Vorratsdatenspeicherung, Inhaltssperren, Internetzensur, ...

Inhalt

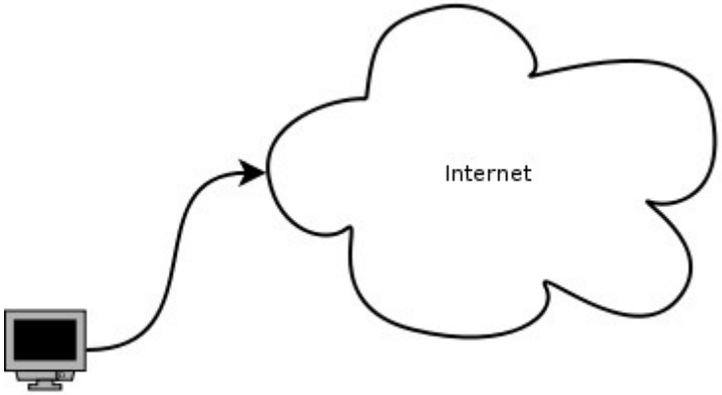
1. Wie funktioniert das Internet?
2. Hackerparagraf
3. Bundestrojaner
4. DNS-Sperren
5. Vorratsdatenspeicherung
6. Zusammnfassung

Disclaimer:

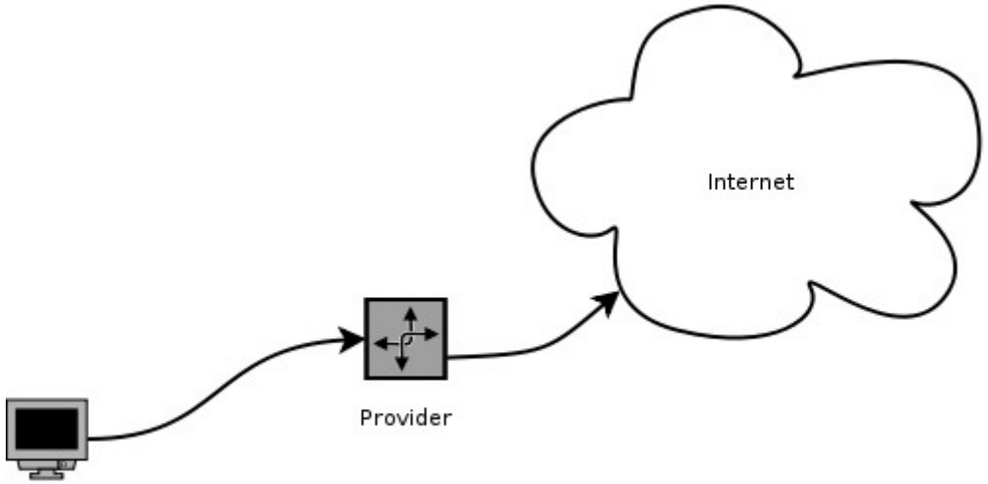
Dieser Vortrag beschäftigt sich mit den Einschränkungen und Überwachungsmöglichkeiten, die sich aus den jeweils angesprochenen Gesetzen und Regelungen heraus ergeben. Darüber hinaus gibt es viele weitere Ansätze zur Überwachung von Kommunikation und Internet, welche aufgrund fehlender rechtlicher Rahmenbedingungen angewendet werden oder wurden.

Daraus folgend kann dieser Vortrag keine Anleitung für absolute Sicherheit bei der Nutzung des Internets sein. Die angesprochenen technischen Konzepte bieten Lösungsansätze für konkrete, definierte Eingriffsszenarien, stellen aber als solche keine allgemeingültige Sicherheitslösung dar.

