Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Cyber-Sicherheitsmaßnahmen gegen DDoS-Angriffe

Prof. Dr. (TU NN)
Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

CS-Maßnahmen gegen DDoS-Angriffe
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Bedrohungen
- Abwehrstrategien
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

CS-Maßnahmen gegen DDoS-Angriffe
→ Inhalt

- **Ziele und Ergebnisse der Vorlesung**
- Bedrohungen
- Abwehrstrategien
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Ziele und Ergebnisse der Vorlesung
→ CS-Maßnahmen gegen DDoS-Angriffe

- Gutes Verständnis für die **Bedrohungen** durch DDoS-Angriffe.
- Informationen über die verschiedenen **Angriffsmethoden**.
- Erlangen der Kenntnisse über verschiedene **On- und Off-Site Abwehrstrategien.**

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

CS-Maßnahmen gegen DDoS-Angriffe
→ Inhalt

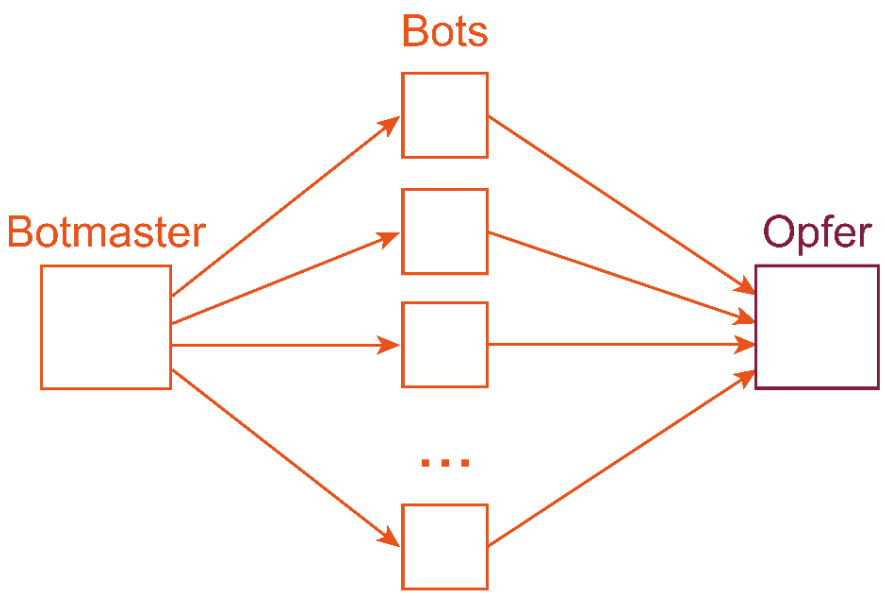
- Ziele und Ergebnisse der Vorlesung
- **Bedrohungen**
- Abwehrstrategien
- Zusammenfassung

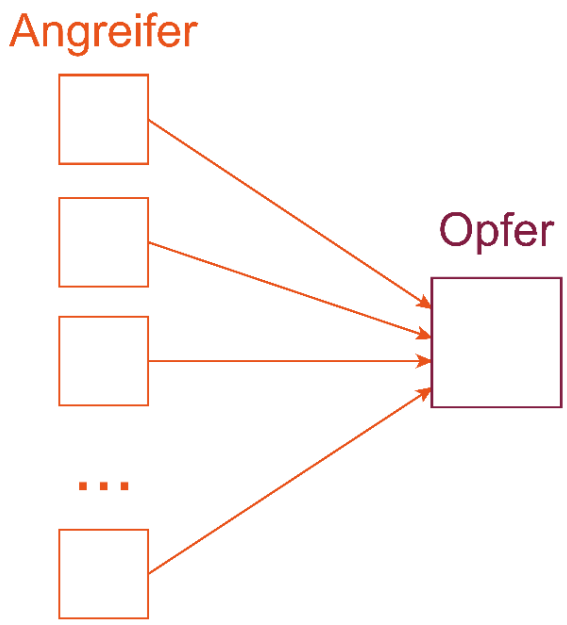
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Bedrohungen
→ Überblick (1/4)

- Die Abkürzung DDoS steht für **Distributed Denial of Service**.

- In der Regel werden die DDoS-Angriffe von **Internet-Aktivisten** und/oder **kompromittierten** IT-Systemen (Bots).





© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Bedrohungen
→ Überblick (2/4)

- **Ziel eines DDoS-Angriffes:**
  Ausgesuchte IT-Systeme koordiniert mit einer großen Last spezieller Anfragen durch **Erschöpfung** der verfügbaren Ressourcen
  - CPU
  - RAM
  - Bandbreite
  - …
  lahmzulegen.

- Es gibt Botnetzte mit sehr vielen Bots (kompromittierten IT-Systemen mit Malware): 1.000, 10.000, 100.000 oder sogar 1.000.000.
  - 100.000 Bots: 100 Kbit/s upstream pro Bot → **10 Gbit/s**
  - 500.000 Bots: 200 Kbit/s upstream pro Bot → **100 Gbit/s**

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Bedrohungen
→ Überblick (3/4)

- IoT-Botnetze stellen eine neue Stufe der Gefahr dar.

- Das **Botnetz Mirai** bestand beispielsweise aus mehr als einer Million kompromittierter IoT-Geräte.
  - Ungesicherte, mit dem Internet verbundene Sicherheitskameras, digitalen Videorekordern, Haushaltsgeräten usw.
  - Verwendete Schwachstelle: **Default-Passwort** des Herstellers.
  - Die Intensität der DDoS-Angriffe erreichte eine bis dahin nicht dagewesene Dimension.
  - Erzeugter Traffic von **665 Gbit/s** bis zu **1,5 Tbit/s**.
  - Basierend auf dem **offenen Quellcode** von Mirai entstanden viele Ableger des Botnetzes.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Bedrohungen
→ Überblick (4/4)

- Die dargestellten Überlastungen sind **schwierig** bis **garnicht zu kontrollieren** und eine kontinuierlich wachsende Herausforderung.

- Nichterreichbarkeit der Internet-Dienste hat **Umsatzeinbußen**, **SLA-Verletzung**, **Kundenabwanderung** oder mögliche **Reputationsschäden** mit oft hohe **Schadsummen** zur Folge.

