Vergessensermöglichende und vergessensfördernde Techniken im Internet?

Prof. Dr. Hannes Federrath

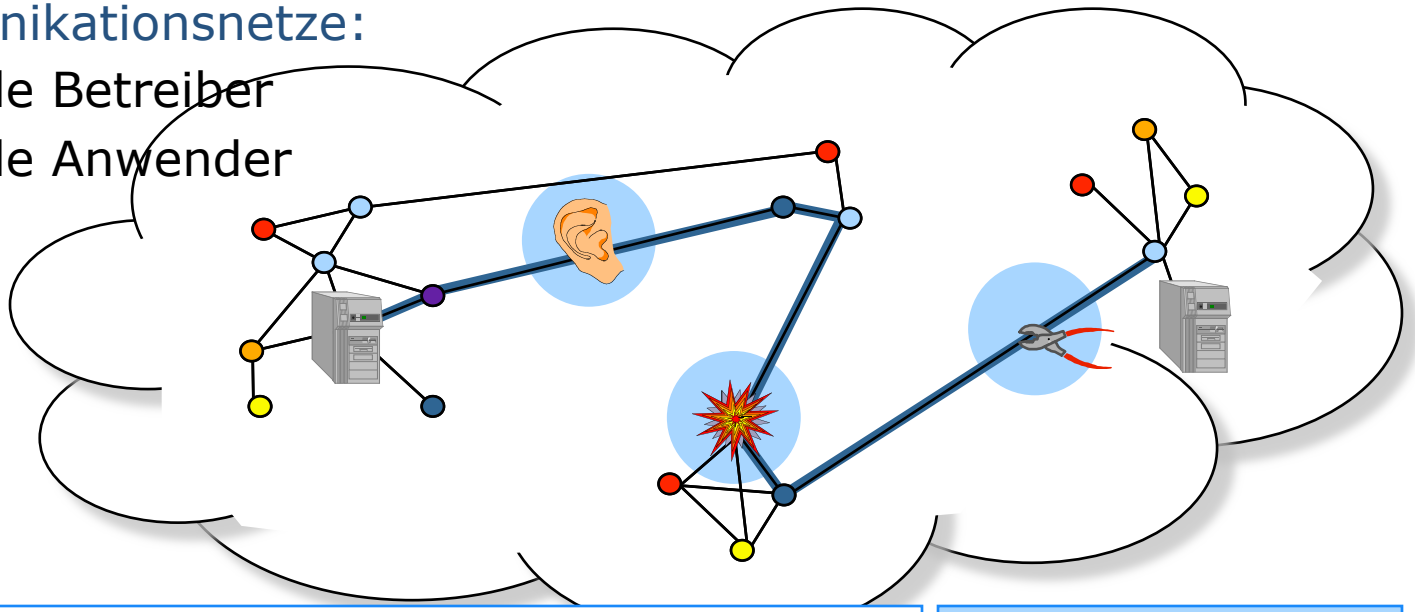
http://svs.informatik.uni-hamburg.de/

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

17. Januar 2014

Sicherheit in Rechnernetzen

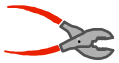
- Telekommunikationsnetze:
  - sehr viele Betreiber
  - sehr viele Anwender



Bedrohungen


unbefugter Informationsgewinn


unbefugte Modifikation


unbefugte Beeinträchtigung der Funktionalität

Schutz der

Vertraulichkeit

Integrität

Verfügbarkeit

Schutzziele mehrseitiger IT-Sicherheit

- Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.

Kommunikationsgegenstand WAS? WORÜBER?	Kommunikationsumstände WANN?, WO?, WER?
Vertraulichkeit Verdecktheit	Anonymität Unbeobachtbarkeit
Integrität	Zurechenbarkeit Rechtsverbindlichkeit
Verfügbarkeit	Erreichbarkeit

Schutzziele mehrseitiger IT-Sicherheit

- Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.

Inhalte der Kommunikation	Kommunikationsumstände
Vertraulichkeit	Anonymität
Verdecktheit	Unbeobachtbarkeit

- Schutzziele — Vertraulichkeit
  - Schutz der Nachrichteninhalte
  - Schutz der Identität eines Nutzers während der Dienstnutzung
    - Beispiel: Beratungsdienste
  - Schutz der Kommunikationsbeziehungen der Nutzer
    - Nutzer kennen möglicherweise gegenseitig ihre Identität

Schutzziele mehrseitiger IT-Sicherheit

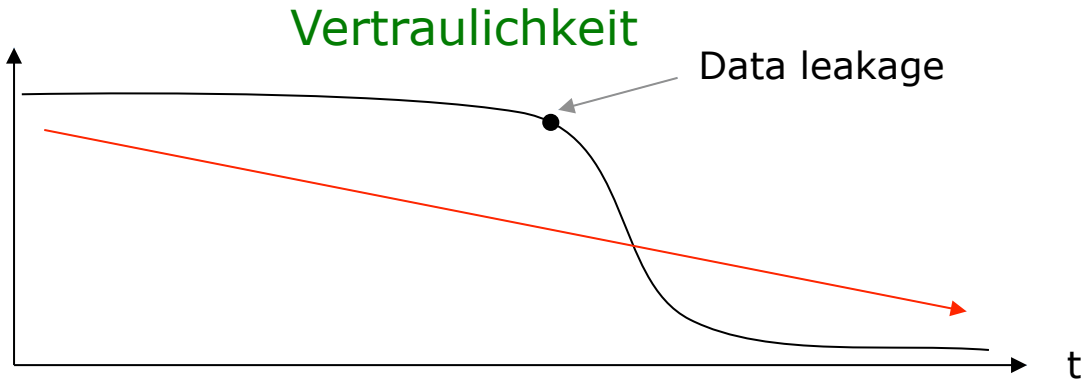
- Mehrseitige Sicherheit bedeutet die Einbeziehung der Schutzinteressen aller Beteiligten sowie das Austragen daraus resultierender Schutzkonflikte beim Entstehen einer Kommunikationsverbindung.

Inhalte der Kommunikation	Kommunikationsumstände
Vertraulichkeit	Anonymität
Verdecktheit	Unbeobachtbarkeit

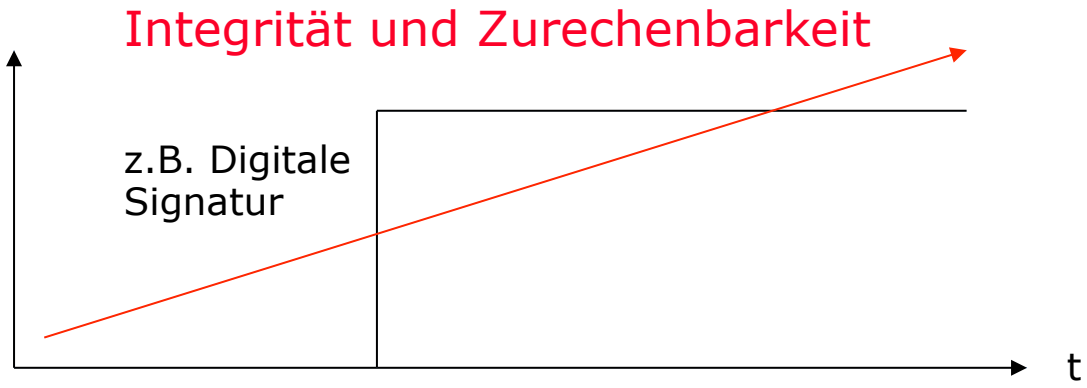
- Datenvermeidung
  - Erfassungsmöglichkeit und Speicherung personenbezogener Daten vermeiden
- Datensparsamkeit
  - Jeder behält seine personenbezogenen Daten in seinem persönlichen Verfügungsbereich.

Beobachtungen zum Monotonieverhalten

- Vertraulichkeit kann nur geringer werden.

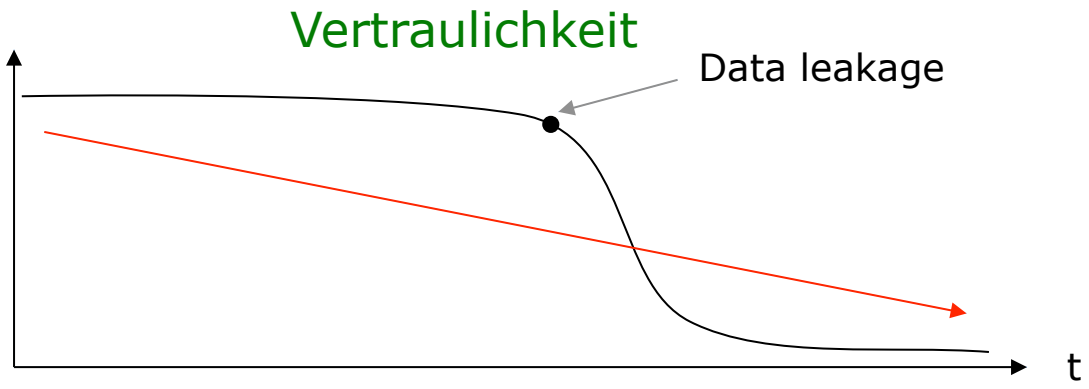


- Integrität und Zurechenbarkeit können nur größer werden.



Beobachtungen zum Monotonieverhalten

- Vertraulichkeit kann nur geringer werden.



- Fazit

Der Mensch sollte sensible Daten die ihn und andere betreffen, besonders sorgsam schützen und nur sehr überlegt weitergeben bzw. veröffentlichen.

