Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

IPv6 unter der Lupe

6. IPv6-Kongress, 23.05.2014

Dominique Petersen
petersen@internet-sicherheit.de

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

Agenda

- Motivation
- Kommunikationsformen von IPv6
- Sicherheitsaspekte IPv6 / Tunnel
- Verwendung von IPv6
- Fazit / Ausblick

Motivation

- IPv4-Adressraum bietet kaum noch Möglichkeiten zur Expansion
- Neue Technologien (z.B. Smart-Home) müssen vernetzt werden
- Lösung: IPv6, was nicht (so einfach) abwärtskompatibel ist
- Herausforderung: Umstellung aller netzwerkfähigen Komponenten von IPv4 auf IPv6
  - Enormer Aufwand, gleichzeitiger Umstieg aller Geräte nicht möglich
- Notwendigkeit von Übergangstechnologien für IPv6 über IPv4 (und vice versa)

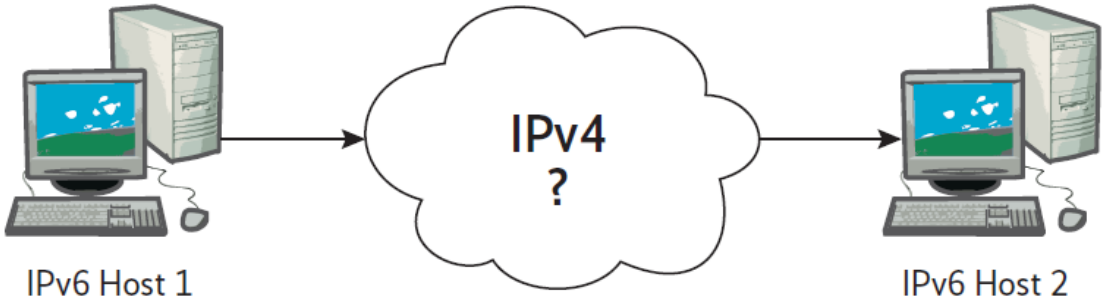
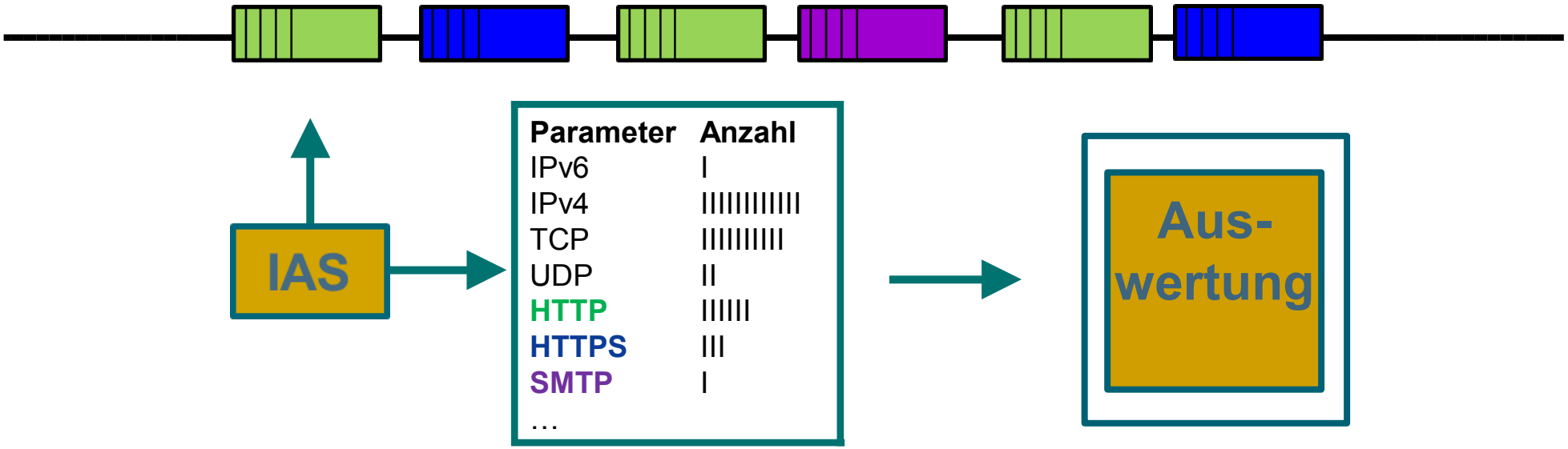