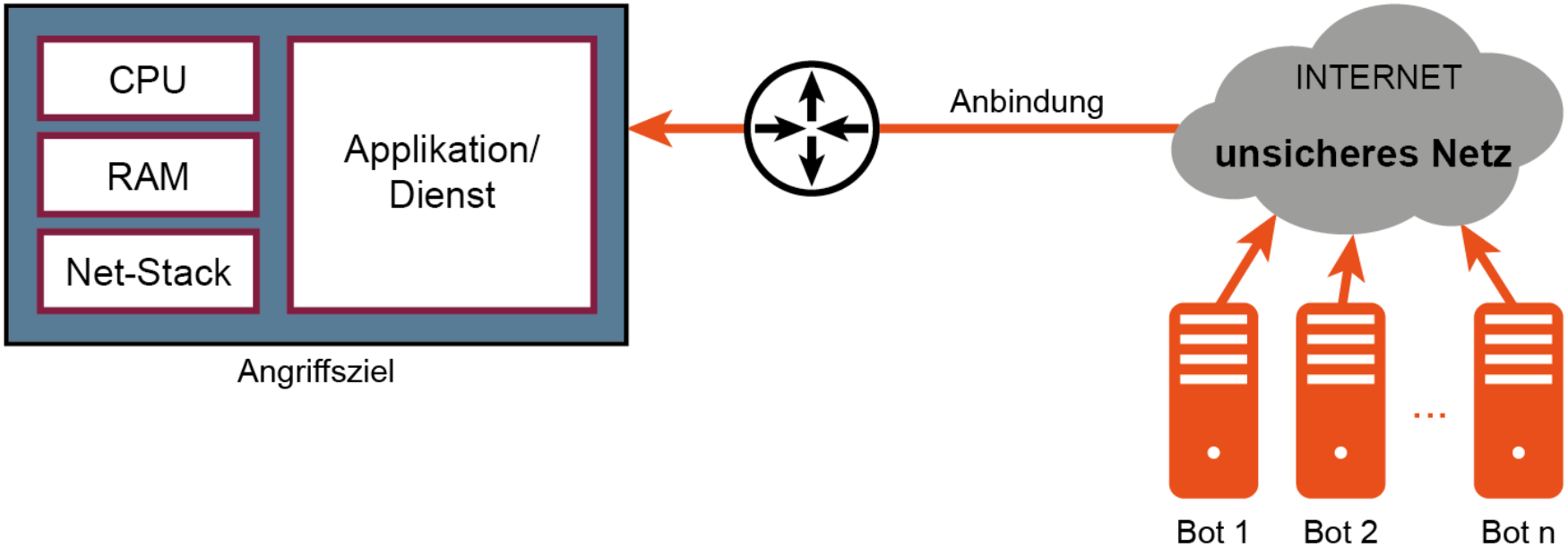
- DDoS-Angriffe werden illegal, kriminell eingesetzt, um Firmen und Organisationen zu **erpressen**, gezielt hohen **Geschäftsschaden** zu verursachen oder um auf **politische Ziele** (Aktivisten) aufmerksam zu machen.

- Technisch wenig bewanderte Kriminelle können solche Angriffe für ihre Zwecke bei „Stresstest“-Dienstleistern und in einschlägigen Portalen **einkaufen**.
  - ab etwa 50 €.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Gezielte Überlastung
→ Ziel

- Durch eine **Kombination unterschiedlicher DDoS-Angriffsmethoden** kann ein Angreifer
  - unterschiedliche Teile eines **Internet-Dienstes** speziell überlasten sowie
  - flexibel auf unzureichende Abwehrmaßnahmen und deren Schwachstellen reagieren.



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Gezielte Überlastung
→ DDoS-Angriffsmethoden (1/3)

Kommunikationsanbindung
→ durch Überlastung der verfügbaren Bandbreite

- Der Angreifer **produziert** so viele **unsinnige Datenpakete**, dass die Bandbreite nicht mehr ausreicht, um die gewünschten Datenpakete zum Server zu transportieren.
- Bei **hoher Last** wird die **Quality of Service schlecht** und
- bei **extremer Last** muss der Router die meisten **Datenpakete verwerfen**, weil die Warteschlangen voll sind.
- Dadurch sind die eigentliche **Anwendung** oder der **Dienst nicht mehr nutzbar**.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Gezielte Überlastung
→ DDoS-Angriffsmethoden (2/3)

Netzwerk-Stack
→ durch Überlastung des verfügbaren RAMs

- Hier kann ein Crash oder ein Überlastungszustand durch Angreifer aufgrund von Fehlern in der Implementierung oder Eigenarten verschiedener Protokollfamilien, insbesondere auch bei eingesetzten Verschlüsselungsverfahren, hervorgerufen werden.

- Ebenfalls kann eine Auslastung des **RAM** durch sehr viele unvollständige Verbindungsanfragen eines Angreifers hervorgerufen werden, was die Verfügbarkeit eines Dienstes schnell stark einschränkt.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

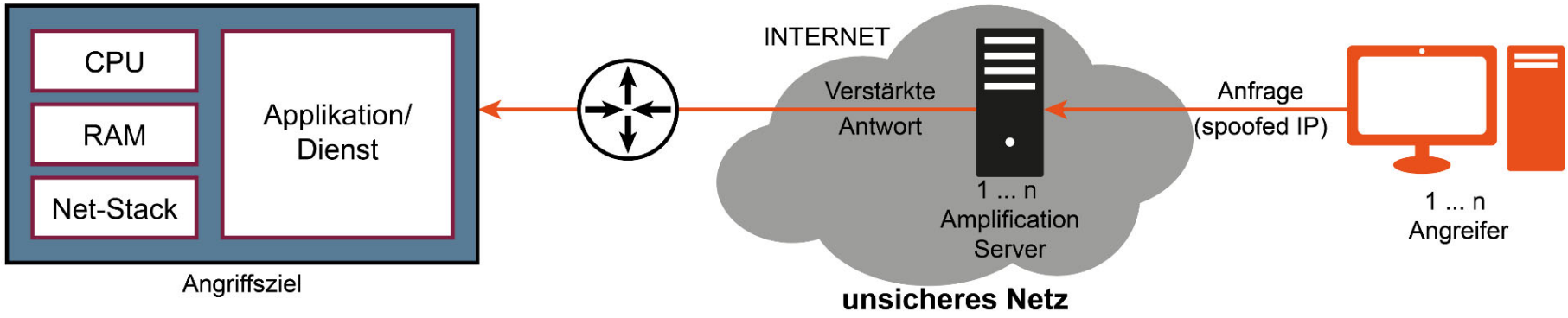
Gezielte Überlastung
→ DDoS-Angriffsmethoden (3/3)

