Denial of Service

Wie können sich Provider dagegen schützen?

10.5.2016

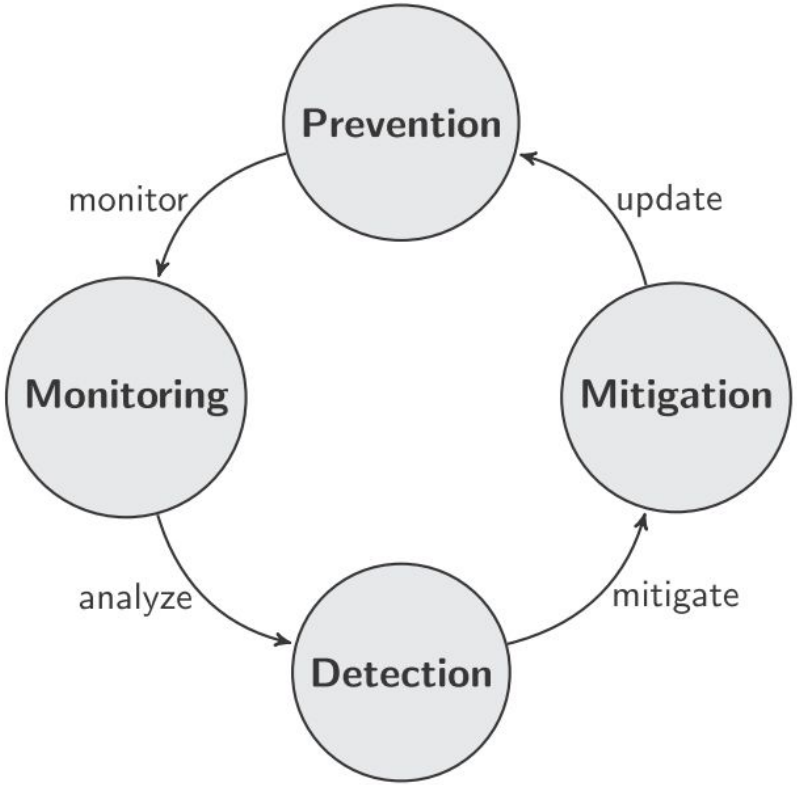
von Lutz Jankowski

Gliederung

1. **Was ist DDoS-Mitigation?**
2. Ist DDoS-Mitigation sinnvoll?
3. DDoS-Attacken vorbeugen
4. DDoS-Attacken erkennen
5. DDoS-Attacken abwehren
6. Fazit

Was ist DDoS-Mitigation?

Eine Menge von Techniken, die darauf abzielt einen DDoS-Angriff abzumildern und zu überstehen.



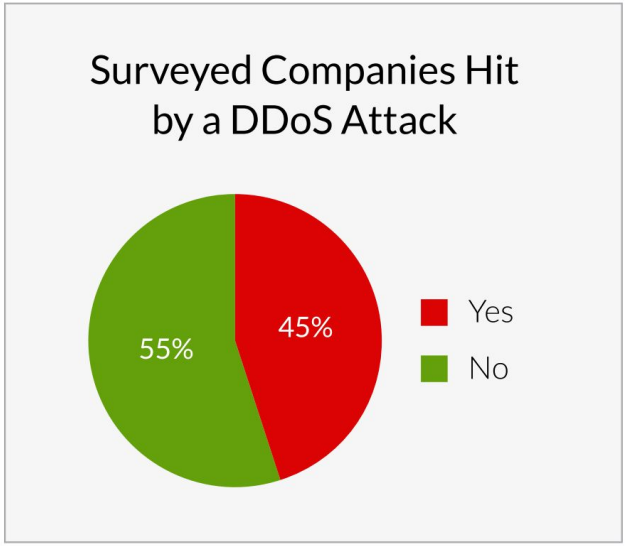
Bildquelle: [10]

Gliederung

1. Was ist DDoS-Mitigation?
2. **Ist DDoS-Mitigation sinnvoll?**
3. DDoS-Attacken vorbeugen
4. DDoS-Attacken erkennen
5. DDoS-Attacken abwehren
6. Fazit

Ist DDoS-Mitigation sinnvoll?