Bild: iX Kompakt IPv6-Leitfaden, Artikel „IPv6 unter der Lupe“

Kommunikationsformen von IPv6
→ Sensor: Internet-Analyse-System (IAS)



- Mehr als **3.000.000 potentielle Kommunikationsmerkmale** helfen, die Kommunikationslage zu **ermitteln, darzustellen und bewerten** zu können.
  - **Verschiedene Informationen in den Kommunikationsmerkmalen** (**Angriffe** (Ports, SYN-ACK, …), **Technologien** (User-Agent, Versionen, …), **Nutzung/Verteilung** (alle), …)
  - Methode ist Datenschutzkonform (**Datenschutz by Design**)

Kommunikationsformen von IPv6
→ Natives IPv6

- „Echtes“ IPv6 ohne Tunneltechnologien direkt in OSI-Ebene 3
  - Serverbetreiber benutzen oft DualStack zur IPv4-Kompatibilität
- Für Betrieb wird oft neue Hardware/Software benötigt, IPv6-DNS („AAAA-Records“) sowie viel Konfigurationsarbeit ausgehend von Servern bis hin zu Routern im Internet
- Viele (vor allem kleine) Unternehmen scheuen noch die (teils hohen) Investitionen
- Privatanwender haben oft IPv6-fähige SW/HW, aber ISP nicht
- Henne-Ei-Problem: Warum soll Unternehmen auf IPv6 umstellen, wenn der Großteil der Kunden praktisch nur IPv4 „spricht“?

Kommunikationsformen von IPv6 → 6in4/6to4/6over4 („6*4“)

- Tunneltechnologien, in der ein komplettes IPv6- in ein neues IP4-Paket verpackt wird (IPv4 protocol id = 41)
  - Macht üblicherweise ein DualStack-Router
  - Verwendet ein Client von sich aus ein Tunnelprotokoll kann ein restriktiver Router Pakete blockieren
- 6in4:
  - IPv6-Adressen müssen im Vorfeld bekannt sein, IPv6-DNS zur Kommunikation benötigt
  - Versand erfolgt dann über die bestehende IPv4-Infrastruktur

Kommunikationsformen von IPv6 → 6in4/6to4/6over4 („6*4“)

- 6over4:
  - IPv6-Adresse (link-lokal): FE80::IPv4_in_hex, Versand über Multicast-IPv4-Netzwerk
  - Nicht oft in Verwendung, da Probleme mit Performanz und Sicherheit
- 6to4:
  - IPv6-Adresse (gültig): 2002:IPv4_in_hex (reserviert ist 2002::/16), Versand normal
  - Ableger „6rd“ (IPv6 Rapid Deployment):
    - Höhere Übertragungsgeschwindigkeit und Sicherheit, da ISP besser blocken kann
    - Nutzung nur für Privatanwender und ISPs praktikabel, da zentrale Vergabe der IPv6-Adressen

Kommunikationsformen von IPv6
→ Teredo

- Tunneltechnologie, in der ein komplettes IPv6-Paket in den Datenteil eines neuen IPv4/UDP-Pakets verpackt wird
- Sinnvoll bei Firewallsystemen, die auf OSI-Ebene 4 nur TCP, UDP und ICMP erlauben
- UDP (Port 3544), da niedrigere Übertragungszeiten, TCP über TCP nicht sinnvoll (Optimierungen von TCP wirken sich negativ aus) sowie keine Echtzeit-orientierten Protokolle möglich (VoIP)
- Teredo eher für Privatanwender geeignet, da ein externer Teredo-Router angesprochen werden muss
  - Ab aktualisiertem Windows XP Standard, IPv6-Verkehr wird dann automatisch über Microsoft-Teredo-Server abgewickelt
  - Pendant für Linux: Miredo

Kommunikationsformen von IPv6 → Weitere

- Es gibt noch viele herstellerspezifische Varianten... (z.B. AICCU/AYIYA)
- Und umgekehrte Wege, also IPv4 über IPv6 zu transportieren
  - 4in6 (Äquivalent zu 6in4)
  - NAT64/DNS64:
    - IPv6-Host fragt bei DNS64-Server nach Adresse, dieser errechnet eine IPv6- aus der eigentlichen IPv4-Adresse
    - Dann versandte IPv6-Pakete werden zwischendurch vom DualStack-Router in echte IPv4-Pakete verpackt
    - Transparent für IPv6-Sender
- Allerdings (bisher) kaum Verwendung von IPv4 über IPv6 im Internet (in internen ISP-Netzen jedoch sehr wohl)

