

Vorlesung Netzsicherheit

Kapitel 10 – DDoS

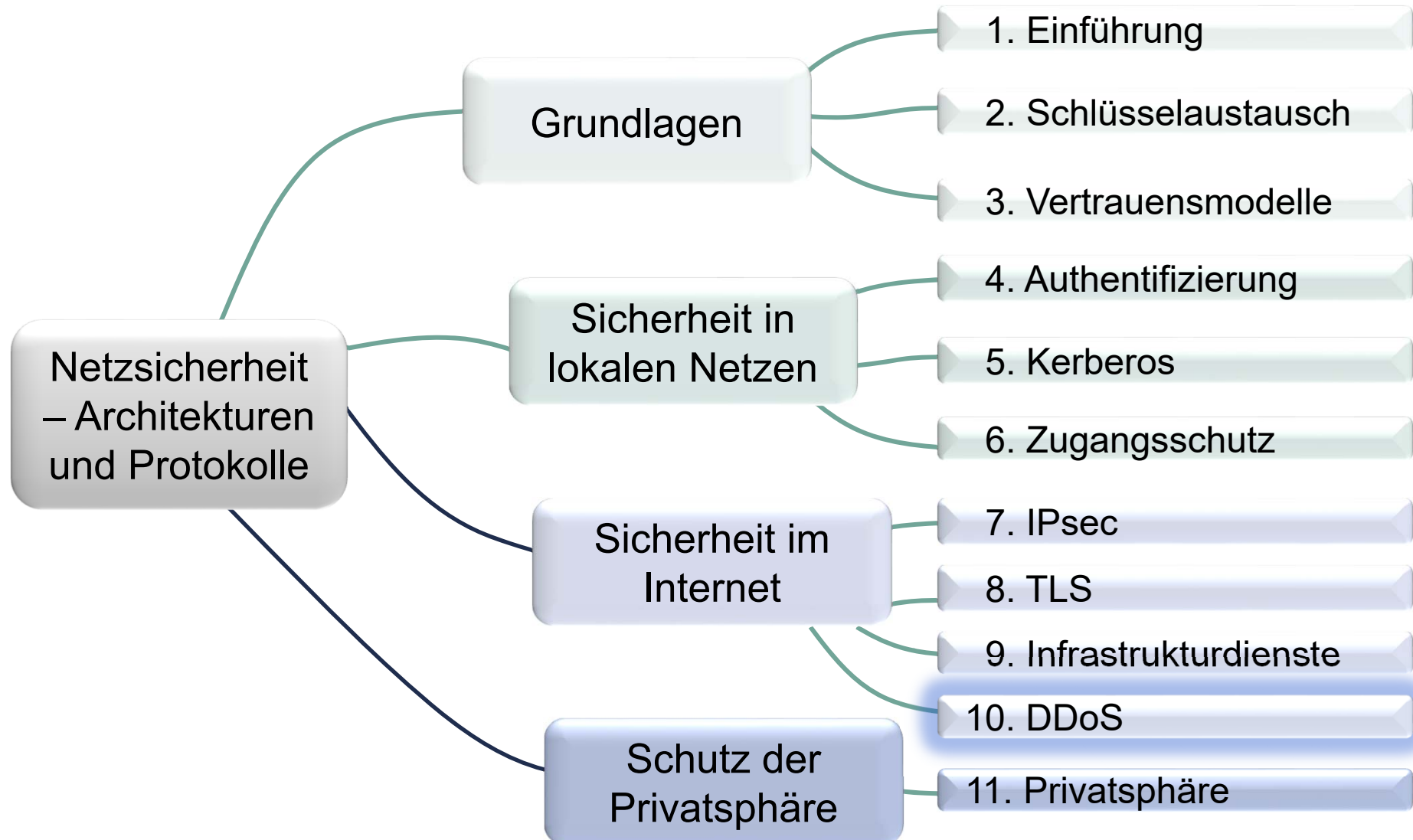
PD Dr. Ingmar Baumgart, PD Dr. Roland Bless, Matthias Flittner, Prof. Dr. Martina Zitterbart
baumgart@fzi.de, [bless, flittner, zitterbart]@kit.edu

