CYBER SECURITY

TYPO3 Websites im Zeitalter von Cyber-Angriffen

Sebastian Kreideweiß
coding. powerful. systems. CPS GmbH
17. September 2025, DMEXCO

CPS coding powerful systems

Gefährdungen/Attacks

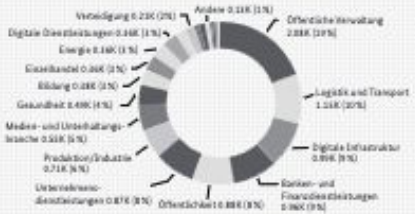
mit resultierender

Schadwirkung/Impact

IT-Sicherheitsvorfälle und Phishing

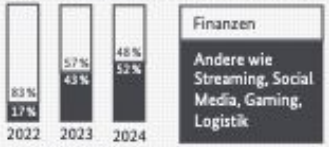
Öffentliche Verwaltung EU-weit von allen Branchen am stärksten betroffen.

IT-Sicherheitsvorfälle in der EU nach Sektor



Phishing durchwächst alle Marktsegmente

Von Verbraucherinnen und Verbrauchern gemeldete Phishing-Mails nach Art der ausgenutzten Marktsektoren (Anteilswerte in %)



Ransomware

Lösegeld pro Fall (in US-Dollar, ca. Durchschnitt):

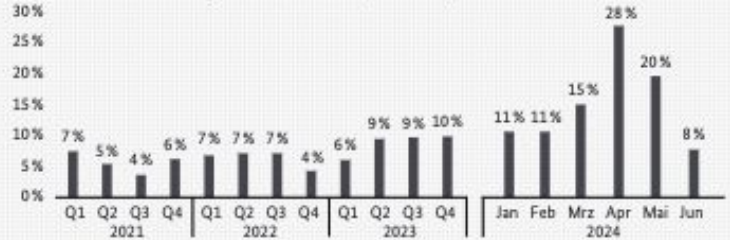
Von Ransomware-Gruppen erbeutete Lösegelder weltweit (in US-Dollar, Mio.):

KRITIS

Störungen bei KRITIS-Betreibern 490

DDoS-Angriffe

Hochvoluminöse DDoS-Angriffe in Deutschland (Anteile in %)



Beispiele

Ransomware-Angriff auf kommunalen IT-Dienstleister im Oktober 2023

Betroffene Kommunen:	72
Betroffene Arbeitsplätze:	rund 20.000
Betroff. Einwohnerinnen und Einwohner:	rund 1,7 Mio.

Geschätzter Schaden durch Systemausfälle eines **fehlerhaftes Update** in der Software Crowdstrike Falcon:
> 8,5 Mio. Geräte > 5 Milliarden Dollar

VerbraucherInnen

Top-3-Schäden für Verbraucherinnen und Verbraucher bei IT-Sicherheitsvorfällen und Cybercrime (%)

Vertrauensverlust in den Onlinedienst	30
Finanzieller Schaden	26
Zeitlicher Schaden	24

- Anteil bandbreitenstarker DDoS-Angriffe hat sich gegenüber dem langjährigen Durchschnitt verdoppelt
- Phishing-Angriffe nicht mehr nur durch Missbrauch von Bank-Namen

- Exfiltrierte Daten wesentlich mehr wert als verschlüsselte → Fähigkeit zur Prävention muss gestärkt werden
- Schäden im Milliardenbereich, unvorhergesehene Ereignisse, menschliches Versagen → Fähigkeit zur Vorfallsbewältigung muss gestärkt werden

Die Webseite ist Offline – ohne Vorwarnung

- DDoS-Angriffe sind *schnell*, **massiv** und teilweise schwer zu erknnen
- Schaden an der Reputation
- Verlust an Einnahmen
- Verlorenes Vertrauen bei Kunden und Partnern
- Abwehr durch die eigene IT aufwändig und oft nicht ausreichend möglich

DENIAL OF SERVICE (DDoS)

Website offline – ohne Vorwarnung

- DDoS-Angriffe sind *schnell*, **massiv** und teilweise schwer zu erkennen
- Schaden an der Reputation
- Verlust an Einnahmen
- Verlorenes Vertrauen bei Kunden und Partnern
- Abwehr durch die eigene IT aufwändig und oft nicht ausreichend möglich

Definition & Bewertung

DEFINITI
N&
BEWERTU
NG

Macht es nicht ehr Sinn dem gesamten Kapitel DDoS eine Trennerfolie zu geben statt mittendrin?