Sicherheitsaspekte IPv6 / Tunnel

- IPv6 ist „junges“ Protokoll (1998...), nicht so viele praktische Erfahrungen wie bei IPv4
- Einige konzeptionelle Schwächen in den letzten Jahren
  - Duplicate Address Detection DoS, Neighbor Discovery MITM (altes ARP-Spoofing / IPv4, ICMPv6 Redirect, Router Advertisement, ...
- Viele Sicherheitssysteme verstehen IPv6 noch nicht so gut wie IPv4
  - Filter sind oft nicht ausgereift genug, alles Negative zu erkennen
  - Tunnelprotokolle werden teilweise gar nicht analysiert und passieren (z.B. doppelte OSI-Ebene 3-Problematik)
- Großes Problem ist Teredo, welches an IPv4-FW-Systemen alles vorbei „schmuggeln“ kann (aufgebaute Verbindung ist stets auch ein Rückkanal!)
  - Windows: Teredo über Microsoft-Server (US-Unternehmen)...

Verwendung von IPv6
→ Allgemein

- if(is) betreibt einige Sensoren bei nationalen und internationalen Unternehmen/Universitäten
- Standort: Übergang Intranet - Internet
- Kleinere ISPs: bspw. 1 IPv6-Paket auf 58 Millionen IPv4-Pakete
- Technologieunternehmen: komplette Unterbindung von IPv6
  - Appell an Hersteller: Sicherheitskomponenten „IPv6-proof“ machen!
- US-Forschungsuniversität:
  2,2% IPv6 (fast nur nativ)

