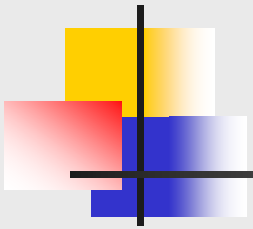
Privatsphäre und Informationsfreiheit: Die Sicherung unserer digitalen Grundrechte

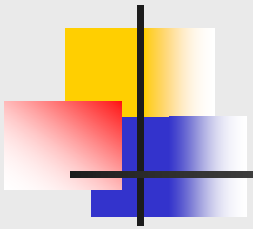
„Wer die Freiheit für Sicherheit aufgibt, wird beides verlieren“

Benjamin Franklin



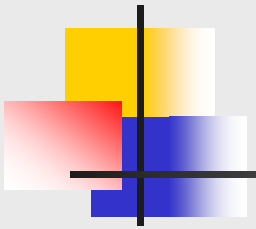
Themenübersicht

- 1 - Bedrohungen für Informationsfreiheit
  - 1.1 The Great (Fire)Wall of China
  - 1.2 Zugangserschwerungsgesetz in Deutschland
  - 1.3 Vorratsdatenspeicherung
  - 1.4 Echelon
  - 1.5 Soziale Netzwerke
- 2 - Technische Grundlagen
  - 2.1 Routing – „Wie findet ein Paket seinen Weg?“
  - 2.2 Unverschlüsselte Protokolle – „Die täglichen Fußabdrücke“



Themenübersicht

- 3 - Technische Schutzmaßnahmen
  - 3.1 Grundlagen
  - 3.2 HTTP Proxy Server
  - 3.3 Anonyme VPN Dienste
  - 3.4 TOR
  - 3.5 Remailer
  - 3.6 Verschlüsselter E-Mail Verkehr mit GnuPG
  - 3.7 Alternative Kommunikationsprotokolle (OTR,XMPP)
  - 3.8 Steganographie
  - 3.9 Temporäre E-Mail Dienste
- 4 – Zusammenfassung & Kontaktmöglichkeit



1 - Bedrohungen für Anonymität und Privatsphäre

- 1.1 Great (Fire)Wall of China
  - „Deep Packet Inspection“
  - Zensur durch:
    - Schlüsselwörter
- 1.2 Zugangserschwerungsgesetz in D.
  - „DNS Redirection“
  - Zensur durch:
    - „Umleiten“ von DNS Anfragen

1 - Bedrohungen für Anonymität und Privatsphäre

- 1.3 Vorratsdatenspeicherung
  - Verdachtsunabhängige Aufzeichnung von
    - Telefonie
      - Wer mit wem wie lange?
      - Art der Kommunikation zB: SMS,MMS?
      - Fehlgeschlagene Anrufe
    - Internet
      - E-Mail – wer mit wem? Zeitpunkt Login/Logout
      - VoIP
  - Mindestfrist: 6 Monate