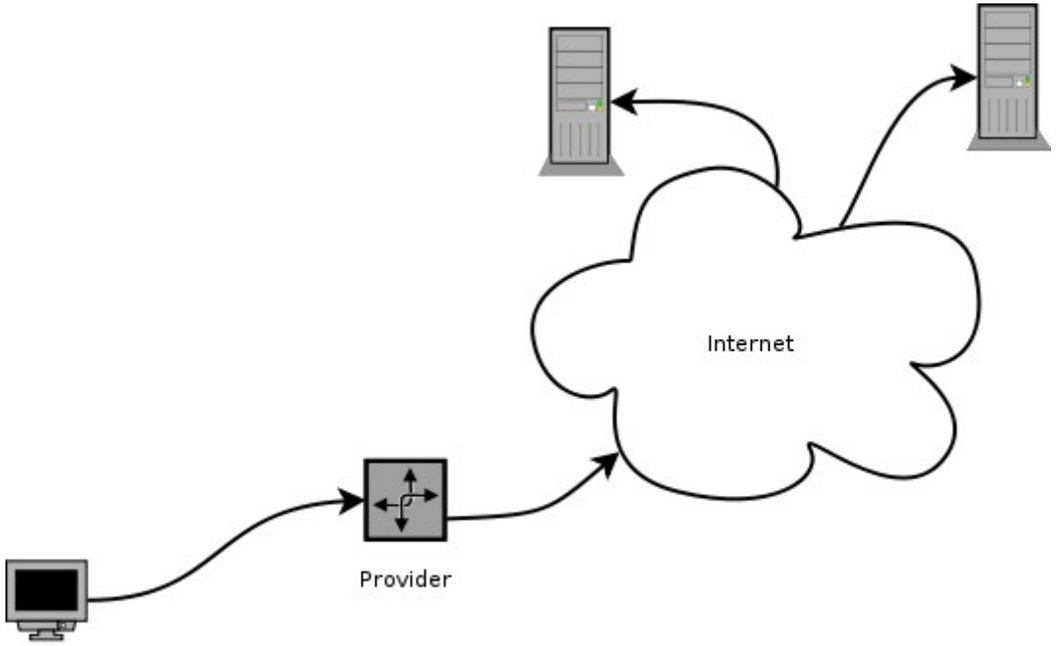
Das Internet


Internet

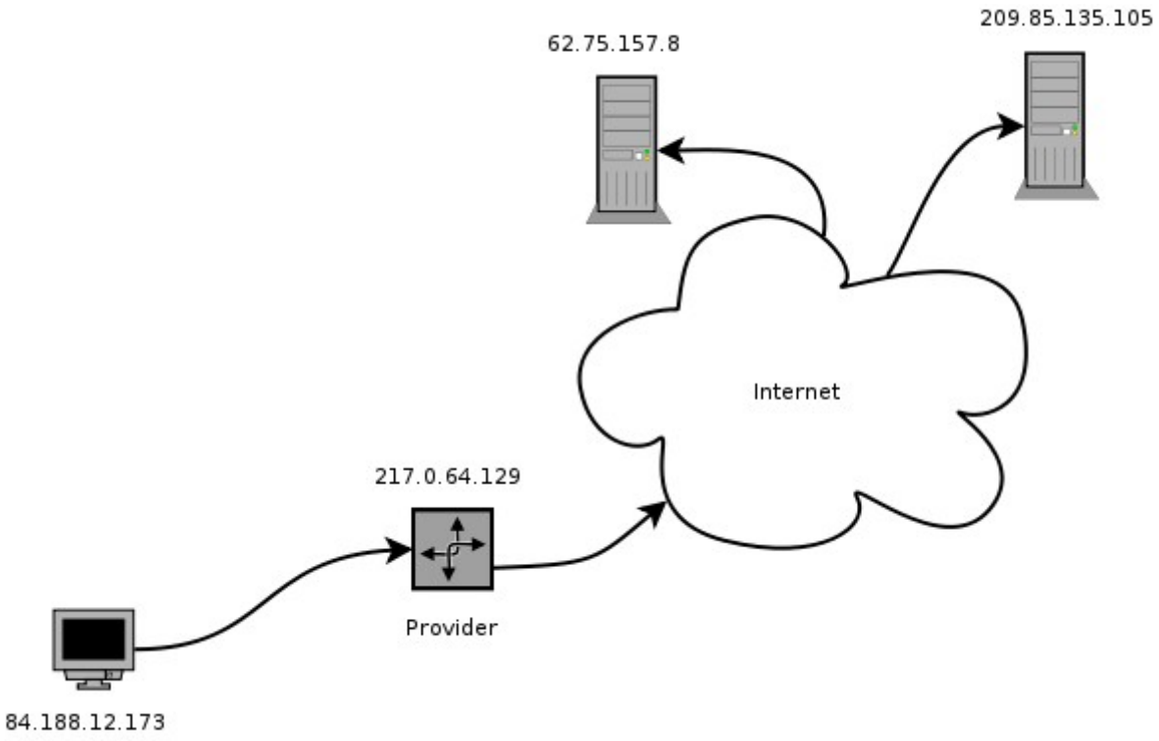
– Provider = Dienstleister für Internetzugang



