Staatlich organisierte Schutz- und Angriffssoftware

Prof. Dr. Hannes Federrath
Sicherheit in verteilten Systemen (SVS)
http://svs.informatik.uni-hamburg.de/

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

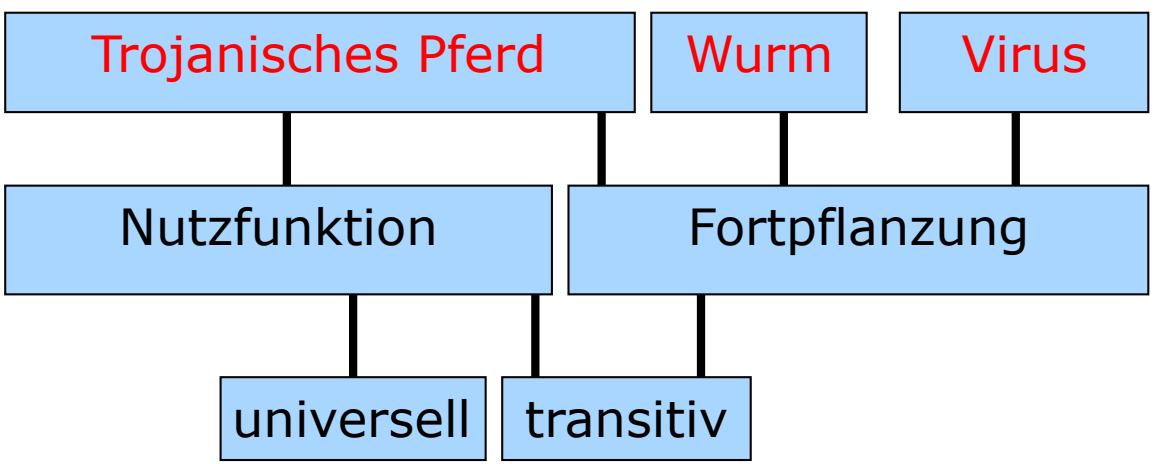
Workshop Cyberpeace - Herausforderungen für Informatik in der Friedenswissenschaft, Universität Darmstadt, 11. April 2013

Gliederung

- Einführung
- Angriff
  - »Bundestrojaner« und das neue Computergrundrecht
  - stattliche Angriffe auf IT-Systeme anderer Staaten
- Schutz
  - Gnu Privacy Guard
  - AN.ON – Anonymity Online
- Schlussbemerkungen

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?



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?