1 - Bedrohungen für Anonymität und Privatsphäre

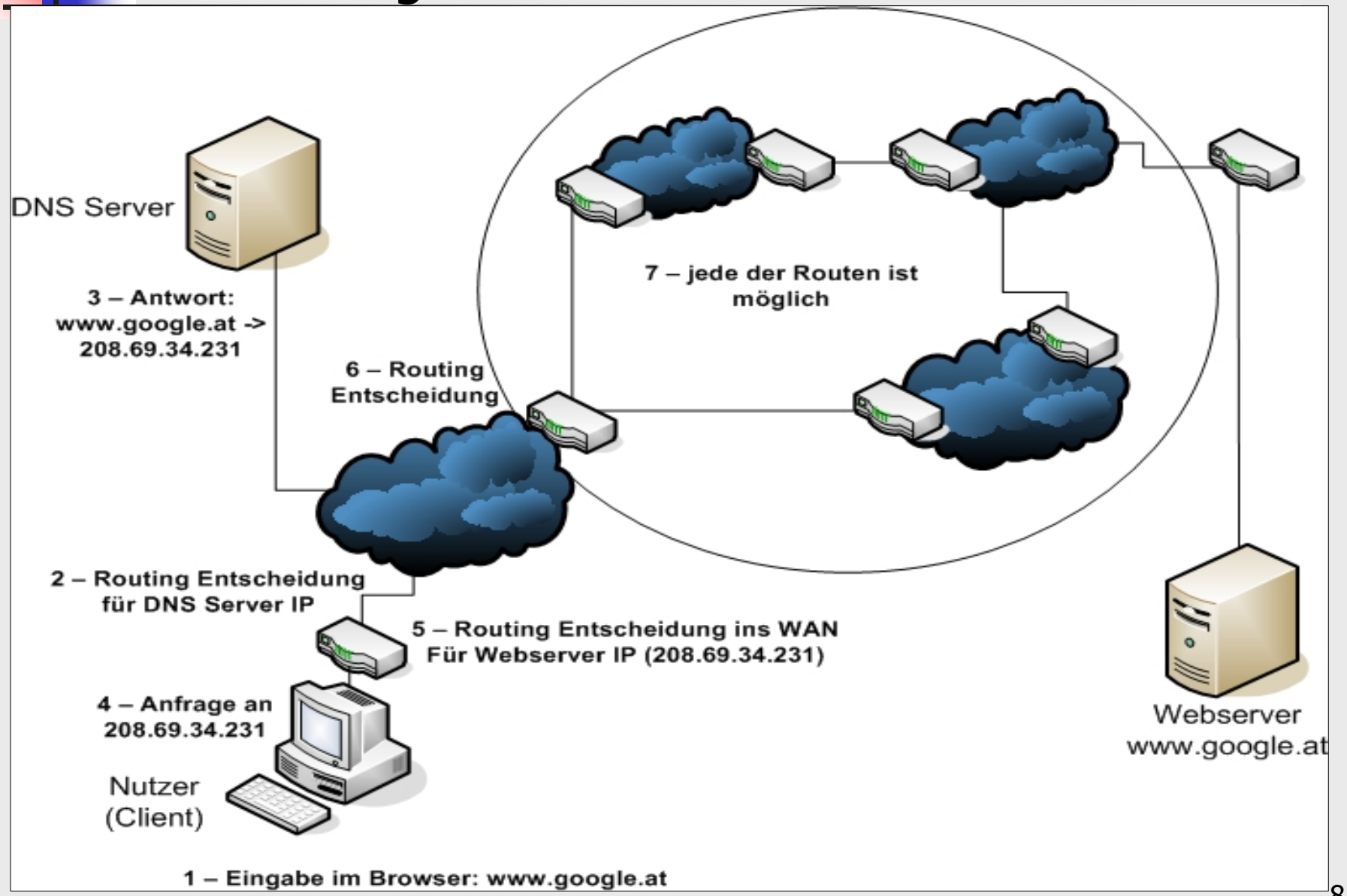
- 1.4 Echelon
  - Überwachung von Satellitenkommunikation
  - „Data-Mining“
  - Industriespionage
  - Analyse von E-Mail Verkehr
    - Schlüsselwörter zB: Terrorist ☺

1 - Bedrohungen für Anonymität und Privatsphäre

- 1.5 Soziale Netzwerke
  - Informationelle Selbstbestimmung
  - Betreiber oftmals Eigentümer der Informationen
  - Unklare Einstellungen für Privatsphäre
  - Scoring für Werbezwecke
  - Digitales „Mobbing“

2 - Technische Grundlagen

2.1 Routing:



2 – Technische Grundlagen

- 2.2 Unverschlüsselte Protokolle – „Die täglichen Fußabdrücke“
  - Browser (Firefox,Internet Explorer usw..):
    - HTTP – Hyper Text Transfer Protocol
    - „Cookies“

```
POST /de/cgi/login HTTP/1.1  Anfrage Browser
Host: service.gmx.net
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.16) Gecko/20080702
SeaMonkey/1.1.11
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9,text/plain;q=0.8,image/
png,*/*;q=0.5
Accept-Language: en-us,en;q=0.5
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-2,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://www.gmx.at/
Content-Type: application/x-www-form-urlencoded
Content-Length: 83
                                                    Benutzername                Passwort
AREA=1&EXT=redirect&EXT2=&uinguserid=&id=testmail%40test.com&p=passwortStrengGeheimHTTP/1.1
```

