

Praktische Netzwerksicherheit: (2) Denial of Service



Prof. Dr. Klaus-Peter Kossakowski



Gliederung der Vorlesung

- Firewall
- Denial of Service



Inhalte dieses Kapitels

In diesem Kapitel wird die Rolle der Verfügbarkeit in Bezug auf die Anbindung heutiger lokaler Netze ans Internet behandelt und die gängigen Methoden für „Denial of Service Attacks“ / Verfügbarkeitsangriffe erklärt.

Besonders wird darauf eingegangen, wie auch hier Eigenschaften des Netzwerk- sowie der Transportprotokolle genutzt werden, um trotz der Separierung von Rechnern durch Firewalls erfolgreiche Angriffe durchzuführen.

Verschiedene Architekturen werden besprochen.



Ziele dieses Kapitels

Sie können erklären was Denial-of-Service-Angriffe sind und warum und wie diese durchgeführt werden.

Sie kennen verschiedene konkrete Angriffe und können diese den Mechanismen innerhalb von Rechnernetzen zuordnen, die dabei ausgenutzt werden.

Sie können Abwehrmechanismen gegen Denial-of-Service-Angriffe mit ihren individuellen Vor- und Nachteilen benennen.



Worum geht es eigentlich?



Schutzziele

- In der Informationssicherheit werden verschiedene Schutzziele definiert, um Bedrohungen zu klassifizieren
- Schutz heißt hier: Sicherstellen der Eigenschaften von Objekten und somit mehr als „nur“ Vermeidung von Angriffen
- Traditionell spricht man hierbei von CIA
 - Confidentiality – Vertraulichkeit
 - Integrity – Integrität
 - Availability – Verfügbarkeit



Schutzziele: CIA

■ Confidentiality – Vertraulichkeit

- Schutz von Daten vor Kenntnisaufnahme durch Unbefugte

■ Integrity – Integrität

- Schutz von Daten und Systemen vor nicht autorisierten Änderungen

■ Availability – Verfügbarkeit

- Sicherstellung der Verfügbarkeit von Daten und Systemen für Befugte



Verfügbarkeit

■ Zugänglichkeit von Daten und Systemen für Befugte

■ Daten

- Kundendaten, Webseite, Fotosammlung, Bachelorarbeit

■ Dienste

- Webseite (Abruf), E-Mail, Netzwerkzugang, Datenbankserver, Hotline

■ Systeme / Anwendungen

- Arbeitsplatz-PC, Router
- E-Mail-Client, Webserver



Warum brauchen wir Verfügbarkeit?

- Verfügbarkeit gewährleistet den autorisierten Zugriff auf Daten und Systeme
- Keine Verarbeitung ohne Daten oder Systeme
 - Webseiten / Onlineshops
 - Präsentation der Firma und Angebote
 - Produktdatenbank
 - Abruf, Suche, Filterung von Angeboten
 - Kundendaten
 - Bestellvorgänge und Abrechnungswesen



Wie messen wir Verfügbarkeit?

- **Verfügbarkeit wird vielfach als anteilige Verfügbarkeit über die Zeit gemessen**
Verfügbare Zeit / gesamte Zeit
- **Service Level Agreements (SLAs)**
schreiben die garantierte Verfügbarkeit fest
- **Ein großer deutscher Internet Provider bietet eine „mittlere Verfügbarkeit [von] 97% im Jahresdurchschnitt“**
- **Ist das viel?**
 - Ein Jahr hat $365 * 24 = 8.760,0$ h
 - Ausfälle: $3\% * 8760 \text{ h} = 262,8 \text{ h} = 10,9 \text{ d}$



Wie messen wir Verfügbarkeit? (2)

■ Verfügbarkeitsklassen (VK) werden z.B. im IT- Grundsatz über die Anzahl führender Neunen definiert

- VK 0: Ohne Verfügbarkeitsgarantie
- VK 1: Normale Verfügbarkeit 99%
- VK 2: Erhöhte Verfügbarkeit 99,9%
- VK 3: Hochverfügbar 99,99%
- VK 4: Höchstverfügbar 99,999%

... und wieviel ist das dann bei VK 4?

- Ausfälle: $0,001\% * 8760 \text{ h} = 8,76 \text{ h}$



Einschränkungen bei SLAs

- **Wichtig ist der zugrunde gelegte Zeitraum, von dem ausgehend die Berechnung erfolgt**
- **Behandlung von Wartungsfenstern**
 - Zählen solche als Ausfall oder verringern diese die Berechnungsgrundlage
 - Erfordern sie eine Ankündigung? Mit welcher Frist?
- **Weitere Einschränkungen nach Art des Ausfalls (höhere Gewalt)**



Angriffe auf die Verfügbarkeit == Denial of Service



Denial of Service

- **Allgemein alle Angriffe mit dem Ziel, die Verfügbarkeit des angegriffenen Objekts für die legitimen Nutzer zu beeinträchtigen**
 - Daten Löschen, Verschlüsseln
 - Diensten Überlast von Systemen/Netzen, veränderte Konfiguration
 - Systemen Zerstörung des Systems, Löschen von Routen, Überlast von Netzen, Absturz von Anwendungen, veränderte Konfigurationen



Warum ...

... werden Denial-of-Service-Angriffe überhaupt durchgeführt?

- Ablenkung
- Cybercrime / Erpressung
- Hacktivismus, politische Ziele
- Online-Auseinandersetzungen
- Vandalismus, Lulz
- Wettbewerb ausschalten



Ablenkung

- **Denial of Service lenkt von anderen Aktivitäten ab**
- **Eine Überlastung von Sicherheitsmechanismen – aber auch Verantwortlichen oder Analysten – verhindert oder versteckt Alarme**
 - Nicht alle eingehenden Daten können verarbeitet werden
 - Flut von Alarmen verhindert Priorisierung und rechtzeitige Reaktion



Cybercrime / Erpressung

- **Ziel eines Angriffs ist die Erpressung des Opfers**
 - Ransomware
 - Verschlüsselung von Daten
 - Entschlüsselung gegen Bezahlung (manchmal)
 - Schutzgelderpressung
 - Androhung von Angriffen
 - Zahlung, damit Angriffe nicht erfolgen oder aufhören



Cybercrime / Erpressung (2)

■ DD4BC: DDoS for Bitcoins (seit Mitte 2014)

- Ziele aus verschiedenen Branchen: Glücksspiel, Bankensektor, Verlage, ...
- Schutzgeld von bis zu 100 BTC
- Nachahmer: Armada Collective, ...
 - Teilweise ohne angedrohte Angriffe

■ Populäre Ziele: Wettbüros

- Insbesondere zeitnah zu sportlichen Großveranstaltungen
 - Olympia, Superbowl, Pferderennen



Cybercrime / Erpressung (3)

- **Angriffe werden auch gegen Bezahlung durchgeführt**
 - DDoS as a Service
 - Booter
 - Angriffe auf Gegner oder Servern von Online-Spielen
 - Stresser
 - Präsentiert als Testdienste für eigene Systeme, allerdings kaum bis keine Kontrolle der Legitimation



Cybercrime / Erpressung (4)

| Name | Boot-Zeit | Verkehr | Preis pro Monat |
|-------------|-----------|------------|-----------------|
| zStress | 1200 | 15-20 Gbps | \$15,00 |
| Data Booter | 900 | 10-20 Gbps | \$15,00 |
| instaBooter | 1800 | 10-20 Gbps | \$20,00 |
| SynStress | 1200 | 10-15 Gbps | \$14,99 |



Hacktivismus, politische Ziele

- **Hacktivismus (aus Hack und Aktivismus) ist die (kreative) Anwendung von Technik zur Verfolgung politischer Ziele**
 - Angriff ↔ Onlinedemonstration
- **Online-Demonstration gegen Lufthansa wegen Zwangsabschiebungen (2001)**
 - Rechtliche Bewertung schwierig, OLG Frankfurt hat die Klage abgewiesen



Hacktivismus, politische Ziele (2)

■ Operation Payback (2010)

- Ursprünglich Reaktion von Anonymous auf DoS-Angriffe auf Torrentseiten, die Take-Down-Notices ignorierten
- Ziele in der Musik- und Filmbranche: Kanzleien, Copyright-Befürworter
- Neue Ziele, nachdem Banken Spenden für WikiLeaks wegen der Veröffentlichung von diplomatischen US-Papieren einfrieren: American Express, Visa, PayPal, ...



Hacktivismus, politische Ziele (3)

- **Politische Ziele werden aber auch im Rahmen von staatlichen Konflikten verfolgt**
 - „Cyberwar“
- **Estland (2007)**
 - Umstellung eines pro-russischen Denkmals in Tallinn führt zu russischen Protesten
 - DoS-Angriffe auf Webseiten der Regierung, des Parlament, von Medien und Banken
 - Angreifer unklar: Aktivisten, Kreml-nahe Aktivisten, ...?



Online-Auseinandersetzungen

- Angriffe, die zur Austragung von Konflikten durchgeführt werden
- DoS auf KrebsOnSecurity (2016)
 - Wahrscheinlich Reaktion auf Veröffentlichungen zum Stresser vDOS
 - zeitnah zur Verhaftung der mutmaßlichen Betreiber



Titanium Stresser Service

TITANIUM Stresser

Dashboard

Stresser

Server Status

Tools 9

- + Skyline Resolver
- + Steam Resolver
- + Cloudflare Resolver
- + Friends & Enemies
- + Geolocation
- + IP Logger
- + Pinger
- + Email Bomber
- + Skynet Bot

Dashboard

Introduction

Welcome to **Titanium Stresser**! Home to the *greatest* stress testing services you will find on the market today and of course tomorrow tool.

We have next generation solutions to all of your issues you will ever have.

With our **sleek** design and **massive** power how could you go wrong?

Even in the unlikely cause of something going wrong we have a dedicated team that work 24/7 to help you do your daily deeds.

News

Servers fixed 06 Jan

We have now fixed the servers, open a ticket if you want 3 days credited to your package (this offer expires the 10th, any tickets received after then will be deleted as you obviously wouldn't have used titanium during the time it was down).

Power is under maintenance for up to 2 days. 04 Jan

We have had a little issue with our server array and the servers will be down for up to 2 days.

User CP

- User Settings
- Store Notes
- Upgrade Package
- Purchase Addons



Titanium Stresser Service (2)

KrebsonSecurity
In-depth security news and investigation

25 UK Man Gets Two Years in Jail for Running APR 17 ‘Titanium Stresser’ Attack-for-Hire Service

A 20-year-old man from the United Kingdom was sentenced to two years in prison today after admitting to operating and selling access to “**Titanium Stresser**,” a simple-to-use service that let paying customers launch crippling online attacks against Web sites and individual Internet users.

Adam Mudd of Hertfordshire, U.K. admitted to three counts of computer misuse connected with his creating and operating the attack service, also known as a “**stresser**” or “**booter**” tool. Services like Titanium Stresser coordinate so-called “distributed denial-of-service” or **DDoS** attacks that hurl huge barrages of junk data at a site in a bid to make it crash or become otherwise unreachable to legitimate visitors.



Vandalismus, Lulz

- Ziel eines Angriffs sind Schlagzeilen, Bloßstellung des Ziels, Rufaufbau, etc.
- LulzSec
 - Verschiedene Angriffe auf prestigeträchtige Ziele
 - Regierungsseiten, Online Gaming
 - „Laughing at your security since 2011“
 - DoS-Angriff auf die Webseite des CIA (2011)



Wettbewerb ausschalten

- Von der Nutzung von Bootern / Stressern zur Austragung von Konflikten hin zur Behinderung von Wettbewerbern ist es nur ein kleiner Schritt
- Lyft ↔ Uber (2014)
 - Gegenseitige Anschuldigungen, Fahrten beim Konkurrenten zu buchen und dann wieder zu stornieren



Wie wird ein DoS erreicht?

- Ein DoS kann an verschiedenen Stellen von IT-Systemen erreicht werden:
 - Programmschwachstellen
 - Protokollschwachstellen
 - Prozessschwachstellen
 - Ressourcenauslastung
 - Plötzliche Popularität:
flash crowd, Slashdot-Effekt
- Selbst verursachte Probleme sehen (fast) genauso aus → Konfigurationsfehler

DoS durch Programmschwachstellen



- Fehler in Software lassen sich ausnutzen, um die Bearbeitung von legitimen Anfragen zu beeinträchtigen
 - Programmfehler, die zum Absturz führen
 - Ressourcen innerhalb des Programms, die verbraucht werden
 - Ressourcen außerhalb des Programms, die durch das Programm belegt werden
 - Hauptspeicher, Festplattenspeicher

DoS durch Protokollschwachstellen



- **Schwachstellen in Protokolldefinitionen lassen sich auf ähnliche Weise ausnutzen sind allerdings häufig schwerwiegender**
 - Nur durch Änderung des Protokolls behebbar
 - Teilweise bewusste Designentscheidung
 - Lässt sich durch Software manchmal abmildern
 - Einschränkung des Protokolls oder des Zugriffs auf Protokollfunktionen

DoS durch Prozessschwachstellen



- **Schwachstellen in definierten Prozessen, die Zustände ermöglichen, die eine Dienstleistung verhindern**
 - Außerhalb der technischen Infrastruktur aber mit Auswirkung darauf
 - Hijacking von Adressbereichen oder Domänen (Umkonfiguration beim Registrar)

DoS durch Ressourcenauslastung



- Angriffe belegen (endliche) Ressourcen, die für die Bearbeitung von legitimen Anfragen dann nicht zur Verfügung stehen
 - Bandbreite
 - Hauptspeicher
 - Zustände
 - offene Verbindungen
 - bearbeitete Anfragen
 - CPU

slashdot-Effekt durch plötzliche Popularität



- Verlinkung auf populären Portalen führt zu verstärkter Nutzung der Angebote
- Legitime Anfragen haben nicht erwartete Nebenwirkungen:
 - Kosten durch hohen Verkehr
 - Schwer von Angriffen zu unterscheiden
- Der beim Nutzer beobachtete Effekt entspricht dem eines DoS



Wie funktionieren Denial of Service Angriffe?



Angriffstypen

- Über die Schwachstellen und konkreten Protokolle und Layer hinweg, kommen grundlegende Angriffstypen vor
 - Einzelnes Paket, einzelne Anfrage
 - Flood
 - Reflection
- **DDoS (Distributed Denial of Service)**
 - Verteilter Angriff von mehreren Quellen, um die Auswirkungen zu verstärken

Angriffstypen

Flood



- Bei einer Flood wird das Ziel mit einer Vielzahl von Daten geflutet, so dass legitime Anfragen darin untergehen
- Eine Überlastsituation kann dabei an unterschiedlichen Stellen der Datenverarbeitung auftreten
 - Router durch zu viele Pakete
 - Leitung durch zu hohe Bandbreite
 - Firewall oder Anwendung durch zu viele Verbindungen

Angriffstypen

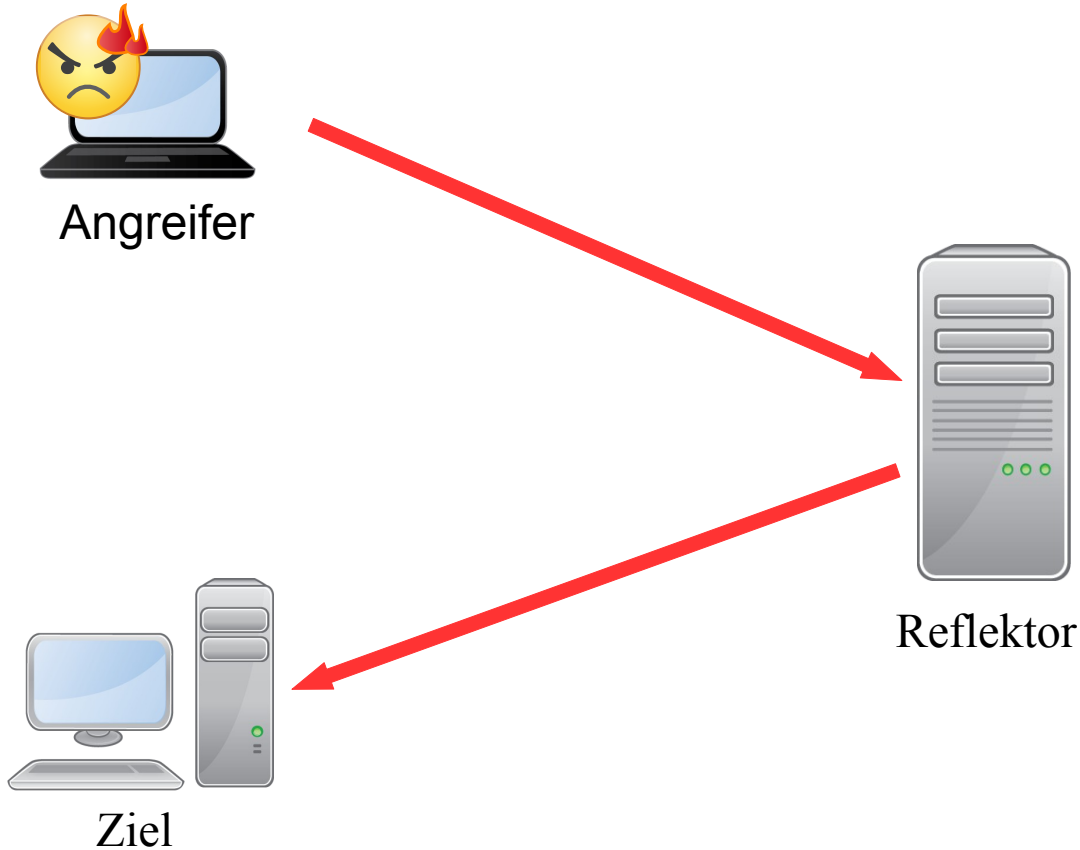
Reflection



- Bei einem Reflection-Angriff wird ein drittes System davon überzeugt, dass das Ziel Anfragen stellt und so quasi „über Bande“ angegriffen
- Der Angreifer ist hierbei auf dem Ziel nicht mehr ersichtlich und somit schwer zu identifizieren
- In Kombination mit Diensten, die auf kleine Anfragen große Antworten erzeugen, lässt sich der Effekt vergrößern (Amplification)