Applikation
→ durch Überlastung der verfügbaren CPU-Ressourcen

- Anwendungsspezifisch erzeugte **Anfragen** durch Angreifer, die auf Fehler oder **wenig performant** implementierte Teile einer **Anwendung** zielen.
- Dazu gehören auch harmlos anmutende Funktionen wie Hashing und datenbankintensive Suchanfragen, die zum Beispiel die **CPU-Ressourcen** für reale, gewünschte Anfragen nicht mehr verfügbar machen.
- Diese Angriffe werden auch **„Low and Slow“** genannt, wenn sich die für einen solchen Angriff benötigten Netzwerkpakete hinsichtlich Frequenz und Payload kaum oder gar nicht vom gewöhnlichen Datenverkehr unterscheiden lassen.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Bedrohungen
→ Reflection und Amplification (1/3)



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Bedrohungen
→ Reflection und Amplification (2/3)

- Diese Angriffe machen sich in erster Linie fremde Server mit UDP-Netzwerkprotokollen zunutze, die ein relativ **kleines Anfragepaket** mit **sehr großen Paketen beantworten**.
- Die Reflection Eigenschaft beruht auf **IP-Spoofing**, womit die Antwort an eine beliebige anzugreifende Ziel-IP **gelenkt** wird.
- Der Angreifer muss für so einen Angriff keine Kontrolle über den fremden Server gewinnen.
- Prominentester Vertreter solcher Angriffe ist der eigentlich veraltete NTP Monlist-Befehl.
  - Dieser sendet als Antwort die Adressen der letzten 600 IT-Geräte, die sich mit dem NTP-Server verbunden haben.
  - Daraus ergibt sich ein **Verstärkungsfaktor von über 200** (1 Byte → 200 Byte an das Angriffsziel).

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Bedrohungen
→ Reflection und Amplification (3/3)

- Viele weitere Protokolle sind ebenfalls anfällig: DNS, SNMP und sogar P2P-Protokolle verschiedener Botnetze.

- Weiteres Beispiel: Pingback-Funktion der bekannten CMS- bzw. Blogging-Software Wordpress.
  - Anfragen von einer Wordpress-Instanz zu anderen Webseiten zu schicken, um Querverweise zwischen Blogs zu generieren.
  - Angreifer schickt Pingback-Requests mit der anzugreifenden Webseite als Ziel an beliebig viele Wordpress-Seiten.
  - Diese kontaktieren daraufhin alle das anzugreifende IT-System.
  - Sicherheitsplugin bereits veröffentlicht.

- Der Anteil von Reflection-Angriffen im Vergleich zu allen DDoS-Angriffen liegt bei etwa 40% (Akamai PLXsert Q4 2014 State of the Internet – Security Report).

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

CS-Maßnahmen gegen DDoS-Angriffe
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Bedrohungen
- **Abwehrstrategien**
- Zusammenfassung

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien
→ Cyber-Sicherheitsrichtlinien (1/2)

- Zu allererst sollte eine **Risikoanalyse** bezüglich der **notwendigen Verfügbarkeit** der eigenen Internet-Dienste durchgeführt werden.
- Durch eine **Kalkulation von Risiko und Folgeschäden** muss das vorhandene **Budget für die Robustheitsmaßnahmen** bestimmt werden.
- Dabei sollte die **Eintrittswahrscheinlichkeit** eines DDoS-Angriffes nicht, wie leider häufig der Fall, deutlich unterschätzt werden.
- Strategie: Ein **Ablaufplan mit Richtlinien** für die Vorgehensweise in einem akuten Angriffsfall muss aufgestellt werden.
- Spezielle **Handlungsrollen** für das IT-Personal, andere Geschäftsabteilungen und eingebundene Dienstleister müssen darin festgelegt sein.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien
→ Cyber-Sicherheitsrichtlinien (2/2)

- Im Anschluss an die Konzeptionierung sollte die Wirkung der Strategie mithilfe **simulierter Angriffsszenarien** getestet werden.

- **Regelmäßiges Überprüfen** und **Testen** der Abwehrstrategie ist ebenso wichtig.
  - Es dient der Verifikation, ob die etablierten Robustheitsmaßnahmen zeitgemäßen Angriffen noch standhalten und sorgt dafür, dass das Personal im Falle eines Angriffs noch planmäßig handelt.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien
→ On-Site: Aufrüsten der Ressourcen

- Zunächst mag es sinnvoll erscheinen, diejenigen Ressourcen aufzustocken, die durch einen DDoS-Angriff überlastet werden könnten.
  - Dafür kommen mehr Anbindungsbandbreite und leistungsstärkere Server (CPU, RAM, …) infrage.
- Die Kapazitäten eines gezielten Angriffs übersteigen jedoch mit Leichtigkeit den Schutz durch jede sinnvolle Ressourcenaufrüstung innerhalb von kurzer Zeit.
- Derartige Cyber-Sicherheitsmaßnahmen haben einen schlechten **Kosten-Nutzen-Effekt**.
  - Mehrkapazität wird nur im Angriffsfall wirklich benötigt und reicht dann selten aus.
- Ein wirksamer Schutz muss bereits **vor der Infrastruktur** ansetzen.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien
→ On-Site: Sofortmaßnahmen (1/3)

- Findet bereits ein DDoS-Angriff statt, können dessen Auswirkungen unter bestimmten Umständen eingedämmt werden.
  - Whitelisting für besonders wichtige, zugriffsberechtigte Nutzer oder Kunden.
  - Login-Wall, Captchas oder eine Überprüfung der Browser-Echtheit.
  - Vorhandenes Sicherheitsequipment passend konfigurieren, um entsprechenden Traffic zu blockieren.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien
→ On-Site: Sofortmaßnahmen (2/3)

- Wenn hingegen die globale Verfügbarkeit des jeweiligen Internet-Dienstes nicht essentiell ist, so besteht die Möglichkeit, kurzerhand bestimmte **IP-Adressbereiche (Geolocation) zu blockieren**, um die Traffic-Flut einzugrenzen.