Beispiele für Bausteine datenschutzfördernder Technik

- Verschlüsselung

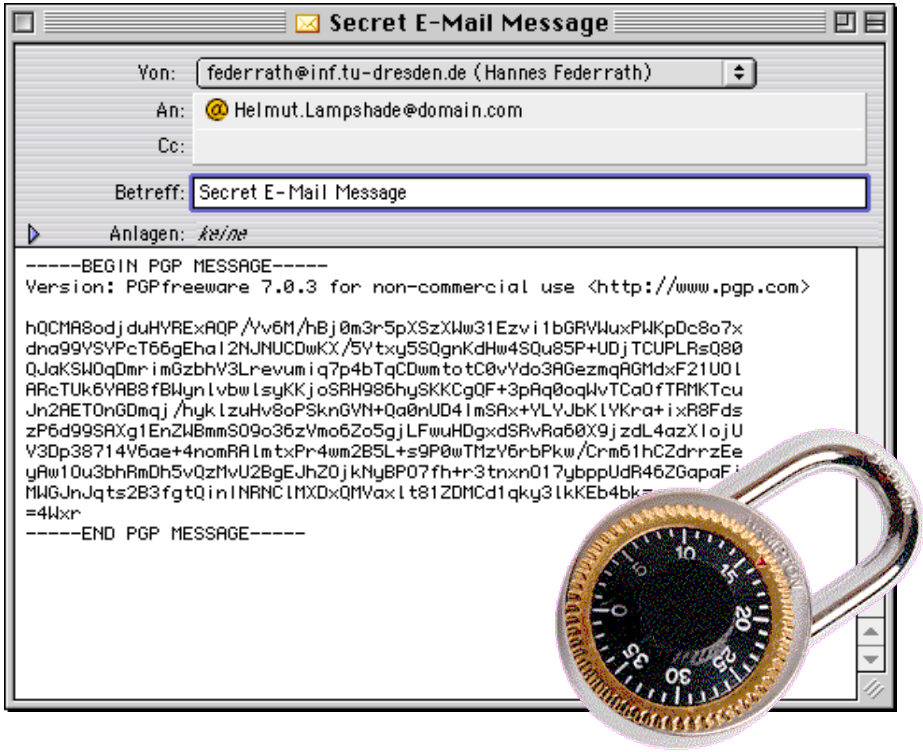
- Schutz von Kommunikationsbeziehungen
  - Broadcast
  - Proxies
  - MIX network

- Schutz von Transaktionen
  - Pseudonyme
  - Credentials (an Pseudonyme gekettete Eigenschaften)

Verschlüsselung

- Verschlüsseln hilft gegen Ausspähen der Inhalte durch Außenstehende

- Empfehlungen:
  - GnuPG für E-Mail-Verschlüsselung verwenden
  - Auf https beim Senden von sensiblen Daten im Browser achten



Verschlüsseln hilft nichts gegen die Beobachtung von Kommunikationsbeziehungen durch Außenstehende und Netzbetreiber

Beispiele für Bausteine datenschutzfördernder Technik

- Verschlüsselung
- Schutz von Kommunikationsbeziehungen
  - Broadcast
  - Proxies
  - MIX network
- Schutz von Transaktionen
  - Pseudonyme
  - Credentials (an Pseudonyme gekettete Eigenschaften)

Broadcast

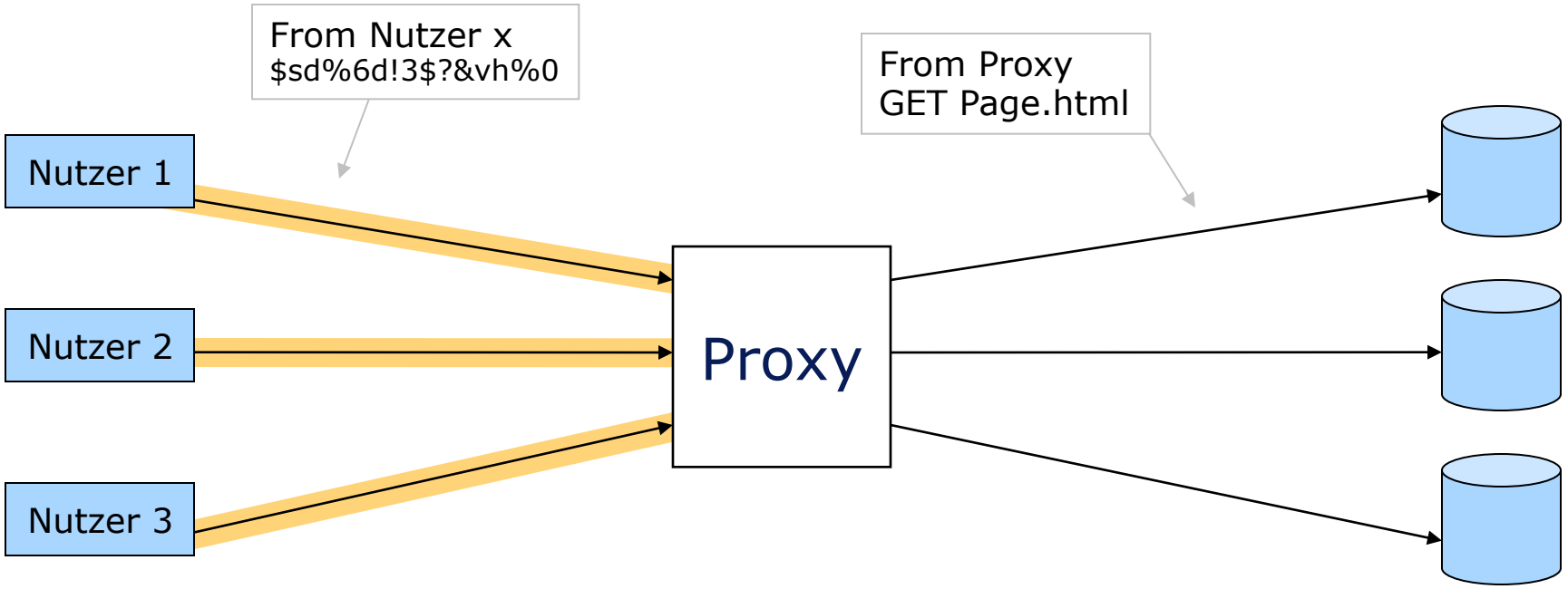
- Das war damals...

  - Zeitung lesen
  - Radio über Antenne hören
  - Fernsehen über Breitbandverteilkabel

- Verteilung (Broadcast) + implizite Adressierung
  - Technik zum Schutz des Empfängers
  - Alle Teilnehmer erhalten alles
  - Lokale Auswahl
  - Es bleibt verborgen, welchen Inhalt der Nutzer konsumiert

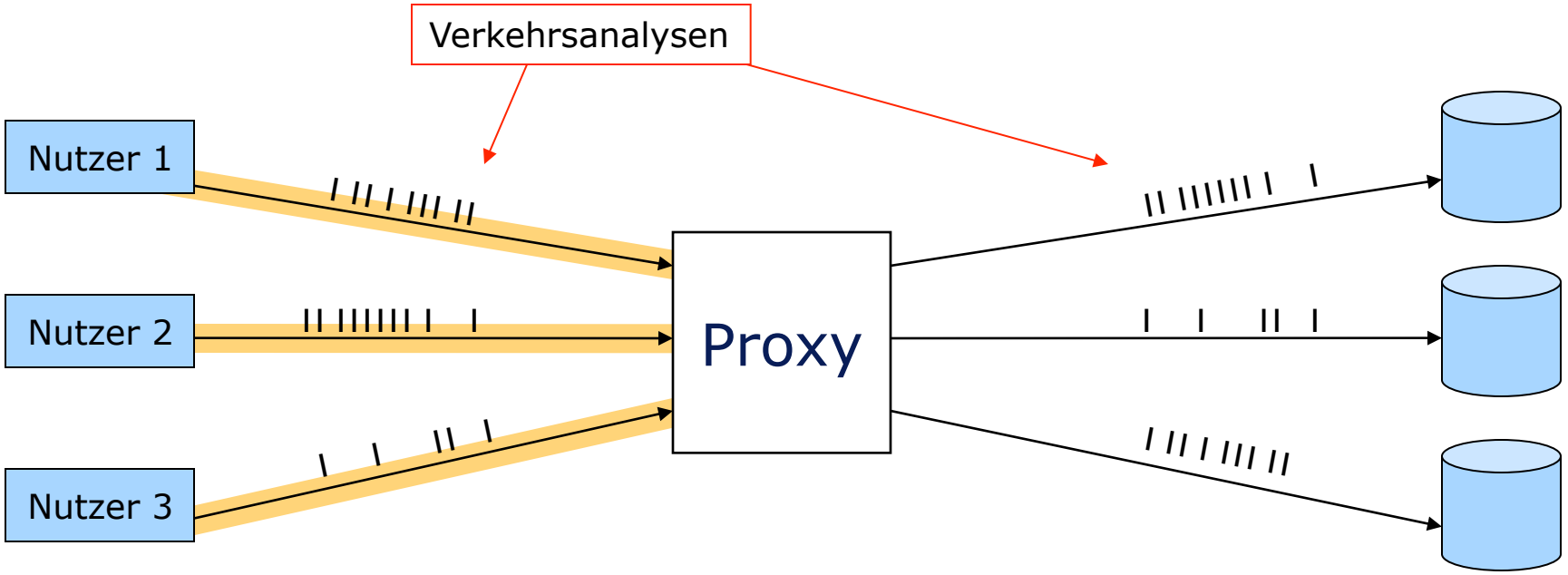
Proxies: Outsider

- Erreichbare Sicherheit (Outsider)
  - Beobachter nach Proxy und Serverbereiber:
    - erfahren nichts über den wirklichen Absender eines Requests
  - Beobachter vor Proxy:
    - Schutz des Senders, wenn Verbindung zu Proxy verschlüsselt