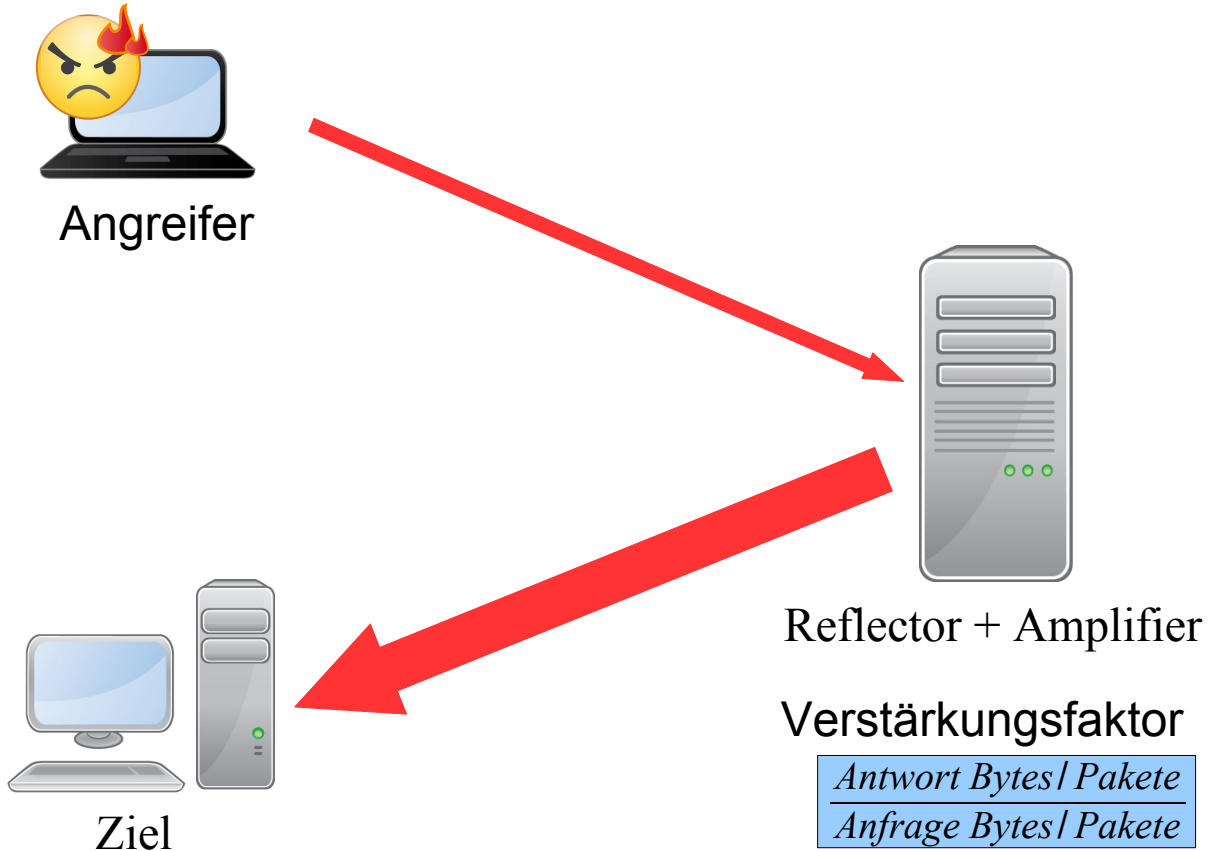
Angriffstypen

Reflection (2)



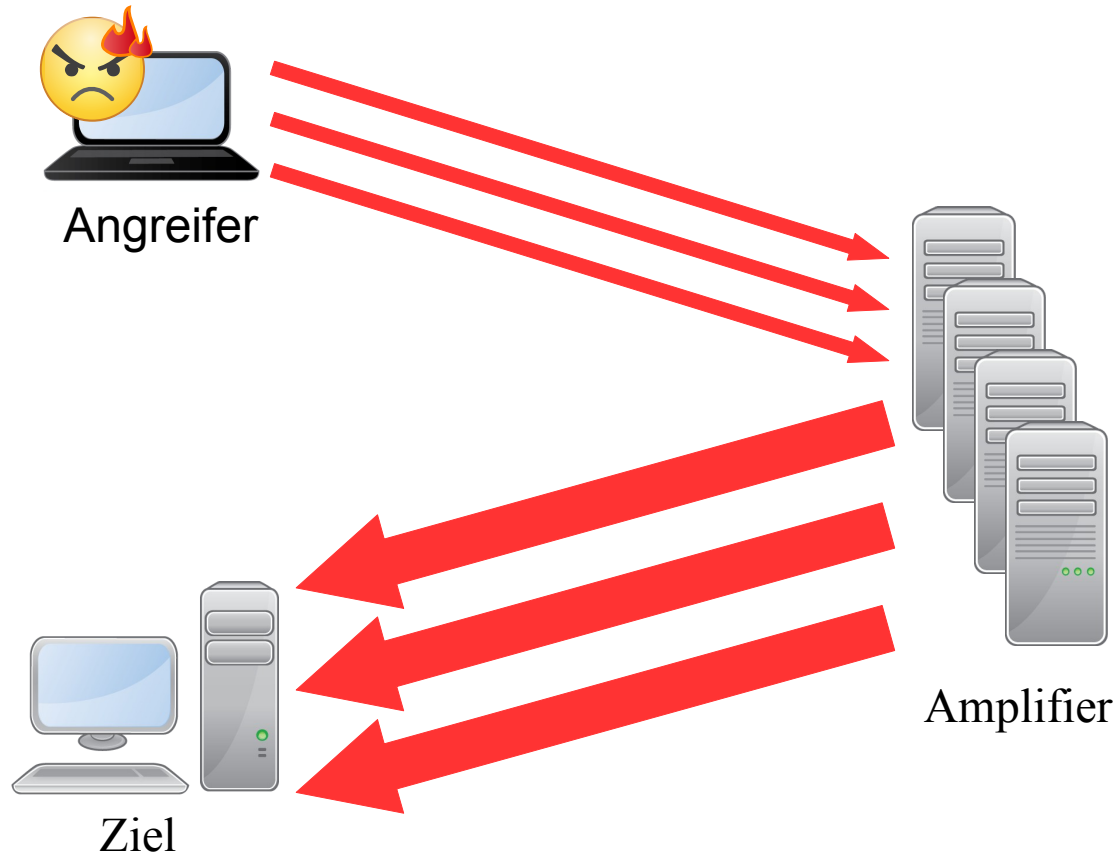
Angriffstypen

Reflection / Amplification



Angriffstypen

Reflection / Amplification (2)





DoS gegen Infrastruktur

- **Um einen Dienst zu stören, muss der Angreifer nicht den Dienst selbst, sondern nur dessen Verfügbarkeit, einschränken**
 - Netzwerkstruktur
 - Router und Leitungen auf dem Weg
 - Firewall vor Webserver
 - Überlastbar durch gespeicherten Verbindungsstatus
 - IDS überlastet Analysten durch getriggerte Fehlalarme
 - Kollateralschäden

Layer 7

Angriffe: Webserver



- Webserver lassen sich je nach Software durch einzelne Anfragen angreifen
 - Programmschwachstelle, einzelne Anfrage
- **PHP Floating Point Bug**
 - CVE-2010-4645
 - Versionen vor 5.2.17 bzw. 5.3.5
 - Endlosschleife mit 100% CPU-Last auf 32- Bit- Systemen:

```
<?php $d = 2.2250738585072011e-308; ?>
```

Layer 7

Angriffe: Webserver (2)



- **Webserver lassen sich durch teure Anfragen angreifen**
 - Ressourcenauslastung, Flood
- **Anfragen an dynamische Seiten, deren Bereitstellung teuer ist:**
 - Hoher CPU-Verbrauch und Belegung von Verbindungen
 - Datenbankanfragen (CMS)
 - Suchfunktionen

Layer 7

Angriffe: Webserver (3)



- Webserver lassen sich durch teure Anfragen angreifen
 - Ressourcenauslastung, Flood
- Anfragen, deren Bearbeitung verlangsamt wird:
 - Belegung von Verbindungen
 - Slowloris
 - Slow Read
 - Schon wenige Anfragen können selbst große Webseiten stören

Layer 7



Angriffe: Webserver – Slowloris

- Slowloris sendet unvollständige HTTP-Anfragen an Webserver, die so nie die Anfrage beantworten können

```
GET / HTTP/1.1\r\n
Host: host\r\n
User-Agent: [...] \r\n
Content-Length: [...] \r\n
...
X-a: b\r\n
...
X-a: b\r\n
...
```

Layer 7



Angriffe: Webserver – Slow Read

- Slow Read sendet vollständige Anfragen, ändert dann aber die Parameter zur Flusskontrolle, um die Antwort sehr langsam zu lesen
- Receive Window Size wird sehr klein
- Empfangspuffer werden langsam geleert

Layer 7

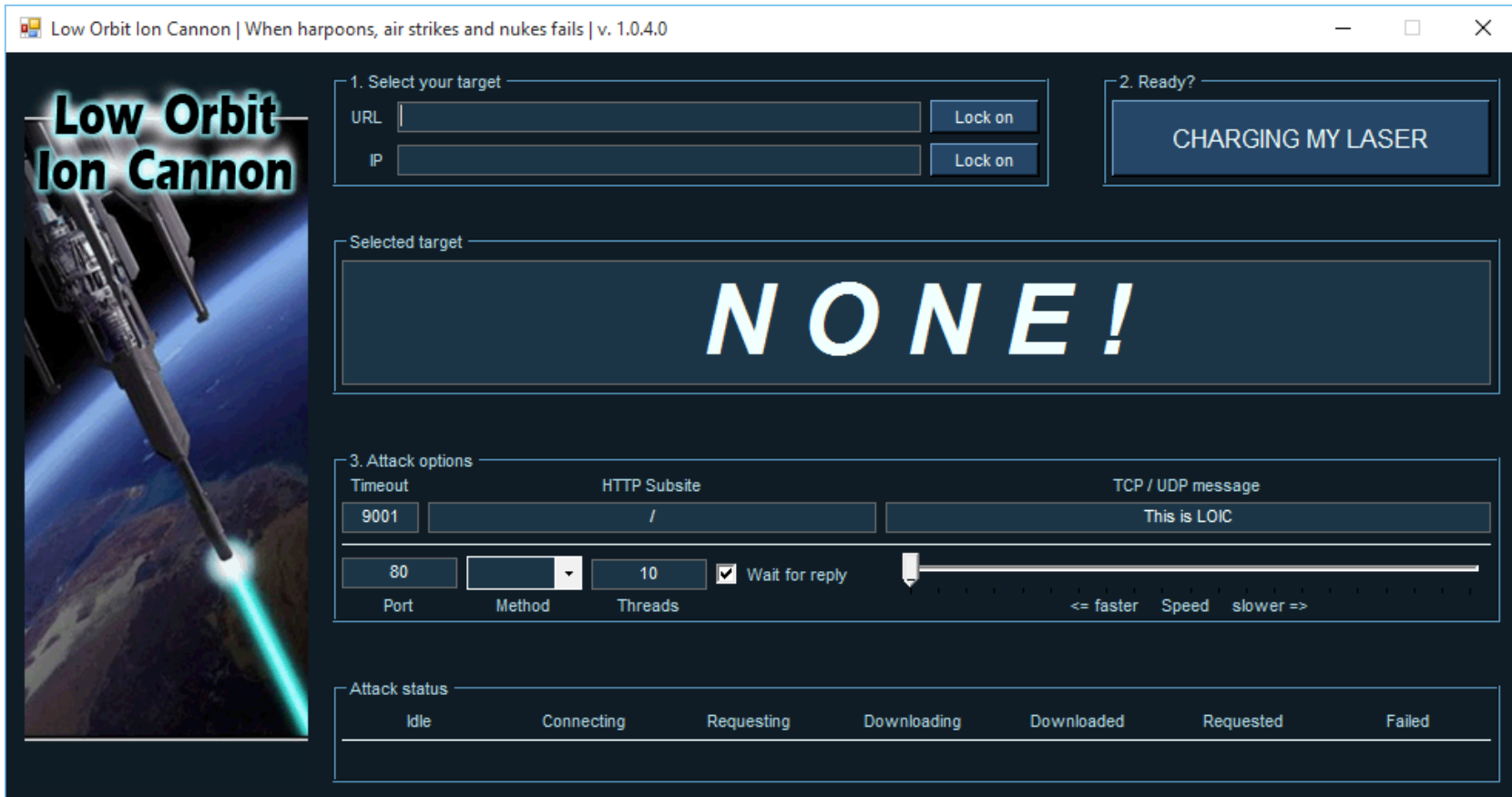
Angriffe: Webserver (4)



- **Webserver lassen sich durch viele Anfragen angreifen**
 - Ressourcenauslastung, Flood
- **LOIC (Low Orbit Ion Cannon)**
 - Tool für Lasttests
 - Sendet Flut von TCP, UDP oder HTTP- Anfragen
 - Verwendet in Operation Payback „Hive Mind“ für Fernsteuerung

Layer 7

Angriffe: Webserver – LOIC



Screenshot by FockeWulf FW 190, Wikipedia, CC BY-SA 4

Layer 7

Angriffe: Spam



- Spam ist ein DoS-Angriff auf den Dienst E- Mail
- ... oder auf den Empfänger der Nachrichten
 - Ressourcenauslastung, Flood
 - Überlast von CPU, Speicher durch Verarbeitung von Nachrichten
 - Überlast des Anwenders durch Filterung von Nachrichten

Layer 7

Angriffe: Spam (2)



■ Verstärkung durch

- Kontaktformulare auf Webseiten, da hierdurch die Filterung erschwert wird
- Sogenannte Joe Jobs
 - Eintragen des Ziels als Absender für versendete E-Mails
 - Ziel bekommt Fehlermeldungen (Bounces) von Reflektoren, landet unter Umständen auf Blacklists

Layer 4

Flood-Angriffe



- **Flood-Angriffe auf diesem Layer nutzen zum Angriff auf die Verfügbarkeit**
 - Das reine Verkehrsvolumen in Paketen oder Bytes
 - Eigenschaften der Verarbeitung auf den durchlaufenen Systemen

Layer 4

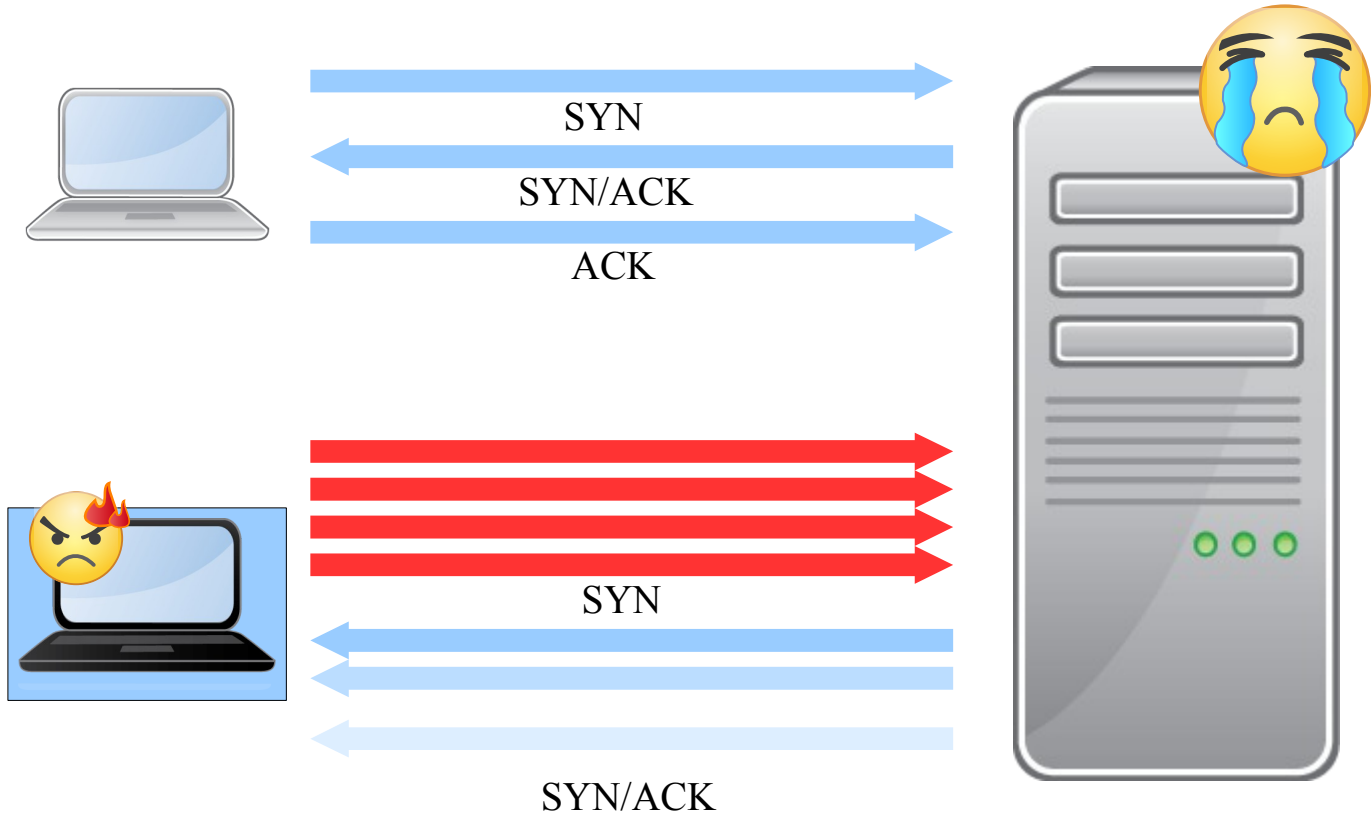
Flood-Angriffe: SYN-Flood



- Bei einer SYN-Flood wird das Ziel mit einer Vielzahl von SYN-Paketen bombardiert
 - Ressourcenauslastung, Flood
- Überlast durch begrenzten Speicher für Verbindungen
 - Der Angreifer sendet SYN-Pakete, ohne sich um den Verbindungszustand zu kümmern
 - Das Ziel baut Verwaltungsstrukturen auf, um den Zustand der Verbindung zu speichern (z. B. Sequenznummern)

Layer 4

Flood-Angriffe: SYN-Flood (2)



Layer 4

Reflection-Angriffe



- **Reflection-Angriffe lassen sich insbesondere durch Anwendungen und Protokolle durchführen, die auf UDP basieren**
 - Ressourcenauslastung, Flood
 - Keine Verifikation von Quell-IP-Adressen
 - Anwendungen schicken große Antworten auf kleine Anfragen
- **Auch TCP ermöglicht solche Angriffe, allerdings mit geringerer Verstärkung**