- Eine solche Sofortmaßnahme ist oft nicht ausreichend, da der Effekt sehr unterschiedlich wirken kann.

- Angreifer können heute sehr schnell ihre Taktik ändern, sowie die Angriffsressourcen problemlos schnell aufrüsten.

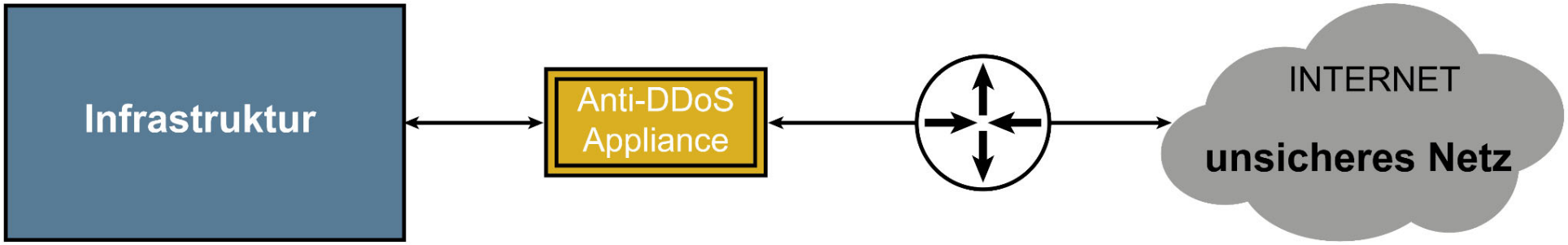
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien
→ On-Site: Sofortmaßnahmen (3/3)

- Ebenso wichtig wie das Einleiten technischer Gegenmaßnahmen, ist der richtige Umgang mit der Öffentlichkeit.
  - Schnell kommt es durch nicht verfügbare Internet-Dienste zu frustrierten Nutzern.
- Es empfiehlt sich, den Angriff und Erpressungsversuch öffentlich mitzuteilen, die Hintergründe zu erklären und das weitere Vorgehen im Sinne der Nutzer ausreichend transparent zu kommunizieren.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien
→ On-Site: Anti-DDoS Appliance (1/3)



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien
→ On-Site: Anti-DDoS Appliance (2/3)

- Einigen Angriffsmustern im Rahmen der verügbaren Anbindungsbandbreite entgegenwirken.

- Filterung des eingehenden Datenverkehrs.
  - Statisch
  - Selbstlernend gegen unbekannte Angriffe auf Applikations-Ebene, „Low and Slow“-Angriffe und Multivektor-Angriffe.

- Einfache Integration in die bestehende Infrastruktur.
  - DDoS-Angriffe frühzeitig erkennen.
  - Robustheit erhöhen.

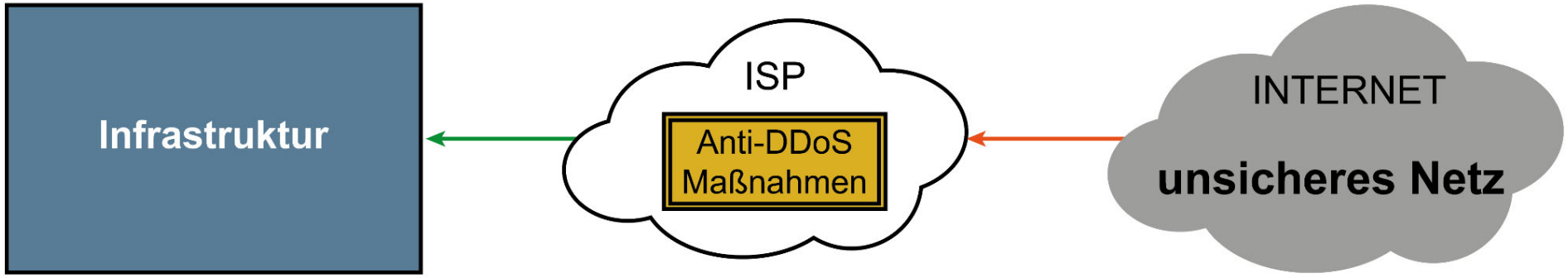
© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien
→ On-Site: Anti-DDoS Appliance (3/3)

- Verfügbare Bandbreite ist schnell erschöpft (z.B. Bei Aplification Attacks):
  - Keine Abhilfe durch Anti-DDoS-Appliance.
  - Die Leitung wird dann bereits am Router zur Infrastruktur „verstopft“.
- Implementierten Filtertechnologien oft nicht gegen alle Angriffe wirksam, insbesondere bei eingesetzter Verschlüsselung und Application-Angriffen.
- Zur Abwehr von Angriffen mit großem Datenvolumen wird unbedingt die Zusammenarbeit mit einem externen Dienstleister benötigt.
  - Dabei gibt es unterschiedliche Schutzmodelle für verschiedene Anwendungsfälle.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien
→ Off-Site Dienstleistungsmodelle