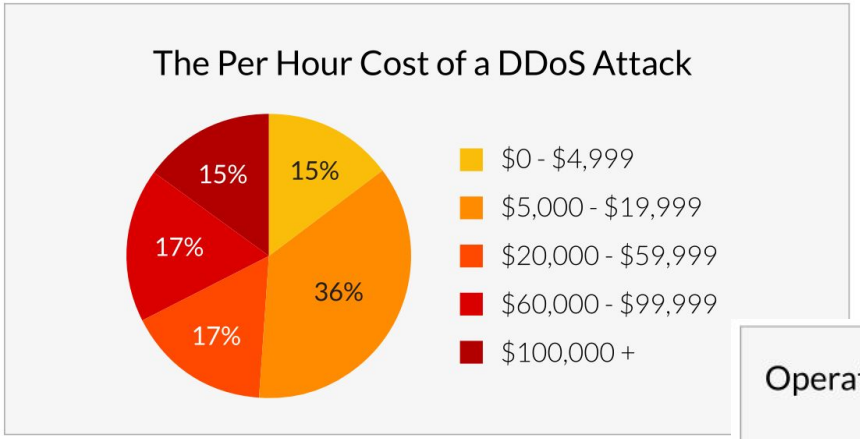
Eine Umfrage mit 270 nordamerikanischen Unternehmen im Jahr 2014 ergab:



- 91 % davon in den letzen 12 Monaten
- 70 % wurden wiederholt angegriffen

Quelle: [4]

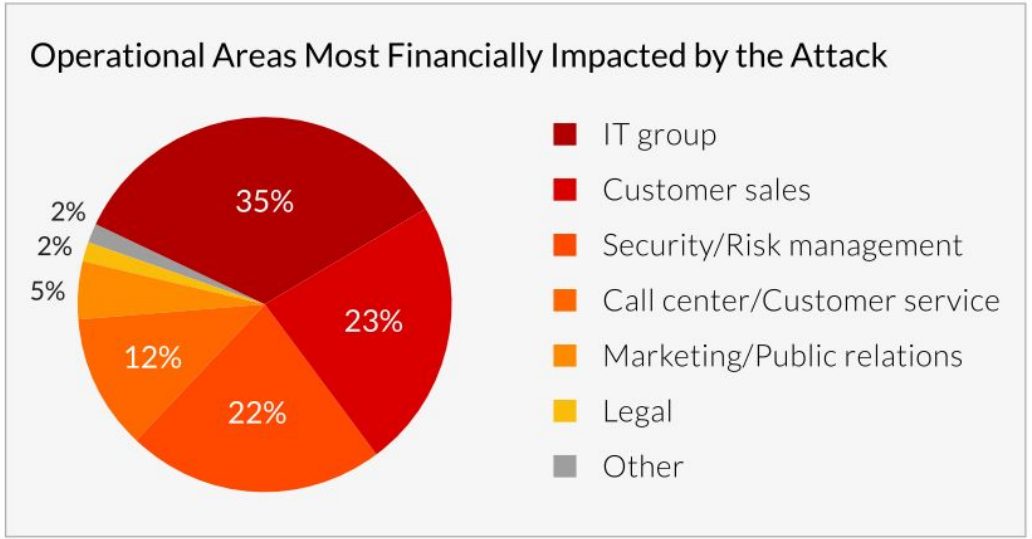
Ist DDoS-Mitigation sinnvoll?



49 % der DDoS-Attacken dauern 6 - 24 h

bei geschätzten Kosten von 40.000 $ pro Stunde kostet eine durchschnittliche DDoS-Attacke

437.000 €



Quelle: [4]

Ist DDoS-Mitigation sinnvoll für ISPs?

- Netzwerkbelastung gering halten
- Folgen bei erfolgreicher Attacke katastrophal

Gliederung

1. Was ist DDoS-Mitigation?
2. Ist DDoS-Mitigation sinnvoll?
3. **DDoS-Attacken vorbeugen**
4. DDoS-Attacken erkennen
5. DDoS-Attacken abwehren
6. Fazit

DDoS-Attacken vorbeugen

durch frühes Verwerfen von Paketen mit gefälschten Quelladressen.