DEFINITION& BEWERTUNG

Macht es nicht ehr Sinn dem gemsaten Kapitel DDoS eine Trennerfolie zu geben?

coding powerful systems

Animation von aussen

Denial of Service (DoS)

Eigenschaften

- Einzelne Quelle
- Überlastung des Service bzw. des Netzwerks
- Ziel: Dienst ist für reguläre Besucher nicht erreichbar

DENIAL OF SERVICE (DoS)

Eigenschaften

- Einzelne Quelle
- Überlastung des Service bzw. des Netzwerks
- Ziel: Dienst ist für reguläre Besucher nicht erreichbar

DISTRIBUTED DENIAL OF SERVICE (DDoS)

Eigenschaften

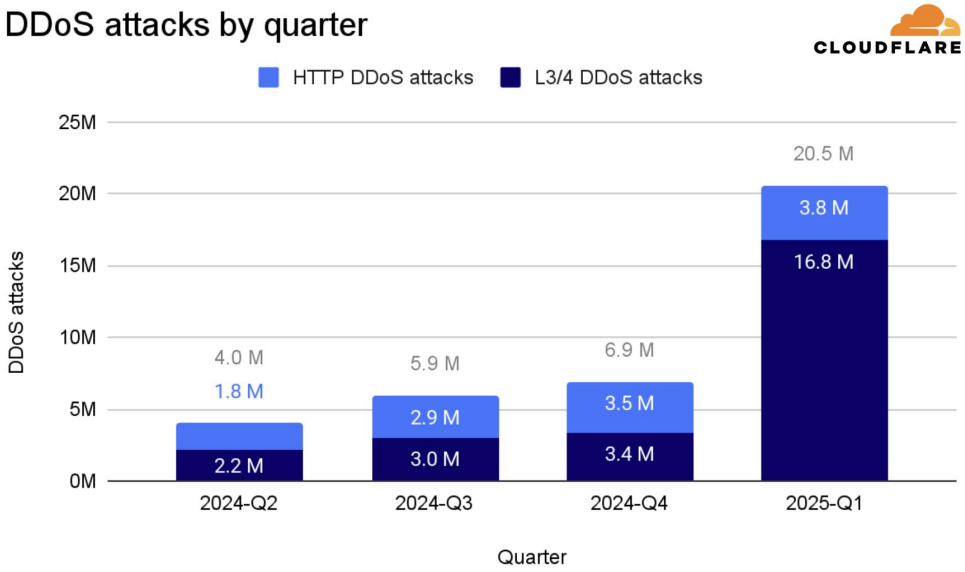
- Angriff wird verteilt
- Viele verschiedene Quellen (in der Regel botnets) greifen gleichzeitig an
- Angriffe in größeren Dimensionen, schwer abzuwehren

Unbeabsichtigtes DoS

Key Characteristics

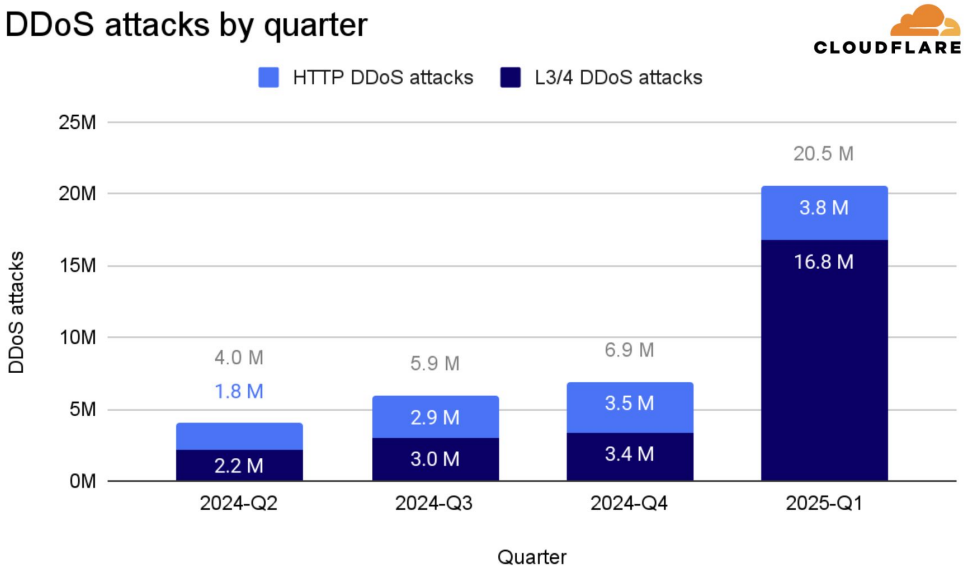
- Accidental service disruption
- Typical use case: Unexpected user behavior or system misconfiguration
- Performance Tests
- Not malicious & no attacker(s)
- Same outcome: Degraded/unavailable service