Layer 4

Reflection-Angriffe: DNS



- Bei einer DNS- Reflection werden Anfragen mit der Adresse des gewählten Angriffsziels als Absender verschickt
- Reflektoren sind „Open Resolver“, die Anfragen für beliebige Systeme aus dem Internet beantworten
 - Open Resolver Projekt
<http://www.openresolverproject.org/>
- Verstärkungsfaktor ~ 75

Layer 4

Reflection-Angriffe: DNS (2)



- Für eine hohe Verstärkung werden
 - Bestimmte Anfragen gewählt
 - Selbst Antworten zur Verfügung gestellt
 - Indem geeignete Antworten auf einem eigenen DNS-Server angeboten und dann über Open Resolver abgerufen werden
- DNSSEC ausgenutzt wird (EDNS)
 - Ursprünglich wurden DNS-Anfragen per UDP bis 512 Byte beantwortet, größere nur per TCP
 - EDNS ist eine Erweiterung von DNS um die größeren DNSSEC-Antworten zu unterstützen
→ MUST 1220 Byte, SHOULD 4000 Byte

Layer 4

Reflection-Angriffe: DNS (3)



■ Bestimmte Anfragen

`dig ANY isc.org`

Anfrage: 48 Byte, Antwort: 3.998 Byte

Verstärkung: 83

■ Selbst Antworten bereitstellen

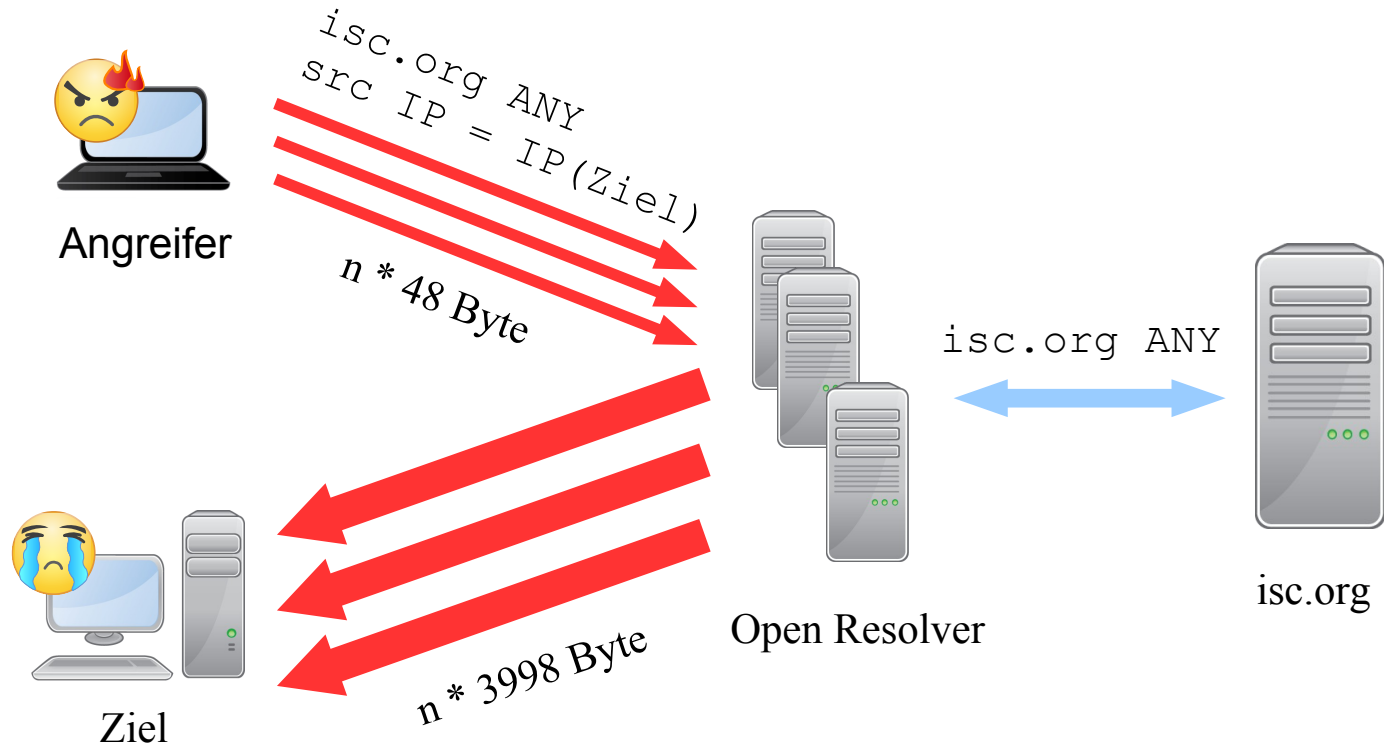
- ghmn.ru und fkfkfkfa.com lösen auf hunderte IP-Adressen auf (2013)

■ DNSSEC platziert Schlüsselmateriale und kryptographische Signaturen im DNS

- Größere Antworten

Layer 4

Reflection-Angriffe: DNS (4)



Layer 4

Reflection-Angriffe: NTP



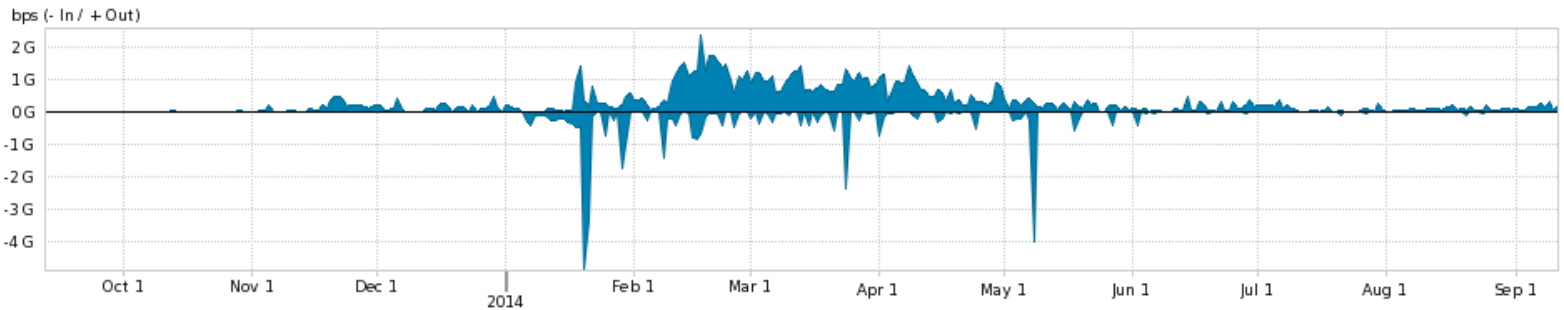
- Bei einer NTP-Reflection werden verschiedene Statusanfragen an NTP-Server mit dem Ziel als Absender verschickt
 - monlist – Liste der letzten NTP-Clients
 - Verstärkung ~ 1.000
 - readvar – Abfrage von Statusvariablen
 - Verstärkung ~ 10
 - Open NTP Project
<http://openntpproject.org/>

Layer 4

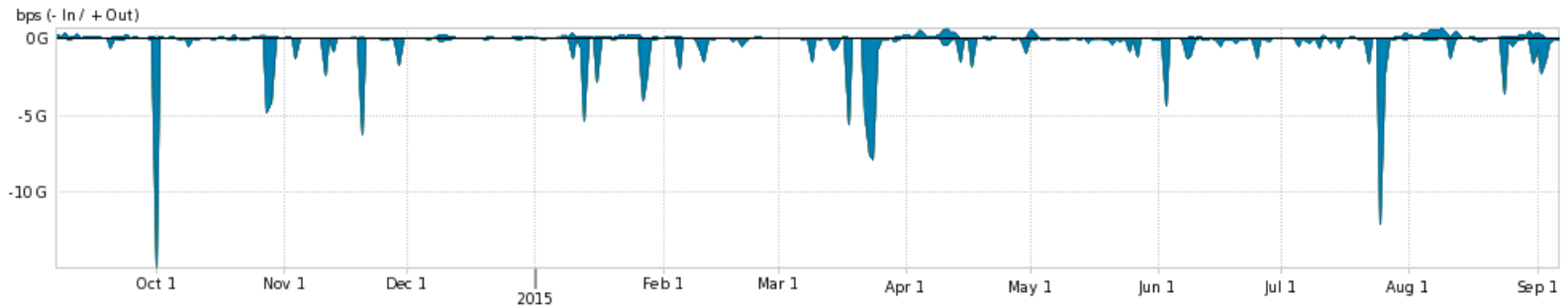
Reflection-Angriffe: NTP



2013/14



2014/15

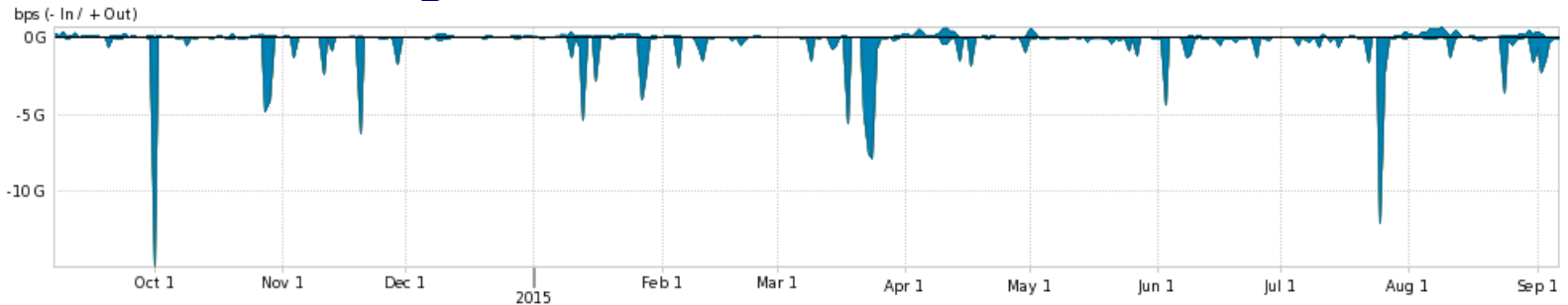


Layer 4

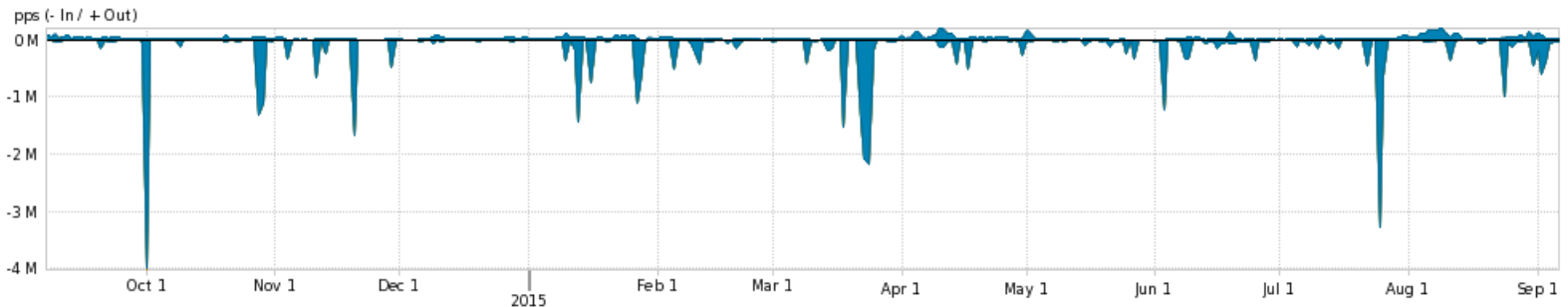
Reflection-Angriffe: NTP



2014/15: Bytes/sec



2014/15: Packets/sec



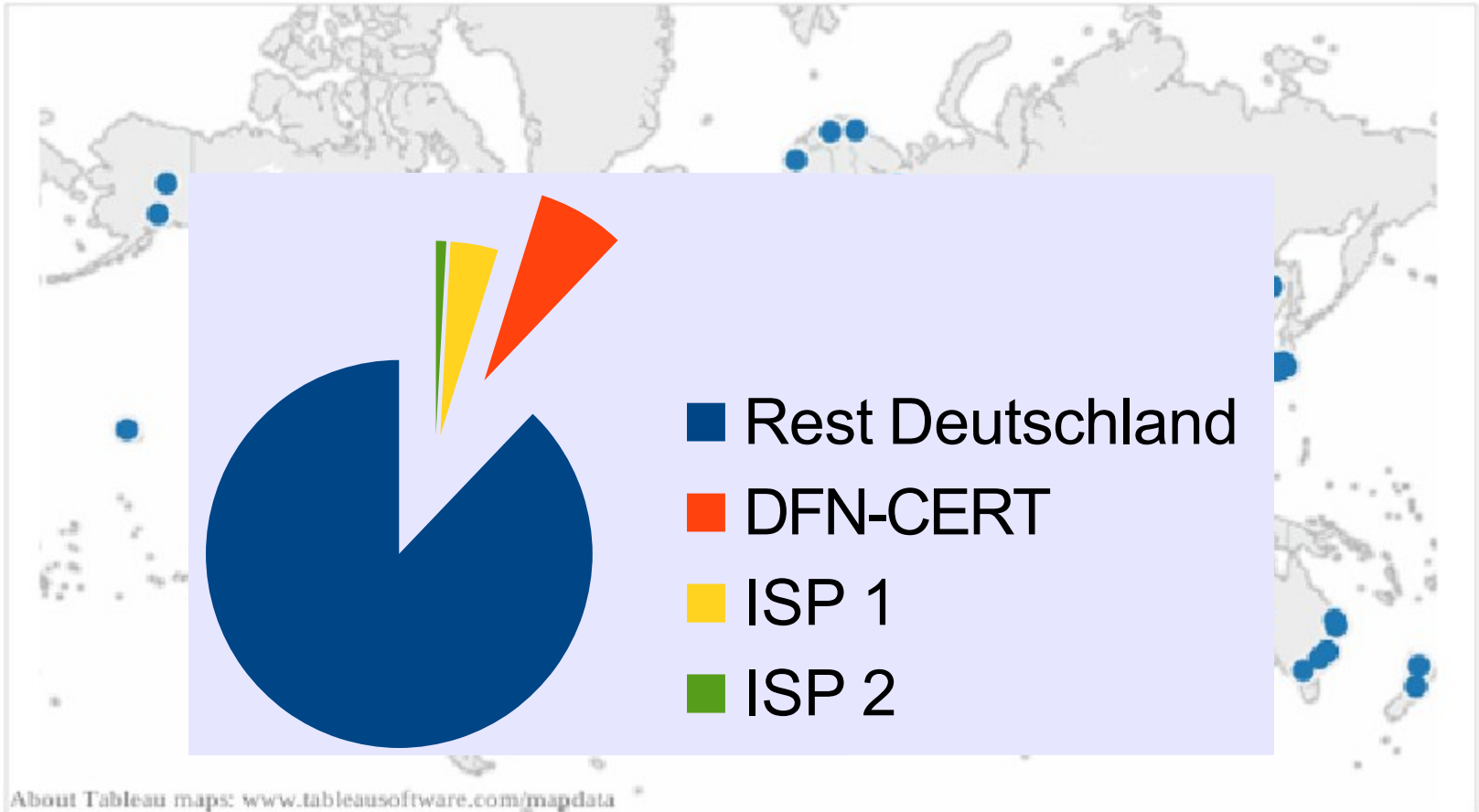
CVE-2013-5211

Reflection-Angriffe: NTP



CVE-2013-5211

Reflection-Angriffe: NTP



Layer 4

Reflection-Angriffe: SNMP



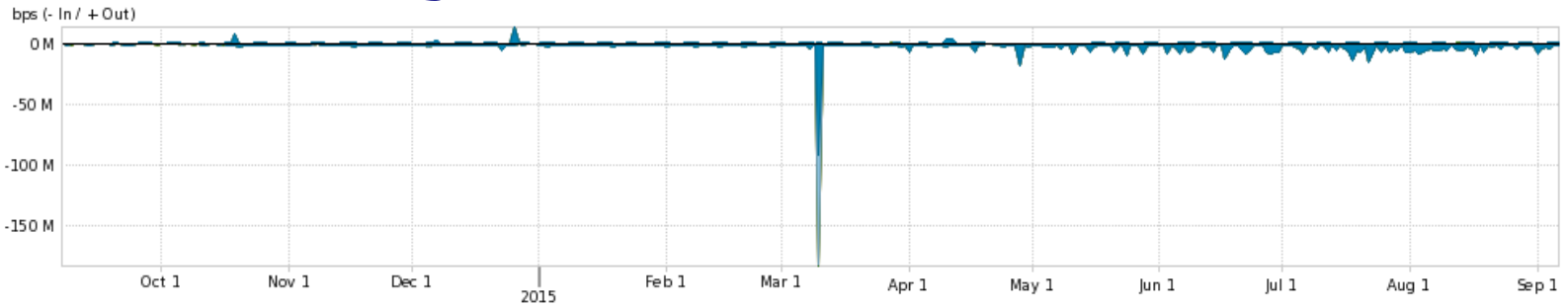
- Bei einer SNMP-Reflection werden SNMP-Anfragen (SNMPv2) mit der Adresse des ausgewählten Ziels (Absender) verschickt
 - GetBulk
 - Verbreitete MIBs
- Dabei werden vielfach Endgeräte verwendet, die ungesicherte SNMP-Anfragen aus dem Internet beantworten
 - Open SNMP Project
<http://opensnmpproject.org/>
- Verstärkungsfaktor ~ 10