2 – Technische Grundlagen

- E-Mail Verkehr:
  - SMTP – Simple Mail Transfer Protocol
  - POP3 – Post Office Protocol
  - IMAP – Internet Message Access Protocol

```
MAIL FROM:<christian.czeczil@fh-hagenberg.at> SIZE=481 Sender
250 2.1.0 christian.czeczil@fh-hagenberg.at....Sender OK
RCPT TO:<heavystorm@gmx.li> Empfänger
250 2.1.5 heavystorm@gmx.li
DATA
354 Start mail input; end with <CRLF>.<CRLF>
Message-ID: <49CE3B6F.6010909@fh-hagenberg.at>
Date: Sat, 28 Mar 2009 15:59:59 +0100          Header
From: Christian Czeczil <christian.czeczil@fh-hagenberg.at>
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.8.1.19)
Gecko/20081204 SeaMonkey/1.1.14
MIME-Version: 1.0
To: URNIL FGBEZ <heavystorm@gmx.li>
Subject: Betreff Betreff
X-Enigmail-Version: 0.95.7
OpenPGP: id=4FD066EA
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 7bit

Inhalt einer E-Mail.Inhalt
.
250 2.6.0  <49CE3B6F.6010909@fh-hagenberg.at> Queued mail for delivery
QUIT
221 2.0.0 mail.fh-hagenberg.at Service closing transmission channel
```

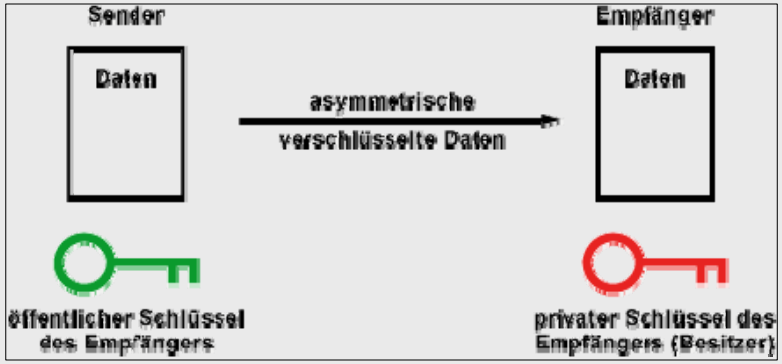
3 - Technische Schutzmaßnahmen

- 3.1 Grundlagen
  - Symmetrische Verschlüsselung (zB: AES)
    - Sender und Empfänger besitzen gemeinsamen Schlüssel

Quelle - Bilder:

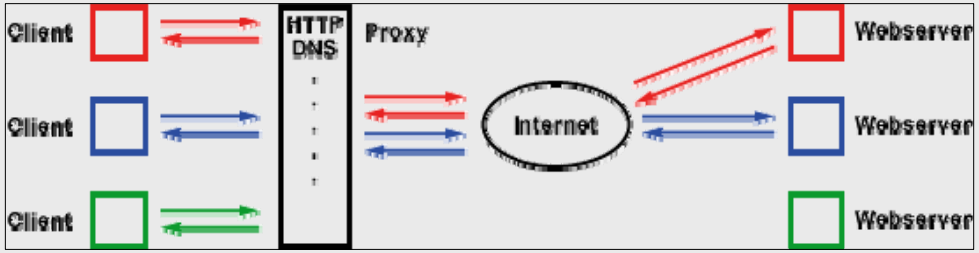
http://www.elektronik-kompendium.de/

  - Asymmetrische Verschlüsselung (zB: RSA)
    - Es existiert je ein Schlüssel zum ver- bzw. entschlüsseln