- keinen Traffic reinlassen, der angeblich von innerhalb kommt
- keinen Traffic rauslassen, der angeblich von außerhalb kommt
- Möglichkeiten zum Erkennen gefälschter Absenderadressen von außerhalb sind für ISPs leider begrenzt

Quelle: [7]

Gliederung

1. Was ist DDoS-Mitigation?
2. Ist DDoS-Mitigation sinnvoll?
3. DDoS-Attacken vorbeugen
4. **DDoS-Attacken erkennen**
5. DDoS-Attacken abwehren
6. Fazit

DDoS-Attacken erkennen

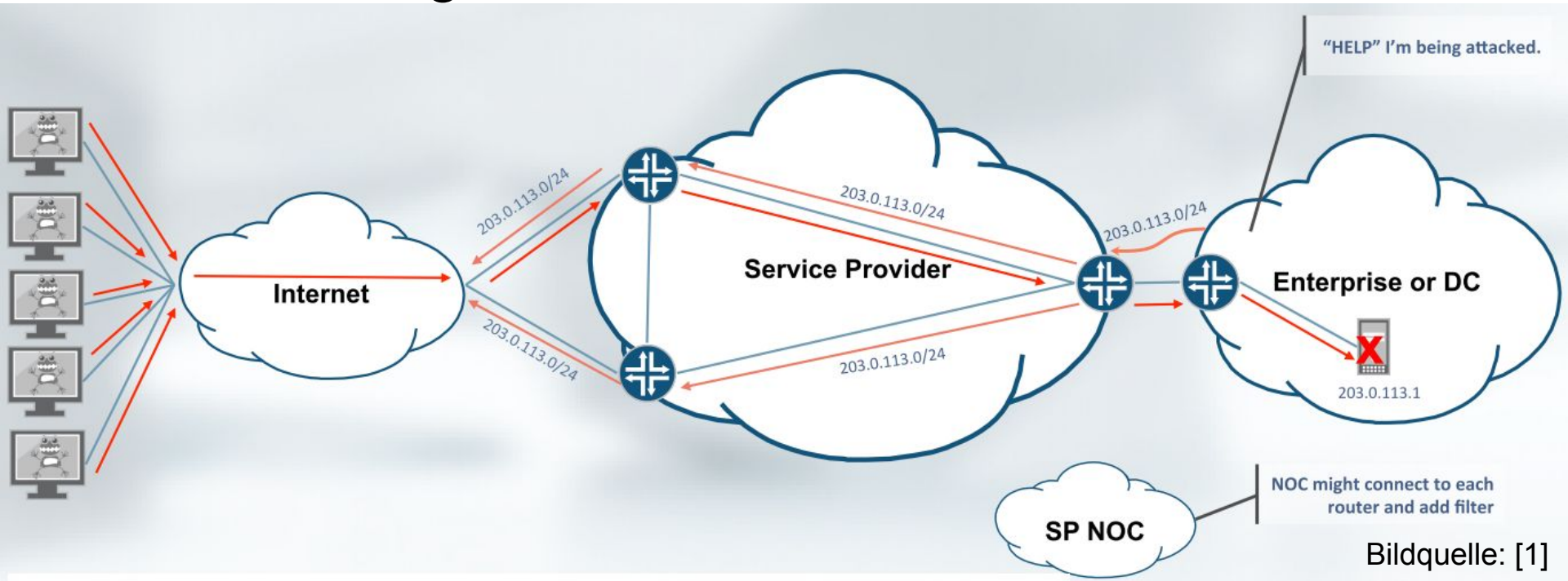
- signaturbasiert
- verhaltensbasiert
  - Menge ein- und ausgehenden Verkehrs vergleichen
  - Statistiken zu Datenflüssen
  - Überwachen der Datenflüsse den eine Verbindung verursacht

Quelle: [10]

