IP Adressen

Wo, was, warum und wer?

Lutz Donnerhacke

IKS GmbH, Thüringen Netz, ICANN

IKS

2001:4bd8:1:2:203:baff:fe09:6280

IP Adressen

- IP Adressen sind Hausnummern
- Datenverkehr sind Pakete an IP Adressen
- Absender IP für die Rückrichtung nötig
- IP Adressen müssen global eindeutig sein
- IP Adressen kann man nicht verstecken
- *Internet = Eindeutige, sichtbare IP*

IKS

Global eindeutige Adressen

- Koordinierte Vergabe:
  - IETF definiert Adressierungsarten
  - ICANN koordiniert Technik und Politik
  - IANA verteilt Blöcke an Regionen (RIRs)
  - RIR reservieren Adresspools für Provider
  - Provider weisen Kunden Adressbereiche zu
- Jeder Nutzer hat eine Adresse, die ihm persönlich zugewiesen ist.

IKS

Nachverfolgbarkeit

- Von IANA bis Provider durchfragen
  - Strafverfolgung kann das tun
- In Datenbanken nachschauen
  - Provider sind verpflichtet, Whois zu pflegen
  - Whois dient der Fehlersuche beim Betrieb
  - Abfrage der Whois Information öffentlich?
  - Wird es von Rechteverwertern mißbraucht?
  - Gibt es ein Recht, nicht im Whois zu stehen?

IKS

Beispiel Whois

- RIPE Whois zu IP:
  - inet6num: 2001:4bd8:1::/48
    descr: Thueringen-Netz e.V.
    admin-c: RS45-RIPE
    tech-c: LD26
  - person: Lutz Donnerhacke
    address: IKS GmbH
    address: Leutragraben 1
    address: 07743 Jena
    address: Germany
    phone: +49 3641 460861
    fax-no: +49 3641 460855
    e-mail: lutz@iks-jena.de
    nic-hdl: LD26

Datentransport

- Daten werden von Routern transportiert
- Router sind Maschinen: Feste Regeln
- Datenaustausch über Standorte von Ips
- Protokoll BGP (Provider as Punkte: AS)
- Router wissen:
  - 2001:4bd8::/32 kommt von AS15725
  - AS15725 ist IKS GmbH
  - BGP findet Pfade durch Providernetze

IKS

Zuweisung vs. Nutzung

- Nutzung kann durch andere Leute erfolgen als die, auf die die Adressen eingetragen sind
- Mißbräuchliche Nutzung (ohne Wissen des „Eigners“) ist möglich und gängig: Spoofing, BGP Injection
- Genaue Zuordnung ist sehr schwierig und muß zeitnah erfolgen

IKS

Protokollieren

- Technisch kann an jedem Gerät möglich
  - A mit B: Wann? Wieviel? (Netflow)
- Auf jedem Dienst möglich
  - Welche IP hatte wann welche Information?
- Proxydienste verschleiern
  - NAT (Adressumsetzung) verschleiert Quelle
  - Webproxy verschleiert Quelle (oder offenbart)
  - Beide Proxies können mitschreiben
- Datenzusammenführung essentiell!

IKS

Fühlen Sie sich überwacht?

Warum nicht?