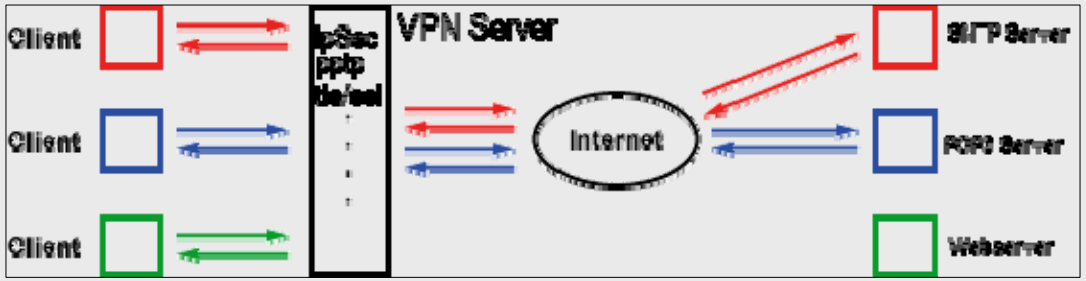
3 - Technische Schutzmaßnahmen

Bildquelle: http://www.elektronik-kompendium.de/sites/net/1101221.htm



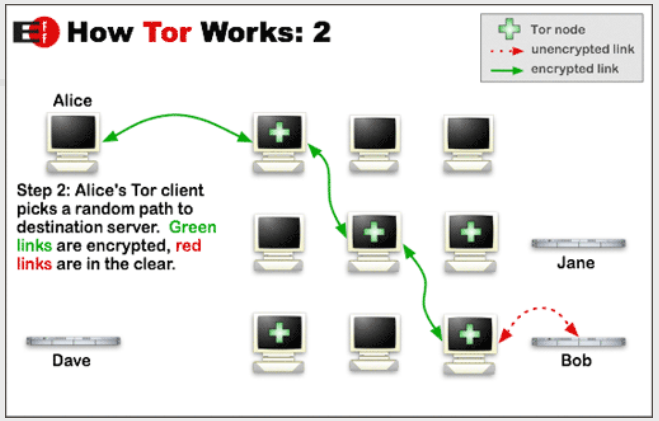
- 3.2 HTTP Proxy Server
  - Proxy Server fungiert als „Mittelsmann“
  - Vorteile:
    - Einfach konfigurierbar
    - „Performant“
  - Nachteile:
    - Unverschlüsselte Kommunikation zum/vom Server
    - Anonymität abhängig vom Serverbetreiber
    - Ausschließlich HTTP wird verarbeitet

3 - Technische Schutzmaßnahmen



- 3.3 VPN Dienste
  - Verschlüsselter „Tunnel“
  - Gesamter Internetverkehr über Virtual Private Network (VPN)
  - <u>Vorteile:</u>
    - Verschlüsselter Kanal bis zum Betreiber
    - „Jeder“ Dienst wird anonymisiert
  - <u>Nachteile:</u>
    - Monatliche Kosten

3 - Technische Schutzmaßnahmen



- 3.4 TOR – „Onion Routing“
  - Netzwerk bestehend aus Knoten
  - Pfad wird zufällig gewählt
  - Asymmetrische wie symmetrische Verschlüsselung
  - <u>Vorteile:</u>
    - Vielzahl von Diensten kann anonymisiert werden (SMTP,POP3,HTTP usw.)
    - Anonyme Dienste können **angeboten** werden für andere Benutzer
    - Frei verfügbar, jeder Benutzer kann partizipieren
  - <u>Nachteile:</u>
    - Performance

3 - Technische Schutzmaßnahmen

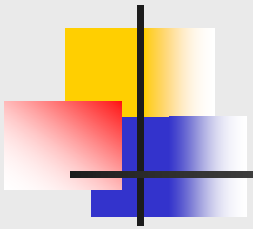
- 3.5 Remailer
  - Historische Bedeutung
  - Server übernimmt Versand der Mail (entfernt Header)
  - Vorteile:
    - E-Mails können anonym versandt werden
  - Nachteile:
    - Implementierung abhängig vom Betreiber
    - Ausschließlich E-Mails
    - Oftmals nur mehr mit Web-Interface