Gliederung

1. Was ist DDoS-Mitigation?
2. Ist DDoS-Mitigation sinnvoll?
3. DDoS-Attacken vorbeugen
4. DDoS-Attacken erkennen
5. **DDoS-Attacken abwehren**
    a. **manuelle Mitigation**
    b. Destination Remotely Triggered Blackhole (D/RTBH)
    c. Source Remotely Triggered Blackhole (S/RTBH)
    d. BGP Flow Specification
    e. DDoS-Mitigation mit BGP Flowspec
    f. DDoS-Mitigation mit BGP Flowspec und Scrubbing Center
6. Fazit

manuelle Mitigation



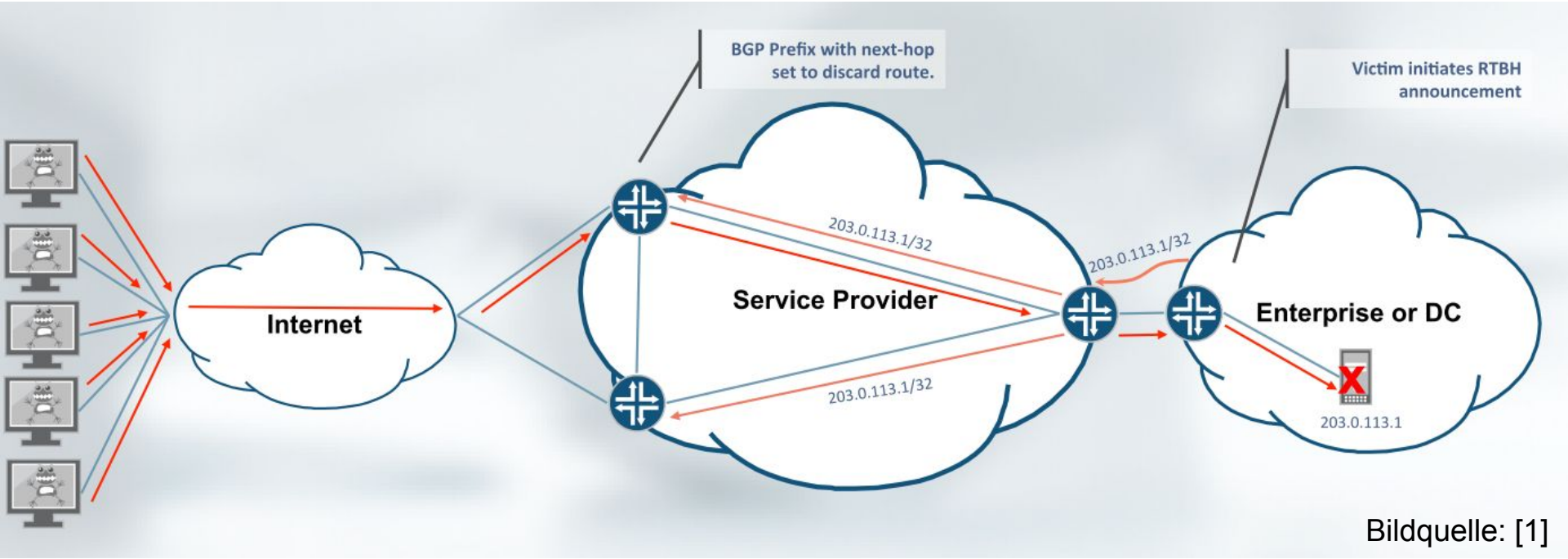
Bildquelle: [1]

- manuell
- langsam
- Gefahr der Fehlkonfiguration

Gliederung

1. Was ist DDoS-Mitigation?
2. Ist DDoS-Mitigation sinnvoll?
3. DDoS-Attacken vorbeugen
4. DDoS-Attacken erkennen
5. **DDoS-Attacken abwehren**
    a. manuelle Mitigation
    b. Destination Remotely Triggered Blackhole (D/RTBH)
    c. Source Remotely Triggered Blackhole (S/RTBH)
    d. BGP Flow Specification
    e. DDoS-Mitigation mit BGP Flowspec
    f. DDoS-Mitigation mit BGP Flowspec und Scrubbing Center
6. Fazit

Destination Remotely Triggered Blackhole (D/RTBH)



