tineo
YOUR COMPANY FOR ENTERPRISE SOLUTIONS

Leistungsbeschrieb

Business Internet Premium Option DDoS

Die sichere, garantierte Konnektivität von Applikationen und Services erfordert einen dedizierten Schutz vor DDoS-Angriffen. Durch den Einsatz eines Always-On Konzepts, bei dem der Datenverkehr in Echtzeit überwacht und geschützt wird, stehen folgende netzwerkbasierte Managed DDoS-Services zur Verfügung:

	Performance Protection	Business Continuity	Enterprise DDoS
Portal zur Echtzeitüberwachung und Reports [2] **Bereitstellung von DDoS-relevanten Daten im Kundenportal in Echtzeit sowie tägliche Security Reports**			
Übersicht Network Traffic & Mitigation Data	○	○	●
Source IPs	○	○	●
Destination IPs	○	○	●
Source Ports	○	○	●
Destination Ports	○	○	●
TTL (time-to-live)	○	○	●
Packet Lengths	○	○	●
Health Status	○	○	●
Kundenspezifische Reporting Engine [2], optional mit proaktiver Best Practice Guidance zu relevanten SoA Controls gemäss ISO 27001 und ISAE 3402 Reporting	○	○	●
Uplink Scrubbing Center Services für hochvolumige Angriffe [1,2] **Kundenspezifische Anpassungen und Analysen [1,2]**			
Blacklisting / Whitelisting von IP Adressen	○	●	●
Port-Adressbereich Filter (für generische TCP/UDP port-basierte Angriffe)	○	●	●
Rate Limiting Policies	○	●	●
Aktivierung von BPF Filtern mittels Flex-Rule	○	●	●
Smart-Rule Einsatz von Machine Learning aufgrund von Heuristik und Behavioural Analysis für Tracking und Eindämmung von L2-L4 Angriffen, inkl. Zero-Day	○	●	●
Sofortige Alarmierung	○	●	●
Schnelle und präzise Erkennung von DDoS Angriffen mittels 100% Inspection und Mitigation durch Tineo			
TCP Flood Attacks	●	●	●
UDP Flood Attacks	●	●	●
UDP Fragmentation Attacks	●	●	●
ICMP Floods	●	●	●
Flood Attacks	●	●	●
SYN-ACK Flood Attacks	●	●	●
NTP Monlist Response Amplification	●	●	●
SSDP/UPnP Responses	●	●	●
SNMP Inbound Responses	●	●	●
Charge Responses	●	●	●
Smurf Attacks	●	●	●
Fraggle Attacks	●	●	●
DNS Amplification	●	●	●
Connectionless LDAP (CLDAP) Amplification	●	●	●
Falsch formatierte und gekürzte Pakete (z.B. missbräuchliche UDP Anfragen)	●	●	●
IP Fragmentierung/Segmentierung AETs	●	●	●
Ungültige TCP Segment IDs	●	●	●
Falsche Checksums und ungültige Flags in TCP/UDP Frames	●	●	●
Ungültige TCP/UDP Ports	●	●	●
Verwendung von reservierten IP Adressen	●	●	●
Command and Control Operations	●	●	●
NTP Monlist Requests	●	●	●

Technische Performance Daten der Tineo DDoS Plattform

Max. Durchsatz [3]	30 Mio.	Latenz (typisch):	≤ 0.5 µs	AMRT [4] (typisch):	≤ 60 µs
Max. SYN Flood:	120 Mio.	Inspection Latenz:	≤ 60 µs		

[1] gilt in Verbindung mit SLA Premium Silber
[2] gilt in Verbindung mit SLA Premium Gold
[3] Pakete pro Sekunde
[4] Attack Mitigation Reaction Time