Layer 4

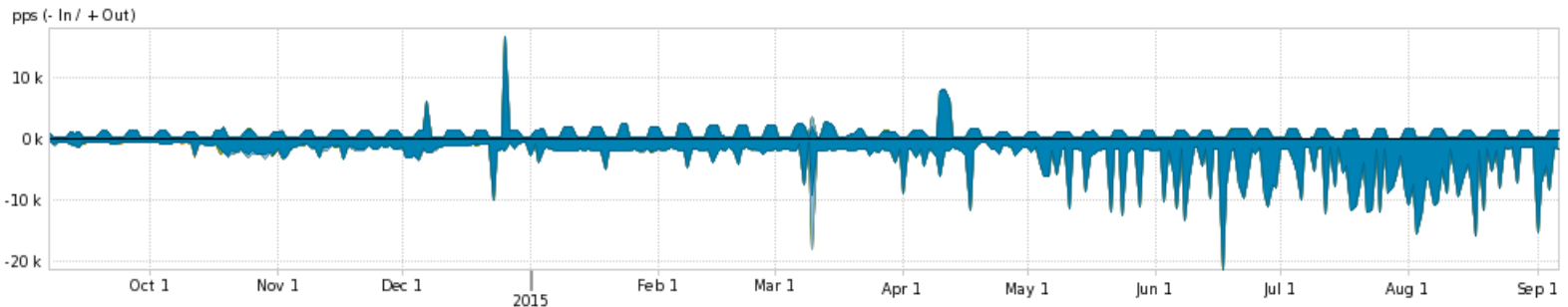
Reflection-Angriffe: SNMP



2014/15: Bytes/sec



2014/15: Packets/sec



Layer 3

Einzelnes Paket: Ping of death



- Programmschwachstellen in TCP/IP-Stacks lassen sich durch einzelne Pakete ausnutzen, die zum Absturz des Systems führen
 - Programmschwachstelle, einzelnes Paket
- **Ping of death (1996 – und wieder 2007)**
 - Durch Fragmentierung wird ein Paket spezifiziert, welches größer als 65.535 Byte ist
 - $\text{Offset} + \text{Size} > 65.535 \text{ Byte}$
- **Weitere Fragmentierungsbasierte Angriffe**

Layer 3

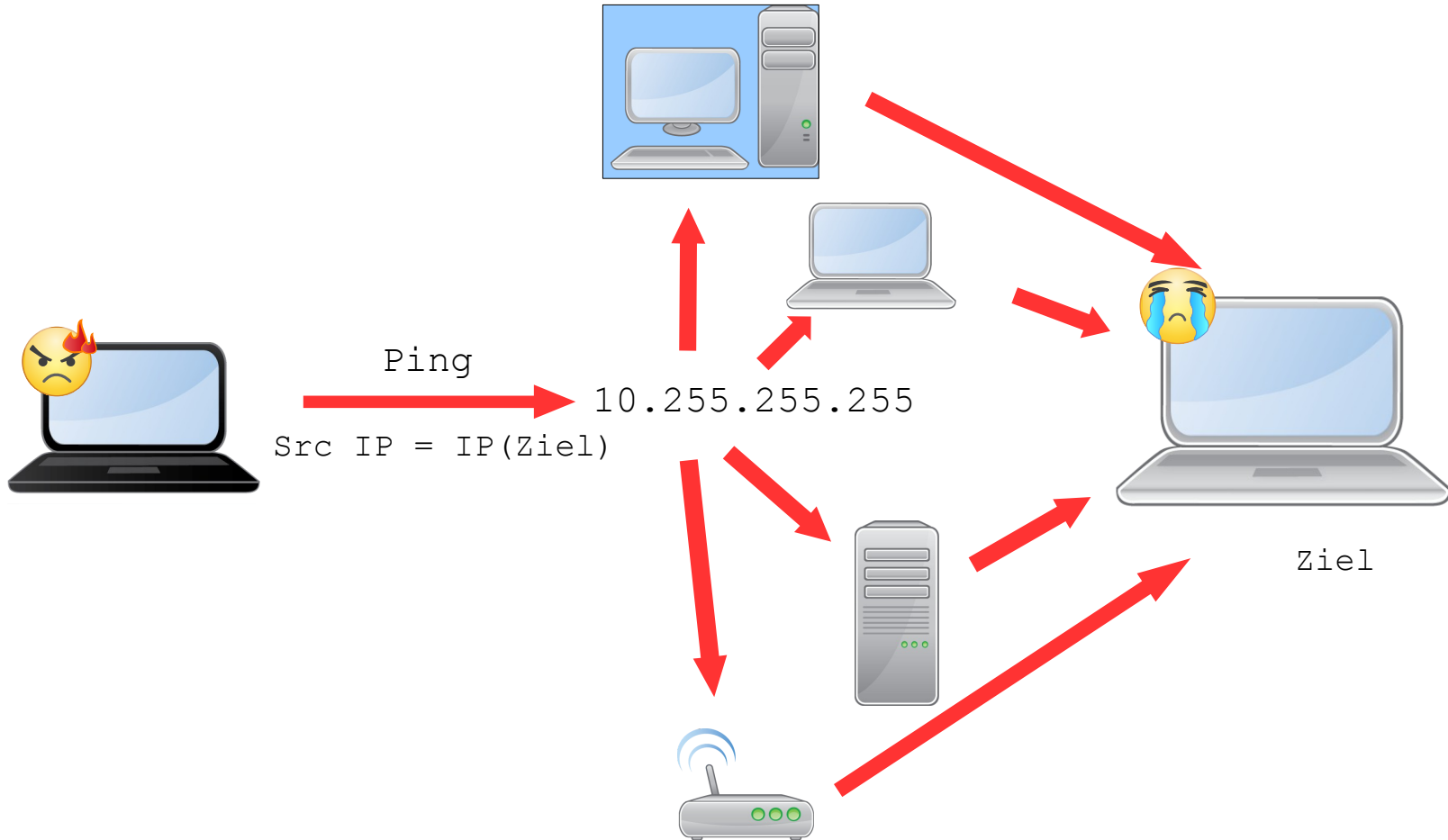
Reflection-Angriffe: Smurf



- Als Klassiker der Reflection-Angriffe werden bei Smurf ICMP-Pings (Echo Request) an die Broadcast-Adresse eines Netzwerks versendet, als Absender wird dabei das Ziel eingesetzt
 - Ressourcenauslastung, Flood

Layer 3

Reflection-Angriffe: Smurf



Layer 2

Einzelnes Paket: SLAAC



- Stateless Address Autoconfiguration ist ein Mechanismus in IPv6, der zur automatischen Konfiguration von IP-Adressen verwendet werden kann
- Nach Wahl einer Adresse, sendet das System eine Anfrage, ob diese Adresse schon verwendet wird
- Antwortet der Angreifer auf diese Anfragen jeweils ablehnend, kann das Ziel keine Adresse einrichten



Zwischenfazit



Überlast bei Diensten

- **Erst der Zugang zu Diensten stellt die Nutzung des Netzes selbst sicher und erlaubt die eigentliche Wertschöpfung!**
- **Gelingt es Angreifern, diesen Zugang zu blockieren**
 - ist dies im Internet üblicherweise auch für Dritte sichtbar
 - können legitime Nutzer nicht arbeiten
- **Vielfältige Beispiele:**
 - DDoS, Flash Crowds, Slash-Dot Effect



DDoS-Angriffe

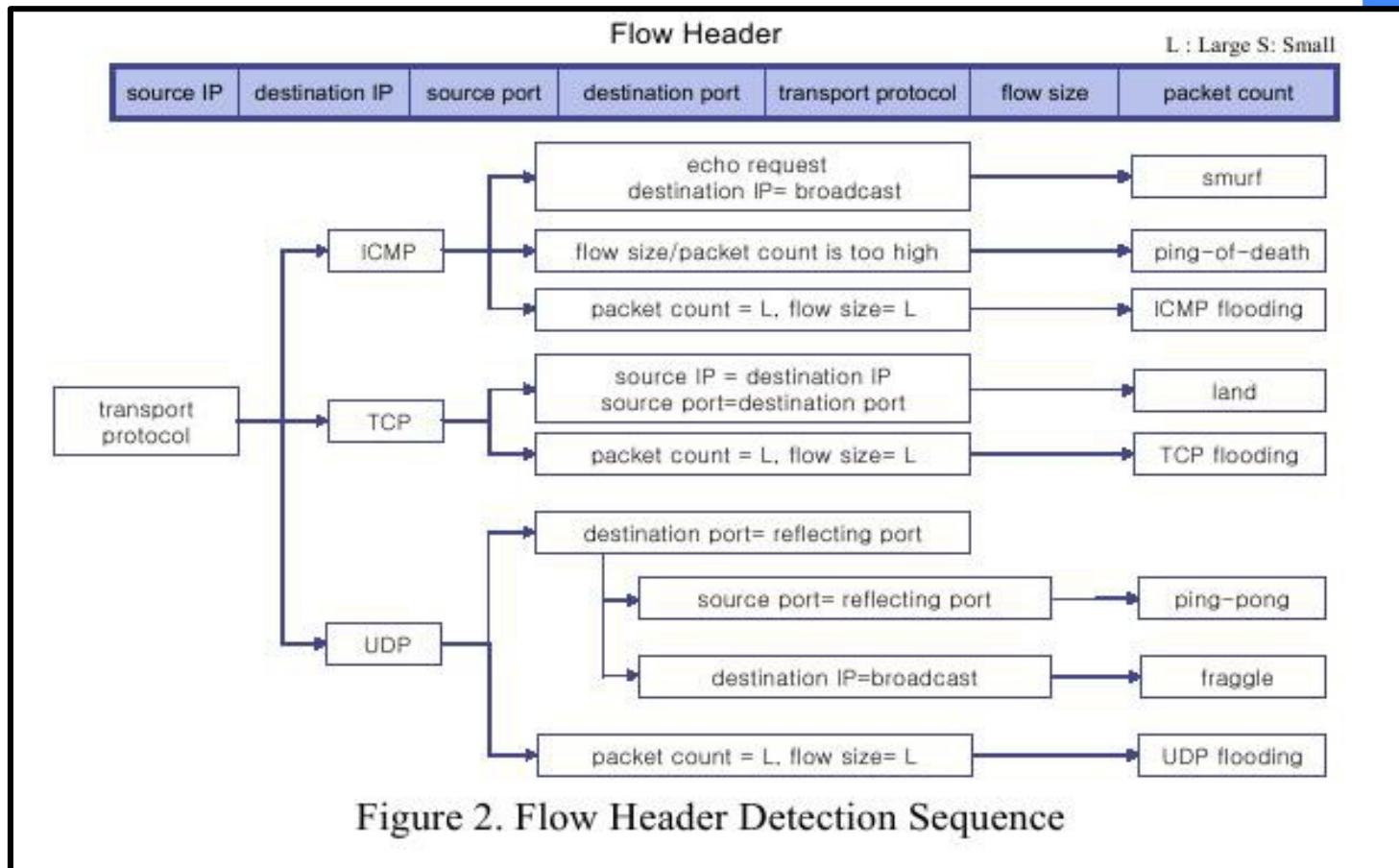
- Techniken sind seit vielen Jahren bekannt und grundsätzlich unverändert!
- Vielzahl von Angriffen hängen von einer konkreten Schwachstelle ab, die vorhanden sein muss, damit „etwas“ passiert:
 - Kaputt machen geht immer – und ist leicht!
 - Neue Buffer-Overflows gibt es immer wieder! (Nun ja, solange Programmiersprachen so was ermöglichen!)



Ein Paket reicht ...

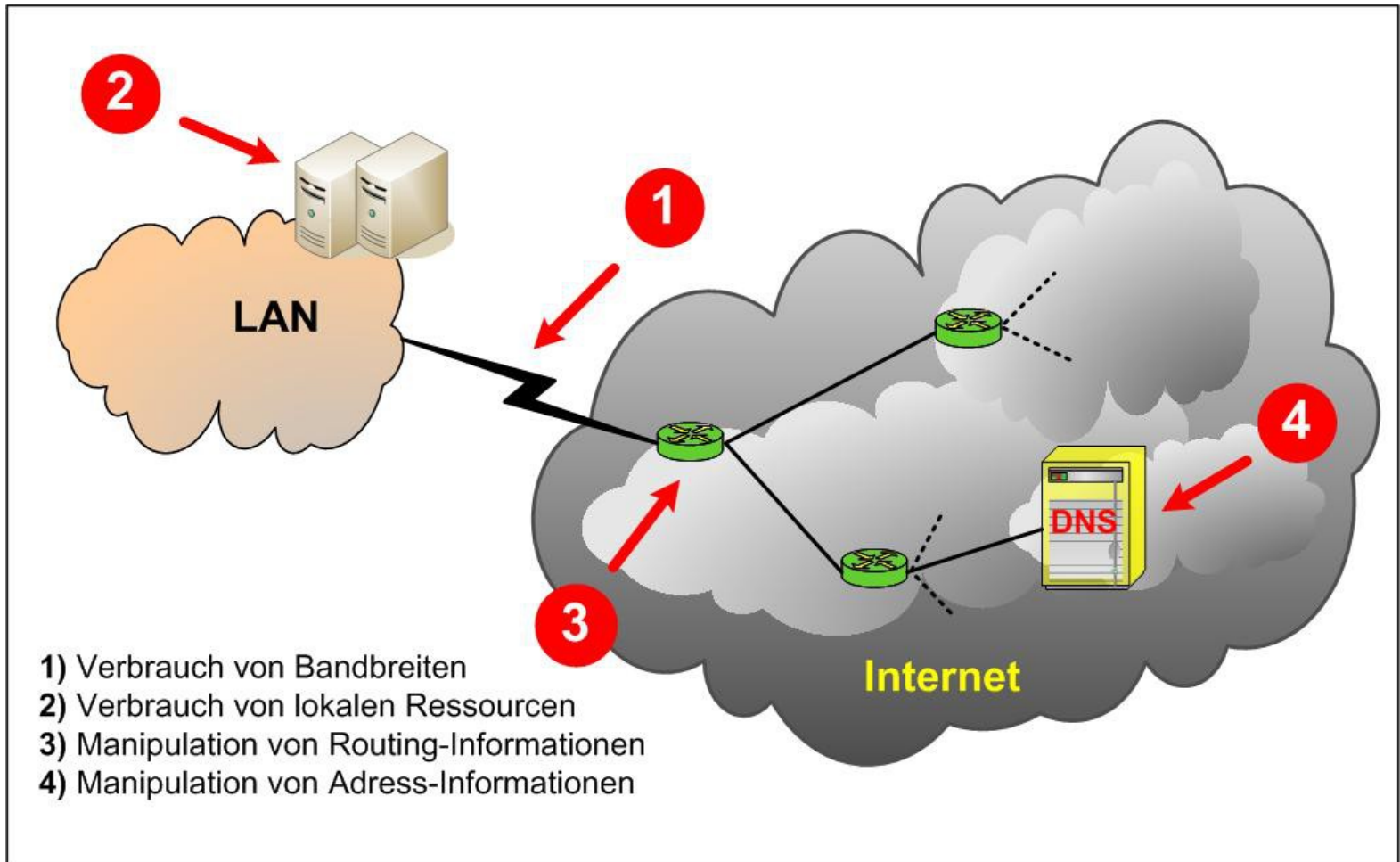
- **Wenn die Schwachstelle im Mittelpunkt steht:**
 - Ausnutzung konkreter Schwachstellen erfordert manchmal nur ein einzelnes Paket
- **Unabdingbar:**
 - Härten und restriktives Patch-Management
 - Angriffsfenster abhängig von Exploits und Schnelligkeit der Prozesse beim Hersteller und betroffenen Organisationen

Einordnung der Angriffsverfahren

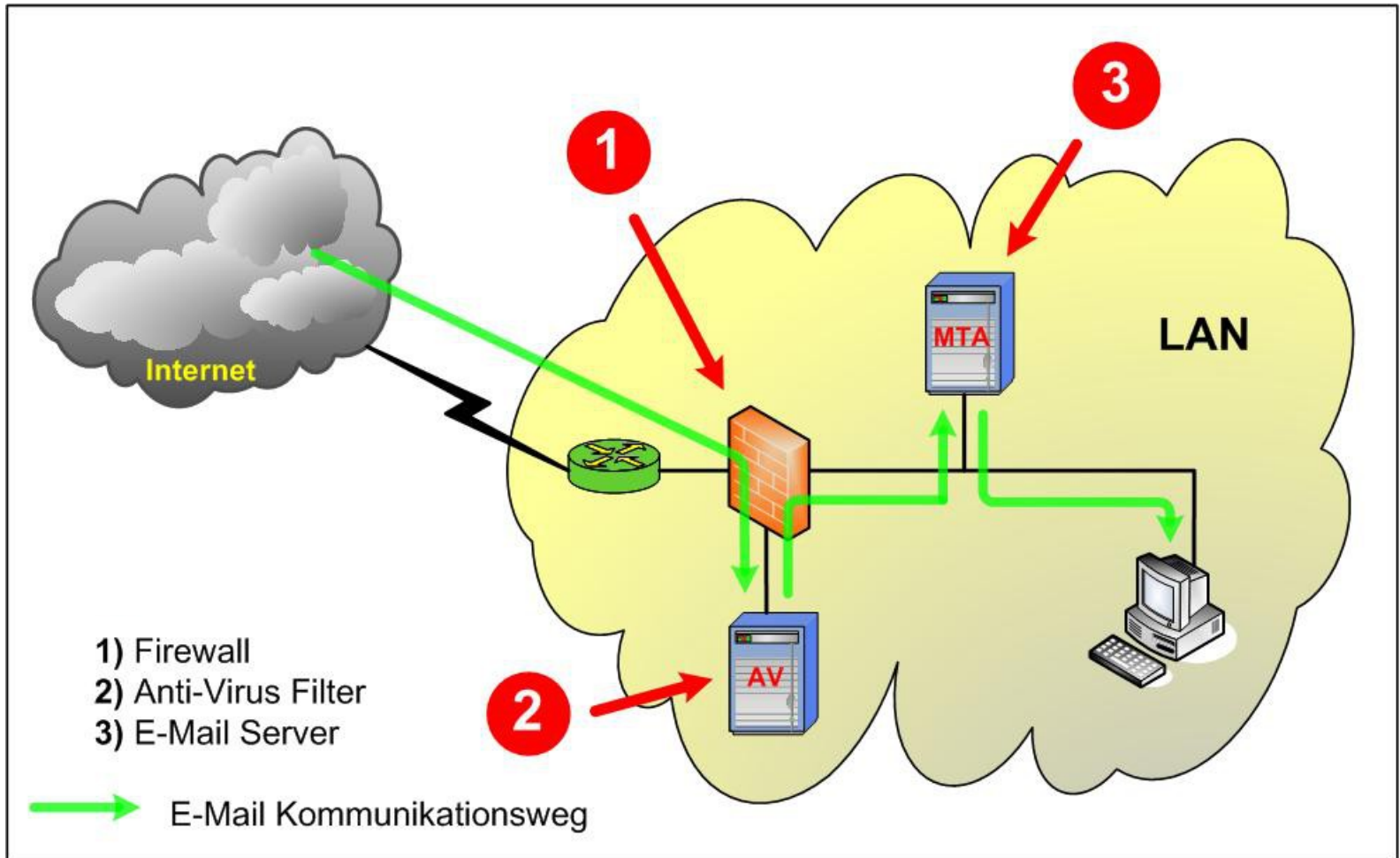


Quelle: A Flow-based Method for Abnormal Network Traffic Detection / Myung-Sup Kim, Hun-Jeong Kang, Seong-Cheol Hong, Seung-Hwa Chung, and James W. Hong. - POSTECH; Dept. of Computer Science and Engineering. 2004.