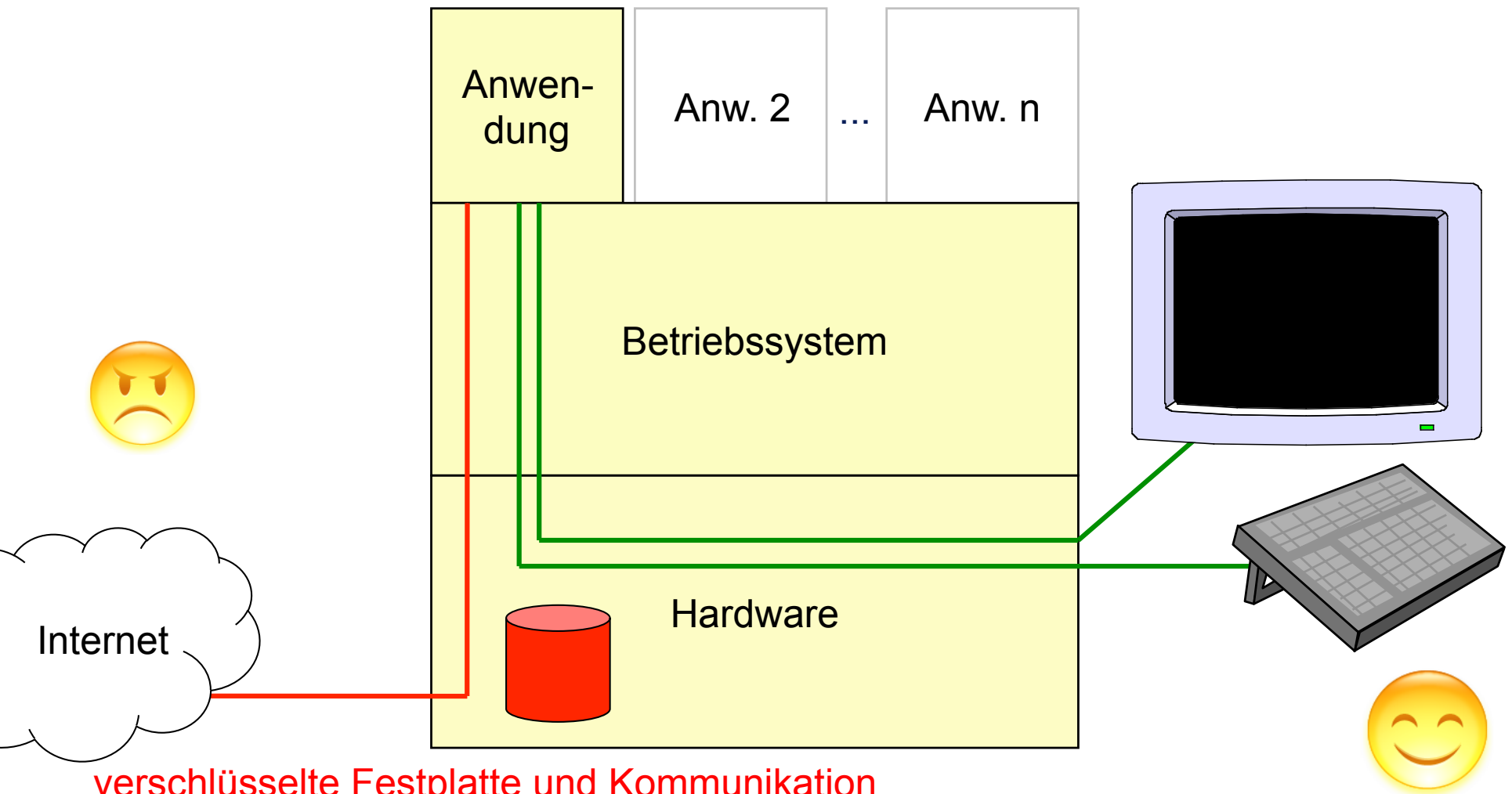
Antwort: »Neues Computergrundrecht«

- 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

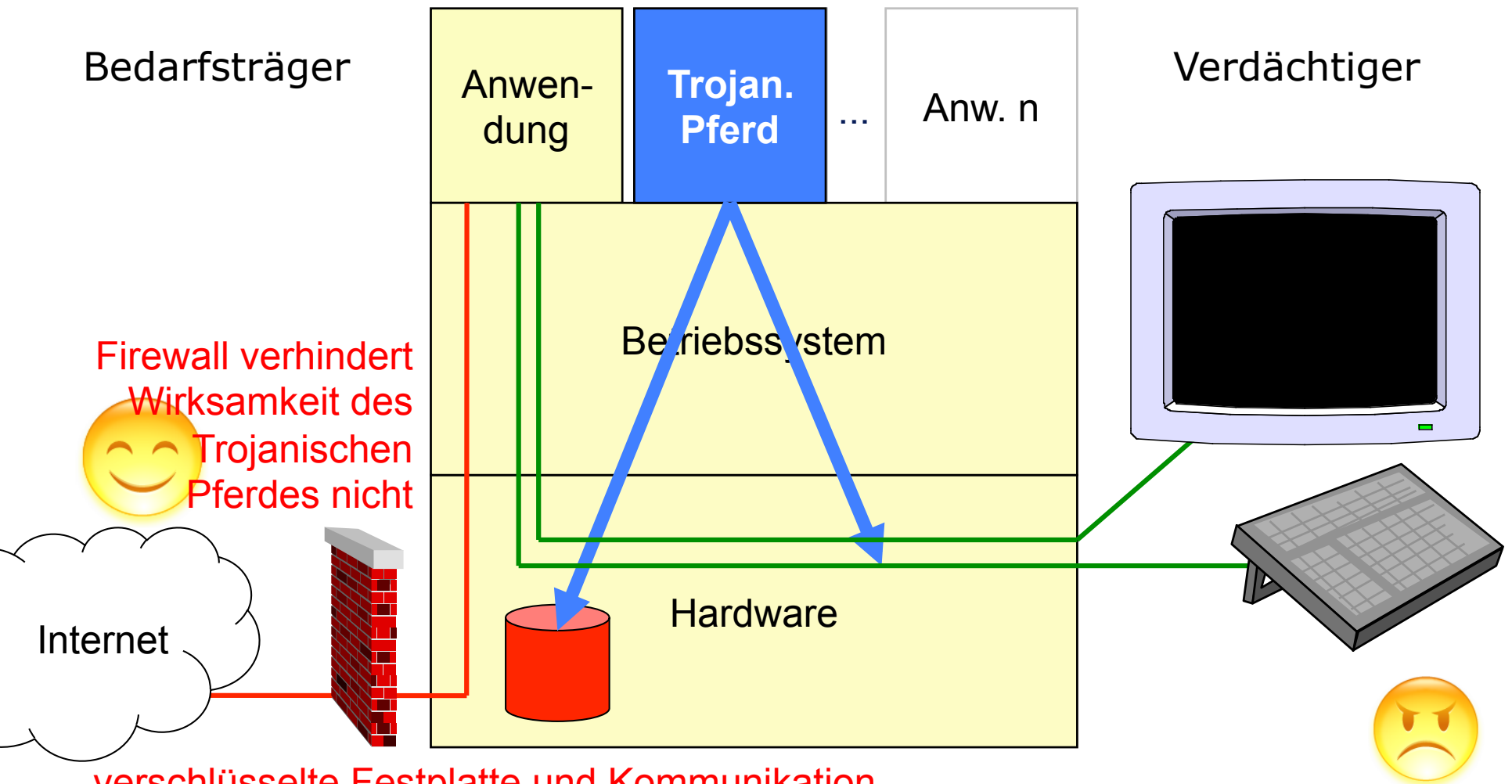
Nutzer schützt Daten auf seinem Rechner durch Verschlüsselung