Institut für Telematik, Prof. Zitterbart

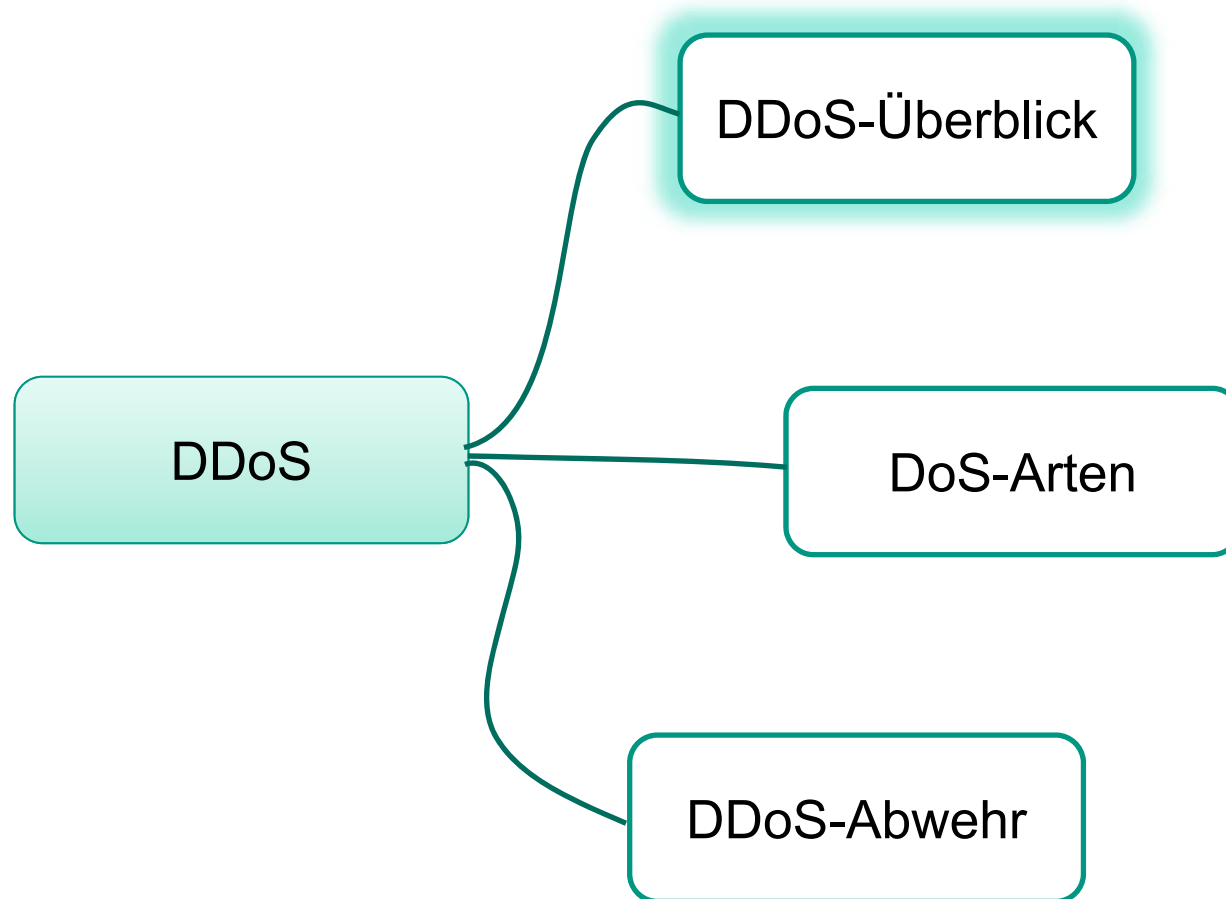


© Peter Baumung

Inhalte der Vorlesung



Überblick



Angriffe auf die Verfügbarkeit/Denial-of-Service

- Angriff auf die Verfügbarkeit eines Dienstes
 - DoS = „Dienstverweigerung“ → gezielte **Sabotage** durch Angreifer
 - Angreifer versucht das Opfer von „sinnvoller Arbeit“ abzuhalten
- Angreifermotivation vielfältig: Erpressung, Rache, Schädigung von Mitbewerbern, Zensur/Unterdrückung von Informationen, ...
- Beispiele für mögliche Opfer:
 - Endsysteme
 - Router
 - Übertragungsabschnitt im Netz
 - ein ganzes Netz
 - ein einzelner Internetnutzer
 - eine Firma (deren Geschäfte vom Internet abhängen)
 - ein Internet-Service-Provider
 - ein Land



Distributed Denial of Service – DDoS

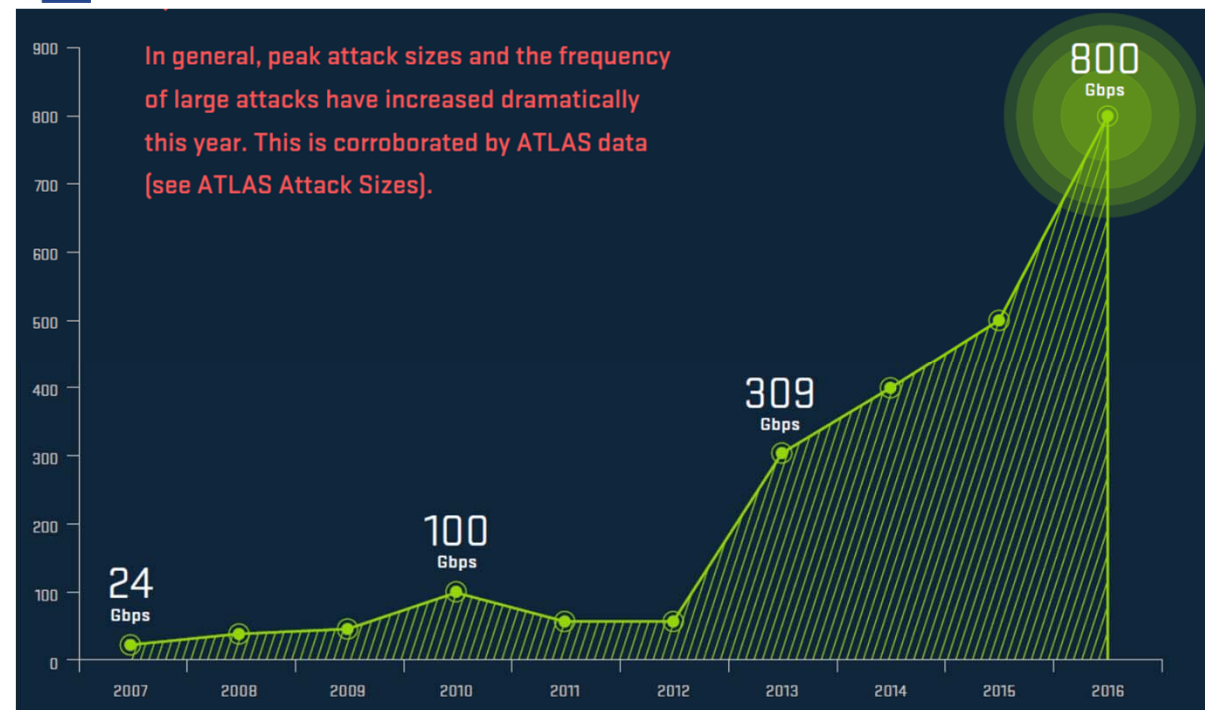
■ Verteilter Angriff durch (sehr) viele Quellen