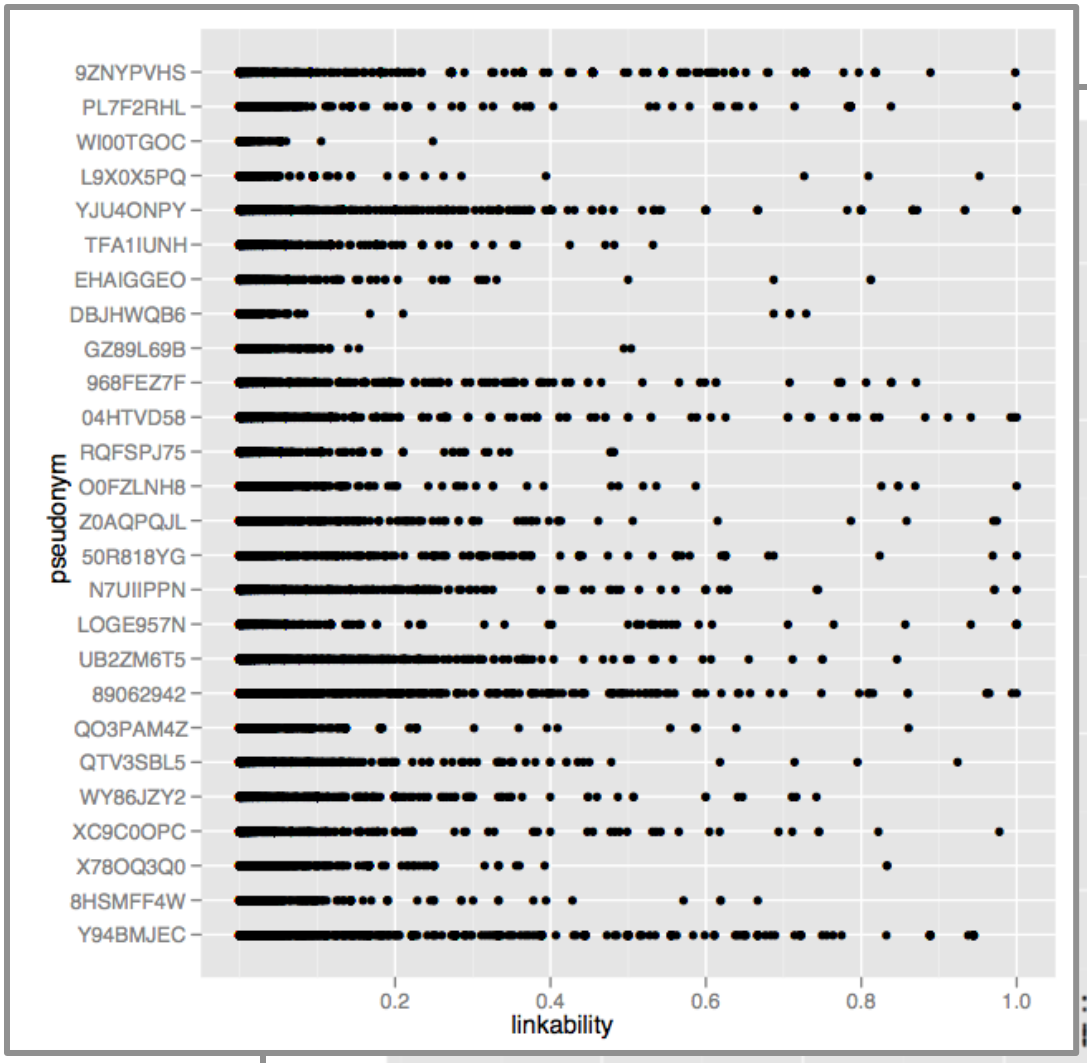
Proxies: Outsider

- Erreichbare Sicherheit (Outsider)
  - Aber: Trotz Verschlüsselung:
    - kein Schutz gegen Verkehrsanalysen
      - Verkettung über Nachrichtenlängen
      - zeitliche Verkettung



Website- und DNS-Fingerprinting

Gerber 2009



Mix-Netz (Chaum, 1981)

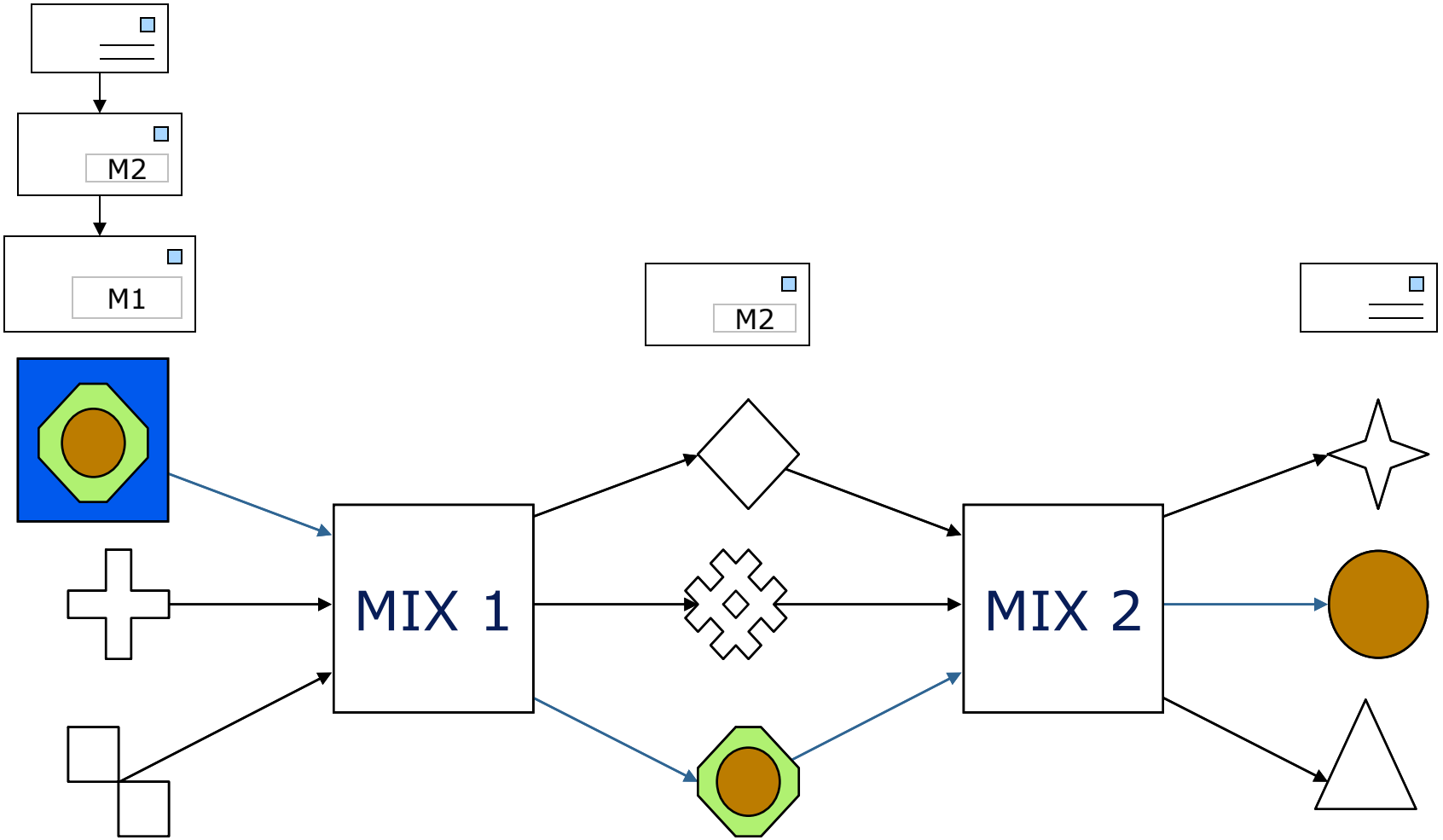
- System zum Schutz von Kommunikationsbeziehungen bei vermittelter Kommunikation

- Grundfunktionen:
  - Nachrichten in einem »Schub« sammeln,
  - Wiederholungen ignorieren,
  - Nachrichten umkodieren,
  - umsortieren,
  - gemeinsam ausgeben
  - Alle Nachrichten haben die gleiche Länge.
  - Mehr als einen Mix und unterschiedliche Betreiber verwenden
  - Wenigstens ein Mix darf nicht angreifen.

- Schutzziel:
  - Unverkettbarkeit von Sender und Empfänger

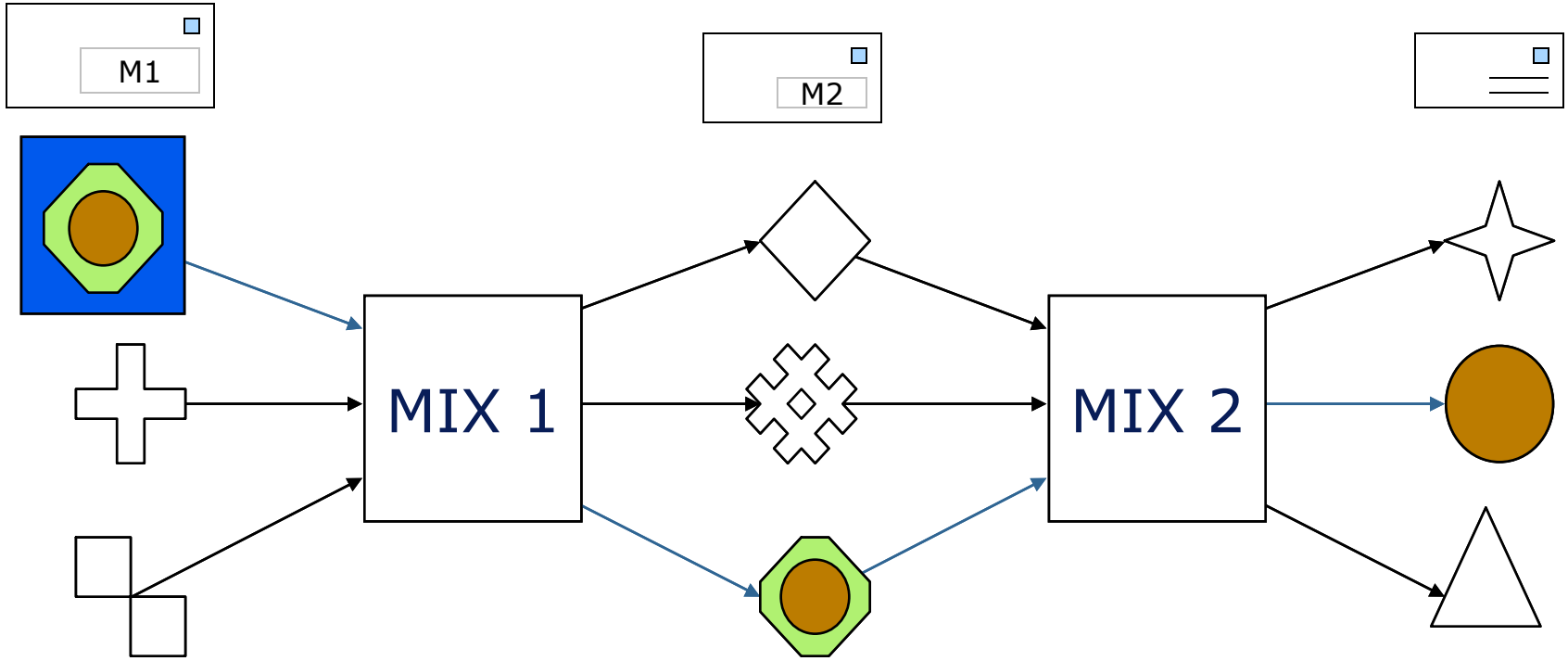
Mix-Netz (Chaum, 1981)

