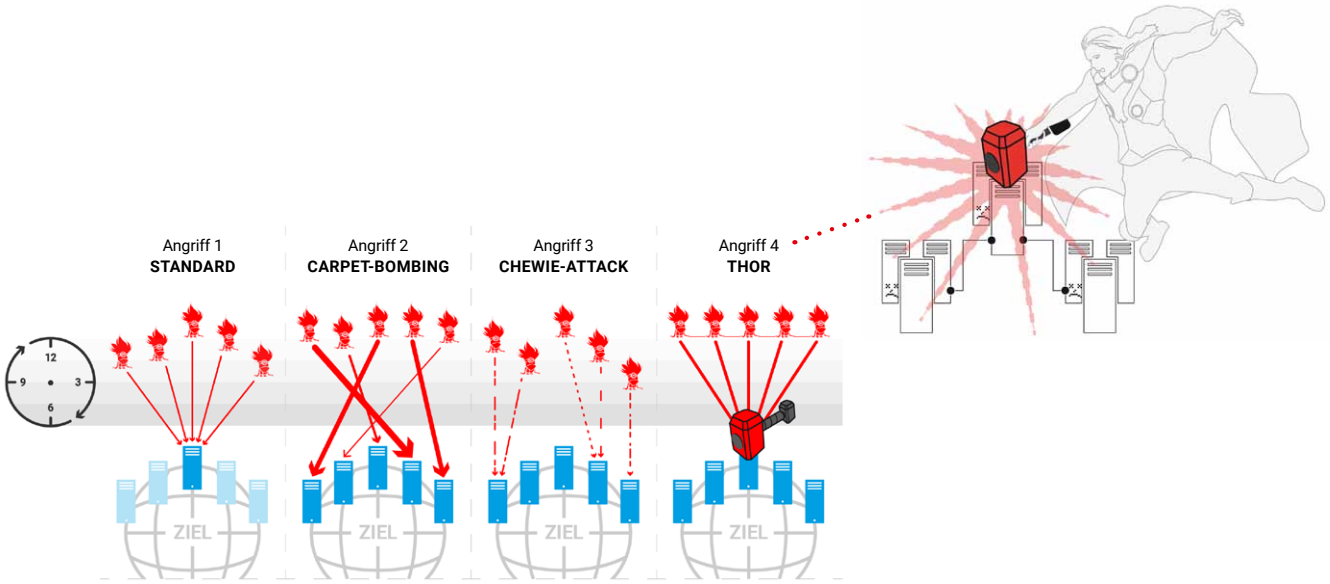
Weitere Kernkompetenzen liegen in der Simulation von Netzwerkangriffen sowie der Überprüfung von Schutzmechanismen Ihrer Infrastruktur.

Unsere individualisierbare Plattform ermöglicht gezielte Tests in Form von Layer 3-, 4- sowie 7-Angriffen und IPv6-Protokollen. Wir evaluieren die Belastbarkeit Ihrer Systeme aus verschiedenen Eintrittspunkten wie: vorhandener Anti-DDoS-Appliances, Firewalls, Loadbalancer, Application-Server – einschließlich BGP-seitiger Entrypoints. Die Bedeutung von DDoS-Stresstests geht jedoch über rein technische Aspekte hinaus: sie dienen auch als effektive Methode zur Schulung Ihres Teams bei gleichzeitiger Ermittlung der Leistungsgrenzen Ihrer Infrastruktur.

Mittels umfangreicher Analysen im Vorfeld und dem integrierten Monitoring angegriffener Ziele können wir aussagekräftige Erkenntnisse über die Performance Ihrer Systeme gewinnen.

In unserer vernetzten Welt ist der Schutz Ihrer Infrastruktur vor Netzwerkangriffen von entscheidender Bedeutung. Unsere DDoS-Stresstests bieten Ihnen die Gelegenheit, Angriffsszenarien jeglicher Art und Umfang in Echtzeit zu testen: **Heben Sie Ihre IT-Security auf ein neues Niveau.**

Attack Modes



1 **Standard – Angriff auf Einzel-IPs:** ideal für Leistungsnachweise / Nachtests

2 **CarpetBombing – Angriff auf ganze Netze:** notwendig für fortgeschrittene Leistungsnachweise und erhöhte Bedrohungslevel*

3 **ChewieAttack – 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**

4 **Thor – auf die Millisekunde abgestimmter Angriff (Thors Hammer):** eine Eigenentwicklung mit durchschlagendem Erfolg