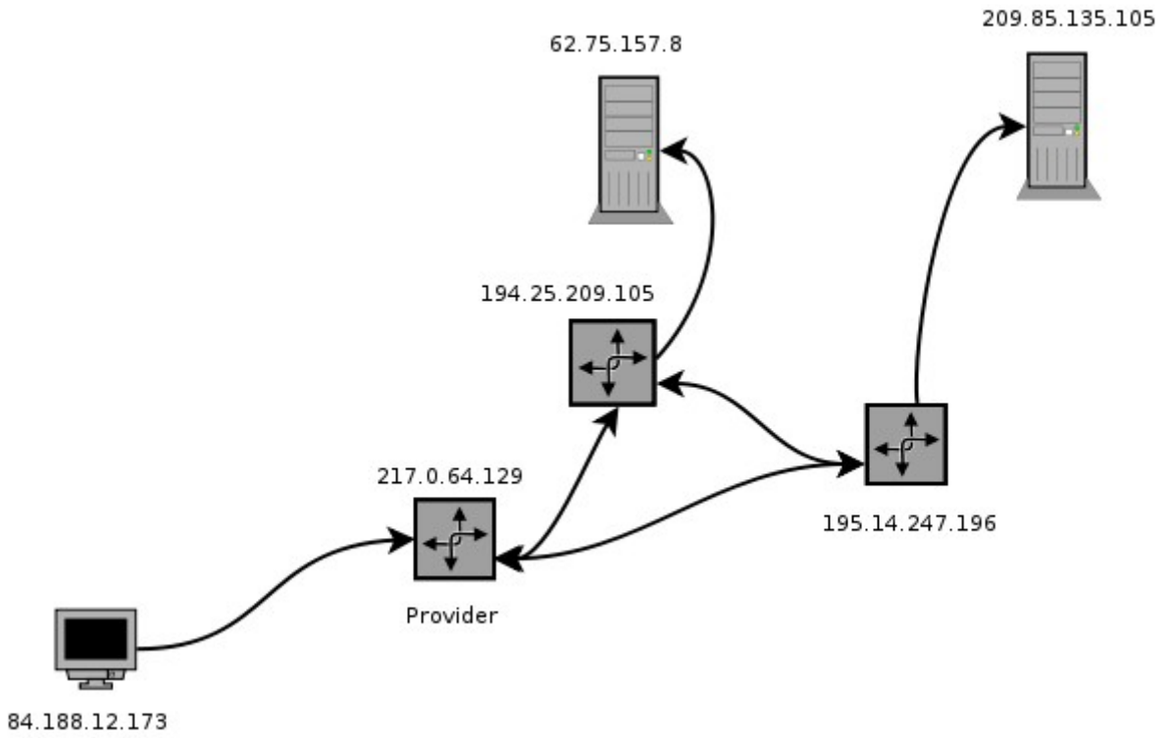
- Server = Computer, welche Dienste im Netz bereitstellen
- Dienst = Websites, Chat, eMail, FTP, VoIP, **DNS**, ...