- System zum Schutz von Kommunikationsbeziehungen bei vermittelter Kommunikation



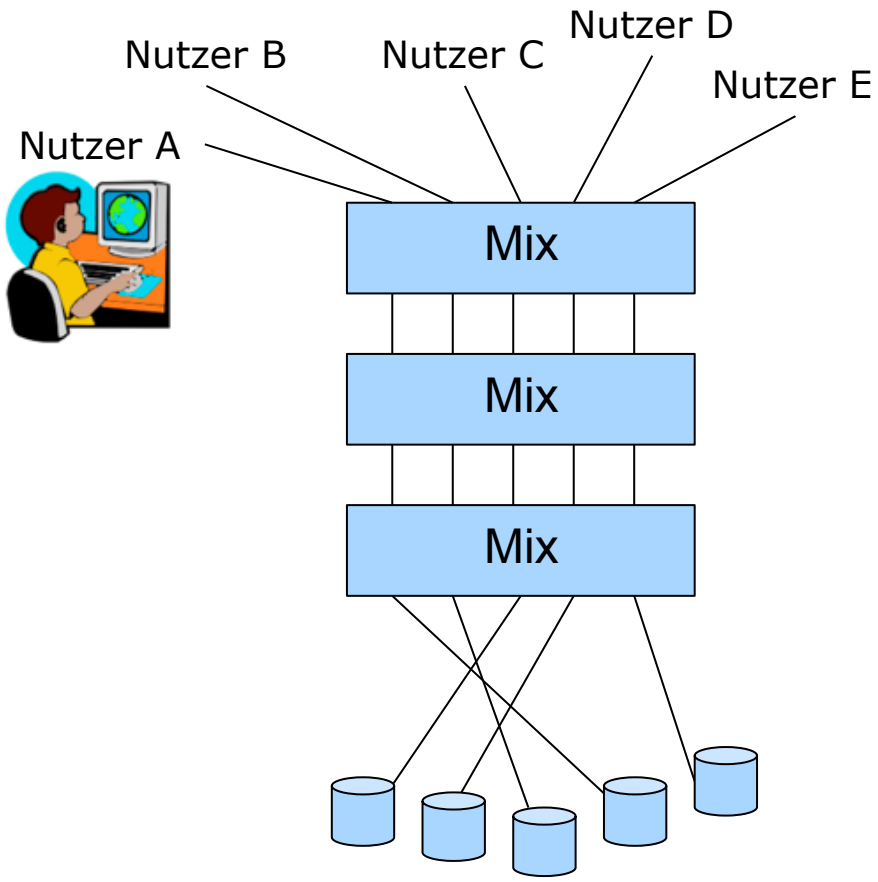
Mix-Netz (Chaum, 1981)

- Stärke der Mixe:
  - Auch die Betreiber der Mixe erfahren nichts mehr über die Kommunikationsbeziehung zwischen Sender und Empfänger.
- Notwendige Bedingungen:
  - Mehr als einen Mix und unterschiedliche Betreiber verwenden
  - Wenigstens ein Mix darf nicht angreifen.



AN.ON und TOR

- Dienste zum anonymen Internetzugriff
  - http://www.anon-online.de
  - http://tor.eff.org
- Schutz des Einzelnen vor Überwachung und Profilierung seiner Internetaktivitäten
- beruhen auf Erweiterungen des Mix-Verfahrens von Chaum
- Schutz auch vor dem Betreiber des Dienstes (Schutz vor Insidern)



Beispiele für Bausteine datenschutzfördernder Technik

- Verschlüsselung

- Schutz von Kommunikationsbeziehungen
  - Broadcast
  - Proxies
  - MIX network

- Schutz von Transaktionen
  - Pseudonyme
  - Credentials (an Pseudonyme gekettete Eigenschaften)

Pseudonyme

- Pseudonym-Arten
  - Vom Teilnehmer selbst gewählte Zeichenketten, die keinen Bezug zu seiner Identität besitzen
  - Große Zufallszahlen (etwa 45 Dezimalstellen)
  - Öffentliche Testschlüssel eines Signatursystems

- Pseudonyme zur Bestätigung von Eigenschaften
  - Einfaches »qualifizierendes Zertifikat«
  - Blenden des Pseudonyms vor dem Zertifizieren

```
BEGIN ZERTIFIKAT
Pseudonym: 30452634272346623424987241375
Öffentlicher Testschlüssel des Pseudonyms:
h833hd38dddajscbicme098342k236egfkw74h5445
84hdbscldmrtpofjrkt0jshuedagaszw12geb3u4b=
Bestätigte Eigenschaften:
Der Inhaber ist über 18 Jahre alt.
Der Inhaber ist deutscher Staatsbürger.
Datum: 19.03.2000
Gültig bis: 18.03.2001
Aussteller: Einwohnermeldeamt Dresden
Signatur des Ausstellers:
23j423vdsaz345kj435ekji3u4z2983734ijo23i72
kj867wdbez2o074j5lkdmcdkki1237t3rgbdvbwdj=
END ZERTIFIKAT
```

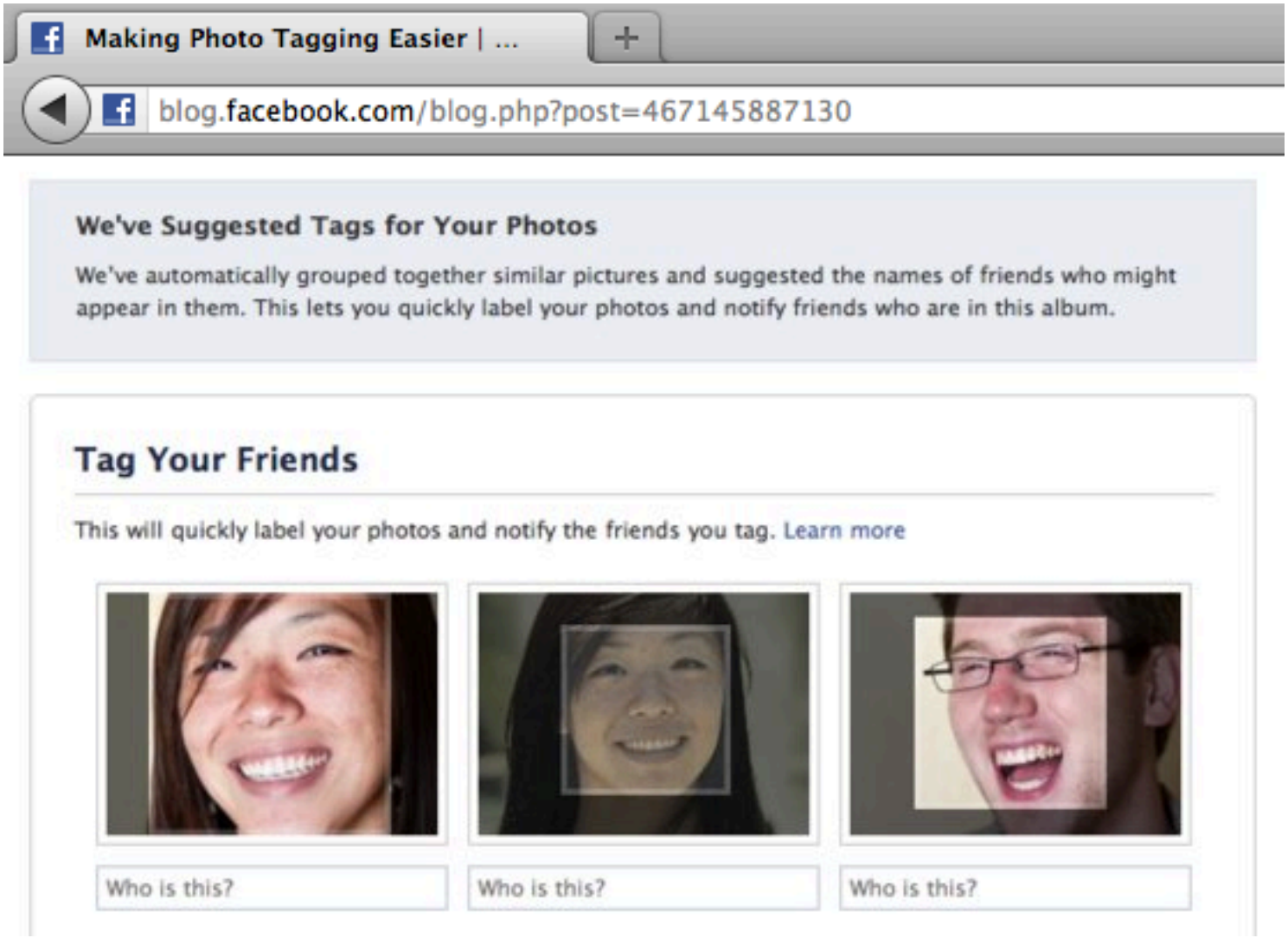
Drei unglückliche Fallbeispiele

- Ziel
  - Verbotenes, unerwünschtes im Internet soll

	Fallbeispiele:
· nicht möglich	maschinelles Lernen
· nicht mehr vorhanden	x-pire!
· wenigstens nicht mehr erreichbar	DNS-Sperre

  - sein.

Gesichter auswerten – Mit und ohne Facebook

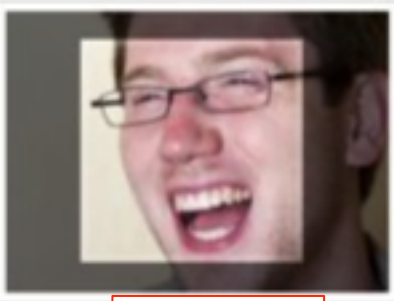


facebook

- Gesichter – nicht nur von Freunden, sondern auch von Menschen, die nicht Mitglied des sozialen Netzes sind – können mit Namen versehen werden

Nicht Mitglied im sozialen Netz

Jane



John

- Soziale Netze wissen selbst über Menschen bescheid, die nicht einmal wissen können, dass sie schon erfasst sind.