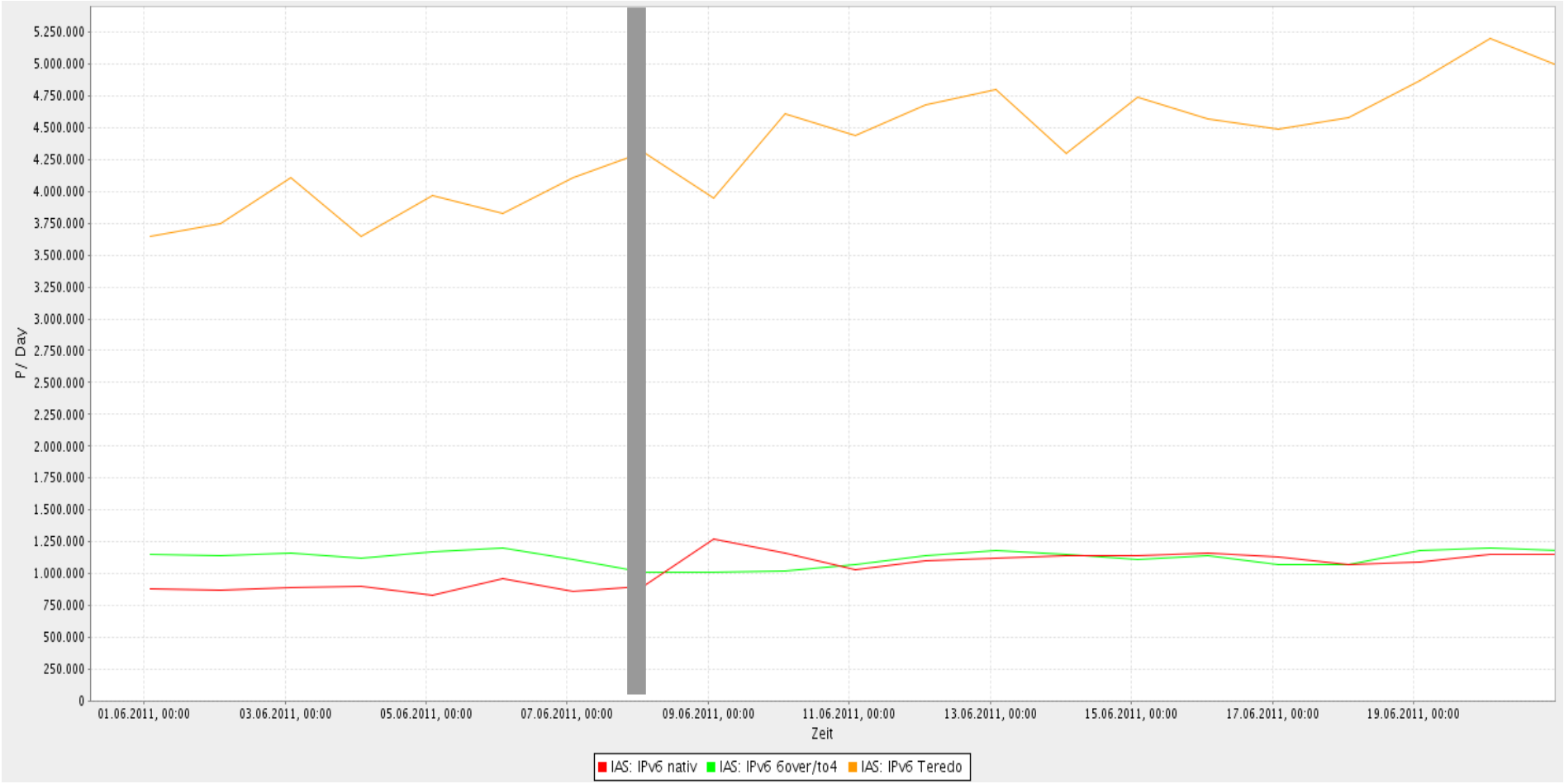
Bild: http://www.clker.com

Verwendung von IPv6
→ Deutscher Austauschknoten (1/6)

- August 2011:
  - IPv4: 99,28% IPv6: 0,72%
    - Nativ: 12,75% 6*4: 21,56% Teredo: 65,69%
  - Hoher Teredo- und geringer nativer IPv6-Anteil (Verkehr geht ins Ausland, wo auch die Teredo-Server stehen)
- IPv6-Tag (08.06.2011):
  - IPv4: 99,14% IPv6: 0,86% (+11%)
    - Nativ: 20,16% 6*4: 16,16% Teredo: 63,68%
  - Client: Weniger Tunneltechnologien, mehr natives IPv6
  - Server: DualStack-Betrieb

Verwendung von IPv6
→ Deutscher Austauschknoten (2/6)

- IPv6-Tag (08.06.2011):



Verwendung von IPv6
→ Deutscher Austauschknoten (3/6)

- Mai 2012:
  - IPv4: 99,03% IPv6: 0,97% (+87%)
    - Nativ: 23,22% 6*4: 22,29% Teredo: 54,49%
- IPv6-Tag (06.06.2012):
  - IPv4: 99,04% IPv6: 0,96% (-3%)
    - Nativ: 26,60% 6*4: 18,86% Teredo: 54,54%
  - Der IPv6-Tag 2012 kam eigentlich schleichend bereits bis Mai
  - Server waren bereits umgestellt
  - Clients haben lieber natives IPv6 benutzt

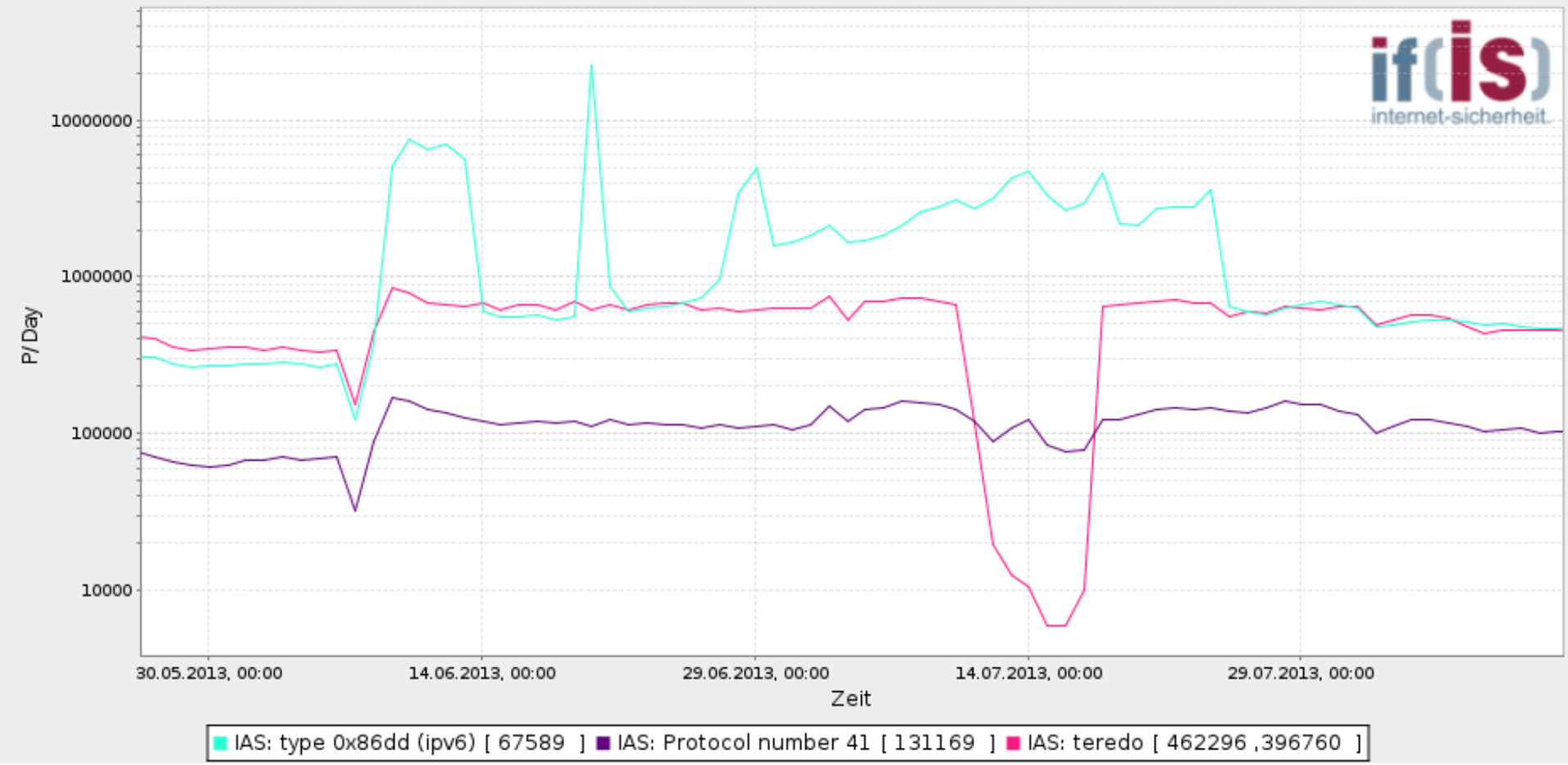
Verwendung von IPv6
→ Deutscher Austauschknoten (4/6)