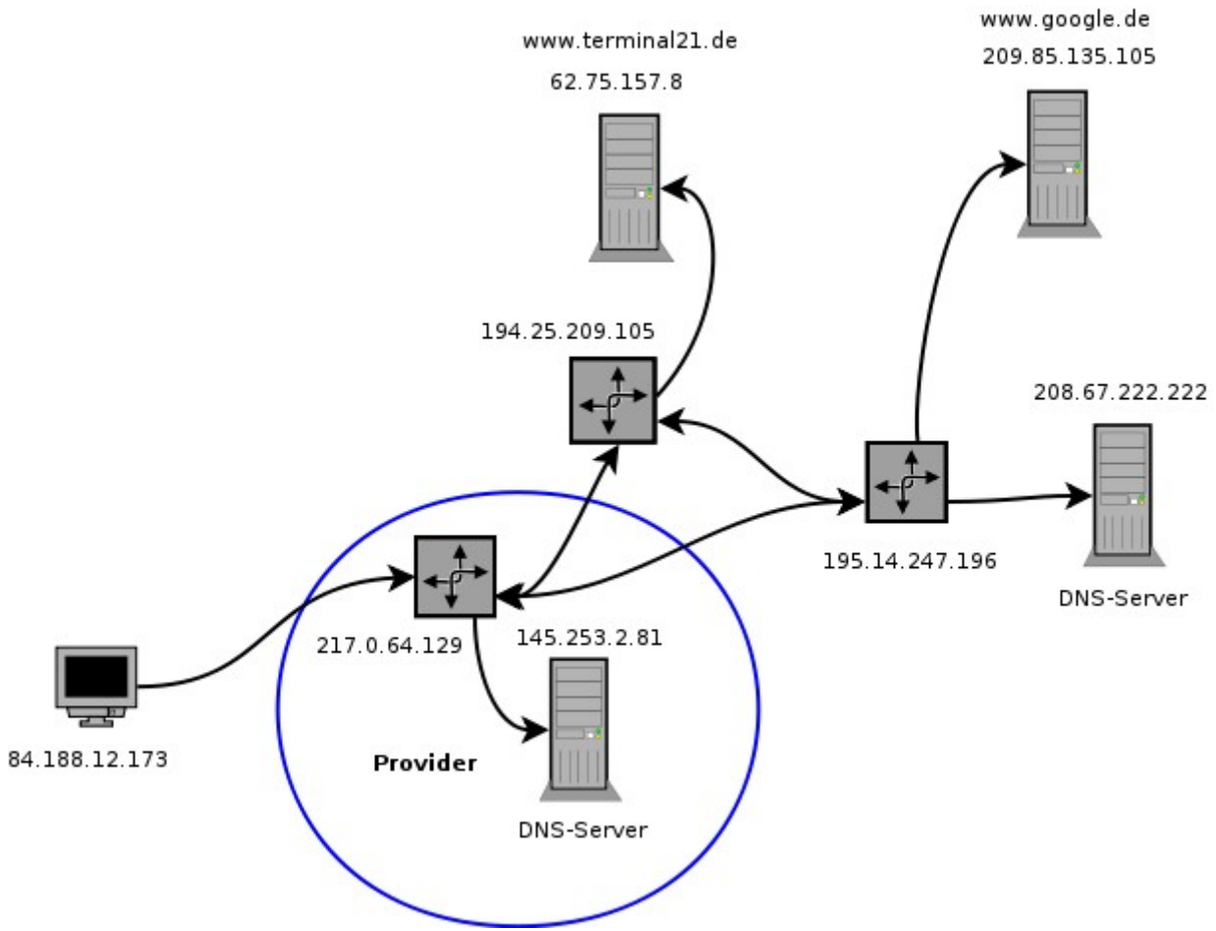
– IP-Adresse = Eindeutige Nummer eines Teilnehmers des Netzes (vgl. Telefonnummer)