- Effektiver
- Abwehr ist schwieriger

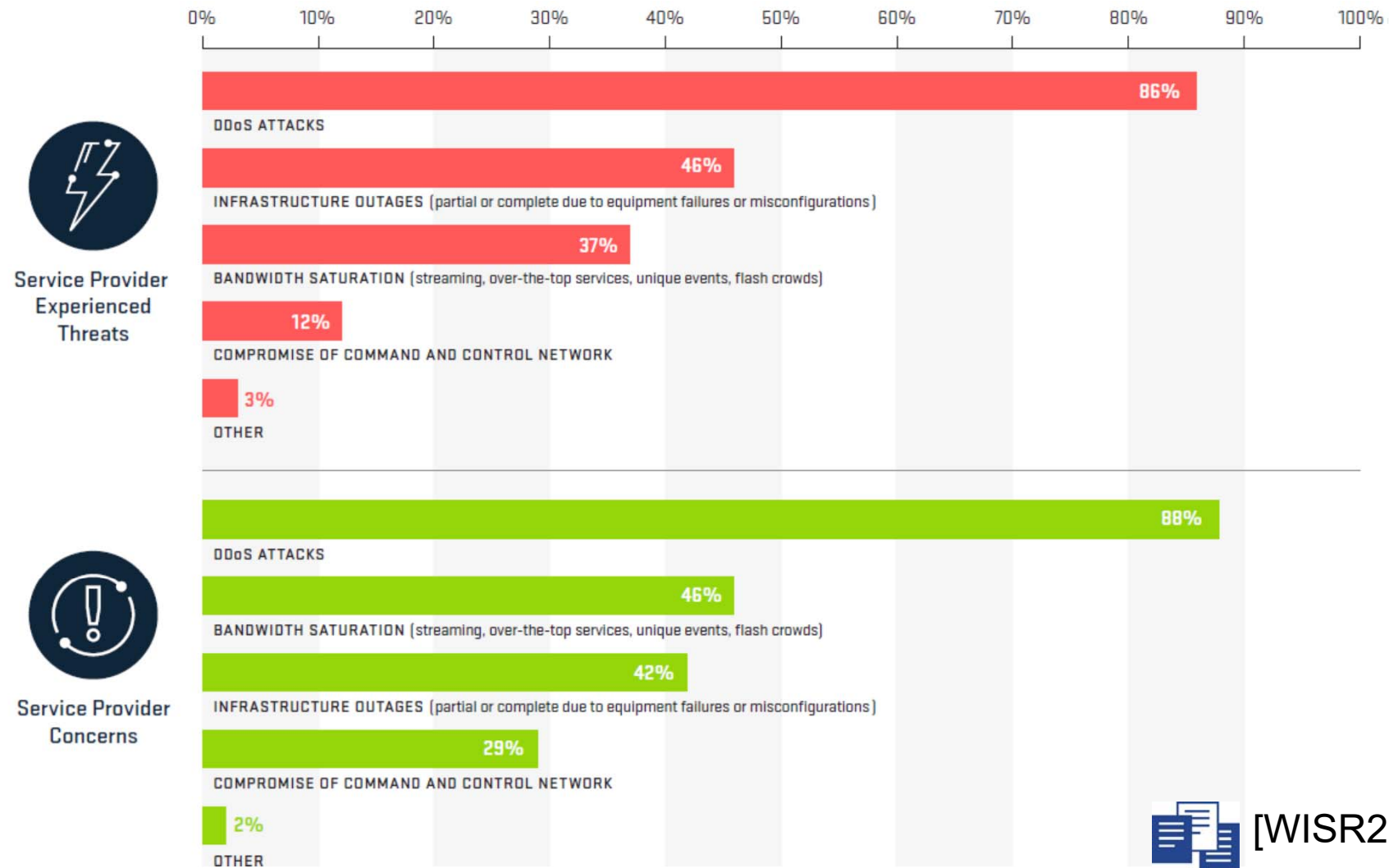
■ DDoS-Zunahme [Heise2016b]

 [WISR2017]

- 2016:
800 Gbit/s
–1,1 Tbit/s
- Mirai Botnetz:
mehrere
10 Millionen
Quellen
identifiziert

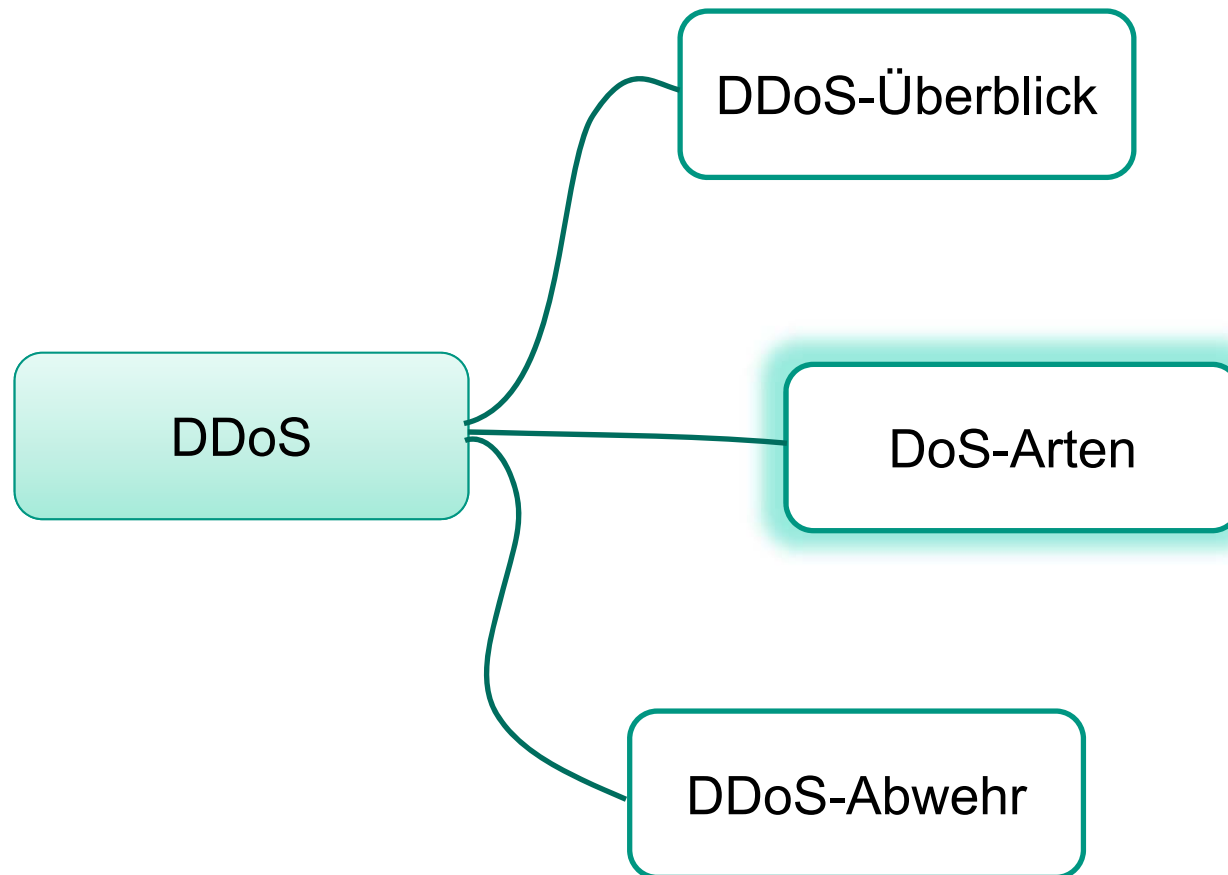
 [Dyn2016]


