SEMINARE
WORKSHOPS
AKADEMIE

zeroBS

Secur|Ty made in Germany

Workshop

Best Practice

zeroBS DDoS-Training

für Admins und Operations

Grafik: Screenshot Dashboard

DDoS Stresstest

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.

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.

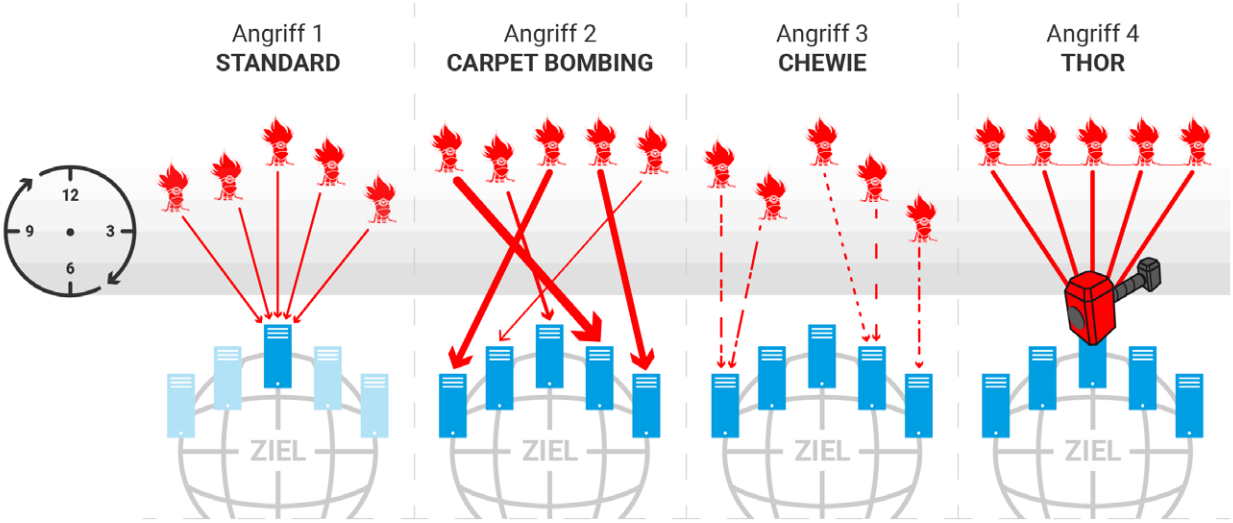
ERFOLGREICH GETESTET

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

Deutsche Telekom, f5, Cisco, Akamai, voxility, A10, colt, Nokia, Cloudflare, Fortinet, Check Point Software Technologies Ltd., Link11, Juniper Networks, amazon web services, Arbor Networks, Citrix NetScaler, Sophos, paloalto Networks, Imperva Incapsula, radware, SonicWall, Symantec, Rohde & Schwarz

Teil unseres Stresstest sind umfangreiche Analysen im Vorfeld und integriertes Monitoring der angegriffenen Ziele, um qualitative, messbare Aussagen zur Performance und Limits treffen zu können.

ATTACKMODES



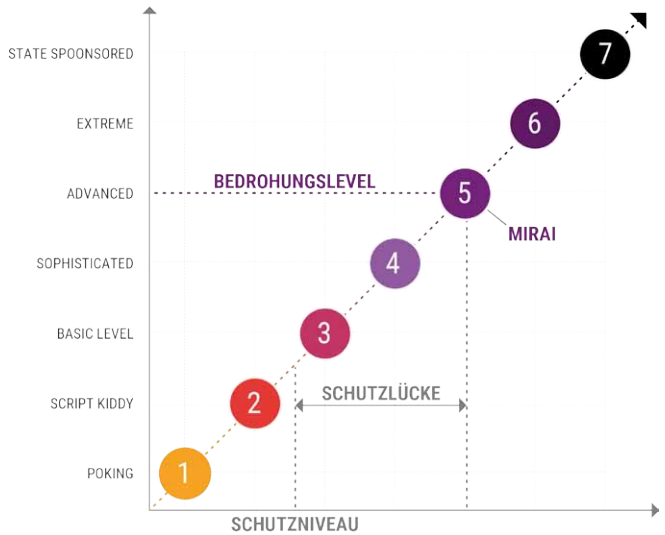
- **STANDARD:**
  Angriff auf einzelne IPs, ideal für Leistungsnachweise und Nachtests
- **CARPETBOMBING:**
  Angriff auf ganze Netze, notwendig für fortgeschrittene Leistungs nachweise und erhöhte Bedrohungslevel
- **CHEWYATTACK** (CarpetBombing v 2.0):
  jede AngreiferIP sendet nur für max 30 Sekunden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

FEATURES

- Volumenangriffe bis 100 GB/s oder 50 Mio pps, TCP oder UDP
- Layer-7-Angriffe mit FullStack-Browsern, bis zu 10 Mio RPS
- 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)
- anpassbare Angriffe

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 eines erfolgreichen Angriffs



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

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)
- 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

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