- Router = leiten Daten an Zieladresse bzw. andere Router weiter
- Tauschen ständig Daten über Wege (Routen) im Netz aus



– DNS (Domain Name System) = Dienst, der Namen auf IP-Adressen abbildet



Hackerparagraf

Was?

Paragraph 202c StGB

Vorbereiten des Ausspähens und Abfangens von Daten

1. *Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er*
    1. *Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder*
    2. *Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.*

Probleme

- Was ist ein „Hacker"-Programm?
- „dual use"
- Rechtslage für Hersteller von Software + Verlage

Reaktionen: Selbstanzeige / Verfassungsbeschwerde

- Herbert Treinen, dit-consulting GmbH → Einstellung des Verfahrens
- Jürgen Seeger, iX-Cheffrdakteur → Einstellung
- Verfassungsbeschwerde abgelehnt, weil kein Risiko einer Strafverfolgung bei verfassungskonformer Auslegung des Gesetzes

Fazit

- Gerichte unterscheiden zwischen „erlaubter" und „verbotener" Anwendung
- bis jetzt keine Kriminalisierung der Anwender

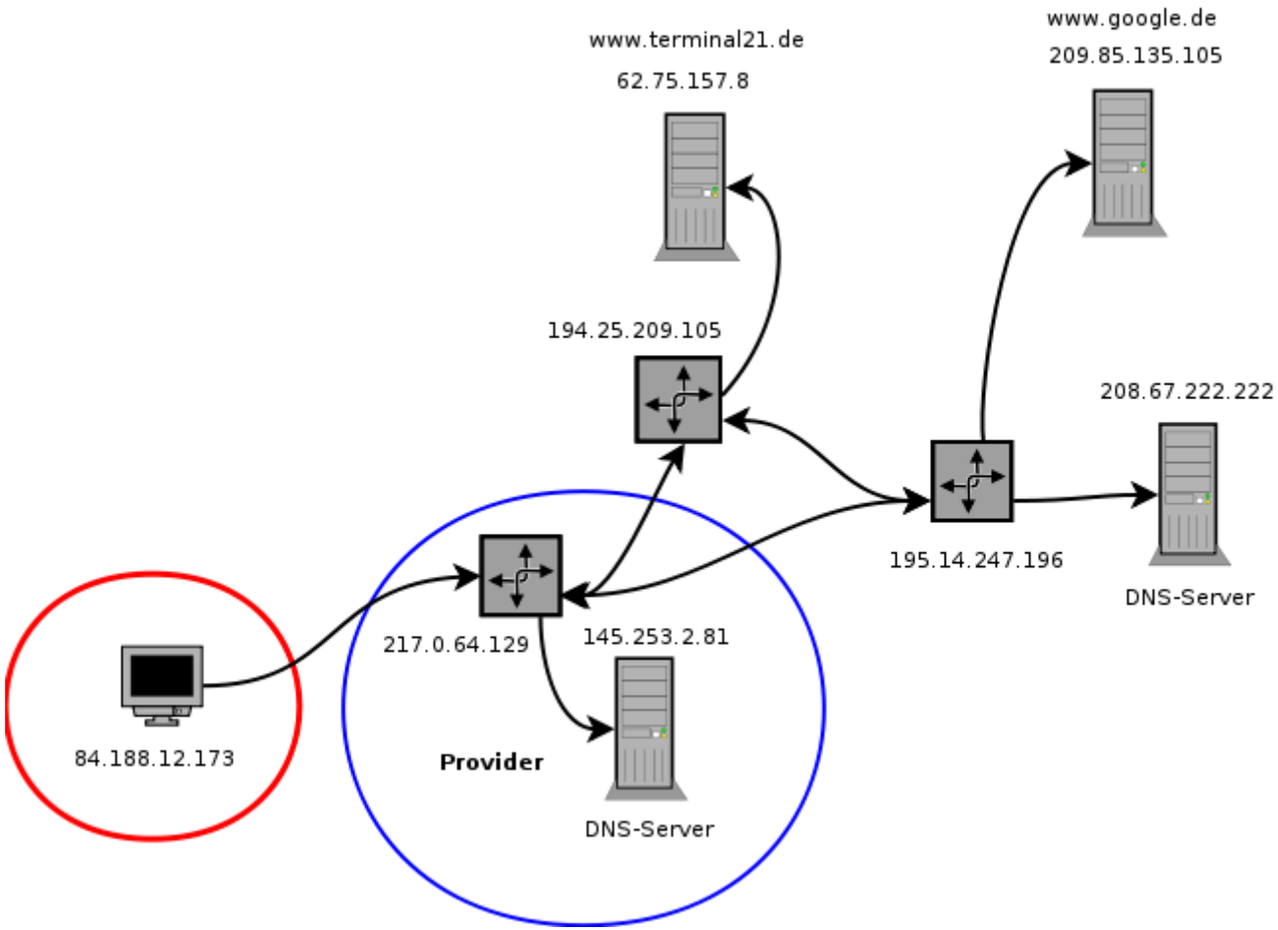
Onlin-Durchsuchung

Bundestrojaner

Was?

- Ziel: Abgreifen von Informationen vor einer Verschlüsselung der Daten
- Programm auf dem Computer von Verdächtigen
  - installiert über Sicherheitslücken aus dem Netz
  - installiert durch heimliches Betreten der Wohnung

Wie?


www.terminal21.de
62.75.157.8
www.google.de
209.85.135.105
194.25.209.105
208.67.222.222
195.14.247.196
DNS-Server
217.0.64.129
145.253.2.81
84.188.12.173
Provider
DNS-Server

Probleme

- heimliches Betreten der Wohnung
- Zugriff über Sicherheitslücken
- Veränderung von Daten auf dem überwachtem Gerät

Was tun?

- Verschlüsselung der Datenträger (bei Zugriff über Wohnung)
- OpenSource-Software / Linux (bei Zugriff übers Internet)
- traue keinem geschlossenem Code
- regelmäßig Updates installieren (= täglich)
- Einsatz einer Firewall, Überwachung der übertragenen Daten
- Advanced: Host Based Intrusion Detection, tripwire

Fazit

- Verfassungsrechtlich umstritten
- OpenSource-Software
- Hürden für Überwachungsversuche einfach zu erhöhen
- Abwehr schwieriger, aber möglich
- kenne deine Technik / Netze