DDoS – Größte Bedrohung im Internet



[WISR2017]

Überblick



DoS-Arten

- **Physischer** Angriff
- Ausnutzung von **Implementierungsschwächen**
- Ausnutzung von **Protokollschwächen**
- Erzeugung eines **Ressourcenmangels**

DoS: Physischer Angriff

- Angreifer benötigt physischen Zugriff auf Übertragungsmedium
 - Festnetz:
 - Durchschneiden eines Übertragungskabels
 - Erzeugen von Schleifen (z.B. durch Stecken von Kurzschlusskabeln an Switch)
 - „Jamming“ mit Störsender bei einem drahtlosen Medium
 - Zerstören eines Endsystems oder einer Übertragungseinrichtung (z.B. Verstärker, Antennen)

- Abwehr
 - Angreifer vom Medium/Komponente fernhalten (Kabel „sicher“ verlegen, Komponente sicher verschließen)
 - Bei drahtlosem Medium praktisch nicht möglich

DoS: Ausnutzung von Implementierungsschwächen

- **Implementierungsfehler** bringt Programm/System zum Absturz
 - Gezieltes Ausnutzen einer solchen Schwäche durch Angreifer, z.B. Senden eines „Ping of Death“-Pakets
 - Unterscheidung zwischen lokalen (Angreifer hat autorisierten Zugang zu System) und entfernten Exploits (Angreifer hat über Netzwerk Zugriff aber keinen autorisierten Zugang)
- **Abwehr**
 - Angriffsfläche verringern
 - System durch Patches aktuell halten → Zero-Day Exploits ☹
→ quasi hoffnungslos
 - Filtern von potentiellen Angriffspaketen bzw. Filterregeln für verwundbare Dienste
 - Verschiedene Implementierungen parallel einsetzen, redundante Server

DoS: Ausnutzung von Protokollschwächen

- Designfehler **im Protokoll** erlaubt DoS
 - Gezieltes Ausnutzen einer solchen Schwäche durch Angreifer
 - Beispiele:
 - z.B. SYN-Flooding-Angriff bei TCP: Server legt Verbindungskontext direkt bei Erhalt eines SYN-Pakets an → Erschöpfen der verfügbaren Verbindungskontexte
 - IPv6 Routing Header Type 0 Extension: ein Router kann mehrfach im Pfad vorkommen → Verstärkungseffekt kann zu Überlastung eines Übertragungsabschnitts führen
 - Unautorisiertes Umlenken von BGP-Routen (Hijacking + Blackholing)
 - Problem: alle Implementierungen eines Protokolls betroffen!
- **Abwehr**
 - Aktualisierung der Protokollspezifikation
 - z.B. Einsatz von Cookie- oder anderen Sicherheitsmechanismen
 - Falls nur unwesentlicher Teil des Protokolls (z.B. Option) betroffen: Gebrauch der Option untersagen, Filtern entsprechender Pakete

DoS: Erzeugung eines Ressourcenmangels

■ DoS in Anwendungsebene

- Angreiferziel: Anfragerate ist höher als Bedienrate
- z.B. Schicken von zu vielen Suchanfragen zur Überlastung der Datenbank-Backend-Server
- 2007: Angriff auf DNS Root Server
- Praktisch nicht von „Flash Crowd“-Effekt (legitimer Verkehr) zu unterscheiden

■ DoS in Transportebene (→ z.B. TCP-SYN-Flooding-Angriff)

■ DoS in Netzwerkebene

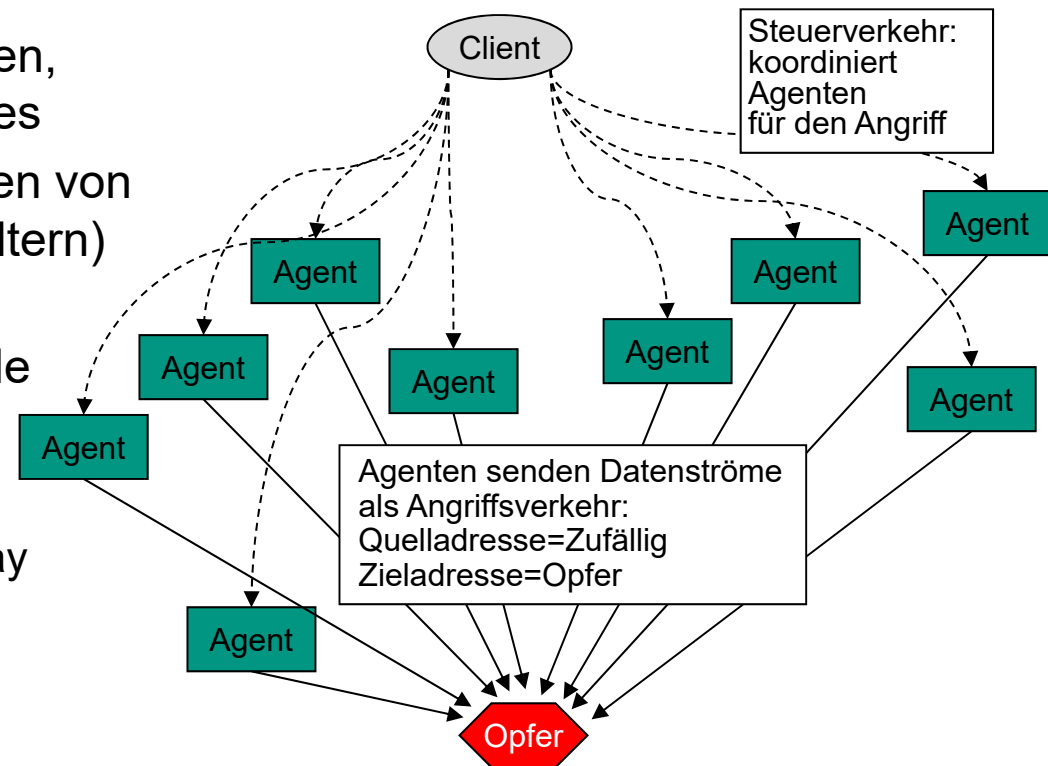
- Angreiferziel: Senderate deutlich höher als Übertragungsrate eines Übertragungsabschnitts entlang des Ende-zu-Ende-Pfads
→ hohe Paketverlustraten für legitime Anfragen