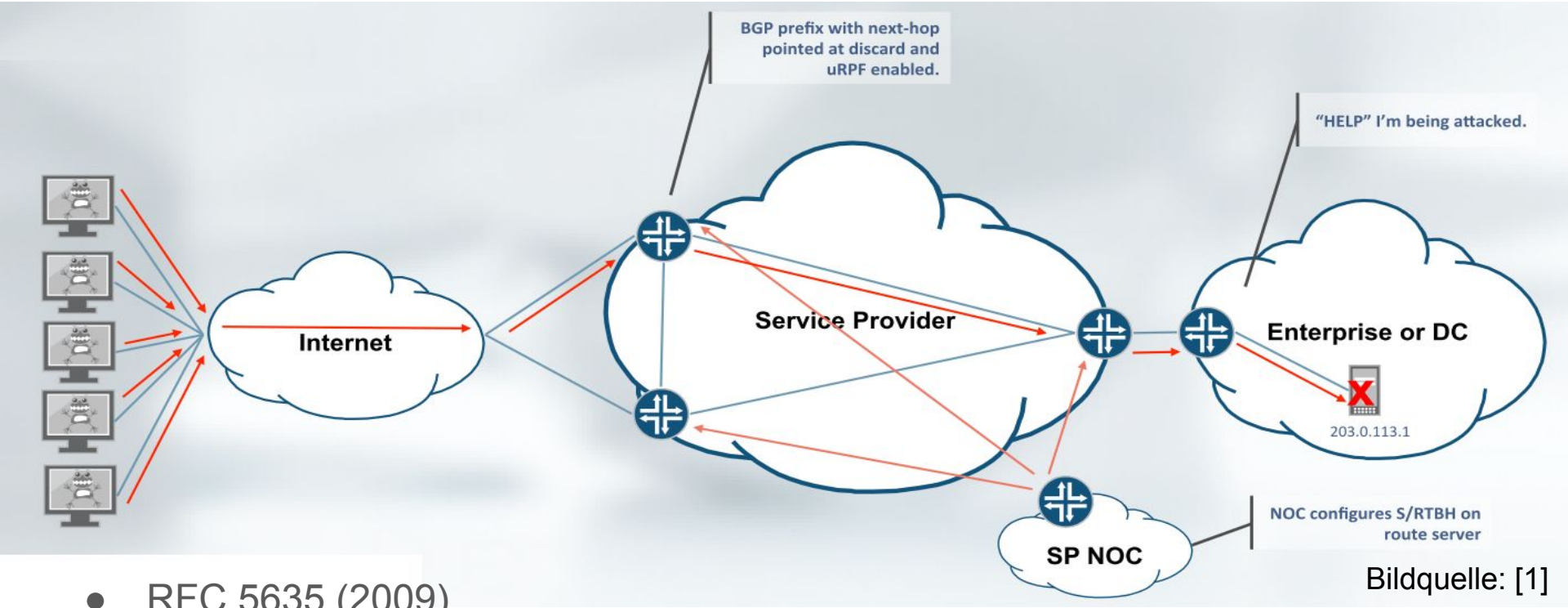
Bildquelle: [1]

- RFC 3882 (2004)
- Ziel ist nicht mehr erreichbar

Gliederung

1. Was ist DDoS-Mitigation?
2. Ist DDoS-Mitigation sinnvoll?
3. DDoS-Attacken vorbeugen
4. DDoS-Attacken erkennen
5. **DDoS-Attacken abwehren**
    a. manuelle Mitigation
    b. Destination Remotely Triggered Blackhole (D/RTBH)
    c. Source Remotely Triggered Blackhole (S/RTBH)
    d. BGP Flow Specification
    e. DDoS-Mitigation mit BGP Flowspec
    f. DDoS-Mitigation mit BGP Flowspec und Scrubbing Center
6. Fazit

Source Remotely Triggered Blackhole (S/RTBH)



Bildquelle: [1]

- RFC 5635 (2009)
- Nur für wenige Quelladressen möglich / Validierungsproblem
- Opfer bleibt erreichbar