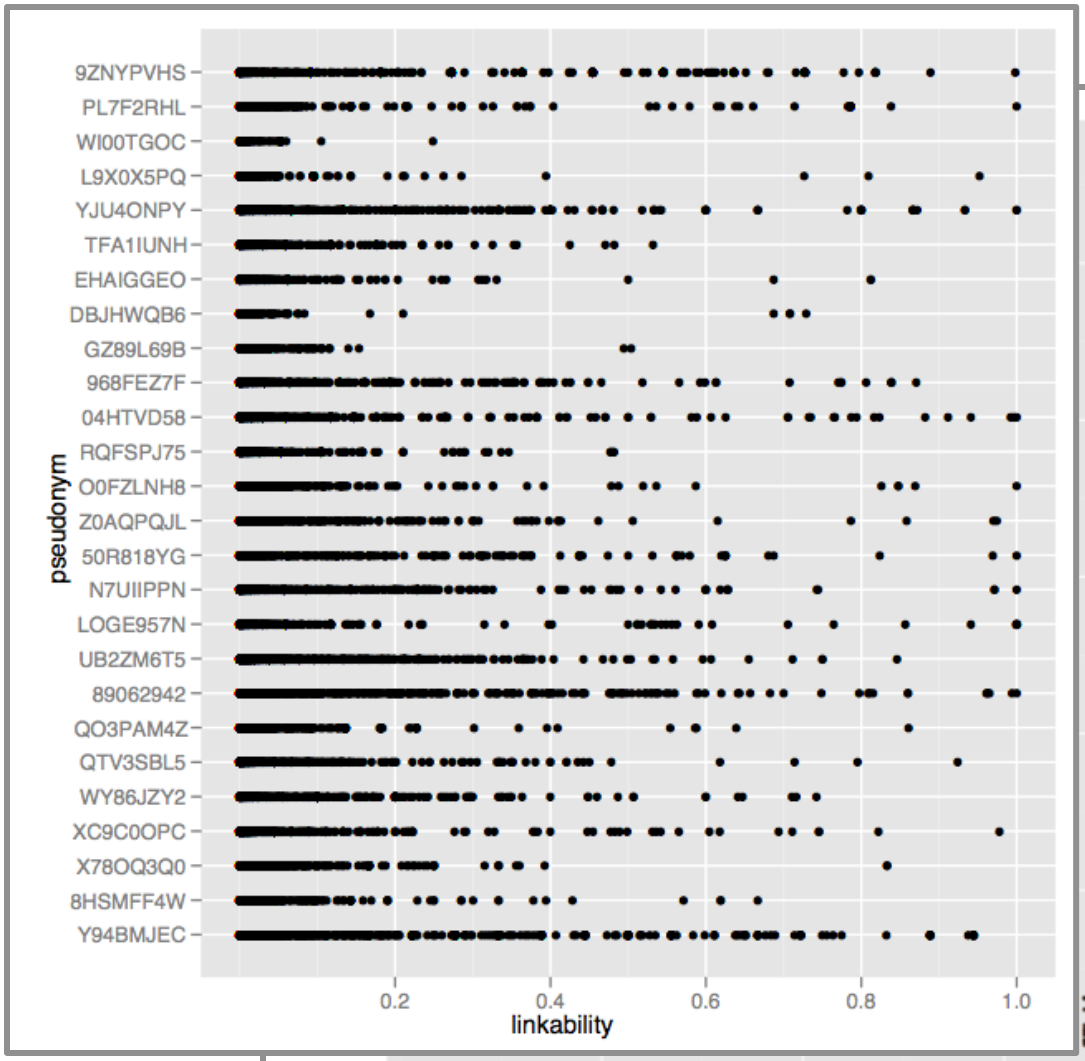
Nicht Mitglied im sozialen Netz

- Soziale Netze wissen selbst über Menschen bescheid, die nicht einmal wissen können, dass sie schon erfasst sind.

- Geschlossene Gruppe wünschenswert

Analogie: Website- und DNS-Fingerprinting

Gerber 2009



Drei unglückliche Fallbeispiele

- Ziel
  - Verbotenes, unerwünschtes im Internet soll

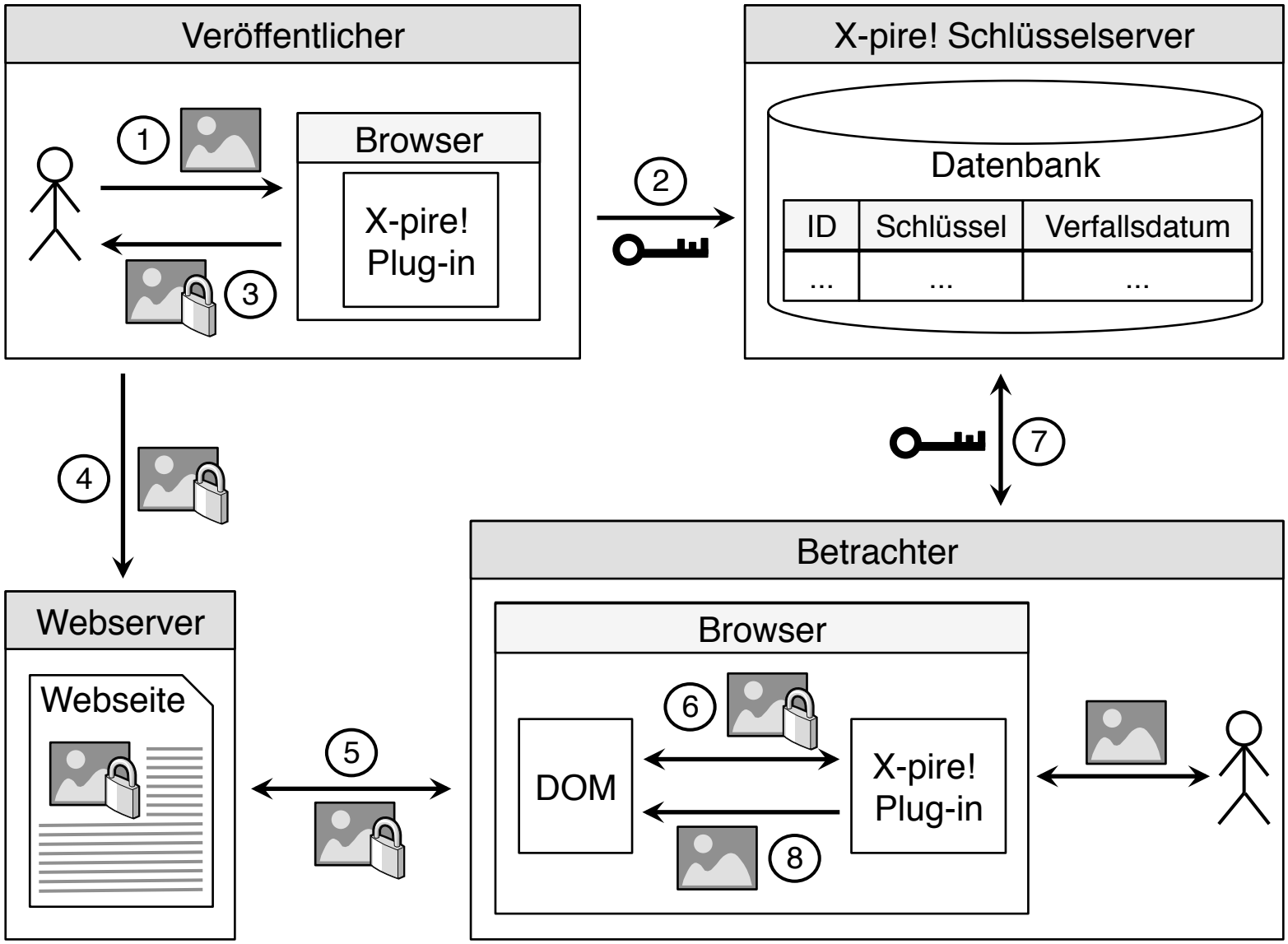
	Fallbeispiele:
· nicht möglich	maschinelles Lernen
· nicht mehr vorhanden	x-pire!
· wenigstens nicht mehr erreichbar	DNS-Sperre

  - sein.

X-pire!


Bildergalerie
http://192.168.2.1/
Google
Bildergalerie
Mit x-pire! geschütztes Bild
Mit x-pire! geschütztes Bild
Fertig

Funktionsweise X-pire!