■ Abwehr

- Anwendungsebene: nur autorisierte Anfragen zulassen (aber: passt für viele Dienste ohne Autorisation nicht, Autorisation kann selbst Engpass sein)
- Netzwerkebene: Einsatz von Dienstgütemechanismen, differenzierte Behandlung für autorisierte Datenströme, mehr Ressourcen bereitstellen

DDoS – Distributed Denial of Service

- Verteilter Angriff ist effektiver
 - Bündelung vieler Ressourcen, z.B. mit Hilfe eines Botnetzes
 - Rückverfolgung und Einleiten von Gegenmaßnahmen (z.B. Filtern) schwieriger
 - Häufig zusätzlich Maskerade durch IP-Spoofing
 - Mirai-Botnet: IoT-Geräte,
 - Können trotz NAT-Gateway gekapert werden



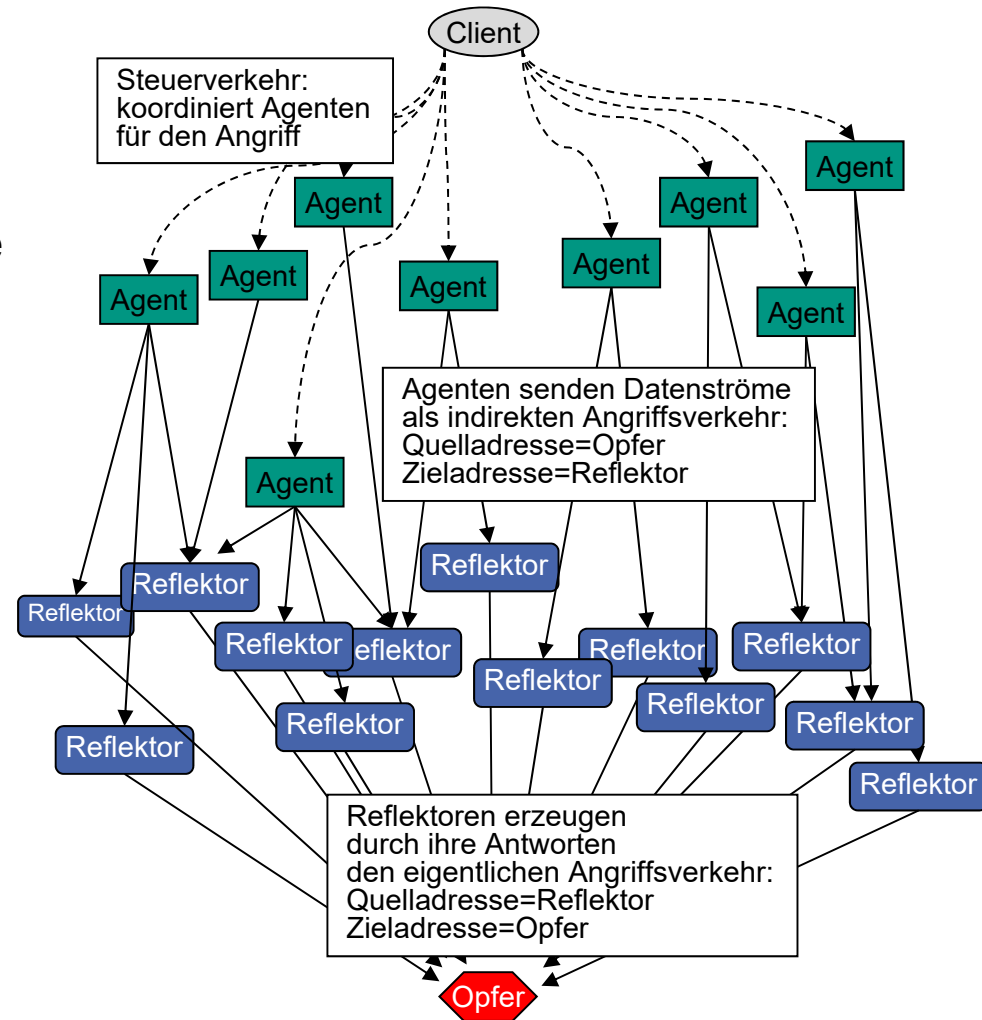