DNS-Sperren

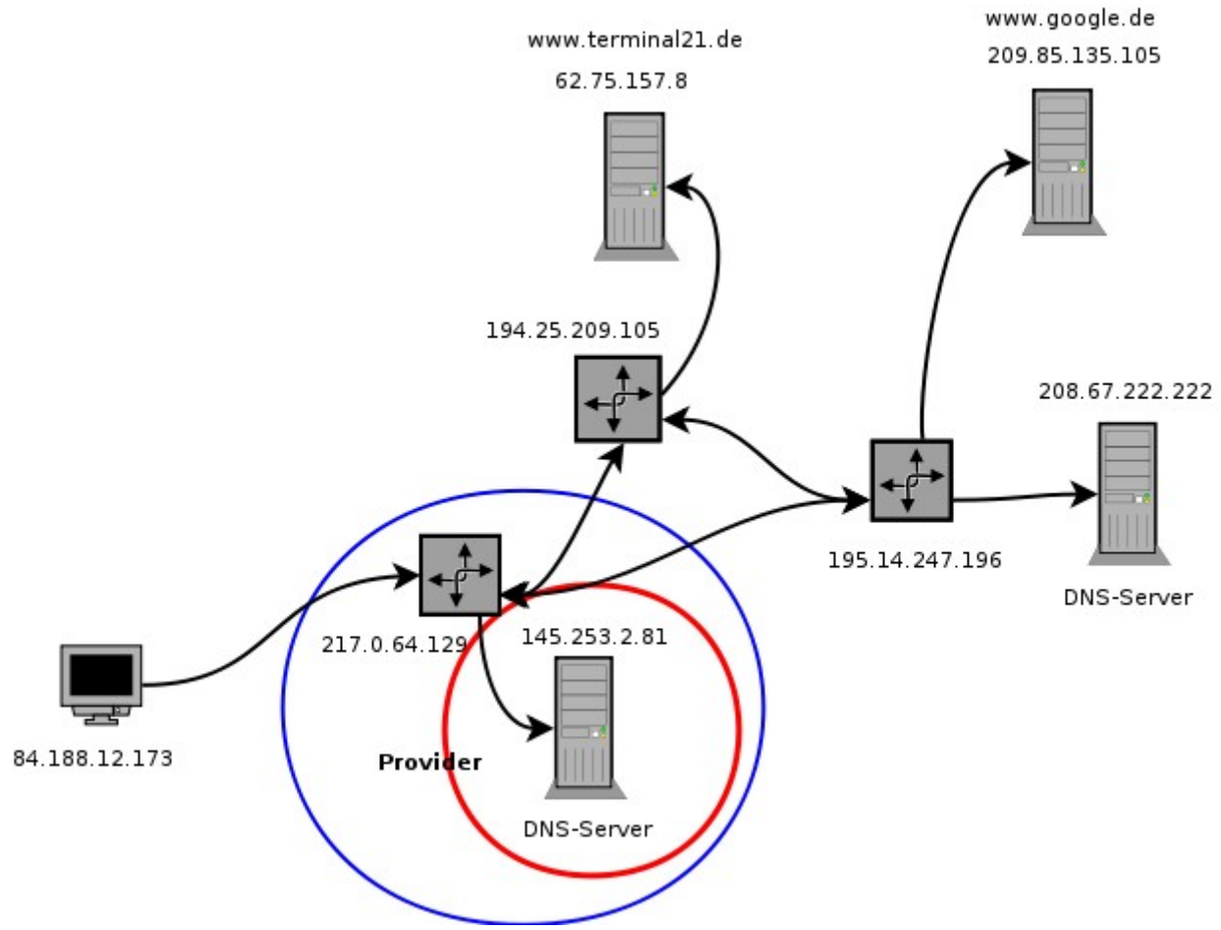
Was?

- Sichtschutz statt löschen
- Umleitung von Zugriffsversuchen auf verbotene Inhalte auf Stoppschild
- Websites
- Analyse der Zieladresse
- Liste vom BKA

Was nicht?

- Usenet, P2P, eMail, Chat, Post, …
- bis jetzt keine Analyse des Inhalts
- bis jetzt keine Umleitung des DNS-Datenverkehrs

Wie?


www.terminal21.de
62.75.157.8
www.google.de
209.85.135.105
194.25.209.105
208.67.222.222
195.14.247.196
DNS-Server
217.0.64.129
145.253.2.81
84.188.12.173
Provider
DNS-Server

Probleme?

- Zensurinfrastruktur
- Aufhebung der Gewaltenteilung (BKA richtet)
- Ausdehnung auf andere Bereiche (Killerspiele, Glücksspiel, Content-Mafia, …, politische unerwünscht)
- Politische Debatte an sich

Was tun?

- bis jetzt: es gibt viele DNS-Server auf dieser Welt
  - 208.67.222.222
  - 208.67.220.220
- später (falls es irgendwann dicker kommt): Verschlüsselte Kommunikation mit DNS-Server

Fazit

- Umgehen von DNS-Sperren trivial
- „Der beste Schutz vor Überwachung ist die Inkompetenz der Überwacher"
- Achtet auf das, was kommt!