Gliederung

1. Was ist DDoS-Mitigation?
2. Ist DDoS-Mitigation sinnvoll?
3. DDoS-Attacken vorbeugen
4. DDoS-Attacken erkennen
5. **DDoS-Attacken abwehren**
    a. manuelle Mitigation
    b. Destination Remotely Triggered Blackhole (D/RTBH)
    c. Source Remotely Triggered Blackhole (S/RTBH)
    d. BGP Flow Specification
    e. DDoS-Mitigation mit BGP Flowspec
    f. DDoS-Mitigation mit BGP Flowspec und Scrubbing Center
6. Fazit

BGP Flow Specification

RFC 5575 (2009)

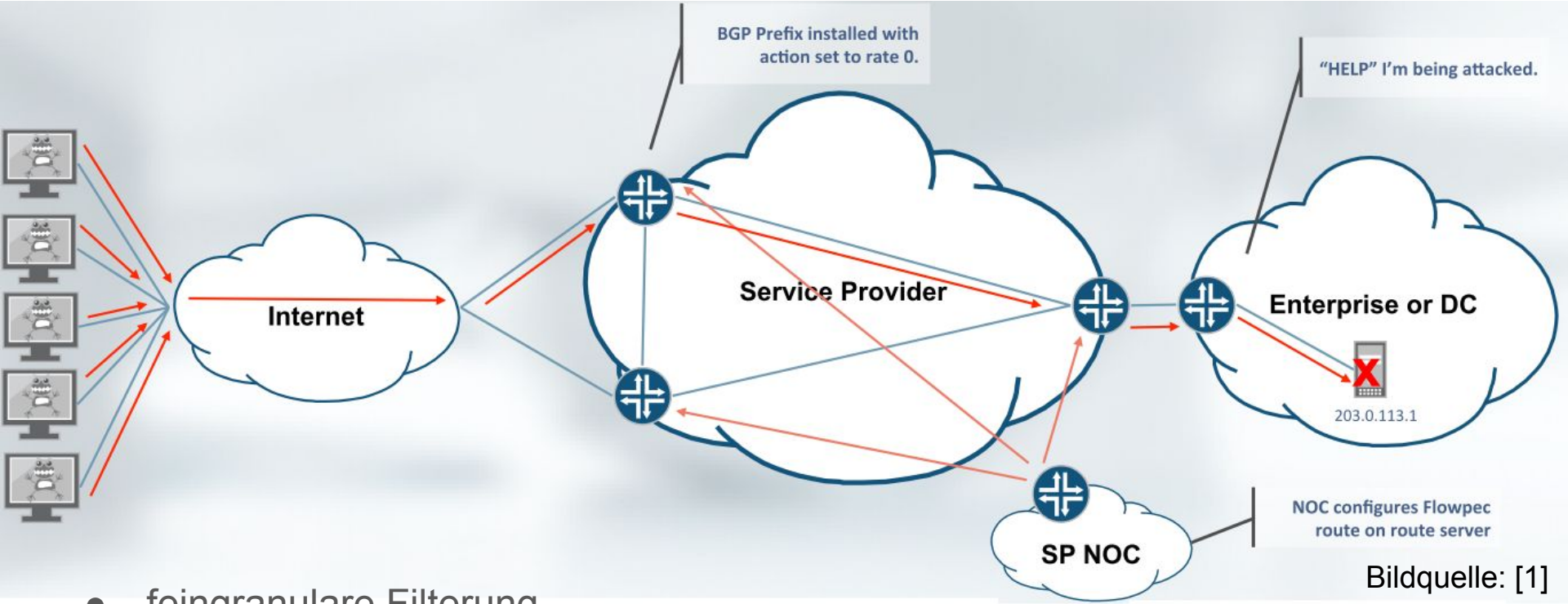
- Feinere Filterung u.a. durch
  - Quell-/ Zielpräfix
  - Quell- und/oder Zielport
  - IP-Protokoll
  - TCP flags
  - Paketlänge
  - Fragmentkodierung

- und entsprechende Aktionen
  - Traffic Rate
  - Sampling & Logging
  - Umleiten