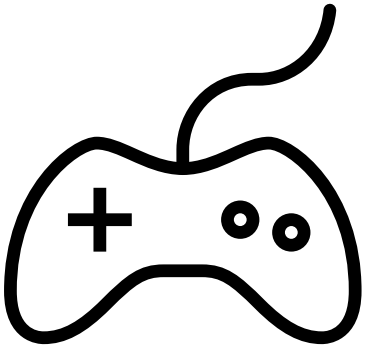
***Def. CarpetBombing von APNIC Global DDoS attack trends 2018**
Carpet bombing attacks are a new variant of the more common reflection or flooding attacks, where instead of focusing the attack on a single destination, the attacker attacks every destination within a specific subnet or CIDR block (for example, a /20). This will both make it more difficult to detect the attack and also to mitigate it, potentially resulting in outages due to the flood of attack traffic across network devices and internal links.

In addition, these attacks are often fragmented, resulting in a flood of non-initial IP fragments, which can be tricky to mitigate. The attacker will often shift their attacks from one subnet (or CIDR block) to another, complicating the detection and mitigation even further.

****Def. ChewieAttack (CarpetBombing 2.0)**
Von der Zielauswahl her dem Carpetbombing sehr ähnlich, bringt der ChewieAngriff mehr Zufälligkeit ins Spiel, indem sowohl Ziel, Stärke, Vector und Protokoll völlig zufällig ausgewählt werden.
Dies sorgt dafür, dass reine Statistik-basierte Erkennungsmethoden völlig verwirrt werden, da der Paketstrom von einer AngriffsIP nie länger als 30 Sekunden dauert, und dann für mindestens 120 Sekunden aufhört, um dann mit neuem Ziel und Pattern erneut zu starten.

Von einem Botnet sind zwar nur 25% der Bots jeweils aktiv, dafür ist der Angriff wesentlich schwieriger zu verteidigen

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
+ Multi-Location-Monitoring

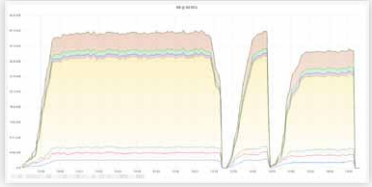
Diese Ziele testen wir (u.a.)

+ **Netzwerke**
+ **BGP-Router**
+ **Firewalls und VPN-Gateways**
+ **Webserver / Web-Infrastruktur**
+ **APIs**
+ **SSL Offloader**
+ **Loadbalancer**
+ **DNS-Infrastruktur**
+ **beliebige TCP-Services**
+ **DDoS-Appliances**
+ **Layer 3/4 (Volumenangriffe)**

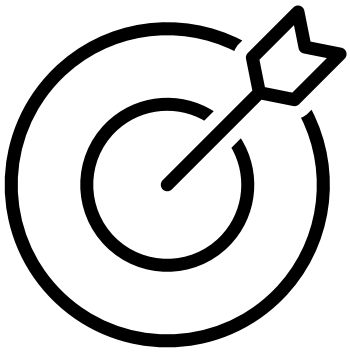
Angriffsvektoren

+ **Layer 7 (Applikationen-Angriff)**
+ **IPv4 oder IPv6**
+ **Angriffe gegen Firewalls**
+ **Angriffe gegen Loadbalancer**
+ **DNS-Waterboarding**
+ **CDN-Reflections**
+ **über 50 Angriffsarten**
+ **individuell gestaltete Angriffe**
+ **Real-World-Botnet-Simulationen (10.000 IPs)**
+ **Paperworks und Trockenübungen für Notfall-Workflows**