DDoS Häufigkeit



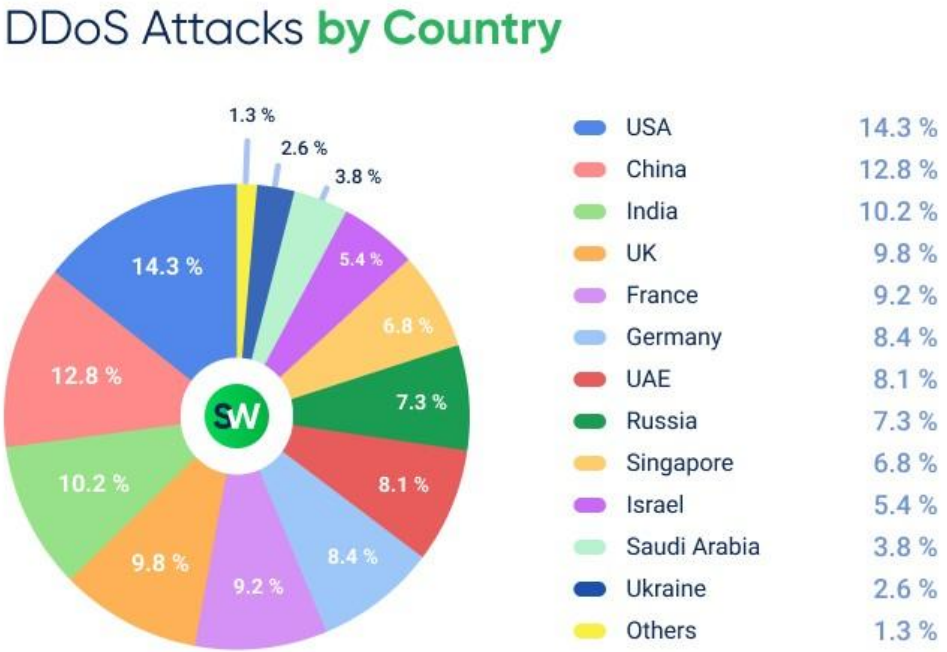
Source: https://blog.cloudflare.com/ddos-threat-report-for-2025-q1

DDoS
Häufigkeit



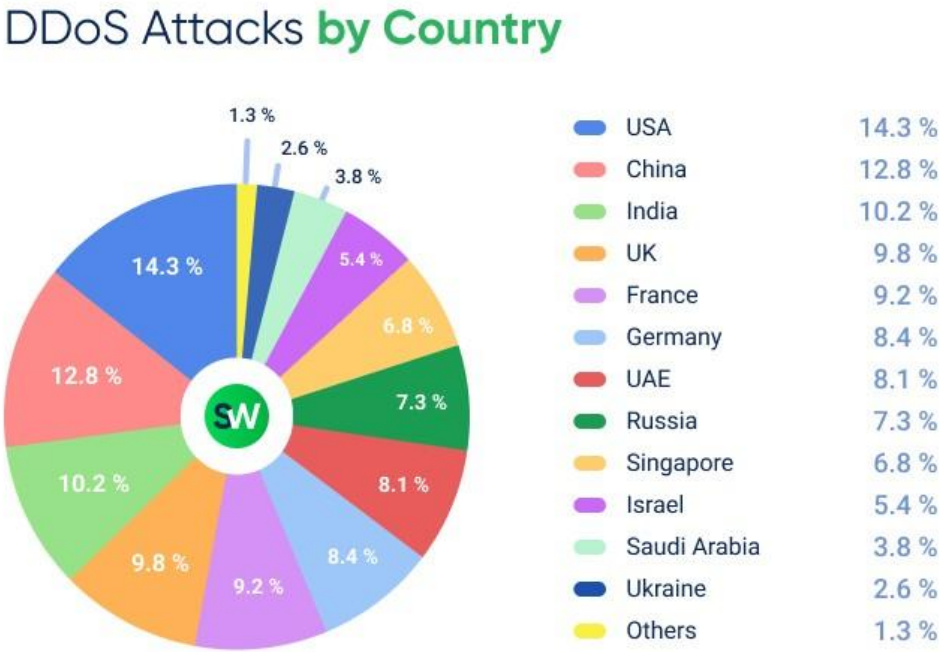
Source: https://blog.cloudflare.com/ddos-threat-report-for-2025-q1

DDoS Angriffe nach Ländern (2024)



Source: https://stormwall.network/resources/blog/ddos-attack-statistics-2024

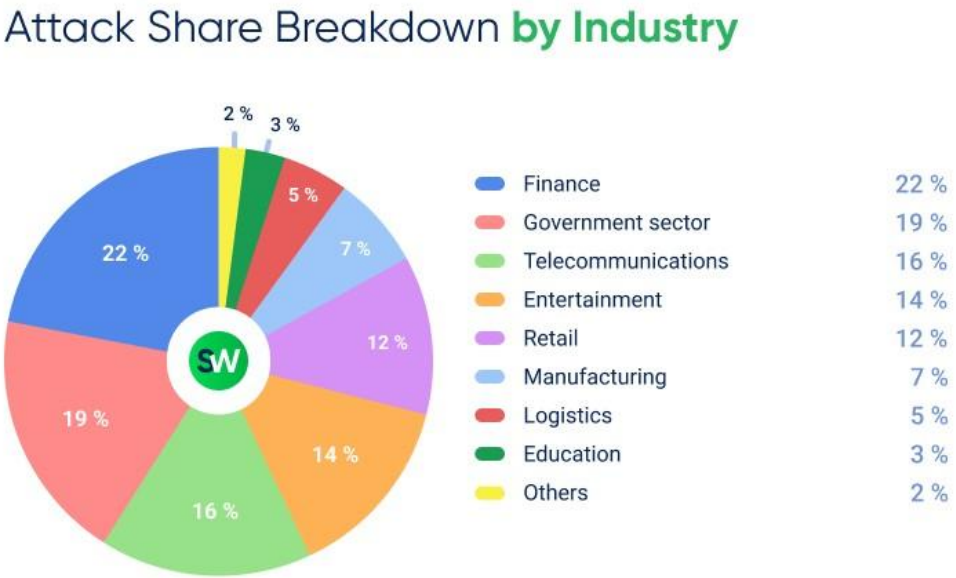
DDoS
Angriffe nach Ländern (2024)