- März 2013:
  - IPv4: 98,76% IPv6: 1,24%
    - Nativ: 41,13% 6*4: 10,48% Teredo: 48,39%
  - Im Dezember 2012 sankt IPv4 das erste Mal unter 99%
  - Im März 2013 stieg natives IPv6 das erste Mal über 0,5%

- Kein IPv6-Tag 2013 mehr, aber es gibt ja noch den IPv6-Kongress... ;-)

Verwendung von IPv6
→ Deutscher Austauschknoten (5/6)

- Teredo-Ausfall (12. bis 16.07.2013):



Verwendung von IPv6
→ Deutscher Austauschknoten (6/6)

- Teredo-Ausfall (12. bis 16.07.2013):
  - Massiver Einbuch bei Teredo, marginaler Gewinn bei nativem IPv6
  - Microsoft hat später bekannt gegeben, dass sie die eigenen Teredo-Server absichtlich vom Netz genommen hätten, um zu prüfen, wie viele Nutzer Teredo verwenden
  - Drittanbieter von Teredo/Miredo spielen deutschlandweit keine Rolle
- Ende 2013:
  - IPv4: 98,61% IPv6: 1,39%
    - Nativ: 46,68% 6*4: 10,01% Teredo: 43,31%
  - Den Verlust von 6*4 holt sich natives IPv6
  - Teredo stagniert, und vermutlich werden alle Windows-Nutzer so lange diese Technologie nutzen, bis die Internetanschlüsse auf echtes IPv6 umgestellt sind (oder die Server wieder abgestellt werden...)

Fazit / Ausblick

- Für eine flächendeckende Nutzung von IPv6 werden nach heutigen Zahlen noch Jahre vergehen
- Bis dahin werden die IPv6-Tunneltechnologien noch große Verwendung finden

Bild: http://blog.savecall.de

- Serverbetreiber und ISPs müssen auf IPv6 umstellen, das aber im echten DualStack (mit DS-Lite werden nur die Kunden vergrault und damit sinkt die Akzeptanz und der Ruf von IPv6)
- Hersteller von Sicherheitskomponenten müssen mehr in IPv6-Security investieren (und „IPv6-proof“ beweisen)
- Noch gute Chancen für Unternehmen aus Deutschland / der EU, wir müssen sie nur schnell nutzen!

Westfälische Hochschule
Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

IPv6 unter der Lupe

Vielen Dank für Ihre Aufmerksamkeit

Fragen ?

Dominique Petersen
petersen@internet-sicherheit.de

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

if(is) internet-sicherheit.