Konkrete Angriffspunkte



Konkrete Angriffspunkte bei Email



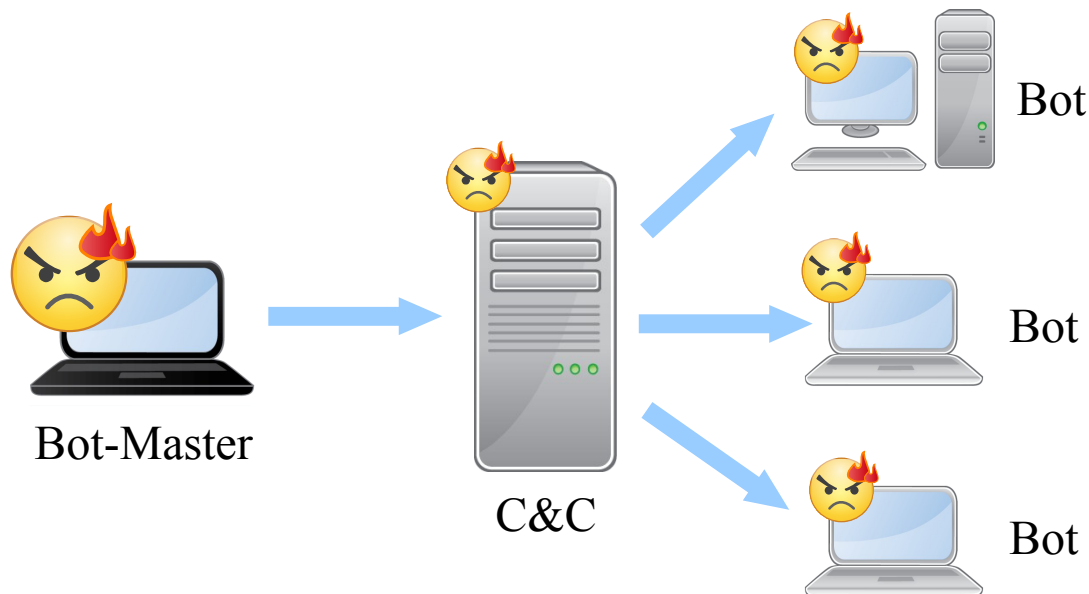


Botnetze



Botnetze

- Ein Botnetz besteht aus kompromittierten Systemen, den Bots, die durch den Command-and-Control Server Befehle bekommen





Botnetze (2)

- Zur Kommunikation zwischen den beteiligten Systemen kommen unterschiedliche Protokolle zum Einsatz
 - IRC
 - HTTP
 - Twitter
 - ...

Botnetze für Denial-of-Service-Angriffe



- Ein Einsatzzweck von Botnetzen sind DoS- Angriffe (u.a.)
 - Nicht zurückverfolgbar zum Angreifer
 - Schwierig zu verteidigen, da verteilt
 - Größere Angriffe durch
 - Viele angreifende Systeme
 - Keine (eigenen) Kosten für Bandbreite
 - Synergieeffekte
 - Schon kompromittiert für Spam, Banking, ..., warum dann nicht auch DoS

Internet of Things

Mirai



- **Mitte 2016 hat mit Mirai eine neue Bedrohung das Internet betreten**
- **IoT-Geräte sind traditionell schlecht gesichert**
 - Günstige Herstellung
 - Leichte Inbetriebnahme, keine Konfigurationsmöglichkeiten
 - Keine Updates
- **Vielfach Telnetzugänge mit unveränderlichen Default-Passwörtern**

Internet of Things

Mirai: Default-Passwörter



- Mirai verwendet 68 hart kodierte Kombinationen aus Nutzernamen und Passwörtern, um Geräte zu übernehmen

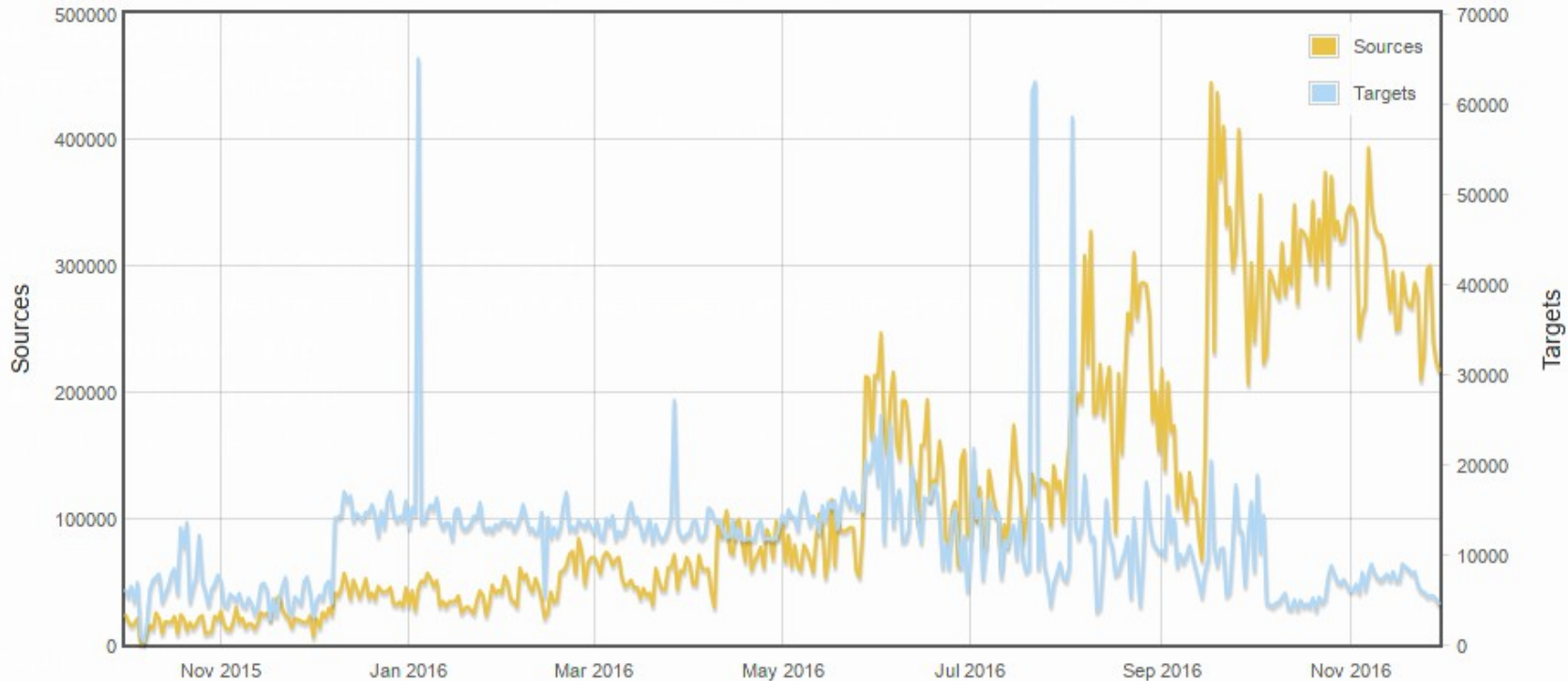
| Typ | Hersteller | Nutzername | Passwort |
|-----------|------------------------|------------|----------|
| IP Kamera | ACTi IP Camera | admin | 123456 |
| DVR | ANKO Products DVR | root | anko |
| IP Kamera | Axis IP Camera, et al. | root | pass |
| DVR | Dahua DVR | root | 888888 |
| Drucker | Panasonic Printer | root | 00000000 |
| Router | RealTek Routers | root | realtek |
| ... | | | |



- **Wie andere Angriffstools unterstützt Mirai eine Liste von verschiedenen Angriffen**
 - SYN, ACK, UDP Floods
 - GRE Floods
 - Paket Flood
 - Aufgrund des Protokolls vielfach durchgeleitet
 - HTTP GET, POST, HEAD
 - DNS „Water Torture“
 - Zufällige DNS-Namen, um autoritative DNS-Server zu überlasten
 - ...

Internet of Things

Mirai: Scans nach Port 23



www.dshield.org

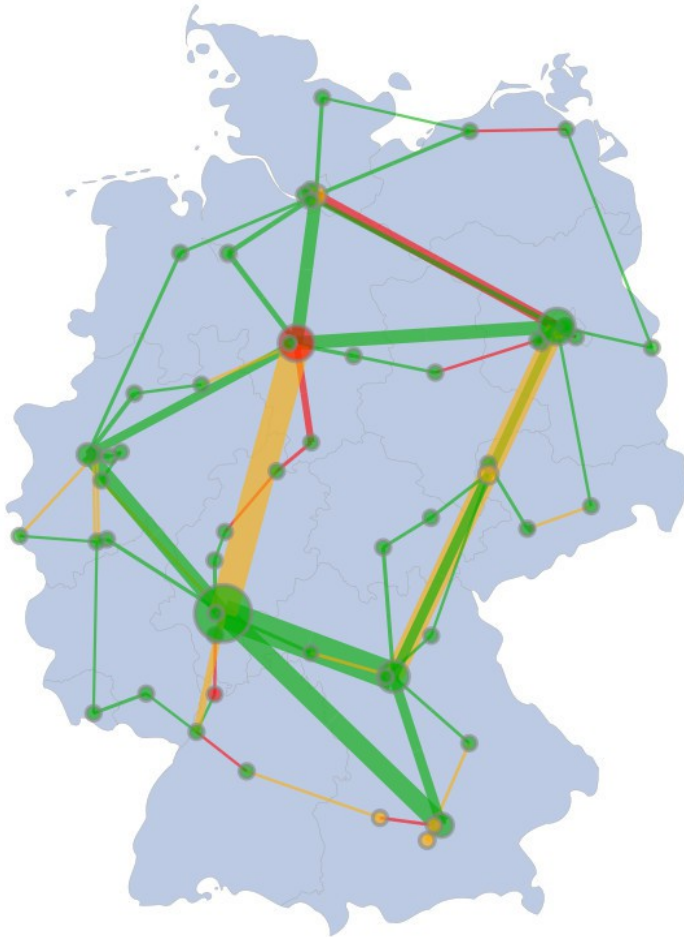


Aktuelle DoS-Angriffe

- Angreifer bauen ihre Kapazitäten mit den Kapazitäten der Verteidiger aus
- Dabei haben Angreifer durch die Verstärkung mittels Botnetzen und Amplification viele Vorteile für DoS-Angriffe
- Französischer Hoster OVH mit 1,1 Tbps angegriffen (2016-09-19)
 - Vermutete Mirai-Beteiligung
 - DE-CIX als einer der größten Internetknoten hatte 2015 eine Spitze von 5,5 Tbps

Network Topology Map

Timeframe: 2016-04-13 08:13 – 08:18 2016-04-14 back forward NOW



Und was
kann man
dagegen tun?
– Allgemeine
Maßnahmen



Dienstentwicklung

■ Sprachen, Bibliotheken kennen

- Wie funktionieren Konstrukte
- Welche Komplexität haben Algorithmen

■ Systeme kennen

- Welche Eigenschaften hat die Zielplattform

■ Sicherheit bei der Entwicklung beachten

- OWASP
(Open Web Application Security Project)
- SANS
Top 25 Most Dangerous Software Errors



Dienstbetrieb

■ Kapazitäten kennen

- Passende Reaktion erfordert Kenntnisse und Vorbereitung
- Reserven schaffen

■ Härtung der Dienste

- Aktuelle Versionen einsetzen
- Konfiguration anpassen
 - Module zur Abwehr spezieller Angriffe
- Basisdienst ermöglichen
 - Statische Seiten im Fall hoher Last



Netzwerkbetrieb

- **Begrenzung der zur Verfügung stehenden Bandbreite, Traffic Shaping**
 - Auswirkung (möglicher) Angriffe begrenzen
- **Segmentierung zum Schutz kritischer Bereiche**
 - Angriff auf externen Webserver beeinträchtigt Intranet nicht
- **Reserven schaffen**
 - Dimensionierung von Router und Leitung
 - Load Balancing, Proxys, Caching

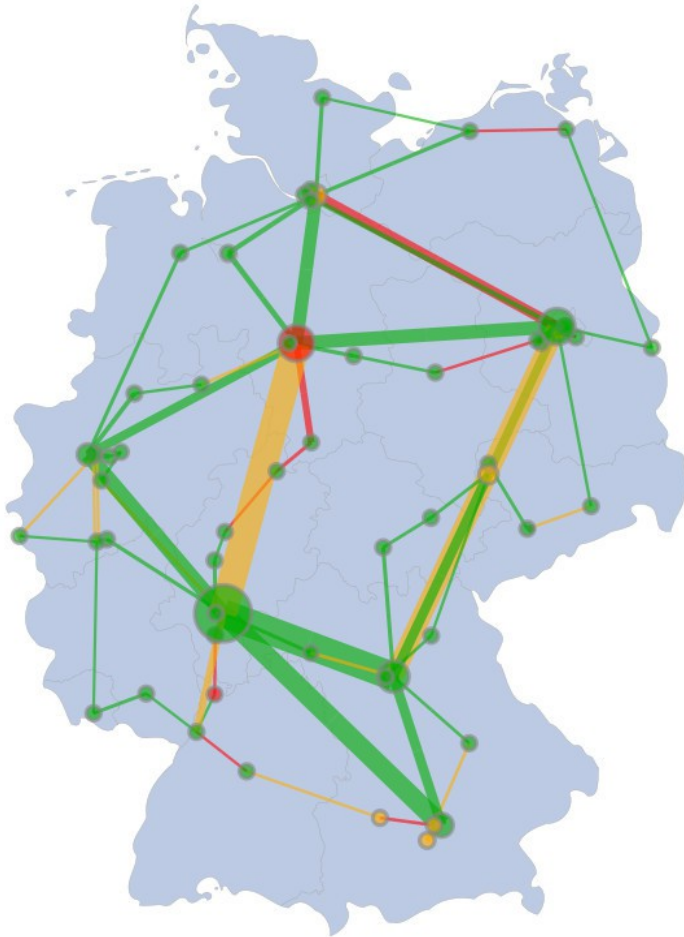


Netzwerkbetrieb (2)

- **Reflection-Angriffe basieren auf der Fälschung von Quell-IP-Adressen**
- **BCP (Best Current Practice)**
 - BCP ist eine Sammlung von Dokumenten innerhalb von RFC, die bewährte Vorgehensweisen dokumentiert
 - BCP 38 – Network Ingress Filtering
 - Filtert eingehende Pakete anhand der Plausibilität der Quell-IP-Adressen
 - Verhindert Fälschung von beliebigen Adressen, wenn dies in relativer Nähe der Angreifer eingesetzt wird (also nicht erst beim Ziel!)

Network Topology Map

Timeframe: 2016-04-13 08:13 – 08:18 2016-04-14 back forward NOW



Und was
kann man
dagegen tun?
– Aktive Abwehr



Mitigation

- Laufende Angriffe lassen sich durch verschiedene Maßnahmen abmildern
- **Filtern, z.B. durch Router oder Firewalls**
 - Pakete an das Ziel werden verworfen
→ weniger Kollateralschäden,
aber Dienst bleibt nicht erreichbar ;(
 - Pakete von identifizierten Quellen werden verworfen
→ Entfernt konkreten Angriffsverkehr
 - Auch legitime Quellen bei Reflection betroffen
 - Botnetze wechseln angreifende Bots durch



Mitigation (2)

- **Filtern, z.B. durch Router oder Firewalls (Fortsetzung)**
 - Pakete mit bekanntem Angriffsinhalt verwerfen
 - Entfernt konkreten Angriffsverkehr
 - Verwirft nur den Angriff, wenn die Pattern korrekt und ausreichend sind
 - Erfordert genaue Analyse des Angriffs
 - Verarbeitung der Pakete ist teuer



Mitigation durch Dienstleister

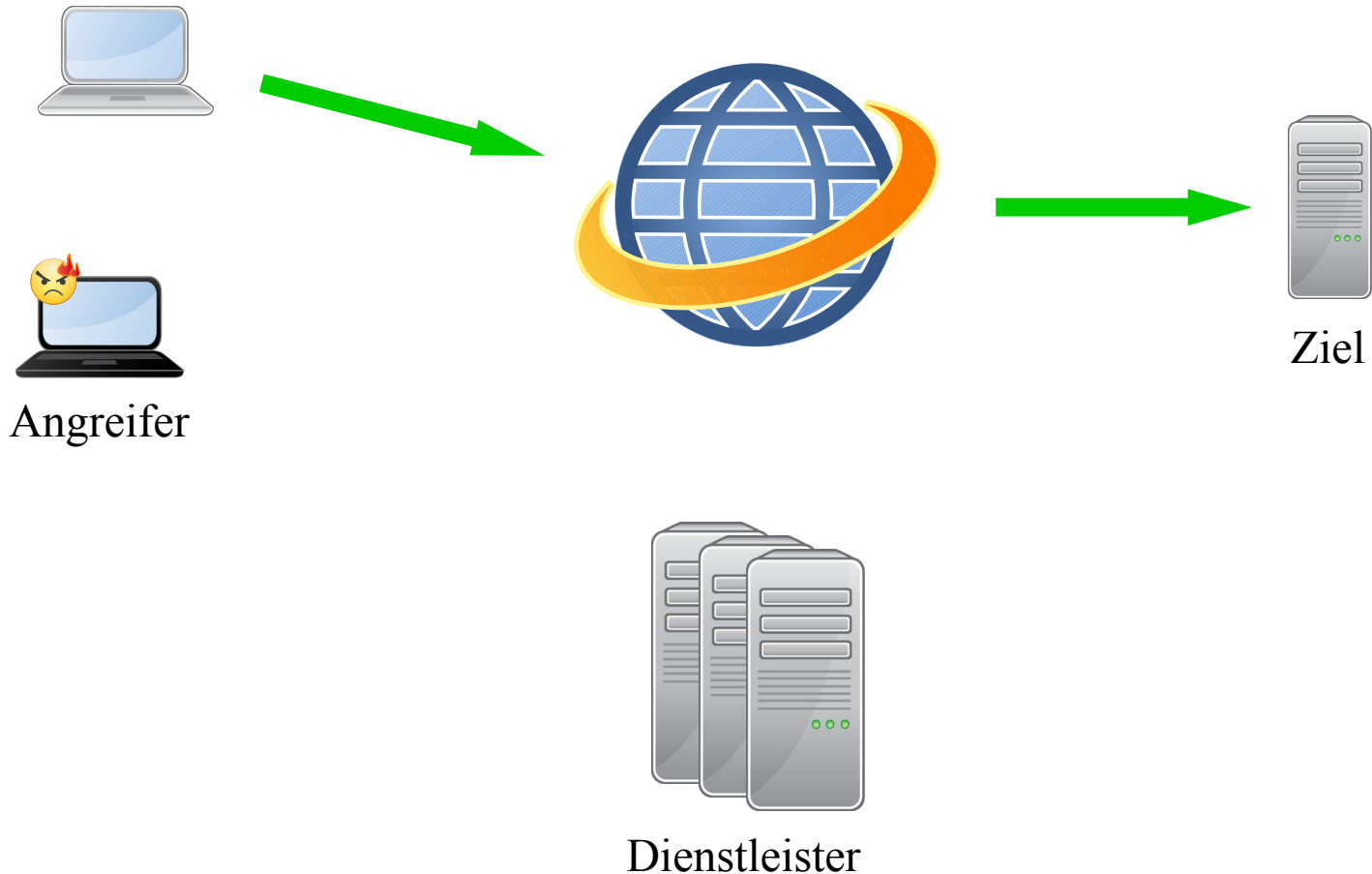
■ ISP / IXP

- Verstopft der Angriff die Zugangsleitung, ist der Provider gefragt
 - DE-CIX Blackholing ist über BGP steuerbare Filterfunktion