Source: https://stormwall.network/resources/blog/ddos-attack-statistics-2024

DDoS

Angriffe nach Sektor (2024)



Source: https://stormwall.network/resources/blog/ddos-attack-statistics-2024

REKORDE

2017
Google Cloud Platform

Angriff über mehrere Wochen

in der Spitze

2,54 Terabit pro Sekunde

2023
Google

in der Spitze

398 Mio Anfragen pro Sekunde

2024
Minecraft Server

in der Spitze

3 Mrd Pakete pro Sekunde

2025 August

Cloudflare berichtet von abgewehrten, 35 Sekunden dauernden Attacke mit gigantischen Dimensionen (Ziel ungenannt):

5,1 Mrd Pakete pro Sekunde

11,5 Terabit pro Sekunde

KLASSIFI-ZIERUNG

- Offener Industrie Standard
- Klassifizierung der Stärke von Angriffen
- Entsprechend:
  Klassifizierung des Abwehr-Potential

Mektriken (Beispiele)

- Traffic-Volumen
- Anzahl gleichzeitiger Anfragen
- Anzahl der angreifenden Systeme

https://www.ddosresiliencyscore.org/


1
POKING
Volume:
100 Mbps
25K PPS
500 TPS
Bots:
10
Time to Mitigate:
6 hrs
2
SCRIPT KIDDIE
Volume:
1 Gbps
250K PPS
5K TPS
Bots:
50
Time to Mitigate:
4 hrs
3
PLAIN
Volume:
10 Gbps
2M PPS
50K TPS
Bots:
500
Time to Mitigate:
1 hr
4
SOPHISTICATED
Volume:
100 Gbps
25M PPS
200K TPS
Bots:
1,000
Time to Mitigate:
10 minutes
5
PERSISTENT
Volume:
500 Gbps
125M PPS
1M TPS
Bots:
5,000
Time to Mitigate:
5 minutes
6
EXTREME
Volume:
1 Tbps
250M PPS
5M TPS
Bots:
50,000
Time to Mitigate:
1 minute
7
STATE SPONSORED
Volume:
5 Tbps
1B PPS
25M TPS
Bots:
1M
Time to Mitigate:
20 seconds

DDoS
als Vorbereitung oder Ablenkung

- DRS Level 1 “Poking Attacke” : Test der Abwehrbereitschaft
- Eine spürbare Abwehr senkt die Wahrscheinlichkeit eines ernsthaften Angriffs

- DDoS Angriff als Ablenkung für einen ungestörten Einbruch an anderer Stelle (Ransom-Ware)

ABWE
RMASSNAH
. . . MEN

Abwehr

ABWEHR

DDoS Protection Service

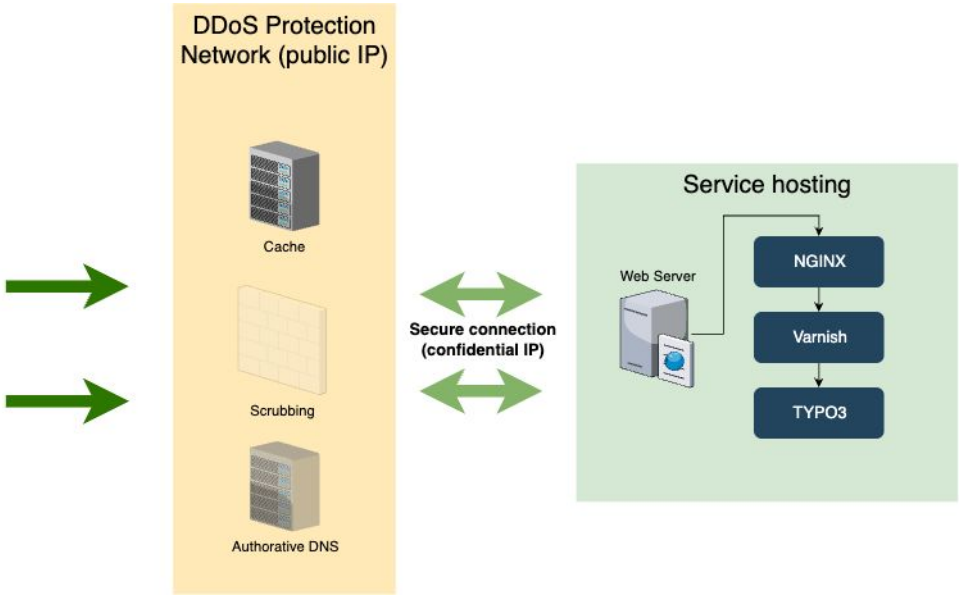
“Traffic scrubbing”