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

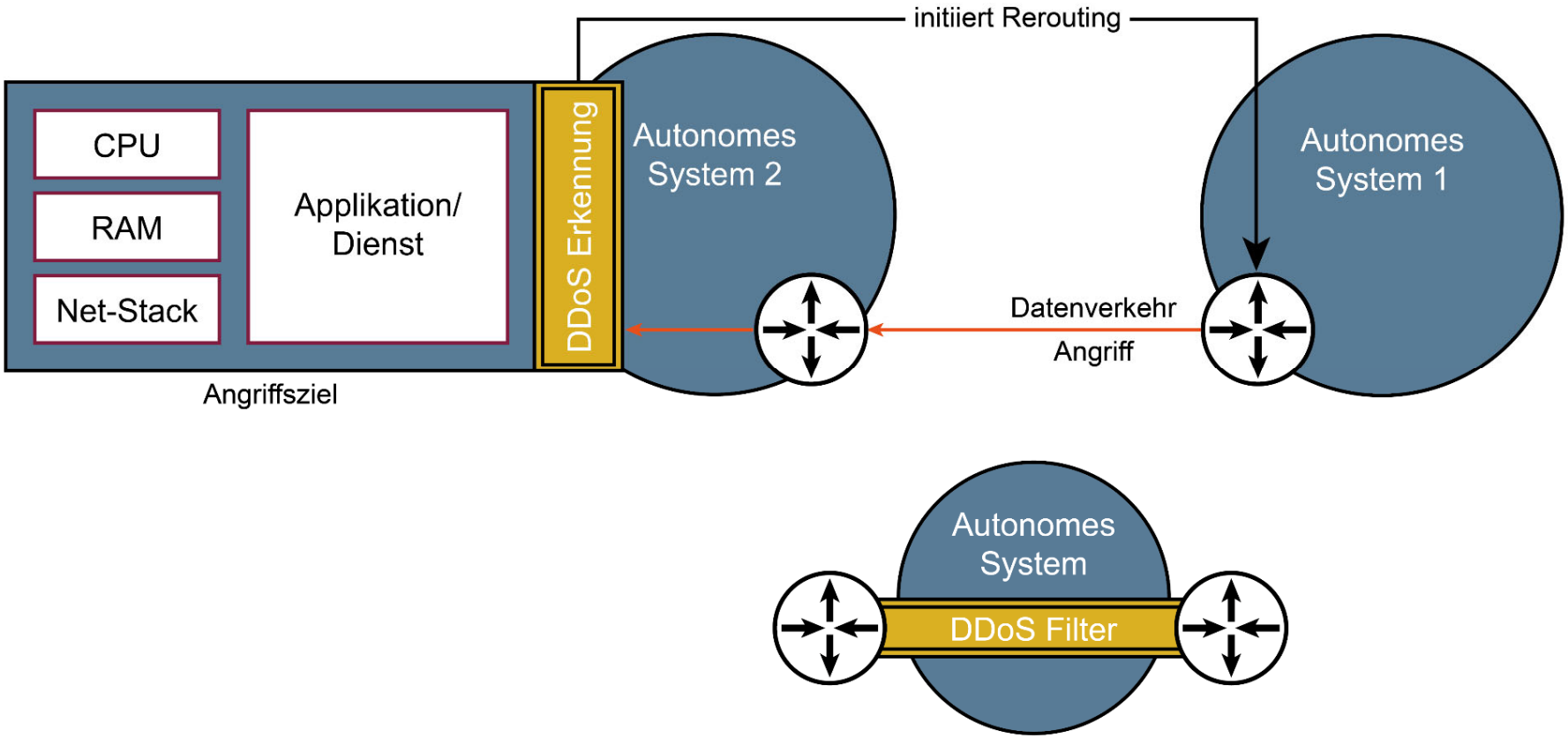
Abwehrstrategien
→ Off-Site: Traffic-Scrubbing-Netze (1/4)

- Robustheitsanbieter betreiben spezielle Autonome Systeme, die sehr gut dabei helfen, DDoS-Traffic zu filtern.
  - Bei dieser Methode ist die Infrastruktur speziell für die Filterung von DDoS-Angriffen konzipiert.
- Mithilfe dieser Abwehr-Technologie kann eine gesamte Infrastruktur mittels eines BGP-Rerouting-Mechanismus vor DDoS-Angriffen geschützt werden.
  - Source- und Destination-IP der Kommunikation bleiben dabei unverändert, die Umleitung durch das Filternetz verursacht nur minimale Verzögerung.
- Alternativ steht meist eine DNS-Umleitung speziell für Webserver zur Verfügung.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien
→ Off-Site: Traffic-Scrubbing-Netze (2/4)

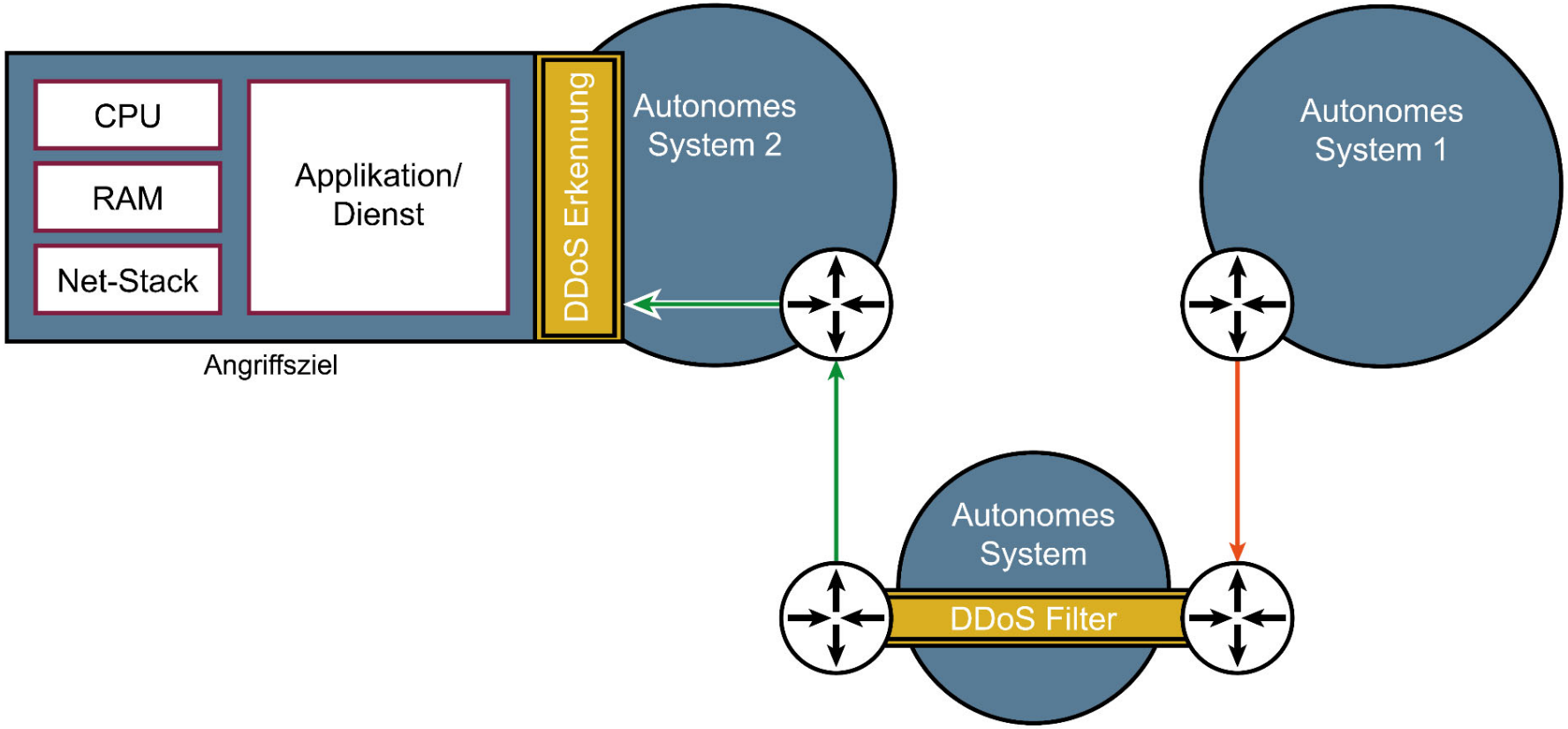
- **Der Schutzmechanismus:**
  Die Filtertechnik steht bei einem DDoS-Angriff im Hot-Standby.