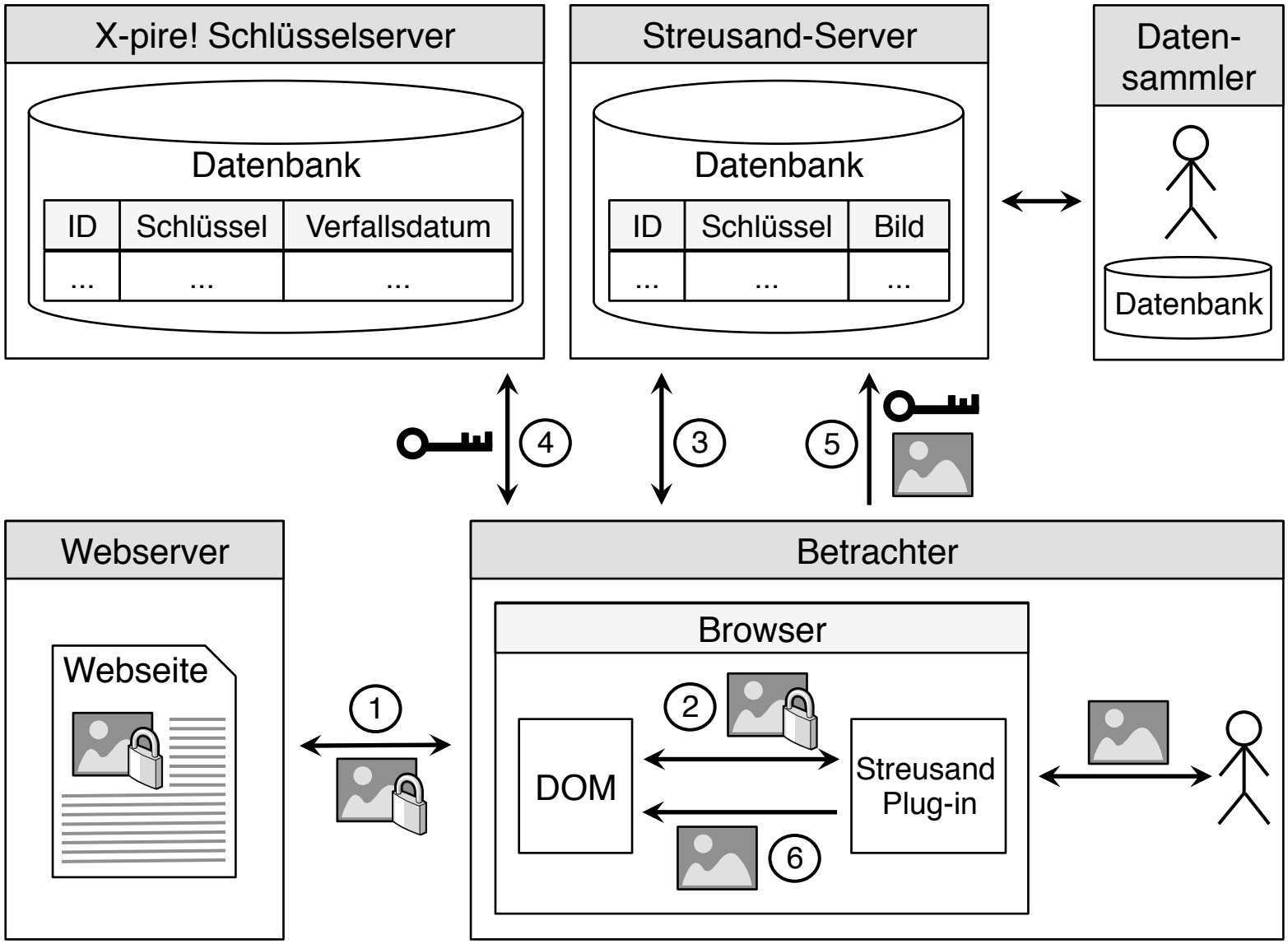


Sicherheit von x-pire!

- Kein Schutz gegen Angreifer in der Rolle »Betrachter«
  - Software im Verfügungsbereich des Betrachters (Browser) erhält Zugriff auf Schlüssel und unverschlüsselten Inhalt

- Streisand-Effekt
  - Insbesondere Inhalte, die wieder aus dem Netz verschwinden sollen, halten sich möglicherweise besonders lange.

Funktionsweise Streusand



Drei unglückliche Fallbeispiele

- Ziel
  - Verbotenes, unerwünschtes im Internet soll

	Fallbeispiele:
· nicht möglich	maschinelles Lernen
· nicht mehr vorhanden	x-pire!
· wenigstens nicht mehr erreichbar	DNS-Sperre

  - sein.

DNS-Sperre und Umgehungsmöglichkeiten

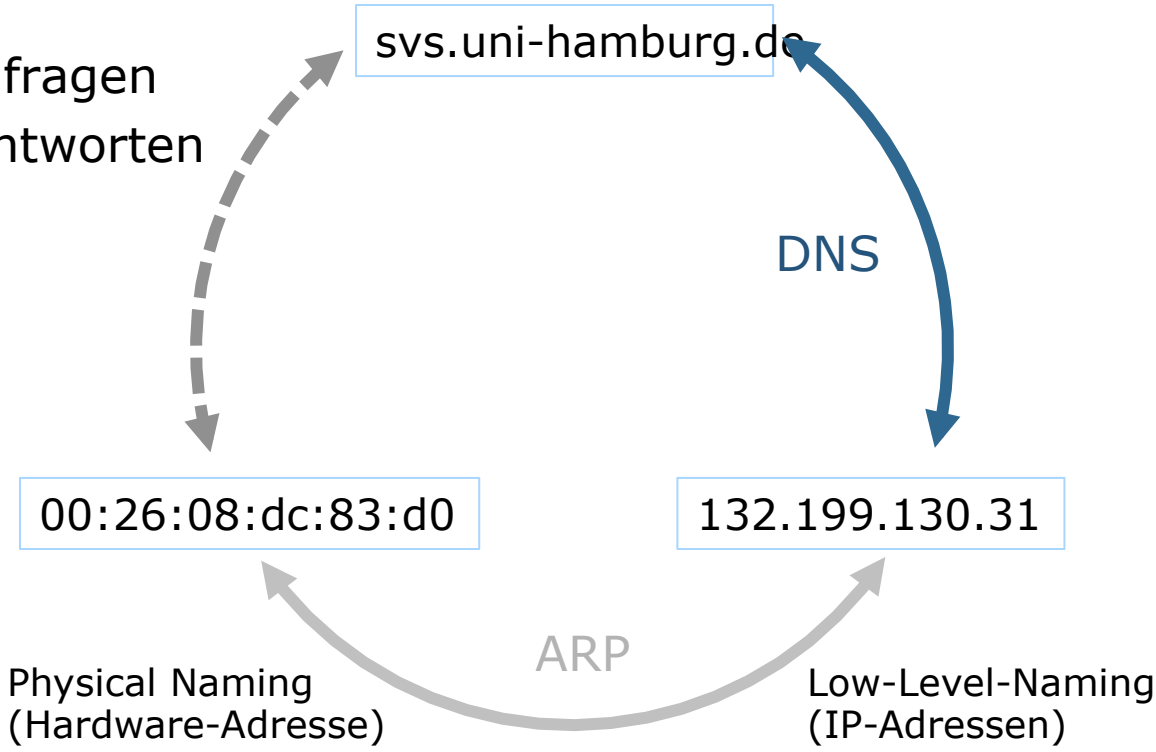
- Zugangserschwerungsgesetz 2009

- Ziel: Sperrung von Webseiten mit kinderpornographischem Inhalt

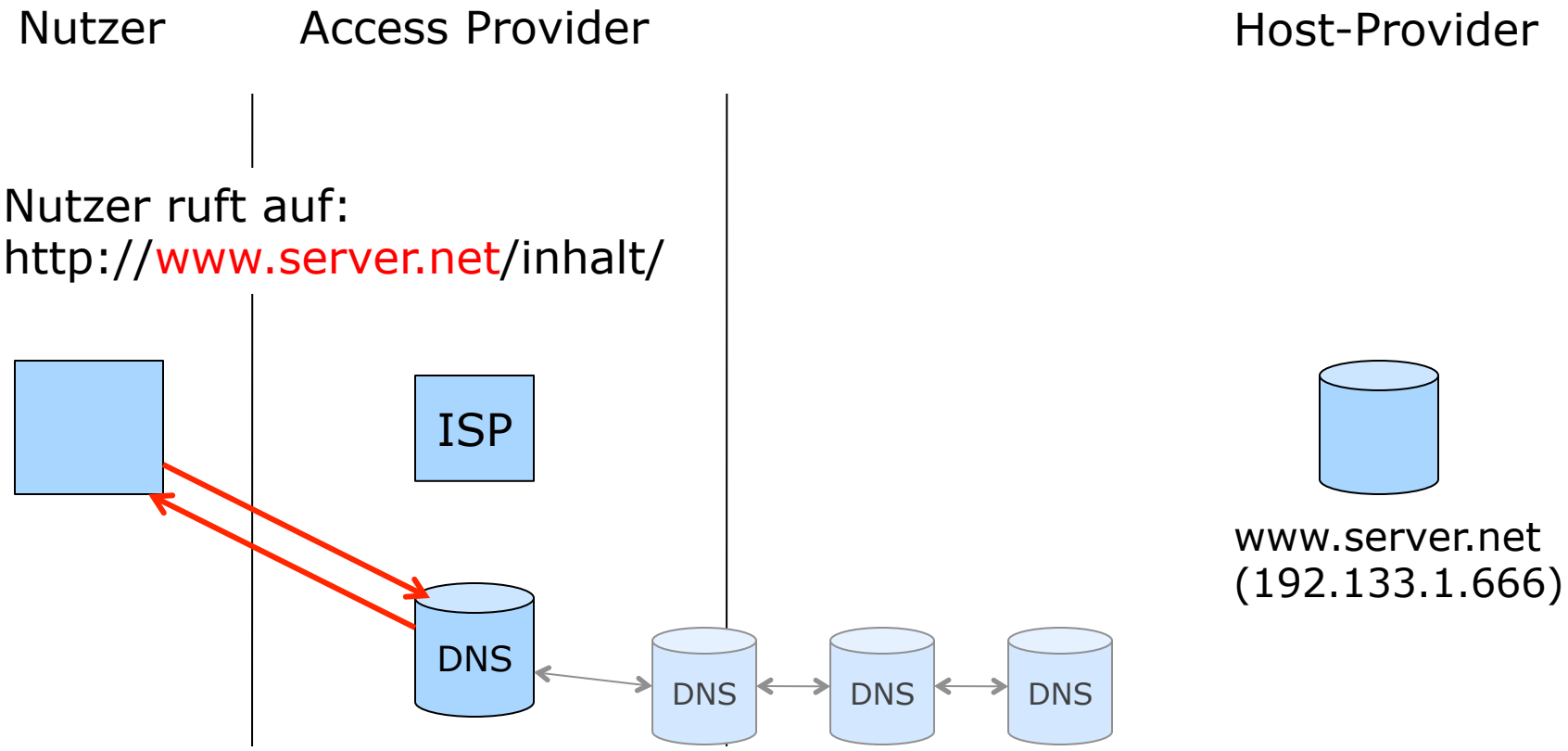
Sicherheit im Domain Name System (DNS)

- DNS: Domain Name System
  - Abbildung des Rechnernamens auf IP-Adresse
  - Anfrage an Nameserver
  - typischerweise in WANs

- Angriffe auf DNS
  - Sniffing von DNS-Anfragen
  - Fälschen der DNS-Antworten
  - Denial-of-Service