Vorratsdatenspeicherung

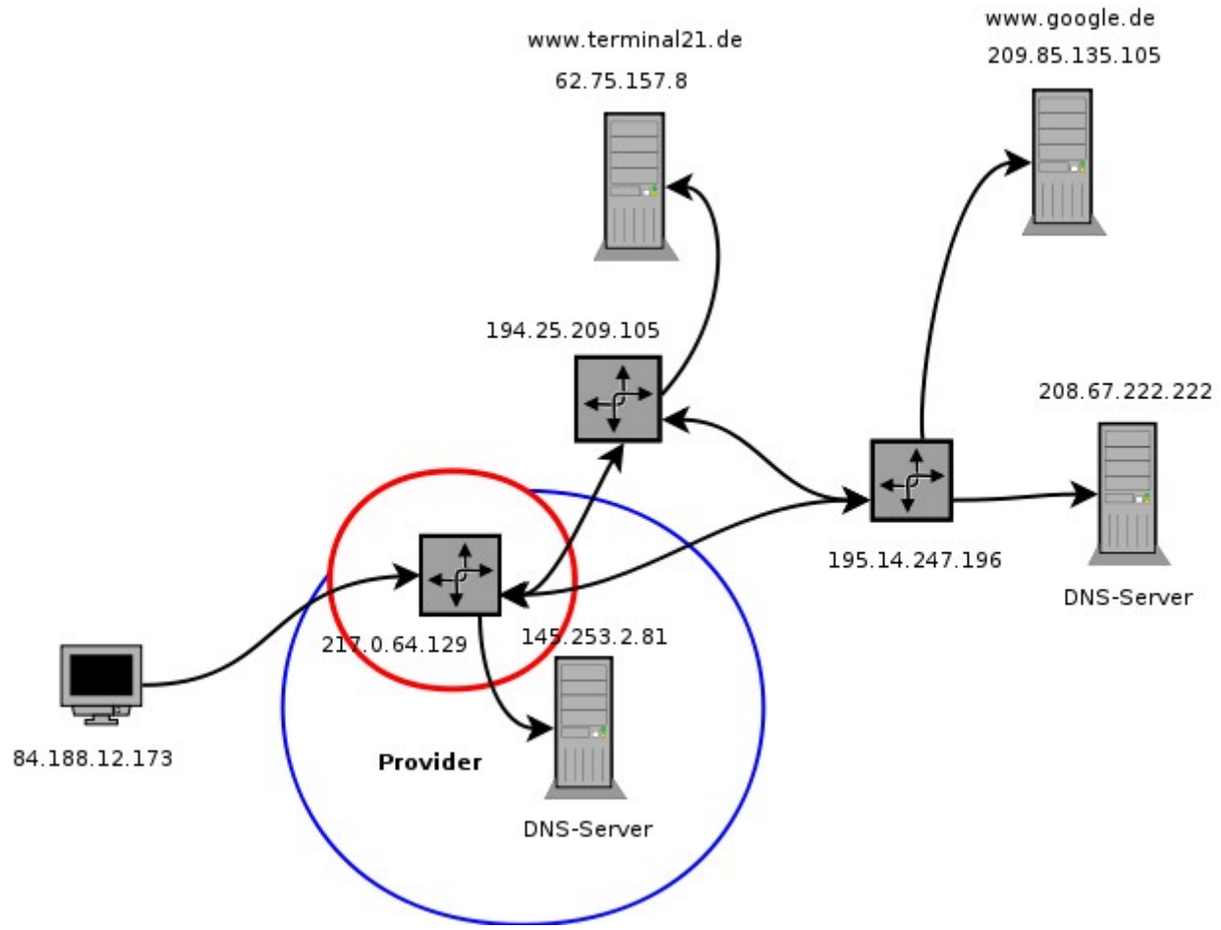
Was?

- Verkehrsdaten jeglicher Telekommunikation für 6 Monate
  - Telefon (auch SMS): Rufnummern der Gesprächsteilnehmer, Anrufzeit, Funkzelle, bei IP-Telefonie IP-Adressen
  - eMail (sowohl beim ansenden, als auch beim Empfang): Absender-IP, eMail-Adressen aller Empfänger, Zeitpunkt des Versands, bei Abholung: Benutzername und IP des Empfängers
  - Internet: an den User vergebene IP-Adresse

Was nicht?

- Inhalt von übertragenen Nachrichten
- Adressen aufgerufener Websites

Wie?


www.terminal21.de
62.75.157.8
www.google.de
209.85.135.105
194.25.209.105
208.67.222.222
195.14.247.196
DNS-Server
217.0.64.129
145.253.2.81
84.188.12.173
Provider
DNS-Server