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien
→ Off-Site: Traffic-Scrubbing-Netze (3/4)

- Nur wenn der DDoS-Erkennungsfilter einen Angriff feststellt, wird der Datenverkehr per Netz-Announcement über das Filternetz geroutet.



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien
→ Off-Site: Traffic-Scrubbing-Netze (4/4)

- Durch die Nutzung eines weiteren Autonomen Systems und sehr gute DDoS-Filter können auch sehr starke DDoS-Angriffe unwirksam gemacht werden.

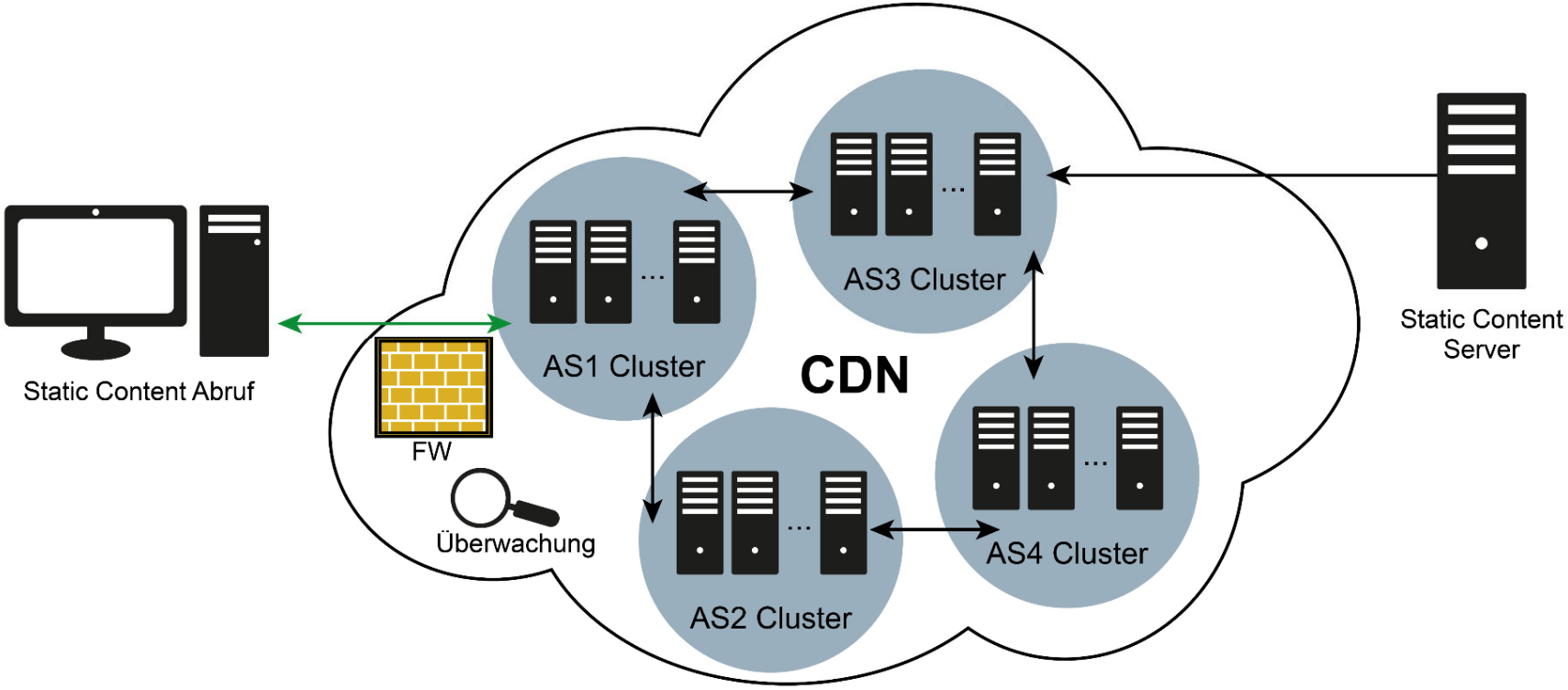
- Für diese Cyber-Schutzmaßnahme ist mindestens ein eigenes /24 Subnetz erforderlich.

- Dienstleister verfügen über Rechenzentren mit 1+ Tbps-Anbindung an verschiedene Carrier und intelligente DDoS-Filter-Technologien.
  - Kriterium für die Filterung von DDoS-Verkehr ist neben bekannten Mustern ein Scoring-Modell.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien
→ Off-Site: Content-Delivery-Network

- Statische Inhalte werden redundant via **Caching** oder **Replikation** auf Servern, die an vielen **verschiedenen Standorten** in verschiedene **Autonome Systeme** eingebunden sind.