- Internet Traffic läuft vollständig durch das System des Anbieters
- Anbieter trennt Traffic des Angriffs von legitimen Anfragen
- Am Dienst kommen (hauptsächlich) legitime Anfragen an
- Dienst bleibt erreichbar

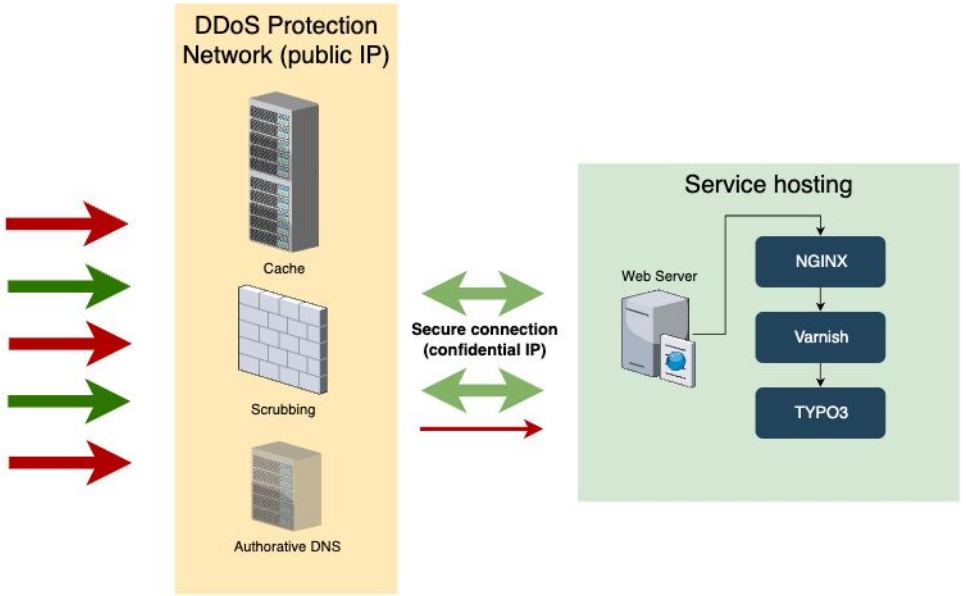
Nebeneffekt:

- CDN: verteilter Cache für statische Inhalte

NORMAL-BETRIEB



WÄHREND EINES ANGRIFFS



ABWEHR

Traffic scrubbing Methoden

- Geo Blocking von IP-Adressen
- Begrenzen der Anzahl gleichzeitiger Anfragen bestimmter Adressen oder Netzwerke
- Fingerprinting von Bot-Aktivitäten
- Spezielle Firewall Regeln
- Duplizieren der Cache Inhalte (CDN)
- Identifikation legitimer Benutzer durch Captcha

ABWEHR

DDoS Protection Service

Alle User Anfragen durchlaufen die Systeme des Protection Anbieters.

Bei der Auswahl eines Dienstleisters beachten:

- Vertrauen
- DSGVO Konformität:
  Betrieb des Dienstes innerhalb der EU
- Bei US-amerikanischen Firmen:
  Zugriff durch Geheimdienste trotzdem möglich (CLOUD Act)
- Abwehr-Potenzial z.B. nach DRS
- Einschätzung des BSI

DIENSTLEISTERLISTE BSI

Empfehlung:
Liste
qualifizierter DDoS-Mitigation-Dienstleister des BSI:

- www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation-Liste.pdf

BSI KRITERIEN

Kriterien (Beispiel)

- Schutz für alle Angriffsverktoren
- Schutz für IPv4 & IPv6 Adressen
- Schutz “on demand”

Dienstleister (Auswahl)