DDoS mit Reflektoren

■ Verstärkungseffekt ausnutzen

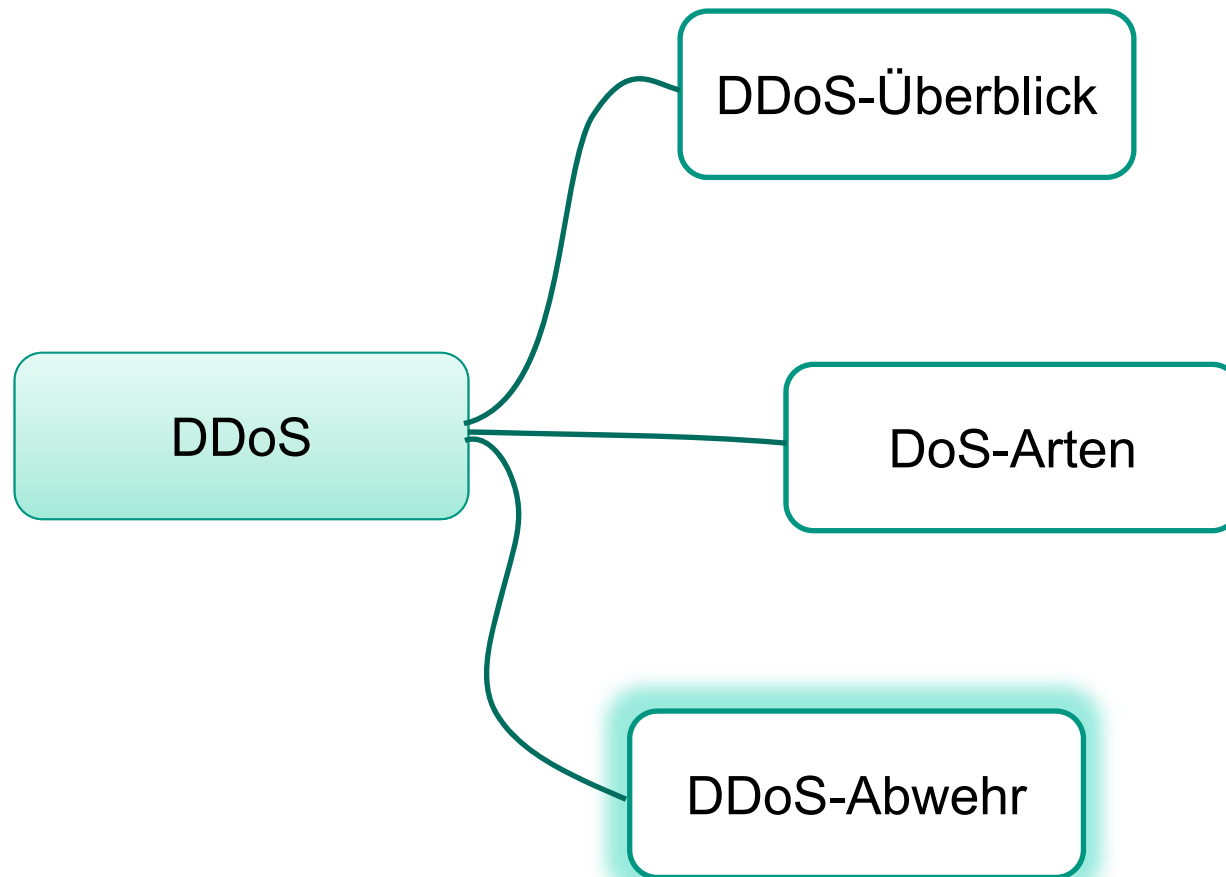
- Agenten senden kleine Anfrage
- Reflektoren erzeugen größere Antwort an Opfersysteme
- gerne UDP-basiert, IP-Spoofing möglich
- Anfang 2014: Angriffe über offene NTP-Server mit >400Gbit/s (ca. 4500 NTP Server, 1300 versch. Netze), Verstärkung bis Faktor 200



[CloudF14]

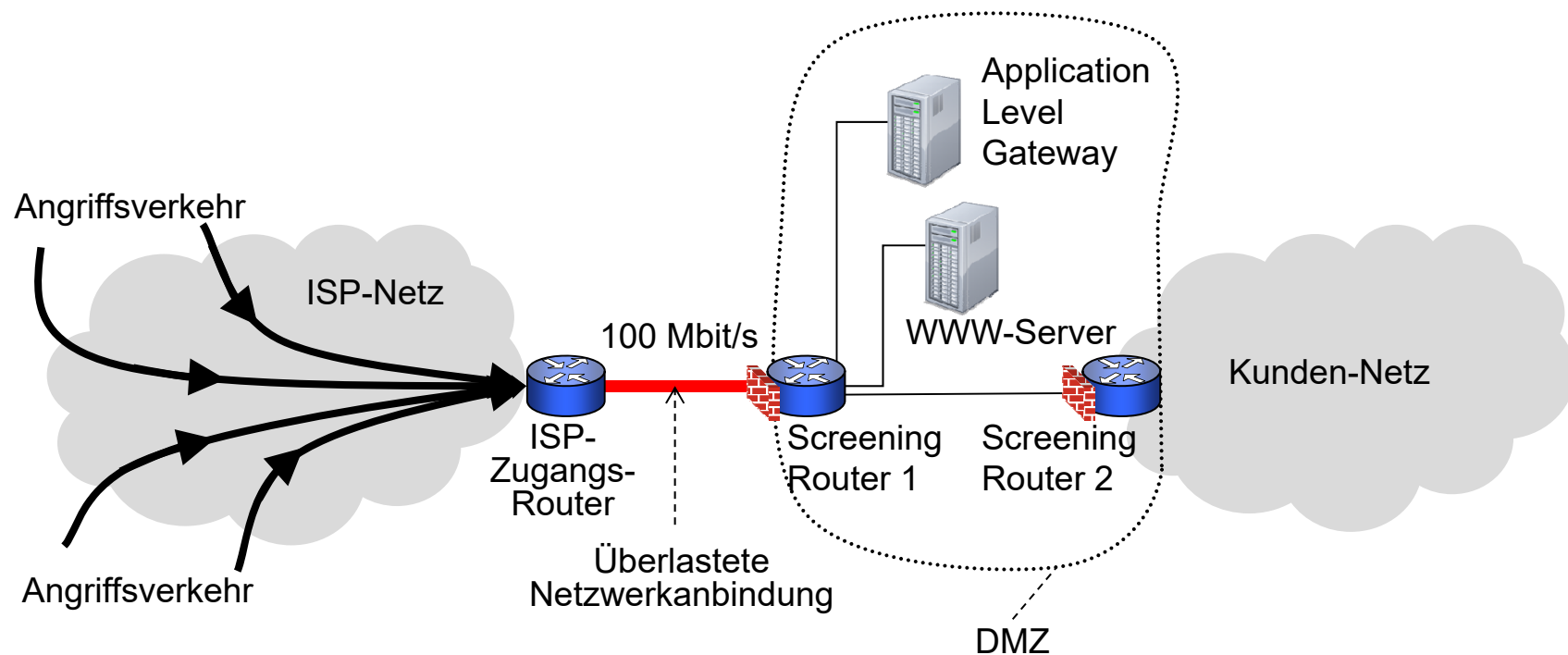


Überblick



DDoS-Abwehr schwierig

- Firewall des Kunden wirkungslos, da Anbindung stromaufwärts überlastet
- Kunde muss Upstream-Provider um Hilfe bitten, um Angriffsverkehr zu filtern (evtl. gezieltes Blackholing durch Bekanntgabe neuer Routen)