Gliederung

1. Was ist DDoS-Mitigation?
2. Ist DDoS-Mitigation sinnvoll?
3. DDoS-Attacken vorbeugen
4. DDoS-Attacken erkennen
5. **DDoS-Attacken abwehren**
    a. manuelle Mitigation
    b. Destination Remotely Triggered Blackhole (D/RTBH)
    c. Source Remotely Triggered Blackhole (S/RTBH)
    d. BGP Flow Specification
    e. DDoS-Mitigation mit BGP Flowspec
    f. DDoS-Mitigation mit BGP Flowspec und Scrubbing Center
6. Fazit

DDoS-Mitigation mit BGP Flowspec



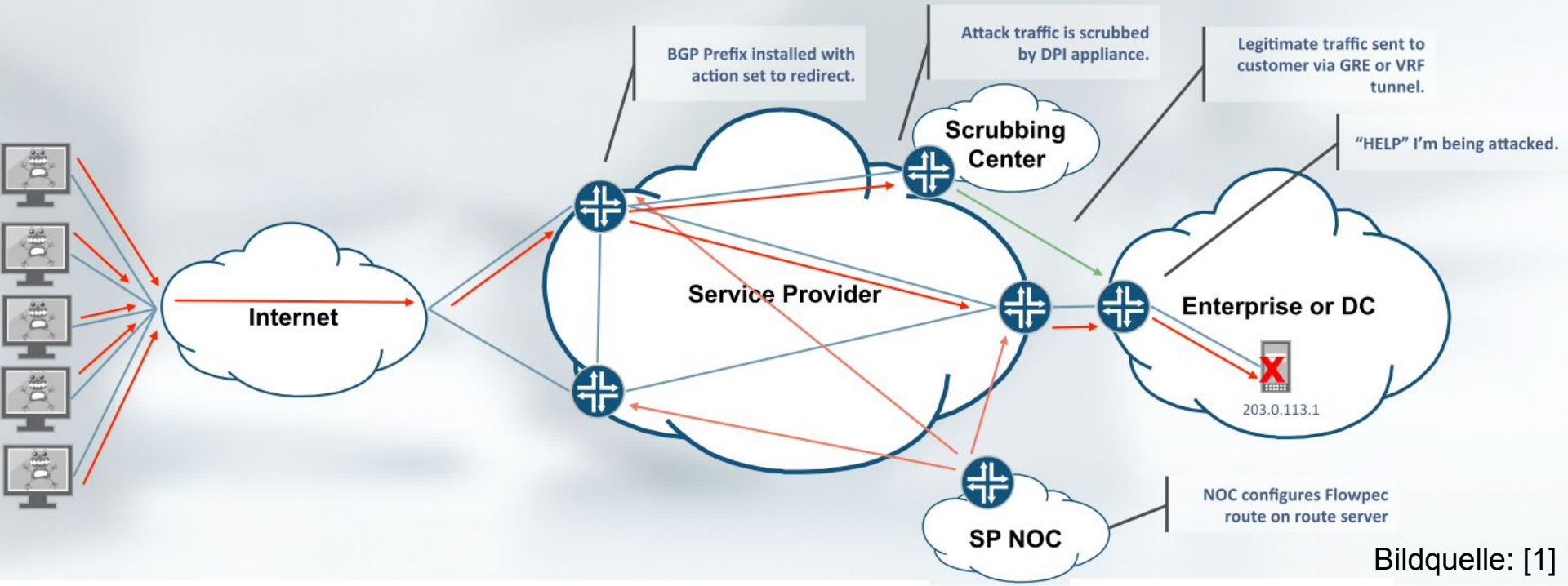
Bildquelle: [1]

- feingranulare Filterung
- noch immer eingeschränkt

Gliederung

1. Was ist DDoS-Mitigation?
2. Ist DDoS-Mitigation sinnvoll?
3. DDoS-Attacken vorbeugen
4. DDoS-Attacken erkennen
5. **DDoS-Attacken abwehren**
    a. manuelle Mitigation
    b. Destination Remotely Triggered Blackhole (D/RTBH)
    c. Source Remotely Triggered Blackhole (S/RTBH)
    d. BGP Flow Specification
    e. DDoS-Mitigation mit BGP Flowspec
    f. DDoS-Mitigation mit BGP Flowspec und Scrubbing Center
6. Fazit