- Akamai
- Amazon
- Cloudflare
- Myra Security*
- Verizon
- Babiel *

* vollständig in Deutschland basierte Anbieter

SCHUTZ FÜR TYPO3 WEBSEITEN

coding powerful systems

Schutz für Webseiten mit TYPO3

FALLBEISPIEL

Bundesgesundheits-ministerium

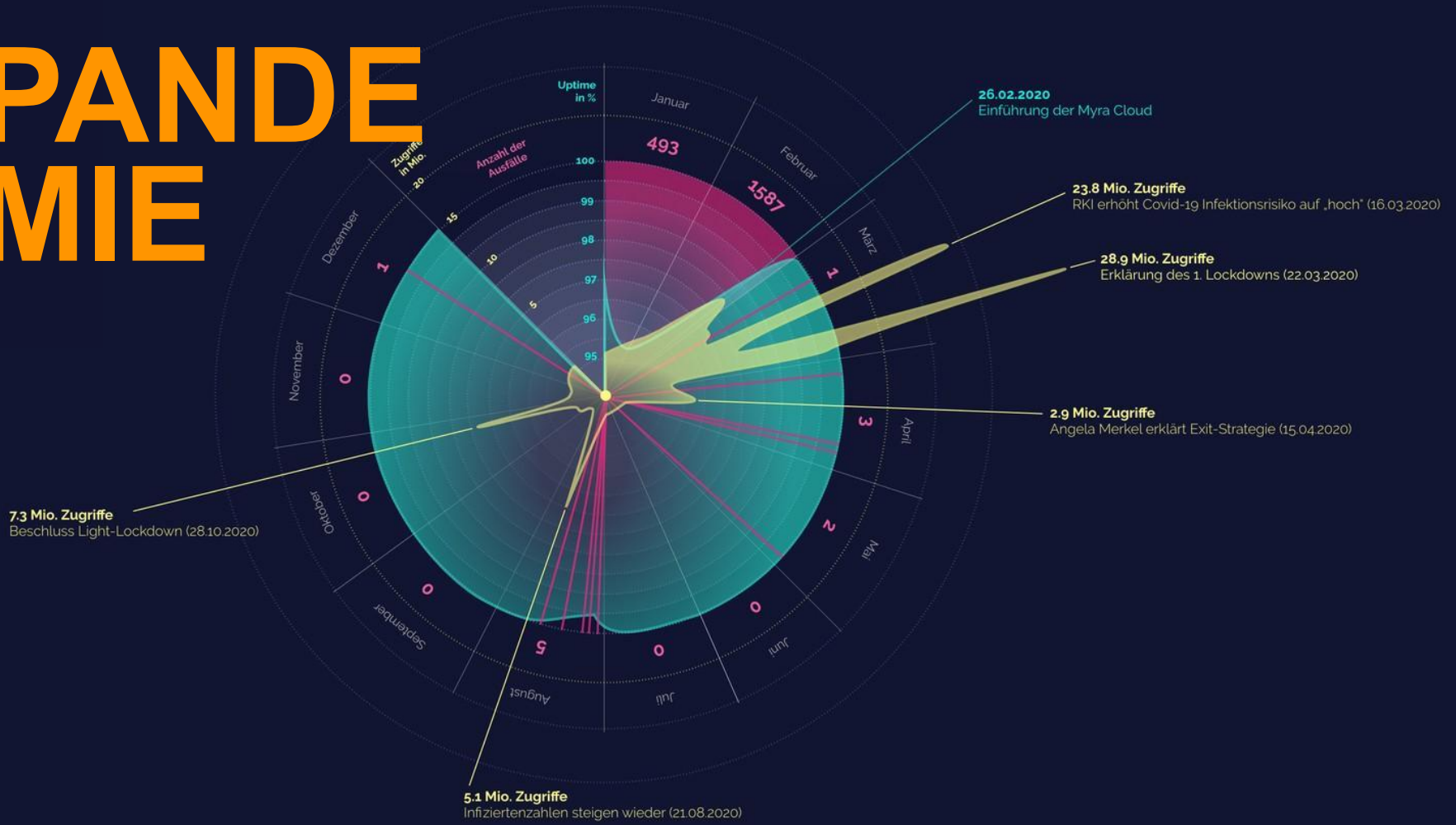
- „Unbeabsichtigtes DoS“ während der Covid19-Pandemie:

  Enorme Anzahl von Zugriffen auf die Webseite erzeugte DoS ähnliche Zustände

Absicherung durch Myra Security GmbH, München

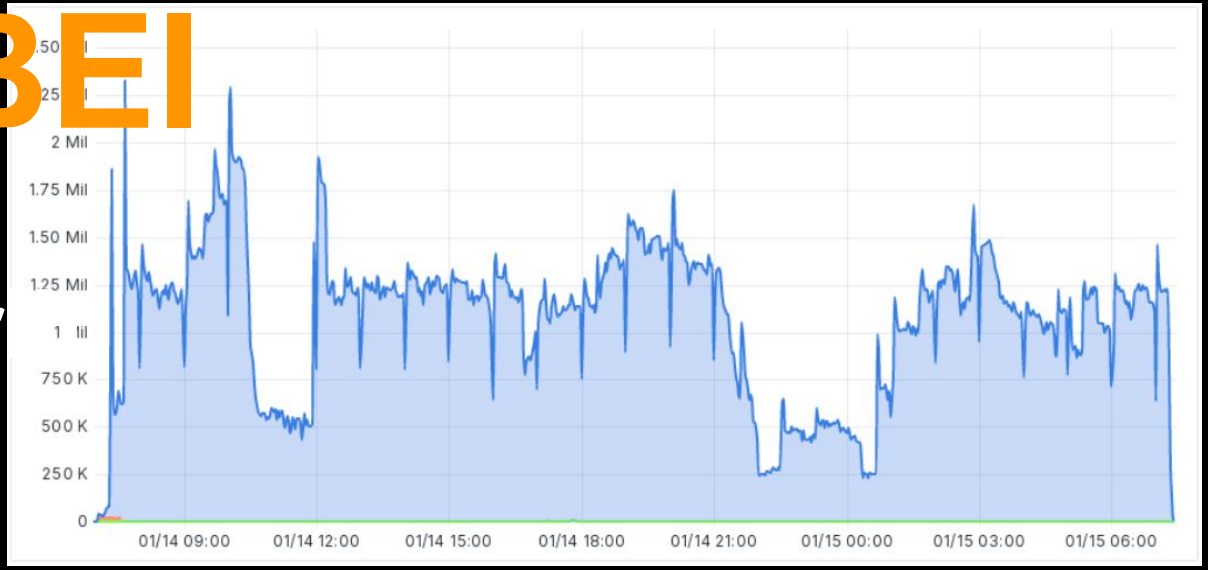
- zu 100% DSGVO konform
- vollständig in Deutschland angesiedelt
- Erfüllt alle Bewertungskriterien des BSI