DDoS – Gegenmaßnahmen (1)

- **Filtern** des Angriffsverkehrs
 - Schwierig legitimen Verkehr von Angriffsverkehr zu unterscheiden
 - Je näher an der Quelle, desto effektiver
 - Erfordert Kooperation unter Providern
- Relokation des Opfersystems
 - Z.B. Wechsel der IP-Adresse
- **Beseitigen** des **Ressourcenmangels**
 - Lässt sich mit physischen Ressourcen nicht schnell realisieren
 - Bessere Lastverteilung, z.B. durch Einsatz von Anycast
- Stoppen der angreifenden Systeme
 - Rückverfolgung oft durch Spoofing erschwert
 - Identifikation der angreifenden Systeme schwierig
 - Erfordert Kooperation unter Providern

DDoS – Gegenmaßnahmen (2)

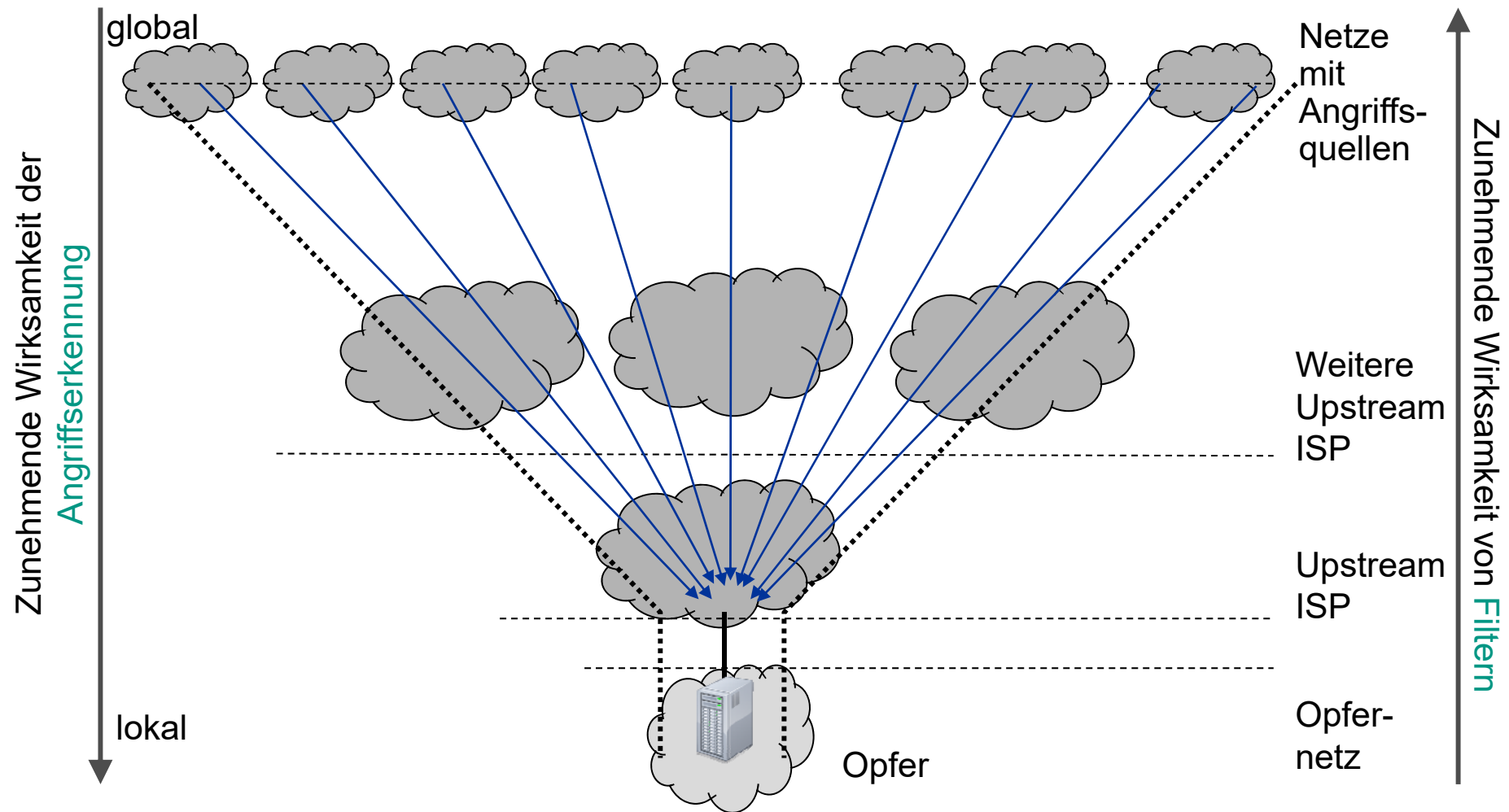
■ Raten-Limitierung

- Problematisch sofern keine Differenzierung zwischen Angriffsverkehr und legitimen Verkehr erfolgt

■ Reaktives Filtern

- Bsp.: Aktives Intrusion Detection System schaltet automatisch Filter für vermutete Angriffsquellen (Blacklisting)
- Mechanismus kann ggf. selbst für DoS ausgenutzt werden: Angreifer bringt IDS dazu Opfersysteme zu Filtern!

