SysEleven

SYSELEVEN DDOS GUARD

Wir haben den SysEleven DDoS Guard so konzipiert, dass er einen wirksamen DDoS-Schutz bei transparenten Kosten bietet. Leistungsfähige Komponenten sowie das Know-how unserer Cloud- und Network-Teams bieten Ihnen einen Rundum-Sorglos-Schutz.

→ Ihre Vorteile mit dem SysEleven-Netz:

- Mehr als 500G Edge Kapazität
- Bestes Peering – angeschlossen an DE-CIX, AMS-IX, BCIX, NL-ix und SwissIX
- Direkte Anbindung zu Amazon, Google, Facebook, Apple, Netfl ix, Twitch uvm.
- Direkte DTAG Anbindung
- Betrieb zertifiziert nach ISO 27001 nativ und ISO 27001 nach IT-Grundschutz (BSI)

→ Sie bestimmen die Anbindung:

- via VLAN auf IXP Plattformen
- via Cross Connect / PNI
- via GRE Tunnel
- Kombination mit Transit Services
- Always-On und OnDemand pro IP
- Self-Onboarding über BGP Communities

DE-CIX amsix swissix SWISS INTERNET EXCHANGE

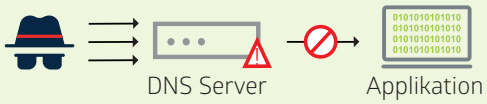
SysEleven Carrier Services made with ♥ in Berlin

Alle Features für Sie im Überblick:

- Automatisches Engineering für DDoS Traffic
- FlowSpec Mitigation / Traffic Washing
- Selektives Blackholing (Drop Traffic außerhalb Europas)
- Manuelle Mitigation für bisherige **unbekannte** Angriffs-vektoren (inline TCP Dumps jederzeit möglich)
- L3/L4 Anomaly Detection und Mitigation
  - per Src IP / TCP / UDP Sessions / Connections
  - per TCP Syn Proxy
  - ICMP / SCTP Sweeping
- Upstream Filtering bis L4
- Geo Filtering auf Ihren Wunsch
- Reporting & Alarming
- Zugriff auf das Mitigationportal

DNS Floods

DNS-Flood-Angriffe unterbrechen die DNS-Auflösung und sorgen so dafür, dass die Performance Ihrer Website, API oder Anwendung nicht mehr ausreicht oder die Verfügbarkeit unterbrochen ist.

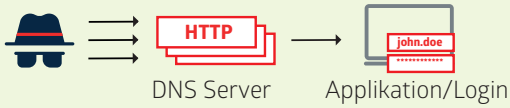


UDP Floods

Angreifer nutzen die Funktionen offener DNS- oder NTP-Resolver, um einen Zielserver oder ein Zielnetzwerk mit verstärktem Anforderungsdatenverkehr zu überlasten, bei dem die Nutzlast größer ist als die ursprüngliche Anforderung.

HTTP Floods

HTTP-Flood-Angriffe erzeugen große Mengen von HTTP-, GET- oder POST-Anforderungen aus verschiedenen Quellen. Sie zielen auf die Anwendungsebene ab und sorgen für eine Serviceverschlechterung oder sogar dafür, dass der Dienst nicht mehr verfügbar ist.



Weitere Filter Protection

SYN-Flood, SNY-ACK-Flood, ACK / Push Flood, Fragmented ACK, RST / FIN Flood, Synonymous IP, Fake Sessions, Session Attacks, Misused / Out of Protocol Attacks, Replay Verb Attacks, Faulty Application Protocol Attacks, UDP Fragmentation Attacks, VoIP Flood, Media Data Attacks, ICMP Floods, Fragmentation Flood, Ping Flood, uvm.

Der SysEleven DDoS Guard ist kombinierbar mit anderen SysEleven Produkten wie z.B. F5 Load Balancing und Web Application Firewalling.

Nehmen Sie Kontakt unter carriersales@syseleven.de auf