PANDE
MIE


Uptime in %
Januar
Februar
März
April
Mai
Juni
Juli
August
September
Oktober
November
Dezember
Anzahl der Ausfälle
Zugriffe in Mio.
100
99
98
97
96
95
5
10
15
20
493
1587
1
3
2
0
5
0
0
0
1
26.02.2020
Einführung der Myra Cloud
23.8 Mio. Zugriffe
RKI erhöht Covid-19 Infektionsrisiko auf „hoch" (16.03.2020)
28.9 Mio. Zugriffe
Erklärung des 1. Lockdowns (22.03.2020)
2.9 Mio. Zugriffe
Angela Merkel erklärt Exit-Strategie (15.04.2020)
7.3 Mio. Zugriffe
Beschluss Light-Lockdown (28.10.2020)
5.1 Mio. Zugriffe
Infiziertenzahlen steigen wieder (21.08.2020)

FALL-BEI SPIEL

S-Bahn Ber
Jan 2025



- 782 Mio abgewehrte Anfragen
- 491.000 nicht abgewehrte Anfragen
- 992.000 legitime Anfragen

- Angriff von 4500 IP-Adressen aus mehr als 30 Ländern
- insgesamt 780 Millionen Anfragen

TYPO3 Extension Kontrolle des Cache

Die TYPO3 Extension myra_cloud_connector von CPS integriert eine TYPO3 Webseite in den Cache der Myra Security:

- Automatische Aktualisierung des Myra Cache bei redaktionallen Änderungen
- Gezielte manuelle Aktualisierung durch Redakteure oder TYPO3 Administratorn möglich
- Kommandozeilen-Befehl zur Verwendung in Scripts oder automatisierten Pipelines

TYPO3 EXTENSION

Kontrolle des Cache

Die TYPO3 Extension myra_cloud_connector von CPS integriert eine TYPO3 Webseite in den Cache der Myra Security:

- Automatische Aktualisierung des Myra Cache bei redaktionellen Änderungen
- Gezielte manuelle Aktualisierung durch Redakteure oder TYPO3 Administrator möglich
- Kommandozeilen-Befehl zur Verwendung in Scripts oder automatisierten Pipelines

TAKE AWAYS

1. Nicht durch dDoS ablenken lassen
2. Händische Abwehr unmöglich
3. Auch für hohen organischen Traffic gewappnet sein (Produktlaunch, Kampagnenstart, …)
4. Vorbereitet sein. Nicht erst anfangen, wenn der Angriff läuft.

Danke!

Jetzt informieren hier am Stand bei CPS!

CPS coding powerful systems

Attack types

ATTA
KTYP
ES

DDoS Attack Vectors

OSI-Layer 3 & 4
(Network, Transport)

- Volumetric attacks
- Protocol attacks

Attacks aim at exhausting bandwidth, network infrastructure or network layer of OS

OSI-Layer 7
(Application)

- Application layer attacks

Attacks aim at exhausting target system resources (CPU/RAM)

Volumetric Attack

- **UDP Flood**
  Huge amount of large and/or malformed UDP packets

- **DNS amplification**
  High number of requests to resolve non-existing domain-names,
  DNS Resolvers send their answer to the target

Protocol Attack

- **SYN-ACK Flooding**
  A large number of deliberately incomplete TCP-handshakes exhaust limit of parallel connections and block server resources

- **Smurf Attacks**
  ICMP Flooding with spoofed source IP address is sent to network broadcast address

Application Layer Attacks

- **HTTP-Flood**
  High number of regular http requests to resources requiring a lot of processing time (e.g. large files, search results)

- **„slow DoS“, Slowloris, HTTP/2 Continuation Frame**
  limit of simultaneous server connec-tions is exhausted by deliberately slow data transfers or ”keep alive” packets to prevent server timeouts from closing connections