Lokationsdilemma: Erkennung vs. Filtern



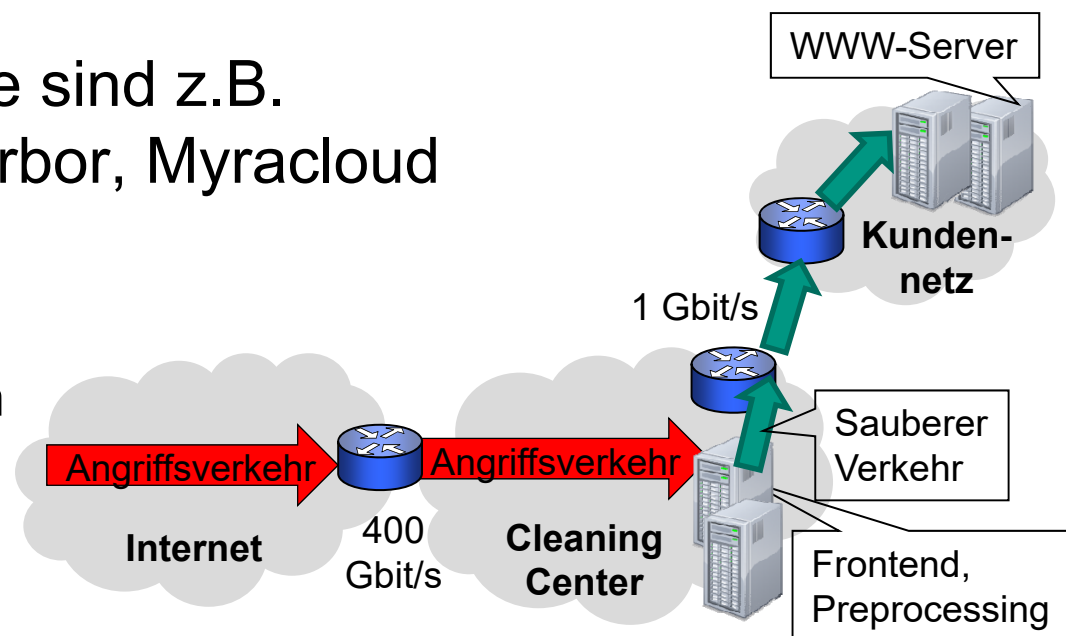
DDoS – Gegenmaßnahmen

■ Benutzung eines **Cleaning Centers**

- Datenverkehr in Richtung eines Kunden wird umgeleitet
- Cleaning Center „wäscht“ DDoS-Verkehr heraus
- Nutzung von Cloud-Ressourcen
- Über eine Clean Pipe erhält Kunde nur legitimen Datenverkehr

■ Anbieter solcher Dienste sind z.B. Tata, Verisign, AT&T, Arbor, Myracloud

- Umleiten des Verkehrs
- Monitoren des Verkehrs
- Entdecken von Angriffen
- Entfernen von Angriffen
- Ausleiten des Verkehrs



DDoS – Gegenmaßnahmen: Grenzen

- Akamai ist auf DDoS-Abwehr spezialisiert
- Angriff auf Brian Krebs Security Blog
 - 620Gbit/s, ohne Reflektoren!
- Akamai konnte Angriff auf Krebs Security nicht mehr abwehren



[Heise2016a]

Einsatz von Ingress Filtering

- **Ingress Filtering:** Filtern von Paketen, deren Quelladresse nicht aus dem zugehörigen Netzbereich stammt
- Möglichst effektiv nahe beim Endsystem (z.B. Filtern per Zugangsport)
- Keine direkte DDoS-Abwehr, ermöglicht aber
 - Effektiveres Zurückverfolgung der Angriffsquellen
 - Effektiveres Filtern
 - Verhindern von Reflektorangriffen

 [RFC2827]

Zusammenfassung

- (D)DoS ist prinzipielles Problem im Internet
 - Jedes System kann unaufgefordert senden

- DDoS-Abwehr schwierig
 - Herausfinden der wirklichen Quellen
 - Oft Kooperation zwischen Betreibern erforderlich
 - “Schutz” durch skalierbare Architekturen

Literatur



- [CloudF14] CloudFlare Blog/Mathew Prince: Technical Details Behind a 400Gbps NTP Amplification DDoS Attack, <http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack>, Feb. 2014
- [DECIX14] <http://www.de-cix.net/products-services/de-cix-frankfurt/blackholing>, 2014
- [Dyn2016] Dyn Statement on 10/21/2016 DDoS Attack, 22.10.2016, <https://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/>
- [ICANN07] ICANN Factsheet: Root server attack on 6 February 2007, <https://www.icann.org/en/system/files/files/factsheet-dns-attack-08mar07-en.pdf>, März 2007
- [Heise2016a] Heise Security: Akamai kapituliert vor DDoS-Angriff auf Security-Blogger, 23.09.2016, <https://www.heise.de/security/meldung/Akamai-kapituliert-vor-DDoS-Angriff-auf-Security-Blogger-3330281.html>
- [Heise2016b] Heise Security: Rekord DDoS-Attacke mit 1.1 Terabit pro Sekunde gesichtet, 29.09.2016, <https://www.heise.de/security/meldung/Rekord-DDoS-Attacke-mit-1-1-Terabit-pro-Sekunde-gesichtet-3336494.html>

Literatur



- [RFC2827] P. Ferguson und D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. RFC 2827 (Best Current Practice), Mai 2000. Updated by RFC 3704. URL: <http://www.ietf.org/rfc/rfc2827.txt>
- [RFC4732] M. Handley, E. Rescorla und IAB. Internet Denial-of-Service Considerations. RFC 4732 (Informational), Dezember 2006. URL: <http://www.ietf.org/rfc/rfc4732.txt>
- [WISR2017] Arbor Special Report, Worldwide Infrastructure Security Report, Volume XII, 2017, [https://pages.arbornetworks.com/rs/082-KNA-087/images/12th Worldwide Infrastructure Security Report.pdf](https://pages.arbornetworks.com/rs/082-KNA-087/images/12th_Worldwide_Infrastructure_Security_Report.pdf)