3 - Technische Schutzmaßnahmen

- 3.6 Verschlüsselter E-Mail Verkehr
  - Thunderbird + Enigmail + GnuPG
  - Asymmetrische Verschlüsselung im Einsatz
  - Vorteile:
    - Einfach zu konfigurieren
    - Hohe Vertraulichkeit der E-Mails – Ende zu Ende Verschlüsselung
    - Öffentliche Schlüssel werden auf „Keyservern" verwaltet
  - Nachteile:
    - Erhöhter organisatorischer Aufwand
    - Sicherung von E-Mails
    - Sicherung von privaten Schlüsseln

3 - Technische Schutzmaßnahmen

- 3.7 Alternative Kommunikationsprotokolle
  - XMMP – Jabber
  - OTR – Off the Record
  - IRC + SSL/TLS
  - ICQ + OTR
  - Foren (über HTTPS)
  - SSH – Secure Shell – dynamisches port forwarding
  - Briefe ☺
  - uvm.



3 - Technische Schutzmaßnahmen

- 3.8 Steganographie
  - Informationen in digitalen Bildern verstecken
  - Bits in Bild „kippen“
  - Für menschliches Auge nicht detektierbar
  - Symmetrische wie asymmetrische Verschlüsselung anwendbar

3 - Technische Schutzmaßnahmen

- 3.9 Temporäre E-Mail Adressen
  - Erhalt einer temporären, gültigen E-Mail Adresse zB: asdfasdf@tempinbox.com
  - Kann bei Diensten mit Anmeldung eingesetzt werden

4 – Zusammenfassung & Kontaktmöglichkeit

- Umgehung von Zensur:
  - TOR, Anonyme VPNs, HTTP Proxies ..
- Aufrechterhaltung der Privatsphäre:
  - E-Mail Verschlüsselung, TOR, Remailer, Anonyme VPNs, Steganographie ..
- Exotische Maßnahmen:
  - SSH,Socket,VPN Server in Land außerhalb EU und USA
- Kontaktmöglichkeit:
  - christian.czeczil@gmx.net

Quellen

- Chinesische Firewall:
  - http://www.greatfirewallofchina.org/
  - https://secure.wikimedia.org/wikipedia/en/wiki/Chinese_firewall
  - http://de.wikipedia.org/wiki/Gro%C3%9Fe_Firewall
  - http://www.cl.cam.ac.uk/~rnc1/ignoring.pdf
- Internetzensur in Deutschland - DNS Sperren:
  - http://de.wikipedia.org/wiki/Sperrungen_von_Internetinhalten_in_Deutschland
  - http://www.netzpolitik.org/2009/mit-lego-die-dns-sperren-erklaert/
  - http://www.ccc.de/censorship/dns-howto/
- Facebook privacy issues:
  - http://en.wikipedia.org/wiki/Criticism_of_Facebook#November.2FDecember_2009

Quellen

- Maßnahmen zum Schutz der Privatsphäre:
  - TOR:
    - http://www.torproject.org/index.html.de
    - +FoxyProxy, Torbutton,Firefox - Erweiterungen
  - OTR - Off The record:
    - http://www.cypherpunks.ca/otr/
  - XMPP (Empfehlung Jabber oder Miranda) -Clients :
    - http://xmpp.org/software/clients.shtml
  - JAP:
    - http://anon.inf.tu-dresden.de/
  - Proxy Server:
    - http://www.publicproxyservers.com/
    - http://www.proxy4free.com/
    - http://www.proxyblind.org/
  - GnuPG:
    - http://www.gnupg.org/
    - +Thunderbird - http://www.mozillamessaging.com/en-US/thunderbird/
    - +Enigmail - http://enigmail.mozdev.org/home/index.php

Quellen

- FireGPG - Firefox Plugin:
  - http://getfiregpg.org/s/home
- Vereine:
  - http://www.privacyfoundation.de/ - German Privacy Foundation
- „Anonyme" VPN Dienste:
  - http://www.ipredator.se/
  - https://www.relakks.com/
- Steganographie:
  - http://de.wikipedia.org/wiki/Steganographie
  - +Steghide: http://steghide.sourceforge.net/
- Temporäre E-Mail Adressen:
  - http://www.tempinbox.com/