DDoS-Mitigation mit Flowspec und Scrubbing Center



Bildquelle: [1]

- verdächtige Pakete können genauer untersucht werden
- Netzwerkbelastung wird reduziert

Gliederung

1. Was ist DDoS-Mitigation?
2. Ist DDoS-Mitigation sinnvoll?
3. DDoS-Attacken vorbeugen
4. DDoS-Attacken erkennen
5. DDoS-Attacken abwehren
    a. der alte Ansatz
    b. Destination Remotely Triggered Blackhole (D/RTBH)
    c. Source Remotely Triggered Blackhole (S/RTBH)
    d. BGP Flow Specification
    e. DDoS-Mitigation mit BGP Flowspec
    f. DDoS-Mitigation mit BGP Flowspec und Scrubbing Center
6. **Fazit**

Fazit

- Möglichkeiten der Adressvalidierung leider eingeschränkt
- Entwicklung ist laufend im Gange
- Hohe Kosten für Aufbau Infrastruktur
- Leider nötig

Quellen

[1] Ryburn, Justin (Juniper Networks): DDoS Mitigation using BGP Flowspec, NANOG 63 2015, San Antonio, TX, USA
https://www.nanog.org/sites/default/files/tuesday_general_ddos_ryburn_63.16.pdf
https://www.youtube.com/watch?v=ttDUoDf6xzM

[2] Serodio, Leonardo (Alcatel-Lucent): Traffic Diversion Techniques for DDoS Mitigation using BGP Flowspec, NANOG 58 2013, New Orleans, LA, USA
https://www.nanog.org/sites/default/files/wed.general.trafficdiversion.serodio.10.pdf

[3] Kaspersky Lab: Global IT Security Risks Survey 2015
http://media.kaspersky.com/en/business-security/it-security-risks-survey-2015.pdf

[4] Matthews, Tim (Imperva Incapsula): Imperva Incapsula Survey: What DDoS Attacks Really Cost Businesses, 2016
http://lp.incapsula.com/rs/804-TEY-921/images/eBook%20-%20What%20DDoS%20Attacks%20Really%20Cost%20Businesses%20%28new%29.pdf

[5] Raghavan und Dawnson (Hrsg.): An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks, Springer India, 2011

[6] Cisco Systems: Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks, 2008
http://www.cisco.com/c/en/us/support/docs/security-vpn/kerberos/13634-newsflash.pdf

[7] Ferguson et al.: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing, RFC 2827, 2000
https://tools.ietf.org/html/rfc2827

[8] Distler, Dennis: Performing Egress Filtering, 2008
http://www.sans.org/reading-room/whitepapers/firewalls/performing-egress-filtering-32878

[9] Cisco Systems: Unicast Reverse Path FOrwarding Enhancements for the Internet Service Provider - Internet Service Provider Network Edge, 2005
http://www.cisco.com/c/dam/en_us/about/security/intelligence/urpf.pdf

[10] Shameli-Sendi et al.: Taxonomy of Distributed Denial of Service mitigation approaches for cloud computing, Journal of Network and Computer Applications 58, 2015, Seiten 165 - 179

[11] McPherson et al.: Source Address Validation Improvement (SAVI) Threat Scope, RFC 6959, 2013
https://tools.ietf.org/html/rfc6959

[12] Kumari et. al: Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF), RFC 5635, 2009
https://tools.ietf.org/html/rfc5635

[13] Ryba et al.: Amplification and DRDoS Attack Defense - A Survey and New Perspectives, 2016
http://arxiv.org/pdf/1505.07892v2.pdf

[14] King et al.: BLACKHOLE BGP Community for Blackholing, 2015
https://tools.ietf.org/html/draft-ietf-grow-blackholing-00

[15] Baker et al.: Ingress Filtering for Multihomed Networks, RFC 3704, 2004
https://tools.ietf.org/html/rfc3704