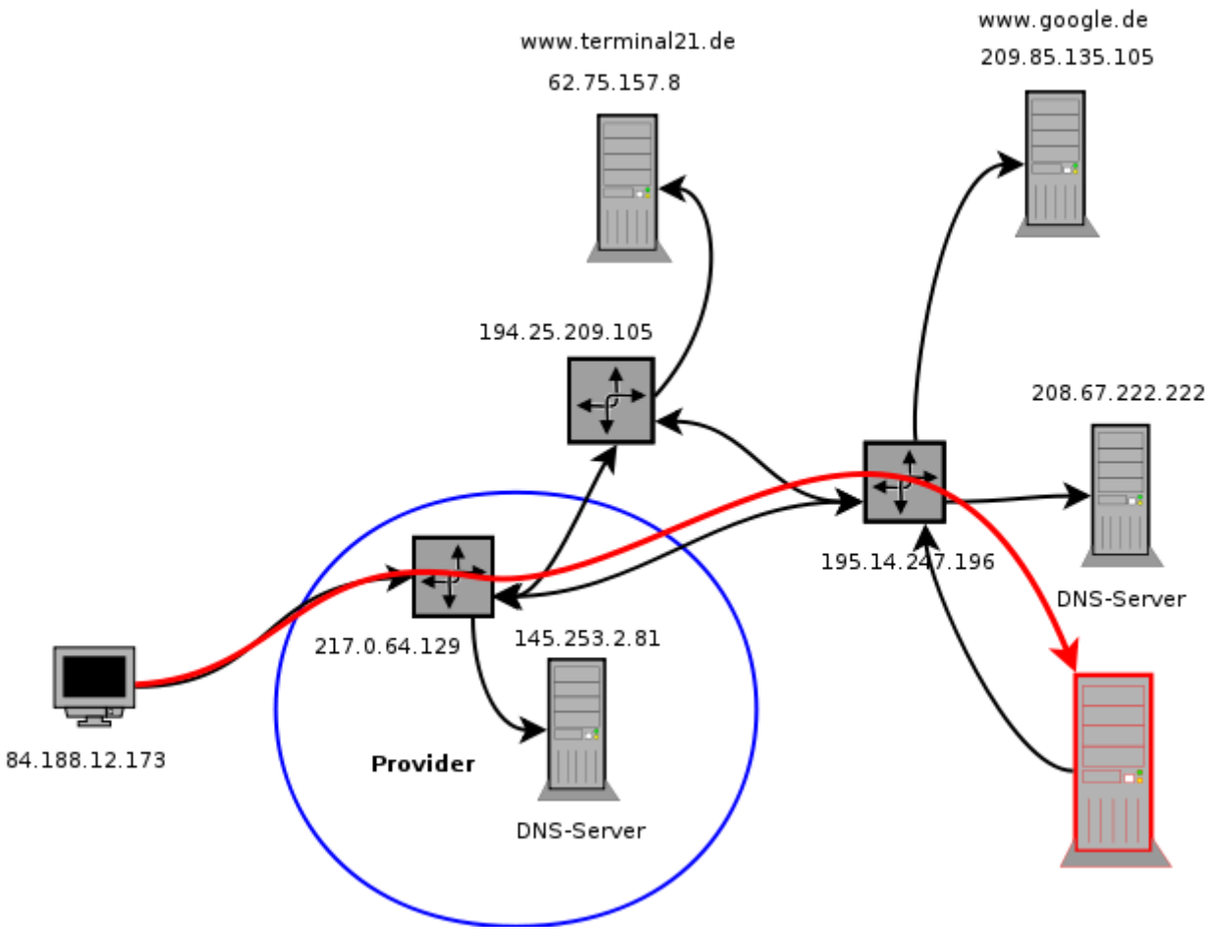
Probleme

- Erhebung ohne Anfangsverdacht
- weitgehende Analyse sozialer Zusammenhänge möglich
- Analyse des Kommunikationsverhaltens

Was tun?

- nicht der Inhalt wird gespeichert, sondern die Kommunikationsteilnehmer → Verschlüsselung einzelner Nachrichten sinnlos
- Lösung: Verschlüsselung des Kommunikationskanals / Kommunikationsnetzes, Anonymisierung
  - Virtual Privat Network
  - Tor
  - Freifunk

VPN-Tunnel


www.terminal21.de
62.75.157.8
www.google.de
209.85.135.105
194.25.209.105
208.67.222.222
195.14.247.196
DNS-Server
217.0.64.129
145.253.2.81
84.188.12.173
Provider
DNS-Server

Fazit

- Verfassungsbeschwerden laufen noch
- Verschlüsselung des Inhaltes hilft nicht
- Umgehung der Vorratsdatenspeicherung möglich, aber nicht trivial

Zusammenfassung

- kümmert euch um eure Computer und hinterfragt die Technik
- ClosedSource-Software will nicht verstanden werden
- viele Überwachungsversuche greifen mit wenig Aufwand ins Leere
- auch komplexere Überwachungsstrukturen haben Lücken
- es gibt immer eine Lösung
- Achtet eure Techies!
- Bildet Banden
- Mehr freie Tech-Crews!

Kontakt

Stefan Walluhn

stefan@terminal21.de

http://www.terminal21.de