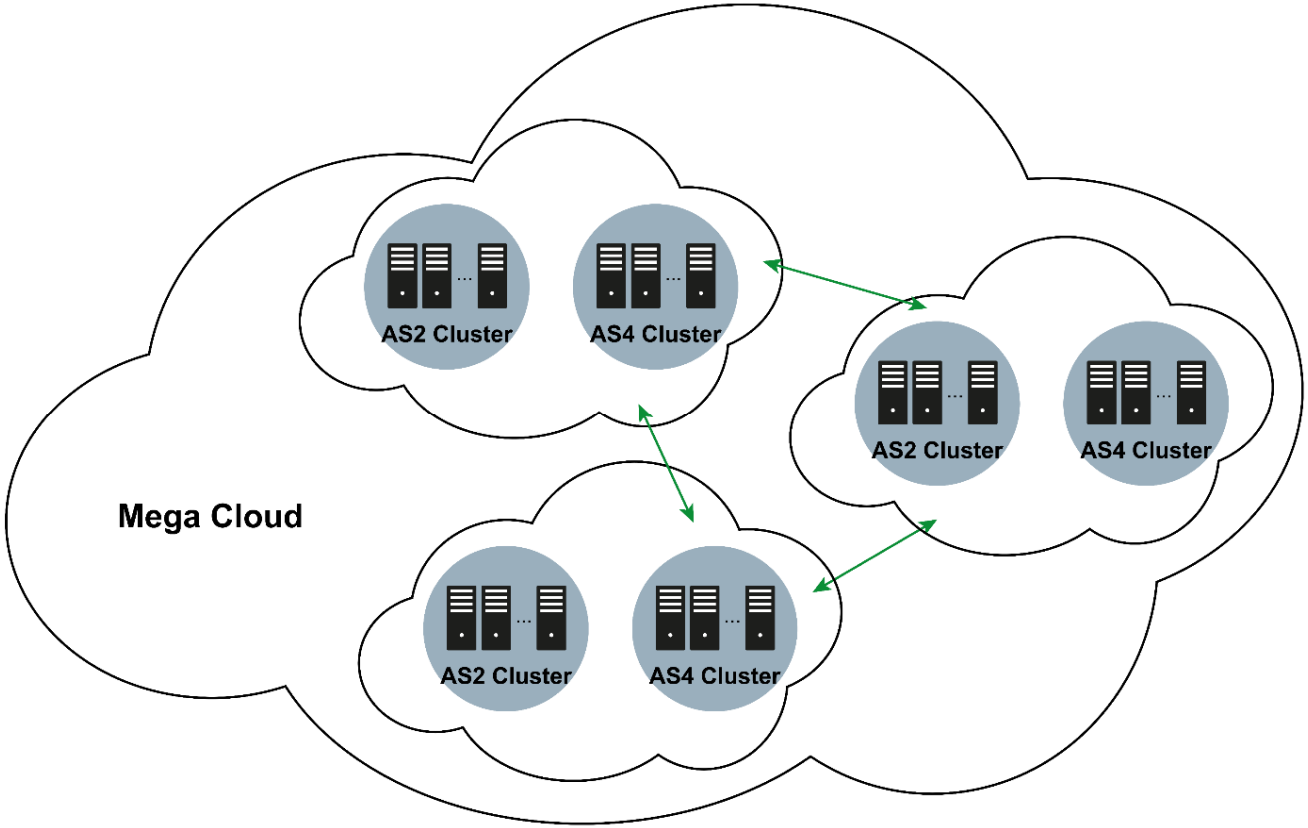


© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien
→ Off-Site: Mega-Cloud

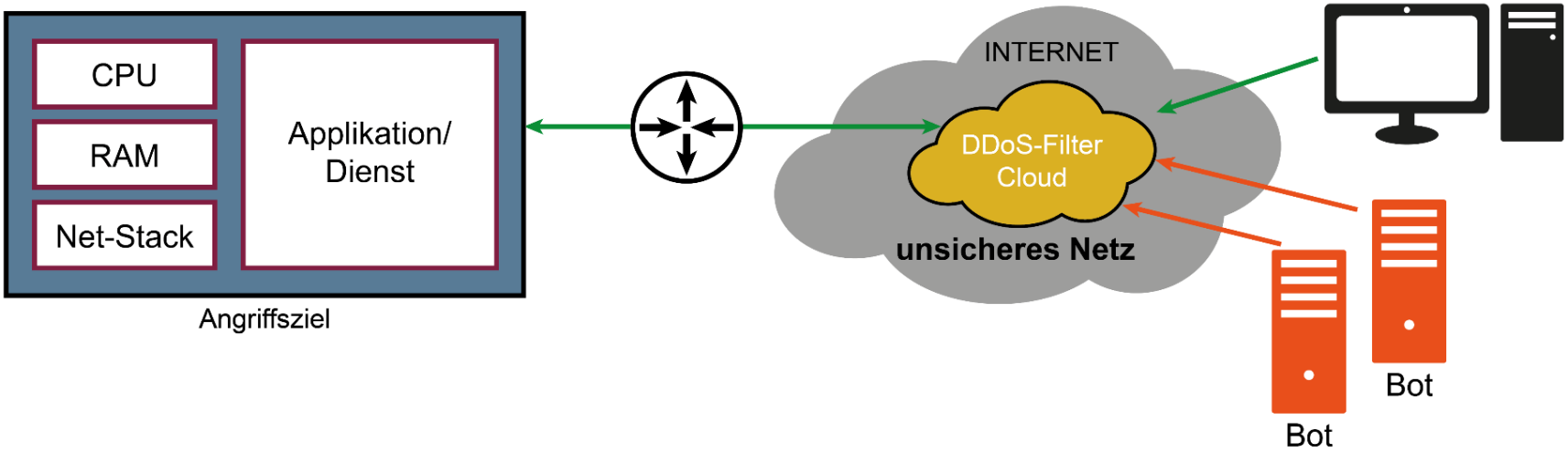
- Die Cloud-Umgebung bietet viele redundante Ressourcen in einer weltweit verteilten Umgebung.

- Umzug kann viel Aufwand bedeuten und nicht für alle Teile der eigenen Infrastruktur in Frage kommen, insbesondere in Bezug auf hochsensible Daten.



© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien
→ Off-Site: Cloud-Filter (1/2)



- Dienstleister von Cloud-Filternetzen vereinen alle bisher vorgestellten Konzepte in einer Lösung.
- Reverse-Proxy über einem weltweiten CDN mit DNS-Servern, Caching, Blocklisten, BGP Origin Protection, Web-Application-Firewall (WAF), Malware-Scanner, Spam-Schutz, ...

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien
→ Off-Site: Cloud-Filter (2/2)

- Die Preise liegen je nach Schutzbedarf, SLA und Support zwischen einem kostenlosen Basis-Schutz und über 5.000 US-Dollar monatlich.

- Die eigenen Server werden hierbei von der Cloud-Infrastruktur vor Angriffen abgeschirmt.
  - Dafür muss der Dienstleister lediglich als verantwortlichen Nameserver der eigenen Domain(s) eingetragen werden.
  - Die übrige Konfiguration findet dann über die Webseite des Anbieters statt.

- Einfachheit und Flexibilität bei der Auswahl der verschiedenen Angebote macht diese Lösung für kleine und größere Unternehmen besonders attraktiv.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien

→ Präventiv: Sichere Konfiguration von Diensten (1)

- **Schlecht konfigurierte IT-Systeme** sind ein großes Problem bei DDoS-Angriffen.
  - Admins sollten verhindern, dass das eigene Netzwerk an DDoS-Angriffen teilnimmt.
  - Die eigenen, öffentlich erreichbaren Server müssen auf Missbrauchspotential geprüft werden.
- Eine wichtige Cyber-Sicherheitsmaßnahme ist beispielsweise das **Abschalten von offener Rekursion** auf DNS-Servern.
  - Ausnahmen nur für vertrauenswürdige Quellen.
- NTP-Server laufen häufig auf älteren Servern, denen oft keine große Beachtung mehr geschenkt wird.
  - Dabei sollten gerade diese unbedingt auf den aktuellen Stand gebracht werden.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Abwehrstrategien

→ Präventiv: Sichere Konfiguration von Diensten (2)

- Grundlegende Cyber-Sicherheitsmaßnahmen wie **Awareness-Kampagnen** und **Endpoint-Protection** dämmen das Infektionsrisiko für Botnetz-Malware weiter ein.

- Zusätzlich sollte IP-Spoofing mittels **Egress-Filtering** (Überwachung von Datenpaketen, die das eigene Netzwerk verlassen) unterbunden werden.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

CS-Maßnahmen gegen DDoS-Angriffe
→ Inhalt

- Ziele und Ergebnisse der Vorlesung
- Bedrohungen
- Abwehrstrategien
- **Zusammenfassung**

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

CS-Maßnahmen gegen DDoS-Angriffe
→ Zusammenfassung

- Mit dem Internet-of-Everything kommt – mit Zombie-Armeen aus vielen schlecht gesicherten Embedded-Devices - ein zusätzlicher Schwung von erfolgreichen DDoS-Angriffen.
- Die Angriffe kommen schnell und meist unvorhergesehen.
- Verantwortliche in Firmen und Organisationen, deren Umsatz und Geschäftsbetrieb von Internet-Diensten abhängig ist, sollten sich um Robustheitsmaßnahmen mit passender Abwehrstrategie bei DDoS-Angriffen kümmern.
- Hundertprozentigen Schutz vor DDoS-Angriffen gibt es ebenso wenig, wie absolute Cyber-Sicherheit.
- Ziel von Cyber-Sicherheitsmaßnahmen gegen DDoS-Angriffe ist immer, das Schutzniveau und somit die Hürden für Angreifer möglichst hoch zu setzen.

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Cyber-Sicherheitsmaßnahmen gegen DDoS-Angriffe

Prof. Dr. (TU NN)
Norbert Pohlmann

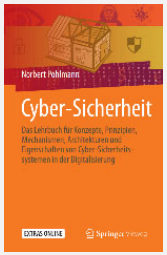
Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
http://www.internet-sicherheit.de

if(is) internet-sicherheit.

Anhang / Credits

Wir empfehlen

- **Cyber-Sicherheit**
  Das **Lehrbuch** für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, Springer Vieweg Verlag, Wiesbaden 2022
  https://norbert-pohlmann.com/cyber-sicherheit/



- **7. Sinn im Internet (Cyberschutzraum)**
  https://www.youtube.com/cyberschutzraum

CYBER SCHUTZRAUM

- **Master Internet-Sicherheit**
  https://it-sicherheit.de/master-studieren/

MASTER internet-sicherheit.

Besuchen und abonnieren Sie uns :-)

WWW
https://www.internet-sicherheit.de

Facebook
https://www.facebook.com/Internet.Sicherheit.ifis

Twitter
https://twitter.com/_ifis

https://twitter.com/ProfPohlmann

YouTube
https://www.youtube.com/user/InternetSicherheitDE/

Prof. Norbert Pohlmann
https://norbert-pohlmann.com/

Quellen Bildmaterial

Eingebettete Piktogramme:
- Institut für Internet-Sicherheit – if(is)

Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.
https://www.it-sicherheit.de/

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen

Literatur
→ Artikel / Bücher

R. Fritzen, N. Pohlmann: „Distributed Denial of Service Attacks (DDoS) – Wie robust sind Dienste im Internet?“, IT-Sicherheit – Management und Praxis, DATAKONTEXT-Fachverlag, 2/2015
https://norbert-pohlmann.com/wp-content/uploads/2015/08/332-Distributed-Denial-of-Service-Attacks-DDoS-Wie-robust-sind-Dienste-im-Internet-Prof-Norbert-Pohlmann.pdf

R. Fritzen, N. Pohlmann: „Von überall her – Internetdienste vor DDoS-Angriffen schützen“, iX - Magazin für professionelle Informationstechnik, Heise-Verlag, 09/2015
https://norbert-pohlmann.com/wp-content/uploads/2017/07/335-Von-überall-her-–-Internetdienste-vor-DDoS-Angriffen-schützen-Prof.-Norbert-Pohlmann.pdf

N. Pohlmann: "Cyber-Sicherheit – Das Lehrbuch für Konzepte, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung“, ISBN 978-3-658-25397-4; 594 Seiten, Springer-Vieweg Verlag, Wiesbaden 2019
https://norbert-pohlmann.com/cyber-sicherheit/

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen