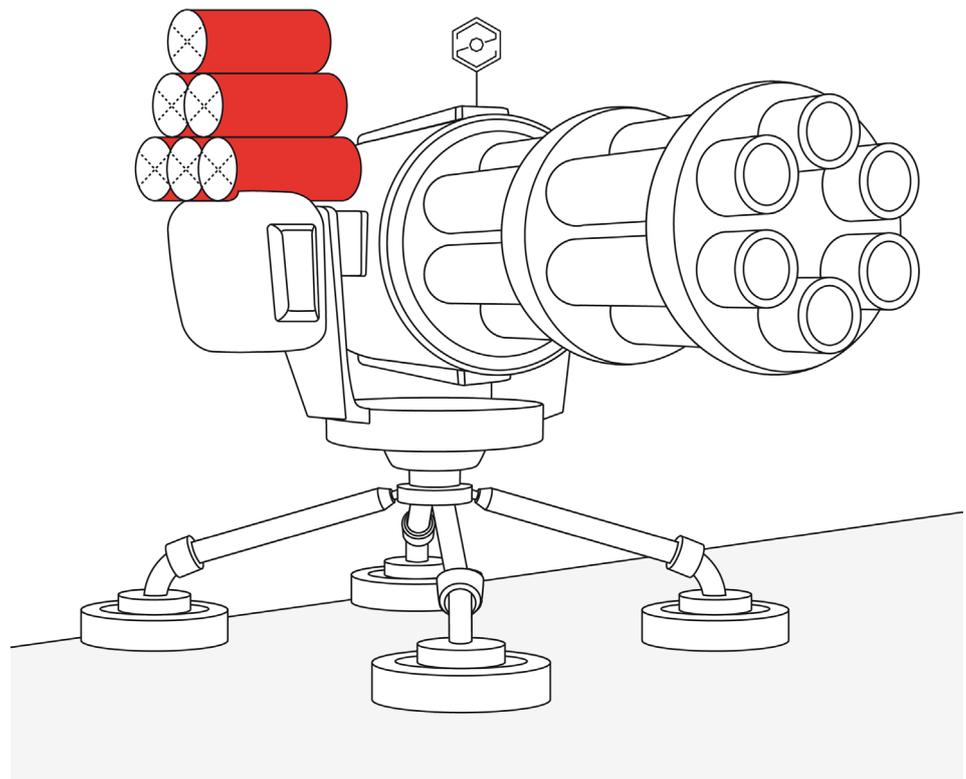


zeroBS – Schulungsunterlagen

DDoS-Abwehr-Toolkit und Handbuch





INHALTSVERZEICHNIS

VOR EINEM ANGRIFF	3
EMERGENCY-WORKFLOW	4
ANGRIFFSFALL	4
Checkliste Angriffsanalyse	5
Nachgang + Lessons learned	5
DDOS PROTECTORS NOTEBOOK // BEST PRACTICES	6
Hybrid-Lösungen mit On-Premise-Appliances	6
Firewalls	6
Loadbalancer/ SSL-Offload	6
ÜBERSICHT ÜBER DIE VERTEIDIGUNGSMETHODEN	7
DDOS RESILIENCY SCORE	8
APPENDIX	9
Angriffslog	10
Changelog	11

VORHER

Vor einem Angriff ...

- » Notfallpläne und Kontaktmöglichkeiten/Eskalationswege ausarbeiten und ausdrucken
- » Kontakt/Alarmierungswege zum ISP (VoIP-unabhängig)
- » Benennung der Verantwortlichen und deren Vertreter
- » Bedrohungsanalyse (Recon), ThreatModel nach DRS
- » Notfallübungen, Stresstests, Paketschießstand
- » Überprüfung der Workflows durch Übungen (Paperwork, Real World Scenarios)
- » Sicherstellen der Sichtbarkeit und Analysemöglichkeit von Trafficflow, Volumen, Charts, Monitoring , Router, Firewalls, IDs
- » Zugriff auf Firewalls, Router, Monitoringsysteme
- » Checkliste Angriff mehrfach ausdrucken und bereitlegen
- » Wie sieht der Traffic im Normalfall aus? (Ingress vs Egress, Volumen, Charts)
- » DevOps, Know your System: wie „fühlen“ sich die Systeme im Normalfall an? Bottlenecks?
- » Identifikation der absolut notwendigen Services (Core-Services), auf die sich im Notfall konzentriert werden muss
- » Identifizieren aller im Notfall zu whitelistenden IPs (Positivliste), externe Dienstleister nicht vergessen
- » Netzwerkseparation, DNS/Mail idealerweise nicht im eigenen Netz
- » DNS-TTL für bedrohte Systeme runtersetzen

EMERGENCY-WORKFLOW

Angriffsfall / Notfallworkflow

□ Lieber einen Service verlieren, als ein ganzes Netz.

- » DONT PANIC
- » Handler festlegen, Schriftführer festlegen
- » alle Schritte mit Timestamp dokumentieren
- » Flipchart bereitstellen
- » Benachrichtigung der Verantwortlichen intern, Technik und Entscheider
- » Identifizieren der Angriffsart/Stärke/Ziele/Auswirkungen:
Checkliste „Angriffsanalyse“ und Angriffslog
- » Benachrichtigung des ISP
- » Benachrichtigung externer Hilfe, wenn vorhanden

Empfehlungen

- » nur eine Mitigation-Maßnahme zur Zeit, wenn möglich keine Überschneidungen, Auswirkungen überprüfen
- » Ermitteln, ob man direkt angegriffen wird oder ob der Angriff einem anderen galt und man die Auswirkungen spürt
- » Ermitteln der bedrohten Systeme und Services, Auswirkungen
- » Auswerten des Angreifer-Netflows (IPs, Länder, ASN, Ports etc)
- » kann eine Signatur geschrieben/deployed werden?
- » Mitigation des Angriffs gegen die Core-Services gem. Methodologie

EMERGENCY-WORKFLOW

Checkliste Angriffsanalyse

- » Notfallworkflow aktivieren
- » Esklationsstrategie und Benachrichtigungskette aktivieren
- » Checkliste Ablauf Angriff bereitlegen, Verantwortlichen zur Buchführung (Handler) bestimmen
- » Wo kommt der Traffic her?
 - » IPs (Anzahl)
 - » CIDRs
 - » Geo
- » Was für eine Art?
 - » Layer 3,4,7
 - » Volumen vs Applikation
 - » direkt vs Reflektoren
 - » AVG Volumen / Bot (75. percentile)
- » Wogegen richtet sich der Angriff? (IP/Applikation/Infra)
- » Wodurch wurde der Angriff bemerkt? (Monitoring, Systemverhalten)
- » Verhältnis Ingress/Egress im Normalfall vs Angriffsfall
- » Logs sichern
- » Wie viele IPs insgesamt?
- » Originator? (Botnet, direkter Angriff, Reflektoren)
- » Füllstand Leitungen / wann wird's kritisch?
- » Auswirkungen auf betroffene oder verbundene Systeme

Nachgang + Lessons learned

- » Waren die Workflows OK?
- » War Sichtbarkeit an allen Punkten gegeben?
- » Gab es ein Erpresserschreiben?
- » Was war die Motivation für den Angriff?
- » Roadmap zum Abstellen gefundener Issues

DDOS PROTECTORS NOTEBOOK // BEST PRACTICES

Hybrid-Lösungen mit On-Premise-Appliances

- » wenn automatischer Switch in ein Scrubbing-Center: BGP-Umrouting nur One-Way, sonst kann ein Angreifer durch Thors Hammer Flapping aktivieren mit High Paket Loss
- » gesicherter Rückkanal

Firewalls

- » Immer HINTER eine DDoS-Appliance, können häufig nicht mit TCP-Garbage auf Open Ports oder massiven Botnet-TCPSessions umgehen (FP: Synflood)

Loadbalancer/ SSL-Offload

- » SSL-Keylength: wenn > 2048, unbedingt Testen, kann zu Problemen auf dem LB testen

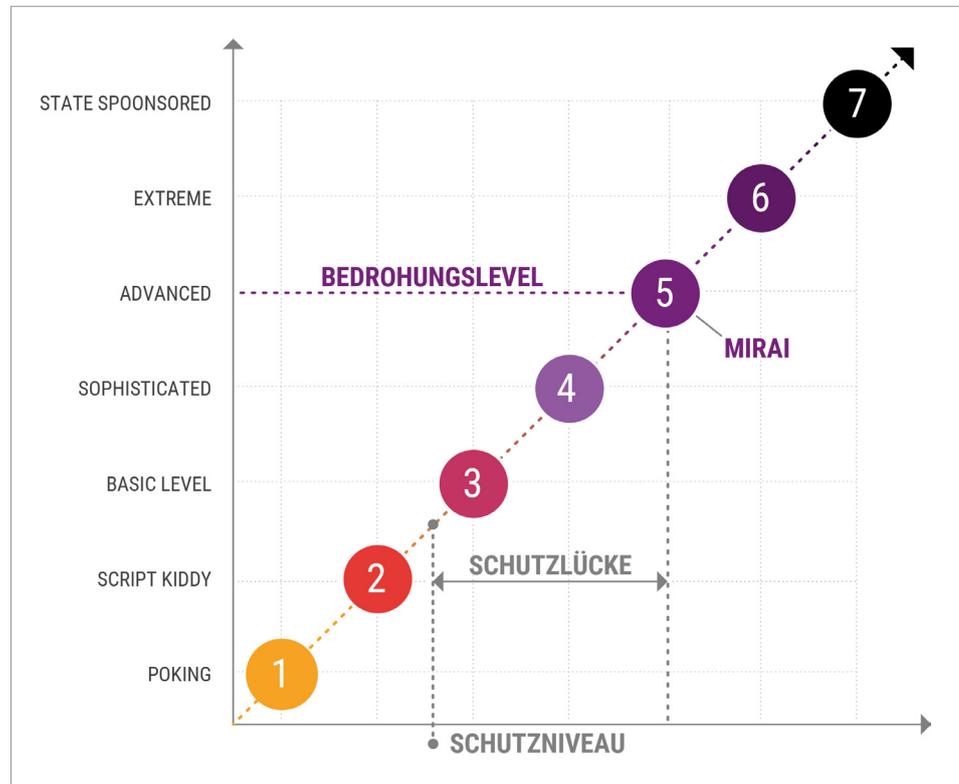
ÜBERSICHT ÜBER DIE VERTEIDIGUNGSMETHODEN

Tabelle 1

Nr	Verteidigungsmethode	Anmerkung
1	IP-Block / Firewall	manuelles Blockieren von identifizierten Angreifer-IP/Netze Manuell == Aufwändig, kann durch Angreifer mitigiert werden, wenn weitere Bots/Quellen vorhanden sind
2	Blackholing	Sperren einzelner eigener IPs via BGP (oder DNS == 127.0.0.1), primär zum Schutz der eigenen Infrastruktur gesamte Infa ist geschützt, einzelne Services können offline sein
3	GeoIP-Block	Blockieren/Whitelisten verschiedener Geo-Regions, Kontinente oder Länder sehr gut gegen Avg Botnetze
4	Anti-DDoS-Appliance	Dedizierte DDoS-Appliance zur Abwehr von DDoS-Angriffen kann meist nur L3/4, gut in Verbindung mit Scrubbing-Center, siehe Hybridlösung
5	NGFW	NextGenerationFireWall (SRSLY?) mehrfach getestet, OK bis Level 2, max 3
6	WAF	WebApplicationFirewall
7	Scrubbing-Center	Always-On cloudbasiertes Scrubbing-Center
8	Hybridlösung	Anti-DDoS-Appliance mit Umschaltung auf Scrubbing-Center, falls der Angriffstraffic > lokal verarbeitbares Volumen
9	ReverseProxy mit Full On	Einsatzzweck primär nur für Webapplikationen CloudFlare, 8ackProtect, MyraCloud Protektion für Volumenangriffe
10	Rate-Limiting SRC-IP	Rate-Limit auf der Absender-IP kann zu Problemen bei Mobile-Providern führen gut gegen High-Vol/Bot
11	Rate-Limiting DST-IP	DST-IP Schützt den Service/Server OK bei kleinen Botnetzen Probleme bei großen Botnetzen, da das Verhältnis User/Bots suboptimal ist
12	Manuelle Signaturen	Z.B. Filter auf User-Agent etc im Webserver

DDOS RESILIENCY SCORE

Grafik zeroBS



Tabelle

Level	Verteidigungsmethode	Anmerkung	RPS	Vektoren
1	Poking, Anklopfen	100 MBit	1000	1
2	ScriptKiddy, Booter-Services	1 GBit	5000	2
3	Basic Level Professionals	100 GBit	10000	5
4	Sophisticated Professionals	500 GBit	100000	10
5	Advanced Professionals	1000 GBit	1 Mio	no limit
6	Extreme Professionals	no limit	no limit	no limit
7	State Sponsored	no limit	no limit	no limit

APPENDIX

Angriffslog

Nr	Timestamp	Ziele (IP/Host/Infra/Carrier)	bemerkt durch / Auswirkung *
Angriffsart	Volumen:	Ingress/Egress	Origin
TCP UDP Port:	Total:	Rein: Raus:	Geo:
Application:	AVG/Bot:	%:	Originator: **
			Handler:

Nr	Timestamp	Ziele (IP/Host/Infra/Carrier)	bemerkt durch / Auswirkung *
Angriffsart	Volumen:	Ingress/Egress	Origin
TCP UDP Port:	Total:	Rein: Raus:	Geo:
Application:	AVG/Bot:	%:	Originator: **
			Handler:

Nr	Timestamp	Ziele (IP/Host/Infra/Carrier)	bemerkt durch / Auswirkung *
Angriffsart	Volumen:	Ingress/Egress	Origin
TCP UDP Port:	Total:	Rein: Raus:	Geo:
Application:	AVG/Bot:	%:	Originator: **
			Handler:

APPENDIX

Angriffslog

*) grundsätzlich können hier Zusatzdaten mit weiteren Erläuterungen gepflegt werden, e.g. via Flipchart

Wodurch wurde der Angriff bemerkt?

- » Monitoring
- » Systemverhalten
- » manuell
- » Ausfall

Auswirkungen des Angriffs?:

- » NIL: keine Beeinträchtigung
- » DROP: einzelne / viele Paket-Drops gesehen
- » SLOW: services/server wird langsam
- » DOWN: server/service ist Down
- » ...

***) Originator:

- » direkter Angreifer
- » Botnet
- » Erpresser
- » ...

APPENDIX

Changelog

Tabelle 2

Version	Datum	Bearbeiter	RMKS
1.5	2020-01-14	mo	DRS-Level an aktuelle Ereignisse angepasst
1.4	2019-05-13	mm	DRS hinzugefügt
1.2	2018-06-10	dh	Typos und Umformulierungen
1.0	2018-05-12	mm	Identifizieren Angriffsarten für Angriffstabelle
0.8	2018-03-12	mm	Angriffsanalyse erweitert
0.7	2018-02-13	mm	Emergency-Checkliste als Anhang
0.6	2017-02-13	dh	Emergency-Workflow
0.4	2016-05-22	dh	Weitere Angriffsarten
0.1	2016-05-18	mm	Initiale Version