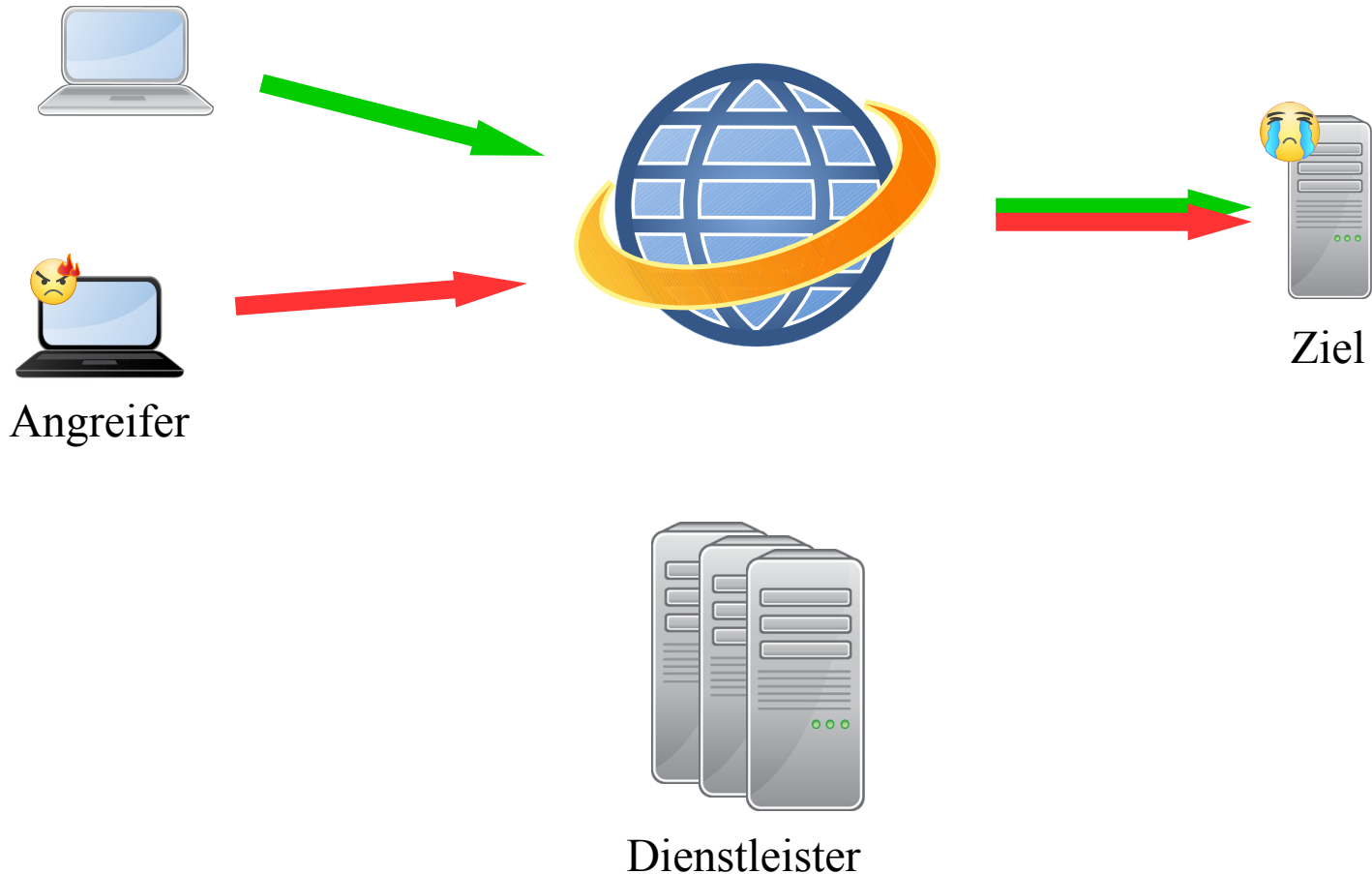
■ Spezialisierte Dienstleister

- Übernehmen Analyse und Mitigation
- Verkehr inklusive Angriff wird per BGP oder DNS zum Dienstleister umgeleitet
- Verkehr exklusive Angriff wird zum Empfänger weitergeleitet

Mitigation durch Dienstleister: Normalzustand ohne Angriff

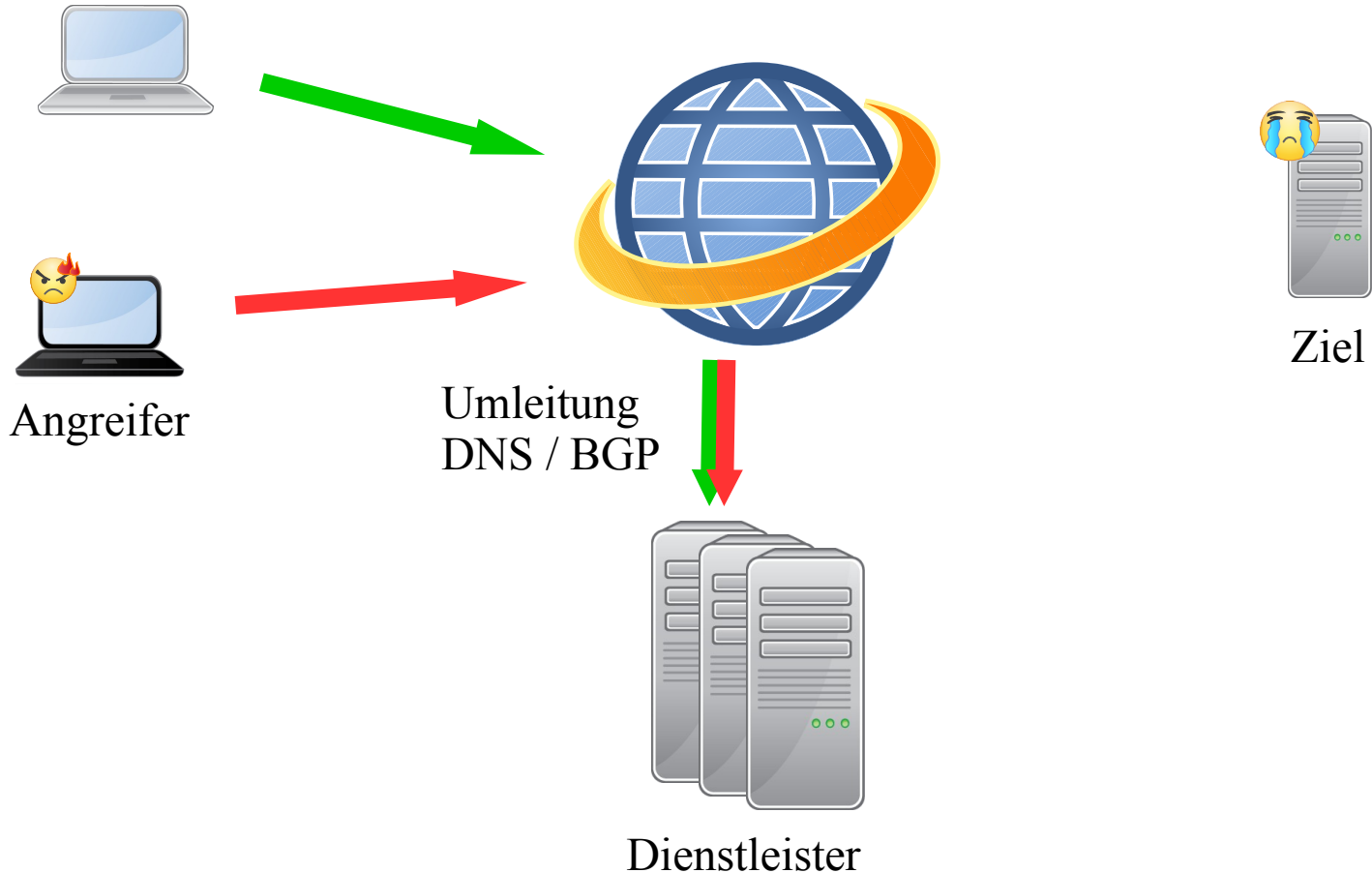


Mitigation durch Dienstleister: Angriff erfolgt parallel

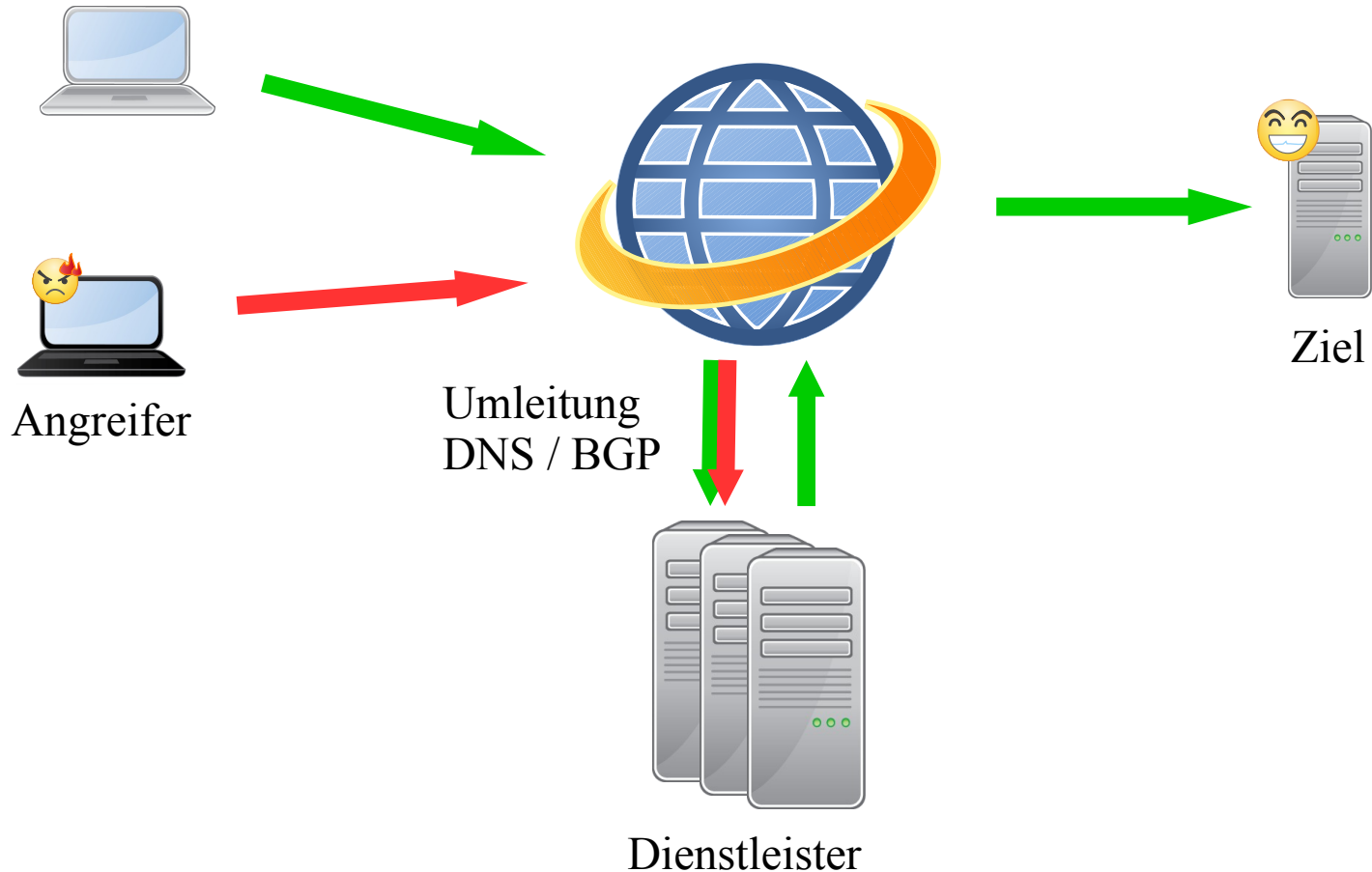


Mitigation durch Dienstleister:

Mitigation wird eingeleitet



Mitigation durch Dienstleister: Erfolgreiche Mitigation

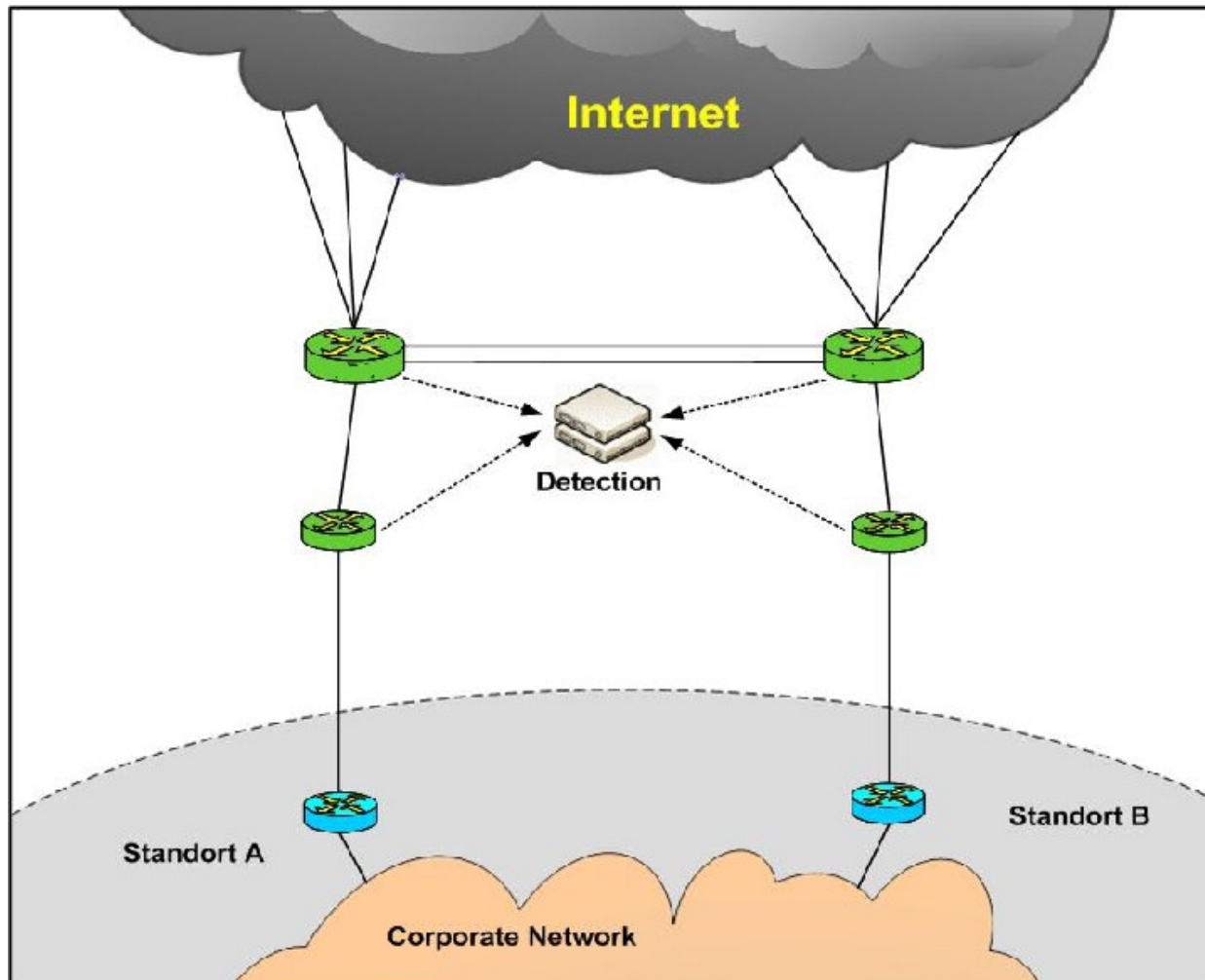


Mitigation durch Dienstleister: Spektrum der Angebote

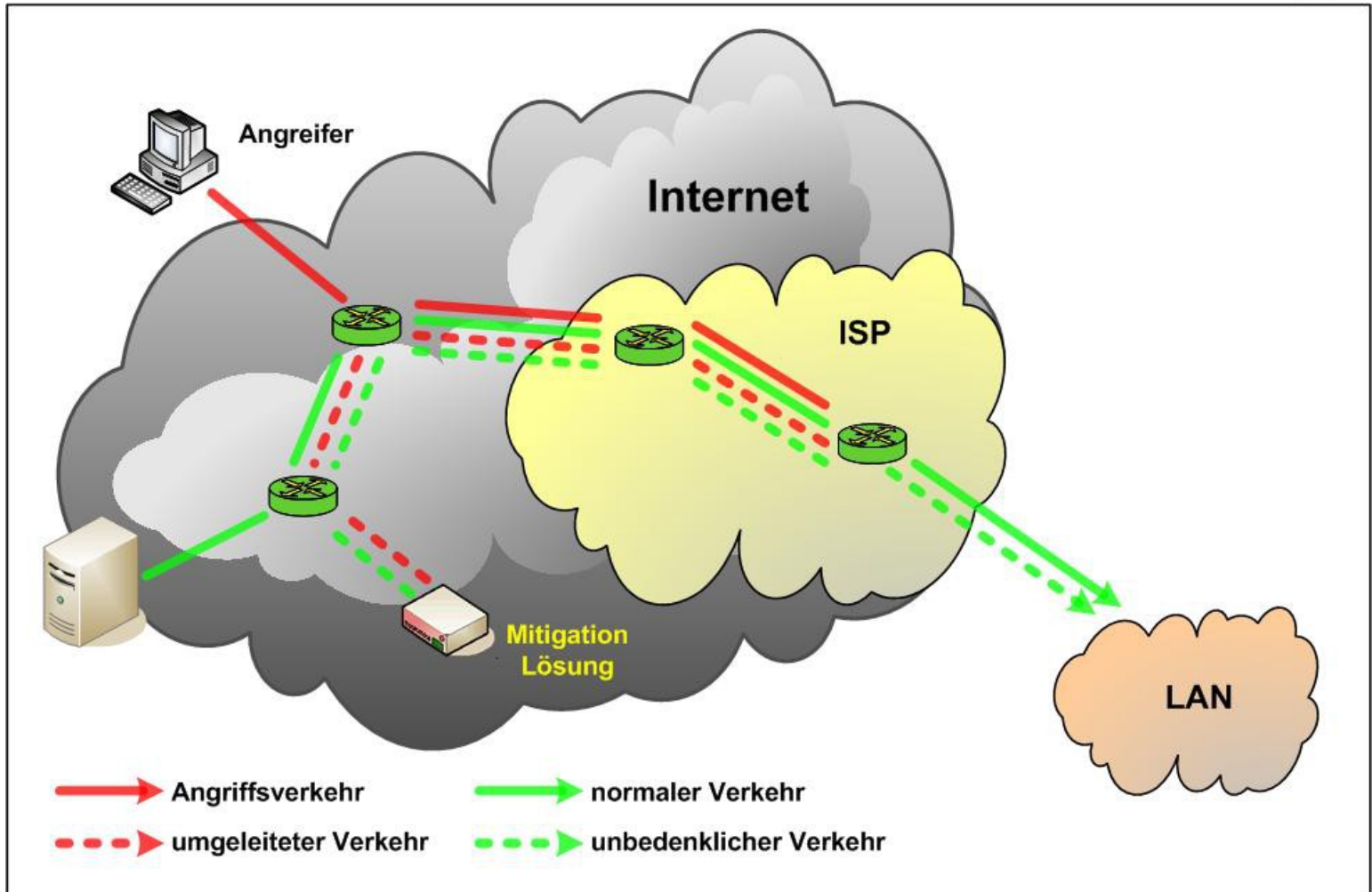


- **Option 1:**
Keine Mitigation, nur Erkennung
 - Maßnahmen verbleiben auf manueller Ebene
 - Längere Response-Zeiten
- **Option 2:**
Mitigation beim Dienstleister (in der Cloud)
- **Option 3:**
Mitigation beim ISP
- **Option 4:**
Mitigation beim Anwender

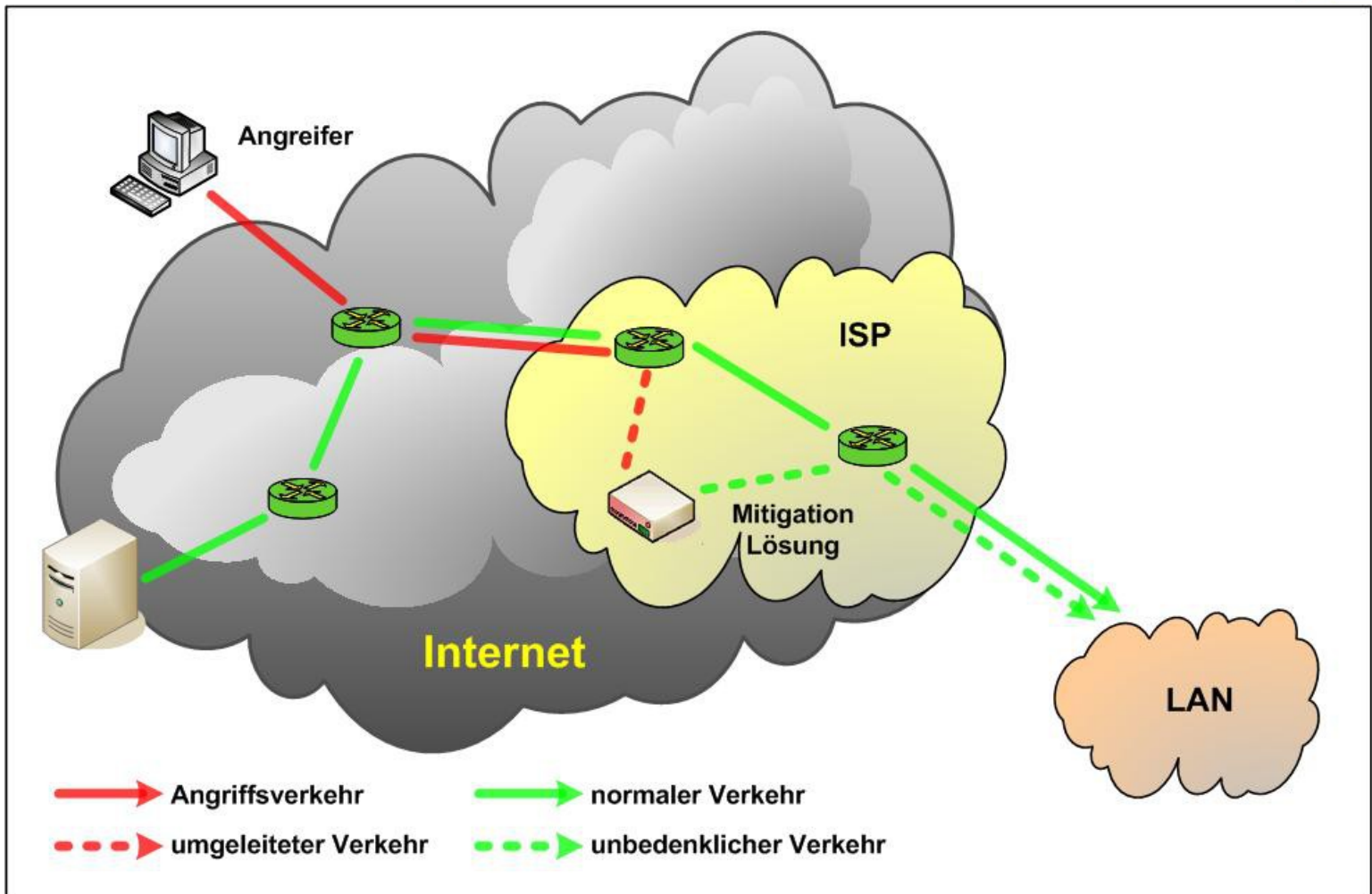
1: Nur Erkennung



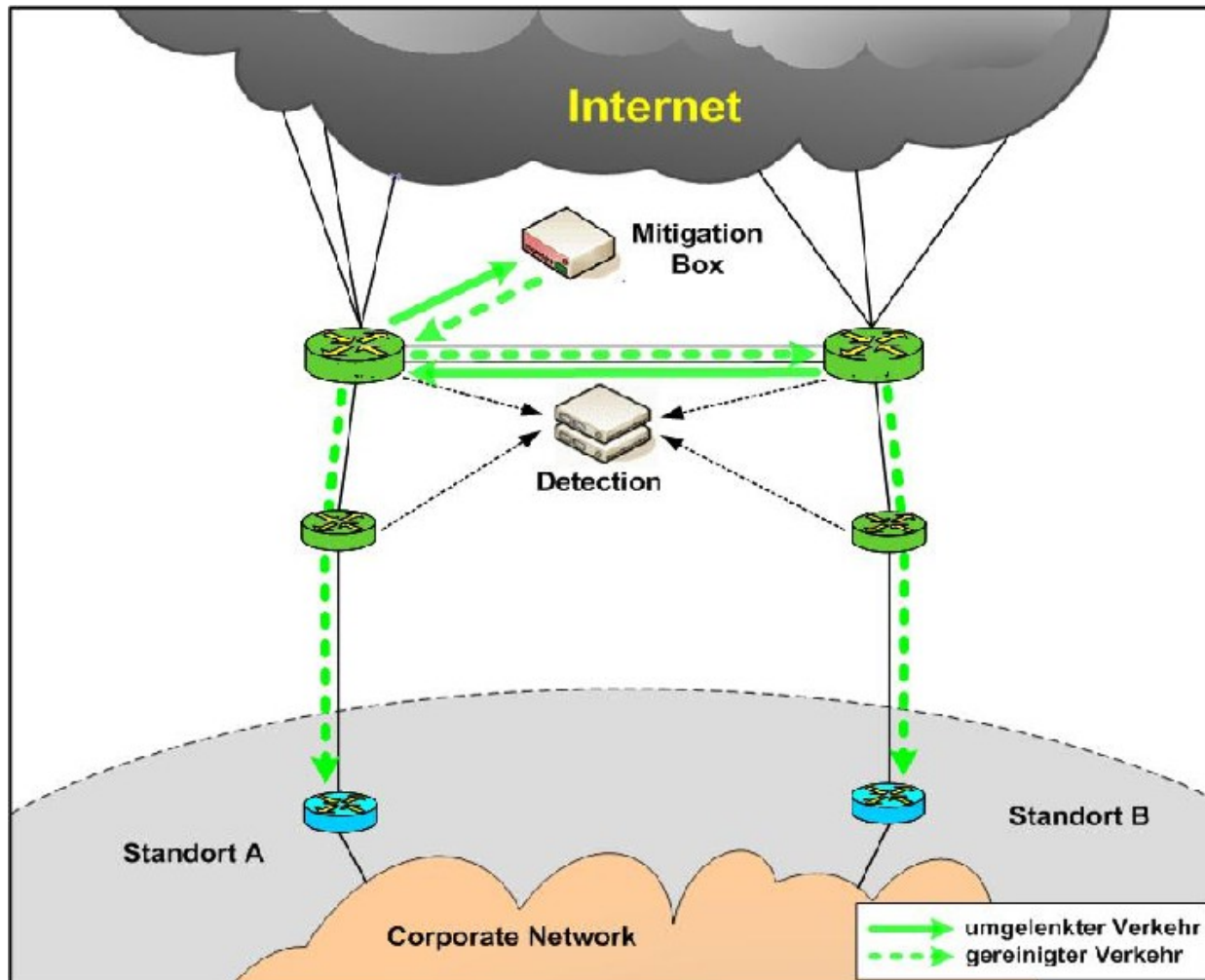
2: Mitigation in der Cloud



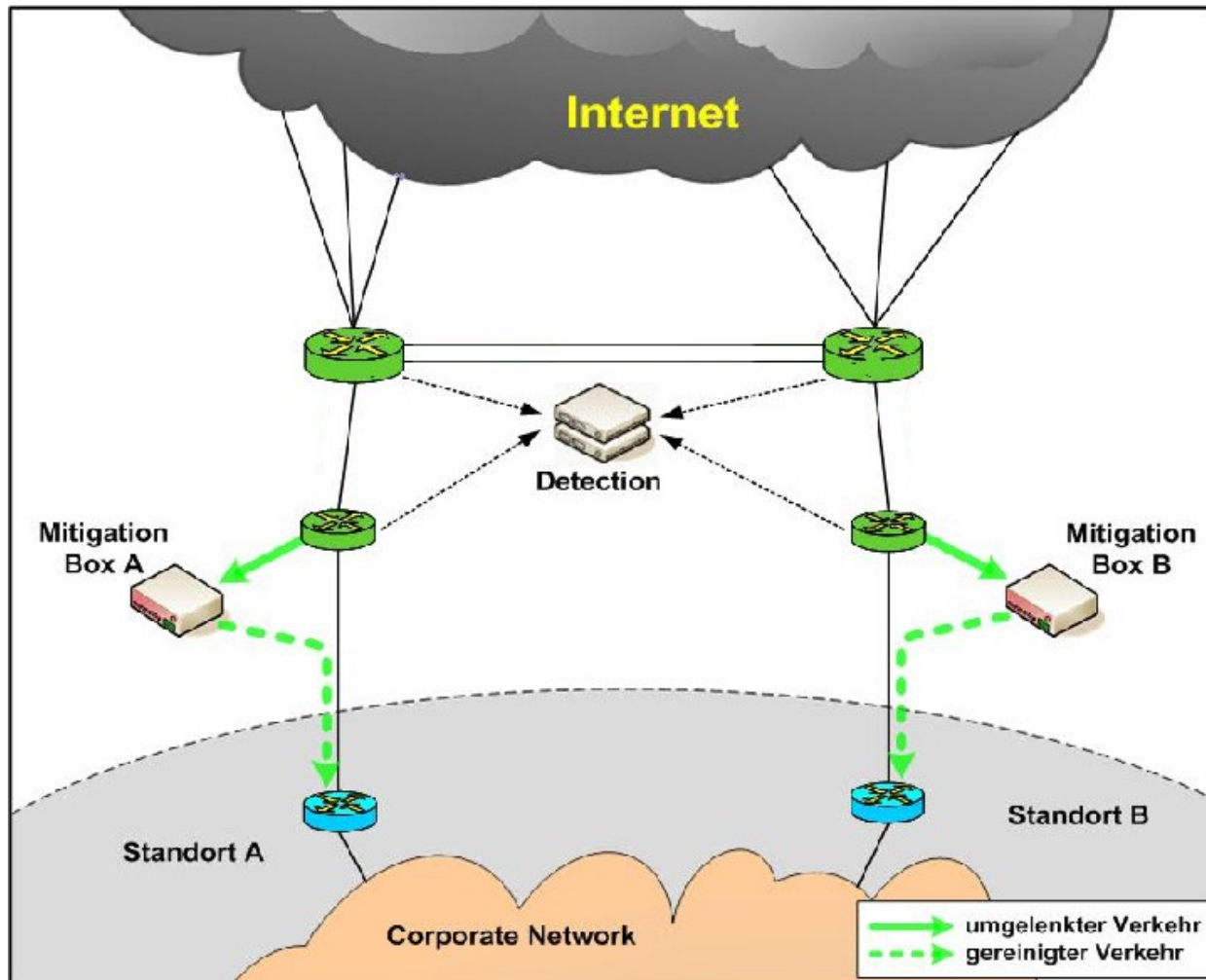
3: Mitigation durch den eigenen ISP



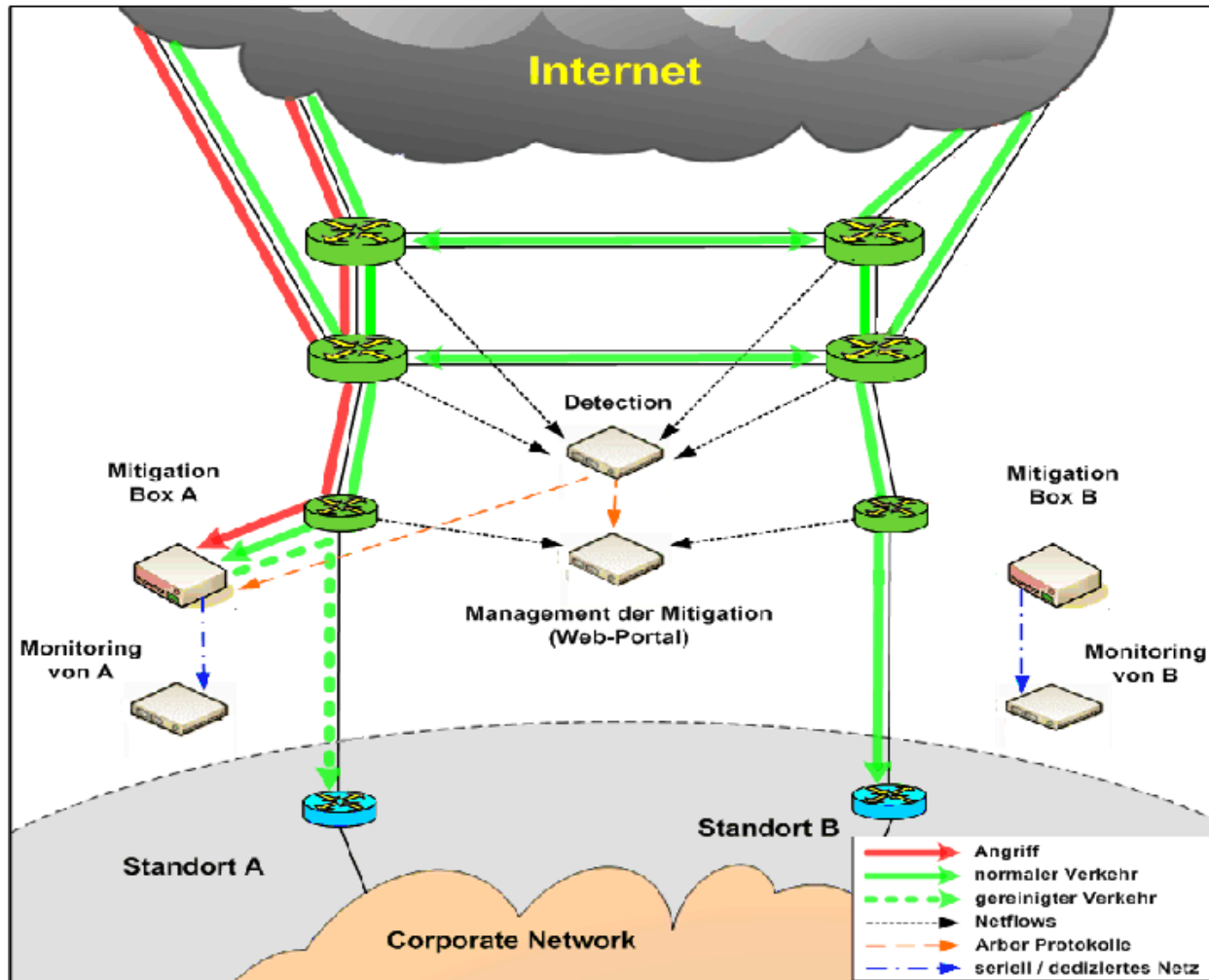
3: Mitigation durch eigenen ISP



4: Mitigation beim Anwender



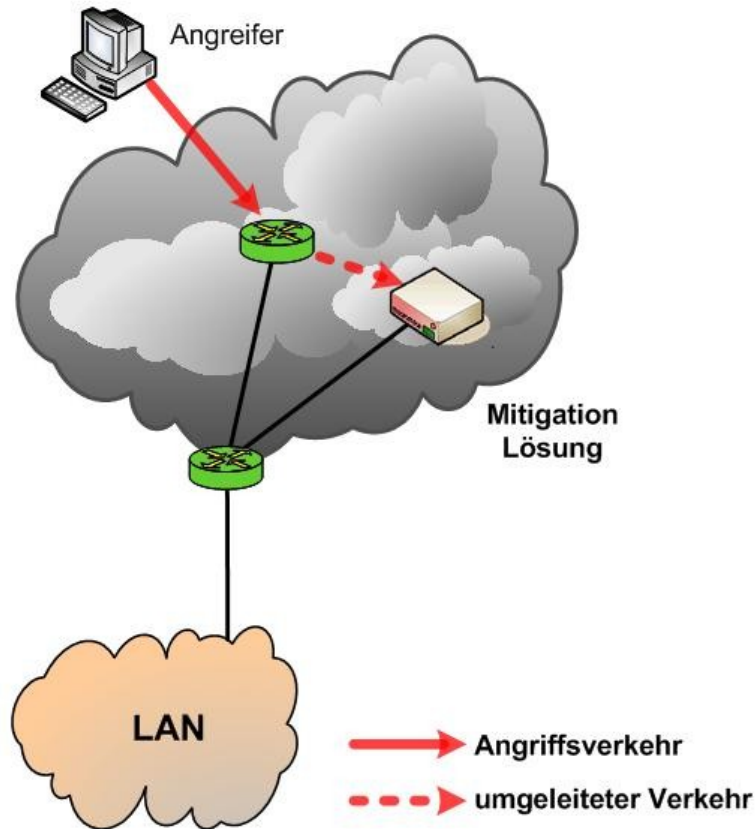
... nicht zu früh freuen



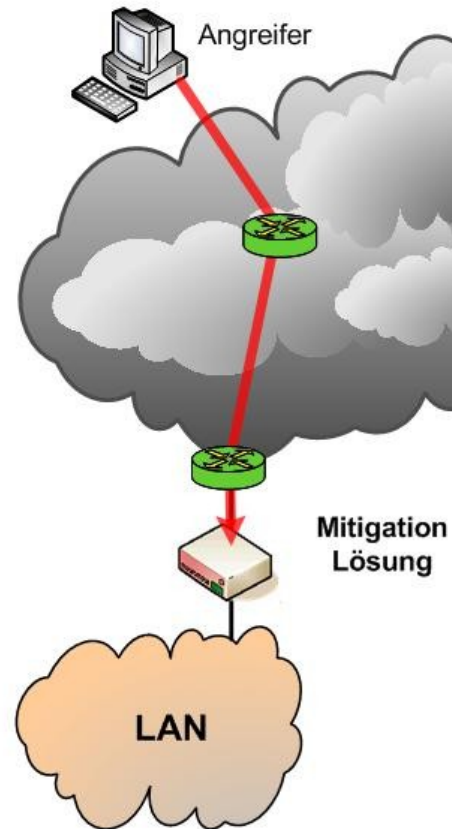
4: Routing vs. Bridging



Mitigation durch eine Routing-Lösung



Mitigation durch eine Bridging-Lösung





Rolle eines Portals

■ Zentrale Information

- Statusinformationen
- Bewertungen und Anmerkungen
- Übersicht aller Ereignisse
- Dokumentation

■ Zentrale Steuerung der Mitigation

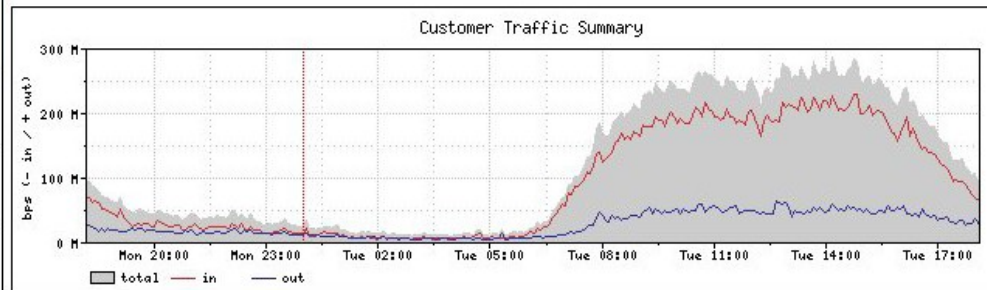
- Analyse
- Initiierung
- Verfolgung

Kommerzielles Produkt: Dashboard



Alert Snapshot

| Alert Totals | | High | Medium | Low |
|---------------|--------|------|--------|-----|
| Ongoing | [1]: | 0 | 1 | 0 |
| Recent | [296]: | 8 | 42 | 246 |
| Last 24 Hours | [19]: | 0 | 4 | 15 |


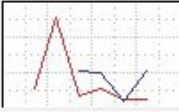
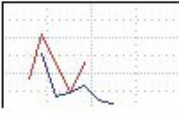
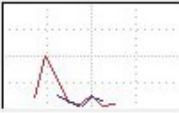
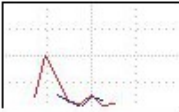
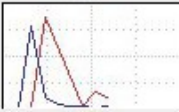
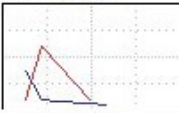
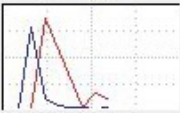


Top Ongoing Alerts

| ID | Traffic | Importance | Impact | Duration | Start Time | Direction | Type |
|-----------------------|---------|-----------------------------|---------------------|----------------------|--------------|-----------|-------------------------|
| 19128 | | Medium 130.7% of 114 pps | 38.8 Kbps 34 pps | 58 mins (Ongoing) | 17:03, Oct 7 | Incoming | Bandwidth (Profiled) |

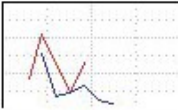
Alarmmeldungen



| ▼ ID | Traffic | Importance | Impact | Duration | Start Time | Direction | Type |
|-----------------------|---|---------------------------------------|----------------------|--------------------|---------------|-----------|----------------------------|
| 18902 |  | Low 50.0% of 68 pps | N/A | 8 mins (Ended) | 20:37, Oct 5 | Outgoing | Protocol TCP (Profiled) |
| 18533 |  | Low 69.9% of 559.9 Kbps | 25.0 Kbps 4 pps | 10 mins (Ended) | 18:11, Oct 1 | Outgoing | Protocol TCP (Profiled) |
| 18507 |  | Medium 105.1% of 59 pps | N/A | 11 mins (Ended) | 10:42, Oct 1 | Incoming | Bandwidth (Profiled) |
| 18506 |  | Medium 177.1% of 559.9 Kbps | 22.1 Kbps 4 pps | 13 mins (Ended) | 10:41, Oct 1 | Outgoing | Protocol TCP (Profiled) |
| 18505 |  | Medium 177.1% of 559.9 Kbps | 22.1 Kbps 4 pps | 13 mins (Ended) | 10:41, Oct 1 | Outgoing | Bandwidth (Profiled) |
| 18245 |  | Medium 286.0% of 559.9 Kbps | 1.6 Mbps 162 pps | 11 mins (Ended) | 11:43, Sep 29 | Outgoing | Bandwidth (Profiled) |
| 18244 |  | Medium 245.8% of 48 pps | 77.7 Kbps 126 pps | 14 mins (Ended) | 11:43, Sep 29 | Incoming | Bandwidth (Profiled) |
| 18243 |  | Medium 286.0% of 559.9 Kbps | 1.6 Mbps 162 pps | 11 mins (Ended) | 11:43, Sep 29 | Outgoing | Protocol TCP (Profiled) |



Alarmmeldungen (2)

| ▼ ID | Traffic | Importance | Impact | Duration | Start Time | Direction | Type |
|-----------------------|---|-----------------------------------|--------------------|--------------------|--------------|-----------|----------------------------|
| 18902 |  | Low 50.0% of 68 pps | N/A | 8 mins (Ended) | 20:37, Oct 5 | Outgoing | Protocol TCP (Profiled) |
| 18533 |  | Low 69.9% of 559.9 Kbps | 25.0 Kbps 4 pps | 10 mins (Ended) | 18:11, Oct 1 | Outgoing | Protocol TCP (Profiled) |
| 18507 |  | Medium 105.1% of 59 pps | N/A | 11 mins (Ended) | 10:42, Oct 1 | Incoming | Bandwidth (Profiled) |

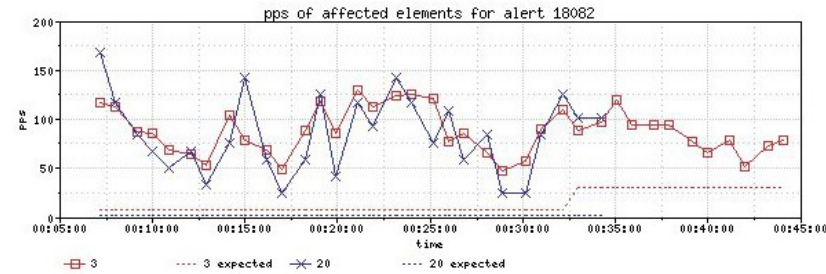
- ID: Die eindeutige Kennnummer des Ereignisses.
- Traffic: Visualisierung der übertragenen Daten im fraglichen Zeitraum
- Importance: Die Risikoeinschätzung anhand der innerhalb der Erkennungskomponenten gesammelten Daten über Netznutzung und Auslastung
- Impact: Die Auslastung angegeben als Bytes pro Sekunde (bei Ereignissen bzgl. der Bandbreiten) oder als Pakets pro Sekunde (bei Ereignissen bzgl. der Protokollnutzung).
- Duration: Die Gesamtlänge des Ereignisses in Minuten mit dem Hinweis „Ongoing“, wenn das Ereignis noch nicht beendet ist.
- Starttime: Der Zeitpunkt, zu dem das Ereignis begann.
- Direction: Entweder „Incoming“ oder „Outgoing“ gemäß der Richtung des Datenstroms, der zur Auslösung des Ereignisses erfolgte.
- Type: Die Hersteller-Klassifikation des Ereignisse

Alert Summary

| ID | Importance | Impact | Duration | Start Time | Direction | Type | Resource |
|-------|-----------------------------|--------|----------------|----------------------------|-----------|-------------------------|----------|
| 18082 | High 203.9% Of 103.0 Pps | N/A | 40m (Ended) | Sun, Sep 28 2008, 00:04:48 | Incoming | Bandwidth (Profiled) | |

Traffic Characterization

| | |
|--------------|---|
| Sources | <div>ipconnect.de</div> <div>0.0.0.0/0</div> |
| Ports | 32768 - 65535 33280 - 33791 |
| Destinations | <div>32</div> <div>Resolve</div> <div>0.0.0.0/0</div> |
| Ports | 80 (http) 1434 (ms-sql-m) |
| Protocol | tcp (6) |
| TCP Flags | FSPA (0x1B) |



Raw Flows

Generate Report

Examine Raw Flows

View

Affected Network Elements

| Network Element | Importance | Expected | Observed bps | | Observed pps | | |
|-----------------|------------|----------|--------------|---------|--------------|---------|--------------------|
| | | | Max | Overall | Max | Overall | |
| Interface 20 | medium | 2.00 pps | 72.82 k | 34.30 k | 167.00 | 84.80 | <div>Details</div> |
| Interface 3 | high | 8.00 pps | 60.30 k | 42.33 k | 130.00 | 88.02 | <div>Details</div> |

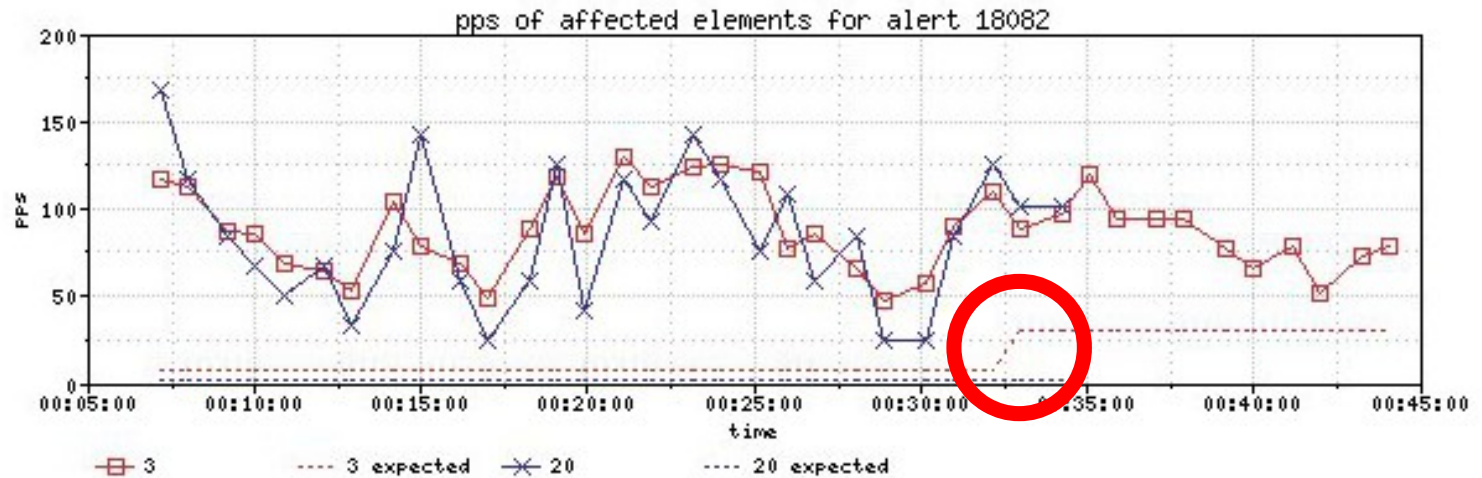
Alert Comments

Enter New Comment:

Standard Annotations

none

Lernen ist Pflicht!



Eigene Lösung seit 2016



Mitigation 0525-nemo-erkennung-test.dfn-cert.de (Version 39)

Mitigation Details Target Filter Statistics

Description

Mitigate attack on Autonomous System CERT/DFN-CERT Services GmbH, Hamburg (AS65052)

Protected Ranges

Rules

| Name | Direction | Source CIDRs | Dest. CIDRs | Protocol | Source Ports | Dest. Ports | Action | bps Limit |
|--------------|-----------|--------------|-------------|----------|--------------|-------------|-----------|-----------|
| ✖ [redacted] | incoming | | [redacted] | Any | | | COUNTERM. | |

Add new rule...

Countermeasures

- ☐ IP Header Validation
- ☐ TCP Flags Validation
- ☒ TCP Handshake Validator

☐ GeoIP Filter

Albania

☒ PCAP Filter

PASS src port
DROP dst port

Status: **Active**

nada-stu: **Started**

Mitigation Target

Autonomous System
Hamburg (AS65052)

Target Filter:

ip [redacted]

Comments / History

today, 09:54
Version 39 changed

today, 09:53
Version 38 changed

today, 09:53
Version 39 changed

today, 09:53
Active version 39 cre

Add comment

Stop Mitigation Save & Update Mitigation

Eigene Lösung seit 2016 (2)

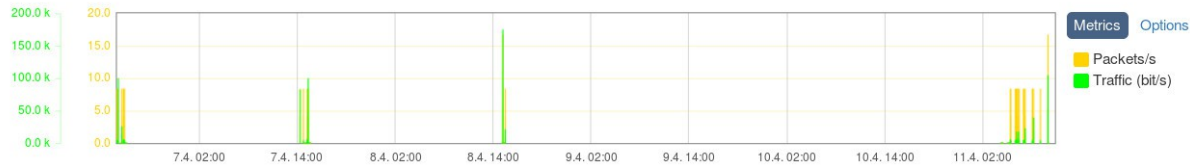


Mitigation 0525-nemo-erkennung-test.dfn-cert.de

Timeframe: 2016-04-06 15:55 - 10:51 2016-04-11 back forward NOW

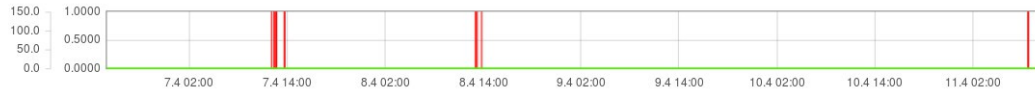
Mitigation Details Target Filter Statistics

Attack Traffic



Rule cm tcp hv

match



geoip



vrify_proto



dn

Status: **Active** (Version 39)

nada-stu: **Started**

Mitigation Target

Autonomous System CERT/DFN-CER
Hamburg (AS65052)

Target Filter:

ip [redacted]

Comments / History

- today, 09:54
Version 39 changed to Active
- today, 09:53
Version 38 changed to stopped
- today, 09:53
Version 39 changed to Starting
- today, 09:53
Active version 39 created by [redacted]

Add comment



Empfehlungen

- Für die grundlegende Architektur sollte beachtet werden:
 - keine Inline-Lösungen für Grobschutz
 - aktive Abwehr, und zwar bevor eigene Komponenten betroffen sind
 - Mitigationskomponenten als Grob- / Mittel- und Feinschutz verstehen
 - Grobschutz outsourcen bzw. vereinbaren
 - Mittelschutz am eigenen Netzwerkübergang
 - Feinschutz direkt am Server



Überlast trotz Mitigation

- **Die Praxis zeigt, dass trotz richtiger Maßnahmen auf ISP-Ebene weiterhin**
 - DDoS-Angriffe nicht erkannt werden, bevor Systemadministratoren Probleme ihres Servers erkennen
 - DDoS-Angriffe nicht abgewehrt werden können, weil die Mitigationsanwendung dafür nicht ausgelegt ist
 - Maßnahmen auf Organisations- bzw. Server-Ebene anderes Wissen über die Dienste erfordern



Kontakt

Prof. Dr. Klaus-Peter Kossakowski

**Email: klaus-peter.kossakowski
@haw-hamburg.de**

Mobil: +49 171 5767010

<https://users.informatik.haw-hamburg.de/~kpk/>