DDoS Amplification

Relation of

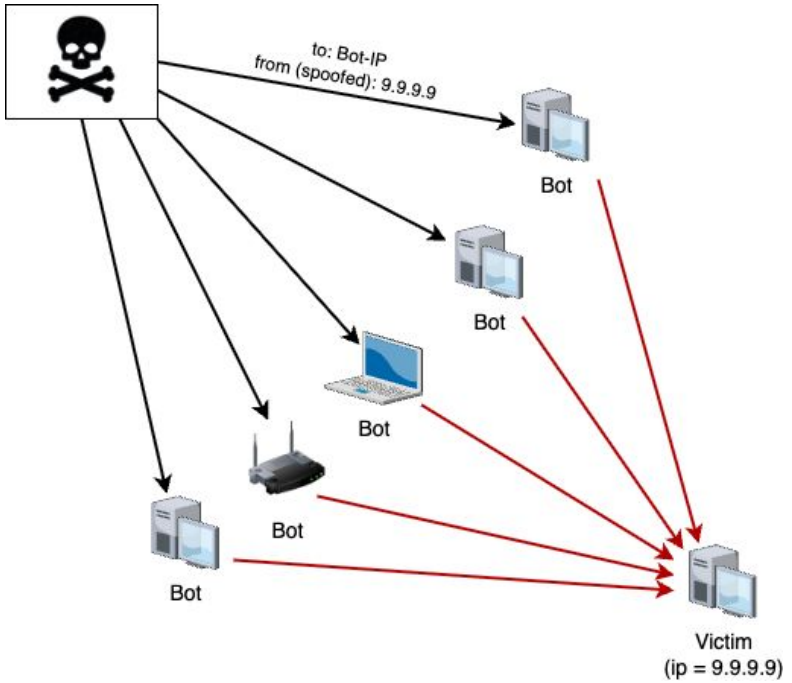
resources (requests/bandwidth)
invested to perform the attack

to

resulting traffic on the target

Smurf Attack

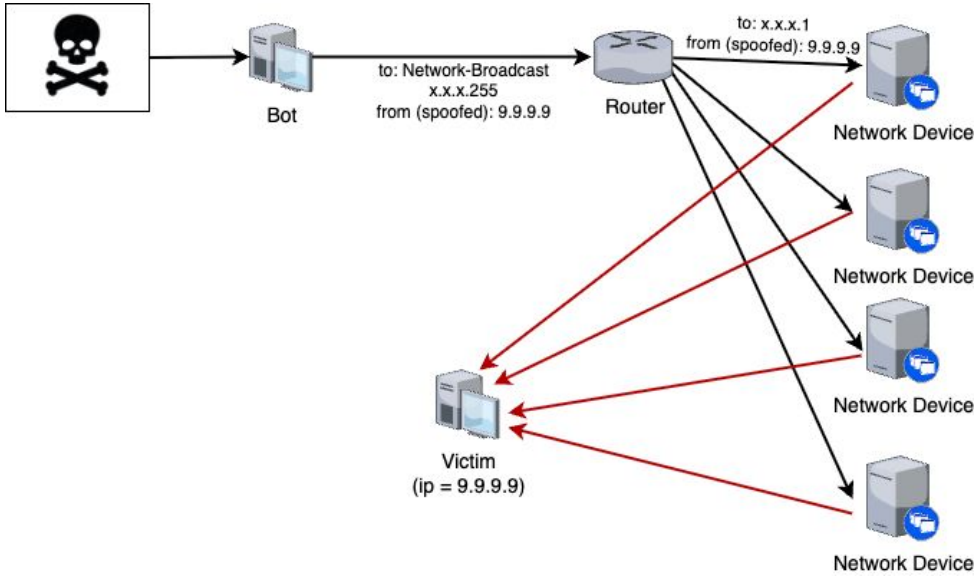
- Attacker sends ICMP packets (ping) using the intended victim's IP-address as forged source IP
- Large number of zombies/bots send answers to target's IP
- Amplification = **1**



Smurf Attack

With a slight modification a significantly larger attack can be performed:

- Bots send forged requests to victim's network broadcast address
- All systems within the network send answers to the victim
- Amplification n = **number of active devices within the network**



Smurf Attack

With a slight modification a significantly larger attack can be performed:

- Bots send forged requests to victim's network broadcast address
- All systems within the network send answers to the victim
- Amplification n = **number of active systems within the network**

DNS Amplification Attack

DNS resolvers can respond to request with large answers:

Request: ~ 60 bytes
Response: ~ 3000 bytes

Amplification: **50**

- spoofed source IP = target's IP
- hard to detect, if multiple DNS Resolvers are used in the attack
- "Reflected Attack":
  attacker's IP address invisible to target

DNS QUERY/ NXDOMAIN Attack

- Large number of DNS resolving requests for randomly created, non-existing subdomains:

  `lkjouz03784469.cps-it.de`

- All resolving requests will be sent to the respective Authoritative DNS server, slowing it down

TAKE AWAYS

1. Measuring = visibility of related components (dependencies)/vendors
2. Eyes on their commitments/roadmap!
3. Have fallbacks! Means options…
4. **Start auditing**, connect