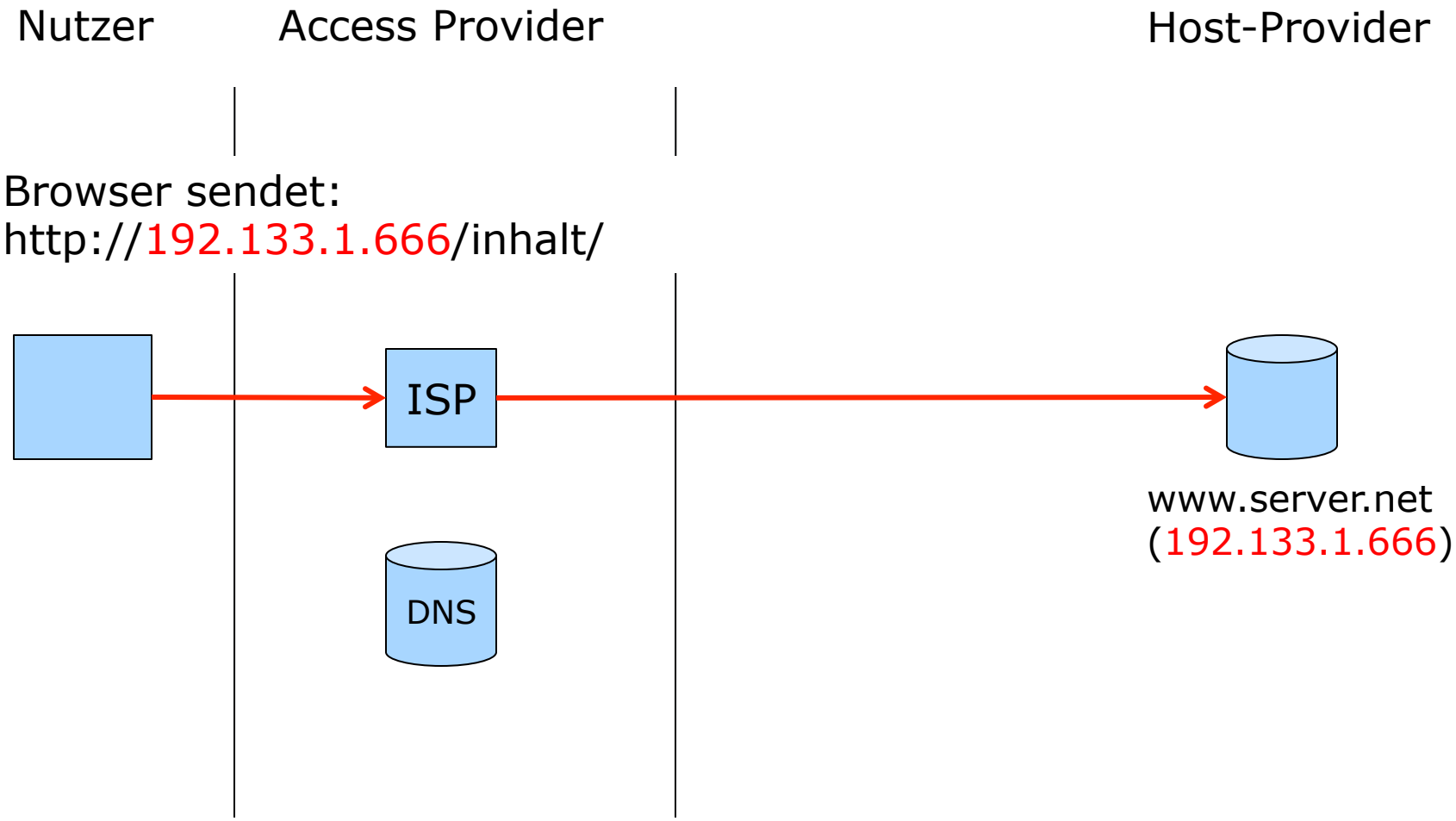


Zunächst wird DNS-Server angefragt

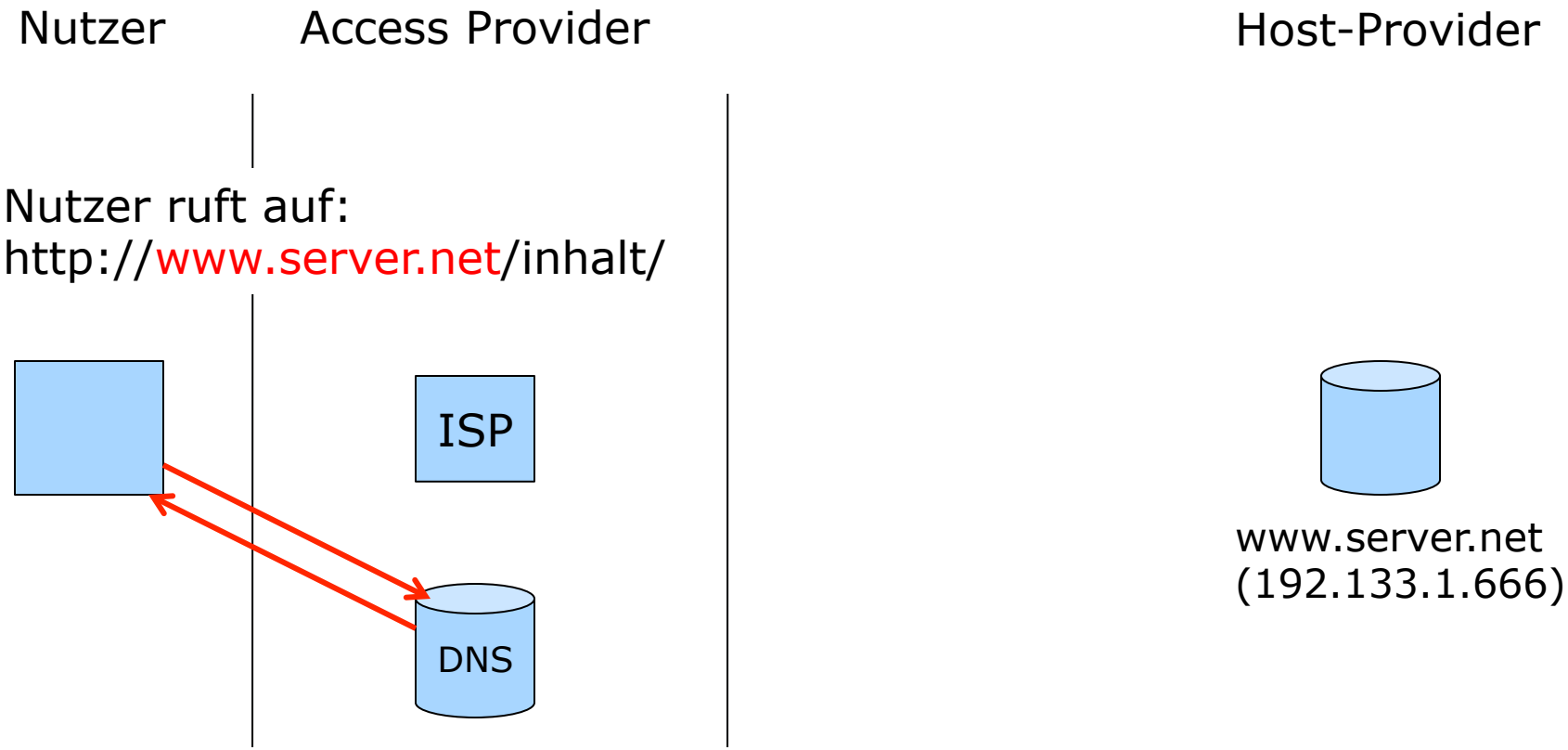


Browser
1. sendet DNS-Request: www.server.net
2. empfängt DNS-Antwort: 192.133.1.666