Screens Dashboard



Weitere Gründe für einen Stresstest



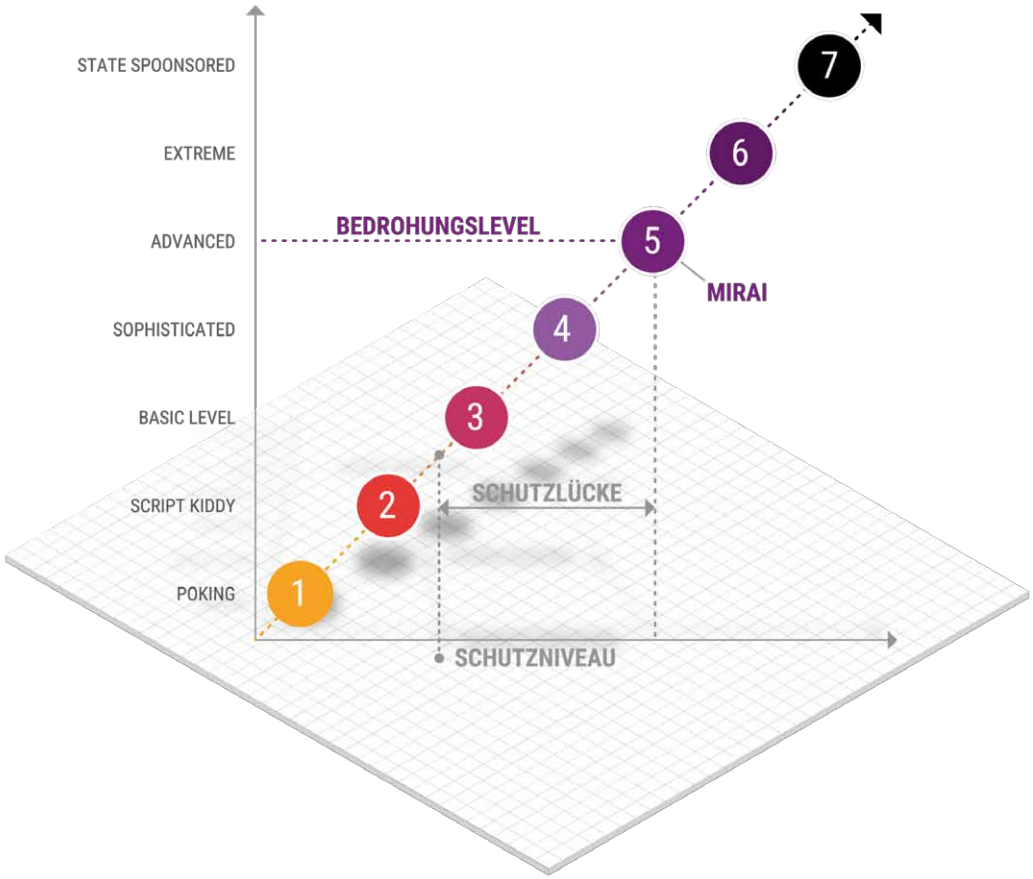
+ **Leistungsnachweis für die einzelnen Netz-Komponenten**
+ **Prüfung, ob DDoS-Schutzmaßnahmen wie gewünscht funktionieren (Funktionsnachweis)**
+ **Messen des eigenen Schutzniveaus im Vergleich zur Bedrohungslage gemäß DDoS Resiliency Score**
+ **Administratoren-Test: geschult und bereit für einen DDoS-Angriff?**
+ **Optimieren des Workflow für den Fall eines DDoS-Angriffs**
+ **Abschätzen der Auswirkungen eines erfolgreichen Angriffs** sowie
+ **Abschätzen der Kosten/Aufwände eines erfolgreichen Angriffs**

Benefit: Leistungsnachweise und Compliance

Die Durchführung von Leistungsnachweisen rückt zunehmend in den Fokus unserer Stresstests. Wir unterstützen Unternehmen bzw. Institutionen mit geschäftskritischen Internetpräsenzen oder spezifischen Audit-Anforderungen im Bereich der Cyber-Security bei der Erbringung, Umsetzung sowie Organisation aller dafür notwendigen Leistungsnachweise (inkl. Reports).

DRS – DDoS-Resiliency-Score

Um das jeweilige Schutzniveau im Vergleich zur Bedrohungslage auch für unsere Kunden nachvollziehbar einzuordnen, nutzen wir den DDoS Resiliency Score (DRS).



Was uns auszeichnet

Die zeroBS GmbH weiß sowohl um die Komplexität von Bedrohungsumgebungen als auch die Herausforderungen hinsichtlich der Optimierung Ihrer Unternehmenssysteme samt Infrastruktur. Auf dieser Basis bilden wir direkt auf Ihre Bedürfnisse zugeschnittene Angriffsvektoren in verschiedenen Intensitätsstufen ab: unser Know How für Ihre Team Trainings (Redteaming) bzw. individuelle Tests.

Referenzen unserer Arbeit

Diese Hersteller, Technologien und Provider haben wir unter anderem bereits erfolgreich getestet.

Teil unseres Stresstest sind neben umfangreichen Analysen im Vorfeld ein integriertes Monitoring der angegriffenen Ziele, um qualitative, messbare Aussagen hinsichtlich Limits sowie Performance treffen zu können

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