Anschließend wird Inhalt abgerufen

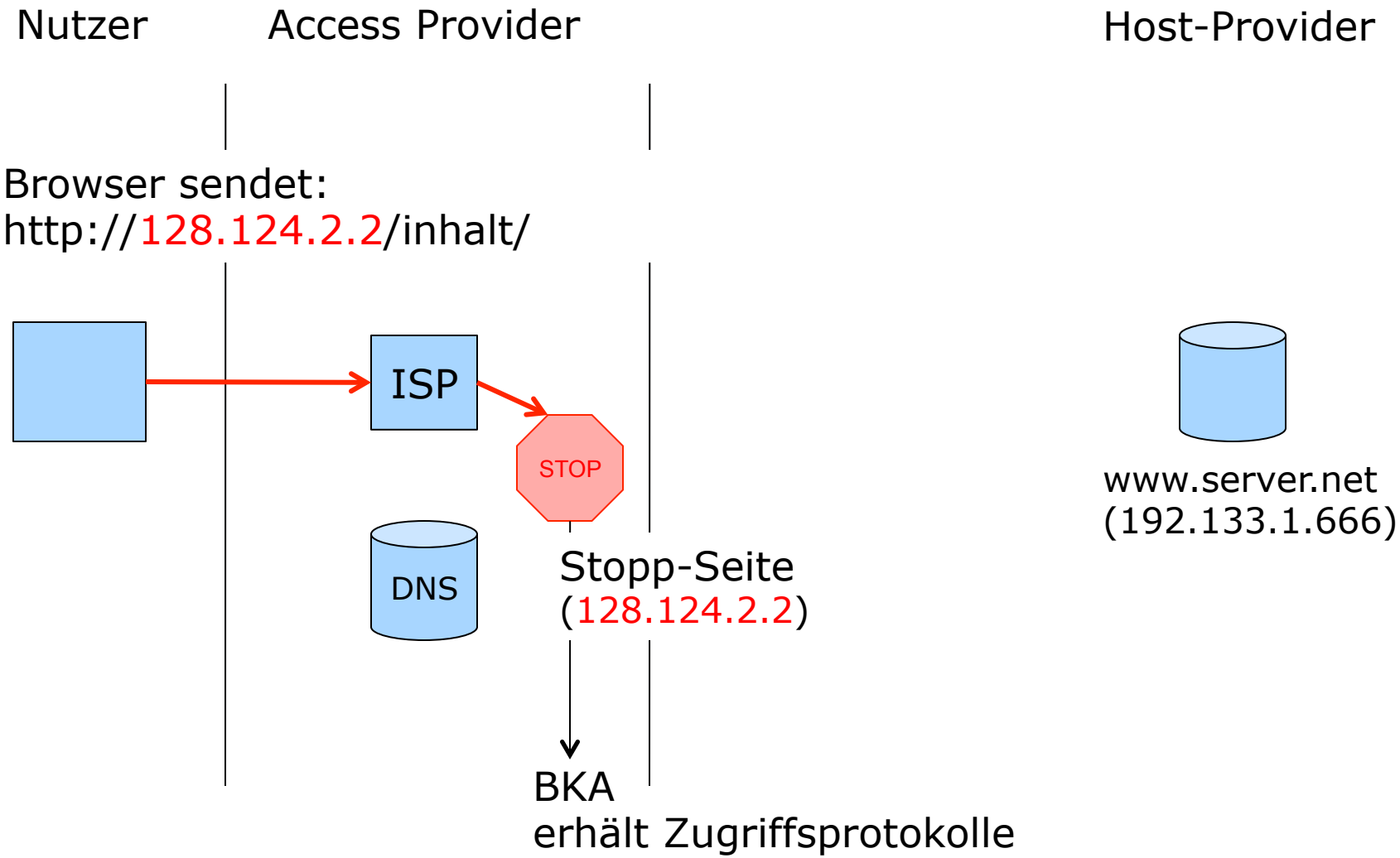


DNS-Sperre: DNS-Server sendet »falsche« Antwort

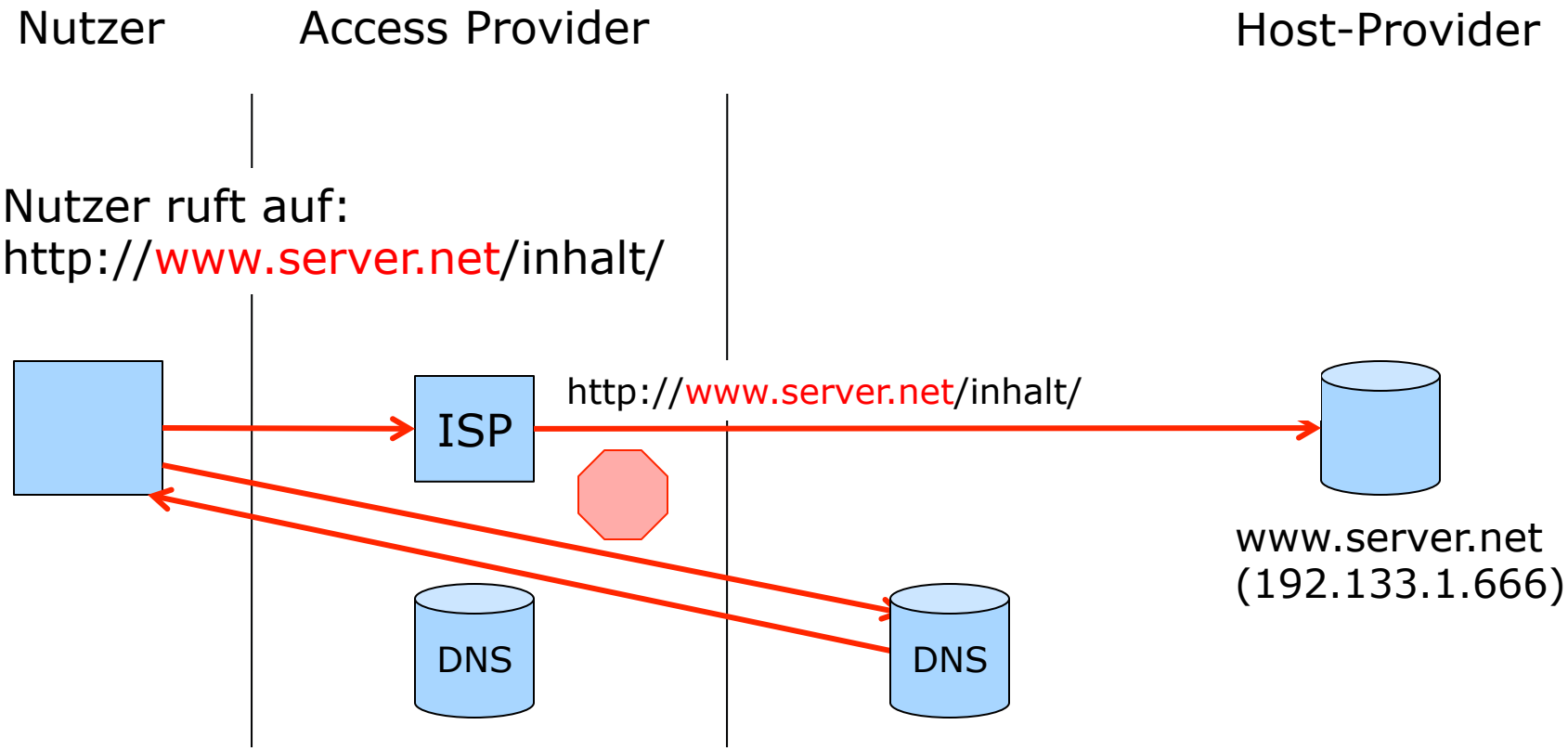


Browser
1. sendet DNS-Request: www.server.net
2. DNS-Server sieht Sperrliste durch (Treffer!)
2. empfängt DNS-Antwort: 128.124.2.2

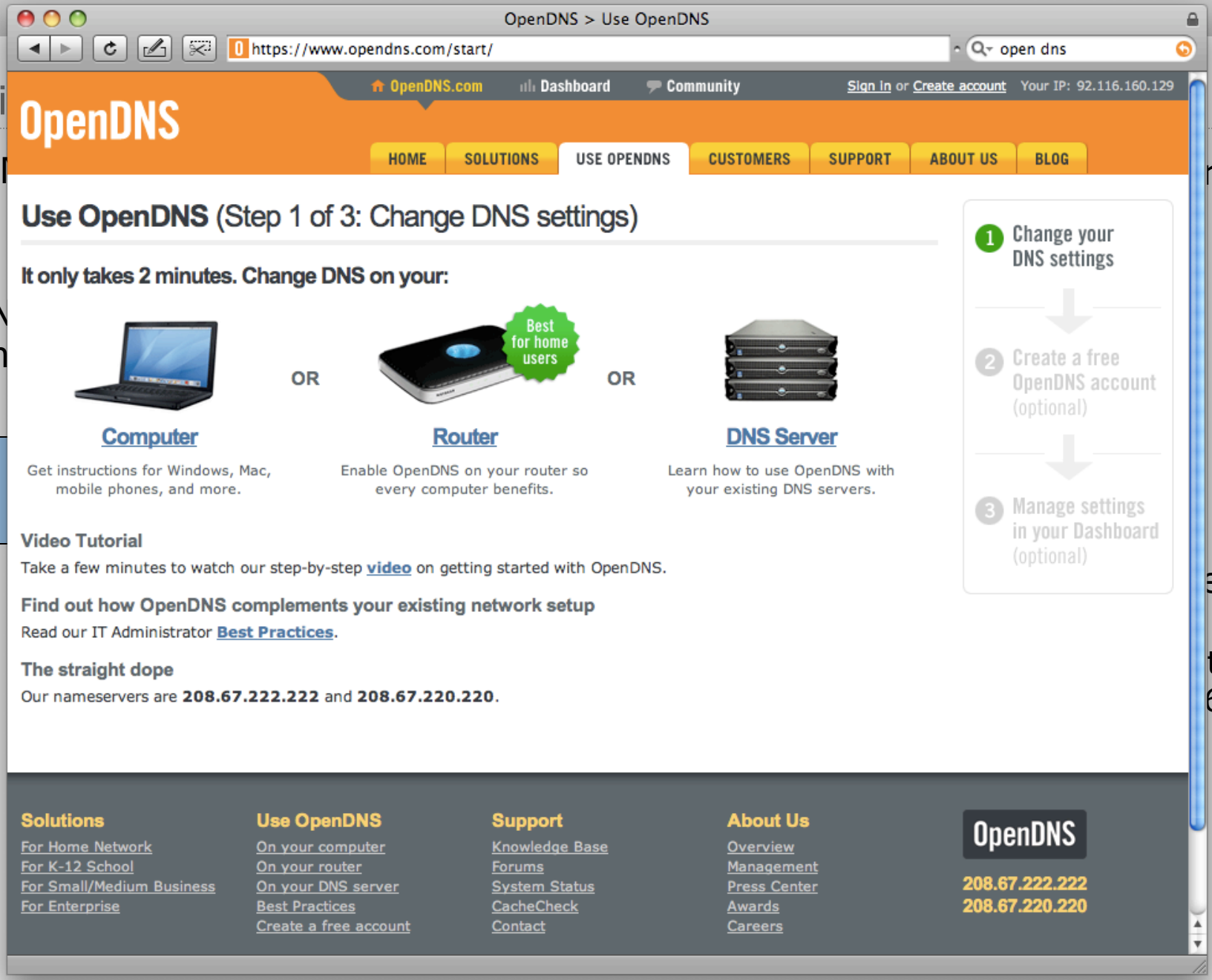
Mit DNS-Sperre landet der Nutzer im WWW auf Stopp-Seite



Mit DNS-Sperre und Open DNS



Browser
1. sendet DNS-Request: www.server.net
2. empfängt DNS-Antwort: 192.133.1.666


OpenDNS > Use OpenDNS
https://www.opendns.com/start/
open dns
OpenDNS.com
Dashboard
Community
Sign In or Create account
Your IP: 92.116.160.129
OpenDNS
HOME
SOLUTIONS
USE OPENDNS
CUSTOMERS
SUPPORT
ABOUT US
BLOG
Use OpenDNS (Step 1 of 3: Change DNS settings)
It only takes 2 minutes. Change DNS on your:
OR
Best for home users
OR
Computer
Get instructions for Windows, Mac, mobile phones, and more.
Router
Enable OpenDNS on your router so every computer benefits.
DNS Server
Learn how to use OpenDNS with your existing DNS servers.
1 Change your DNS settings
2 Create a free OpenDNS account (optional)
3 Manage settings in your Dashboard (optional)
Video Tutorial
Take a few minutes to watch our step-by-step video on getting started with OpenDNS.
Find out how OpenDNS complements your existing network setup
Read our IT Administrator Best Practices.
The straight dope
Our nameservers are 208.67.222.222 and 208.67.220.220.
Solutions
For Home Network
For K-12 School
For Small/Medium Business
For Enterprise
Use OpenDNS
On your computer
On your router
On your DNS server
Best Practices
Create a free account
Support
Knowledge Base
Forums
System Status
CacheCheck
Contact
About Us
Overview
Management
Press Center
Awards
Careers
OpenDNS
208.67.222.222
208.67.220.220

Zusammenfassung

- Sensible Daten besonders sorgsam schützen
  - nur sehr überlegt weitergeben und veröffentlichen
- Möglichst immer Pseudonyme verwenden
  - Verhindert (leichte) Verkettbarkeit von Daten
- Verschlüsselung und Anonymisierung verwenden
  - Verhindert Beobachtung der Aktivitäten