verschlüsselte Festplatte und Kommunikation

Trojanisches Pferd greift von innen an

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



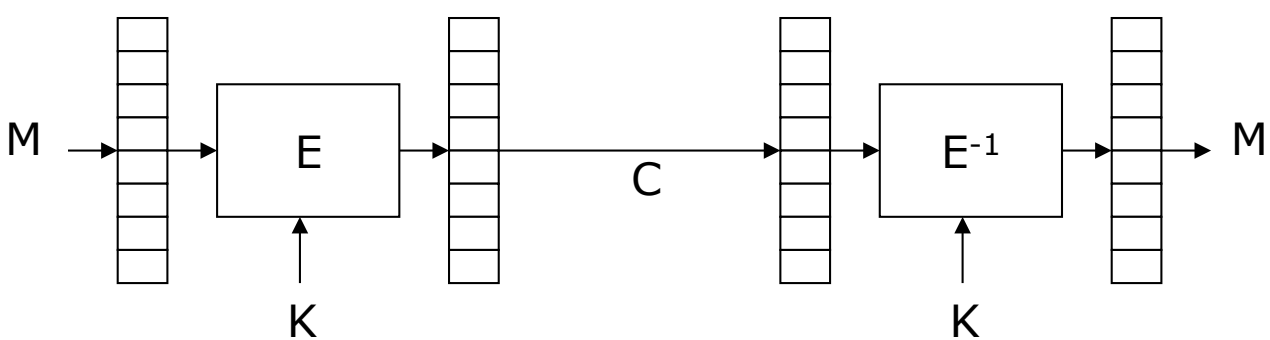
»Staatstrojaner«

- 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 Skype-Capture-Unit

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

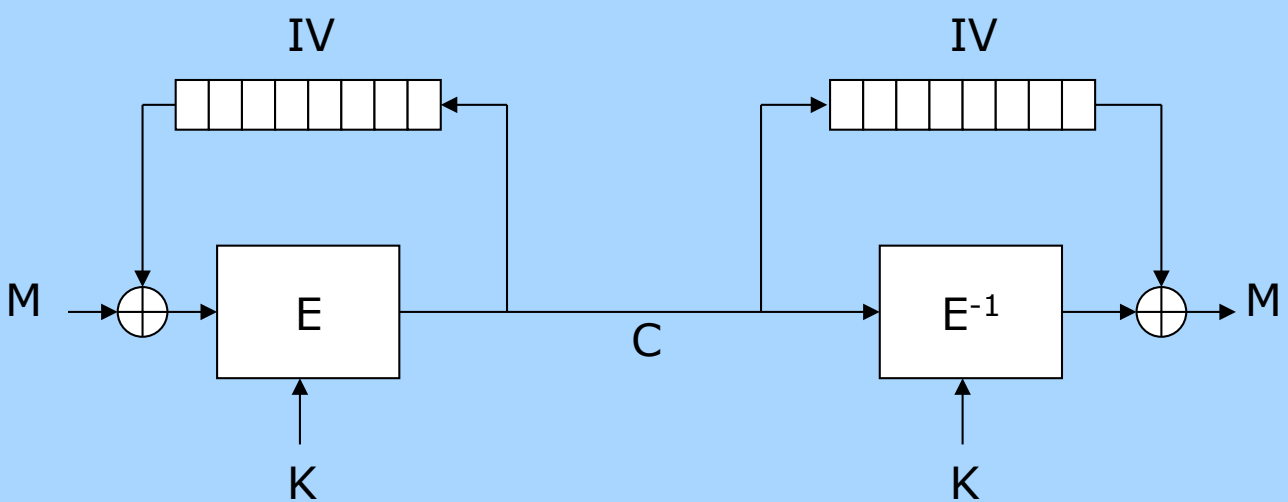
  - Schwach verschlüsselte Kommunikation mit einem Command-and-Control-Server im Ausland (USA)
    - AES im ECB-Mode mit fest kodiertem Schlüssel



$C=E(K,M)$ $M=E^{-1}(K,C)$

- 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.



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

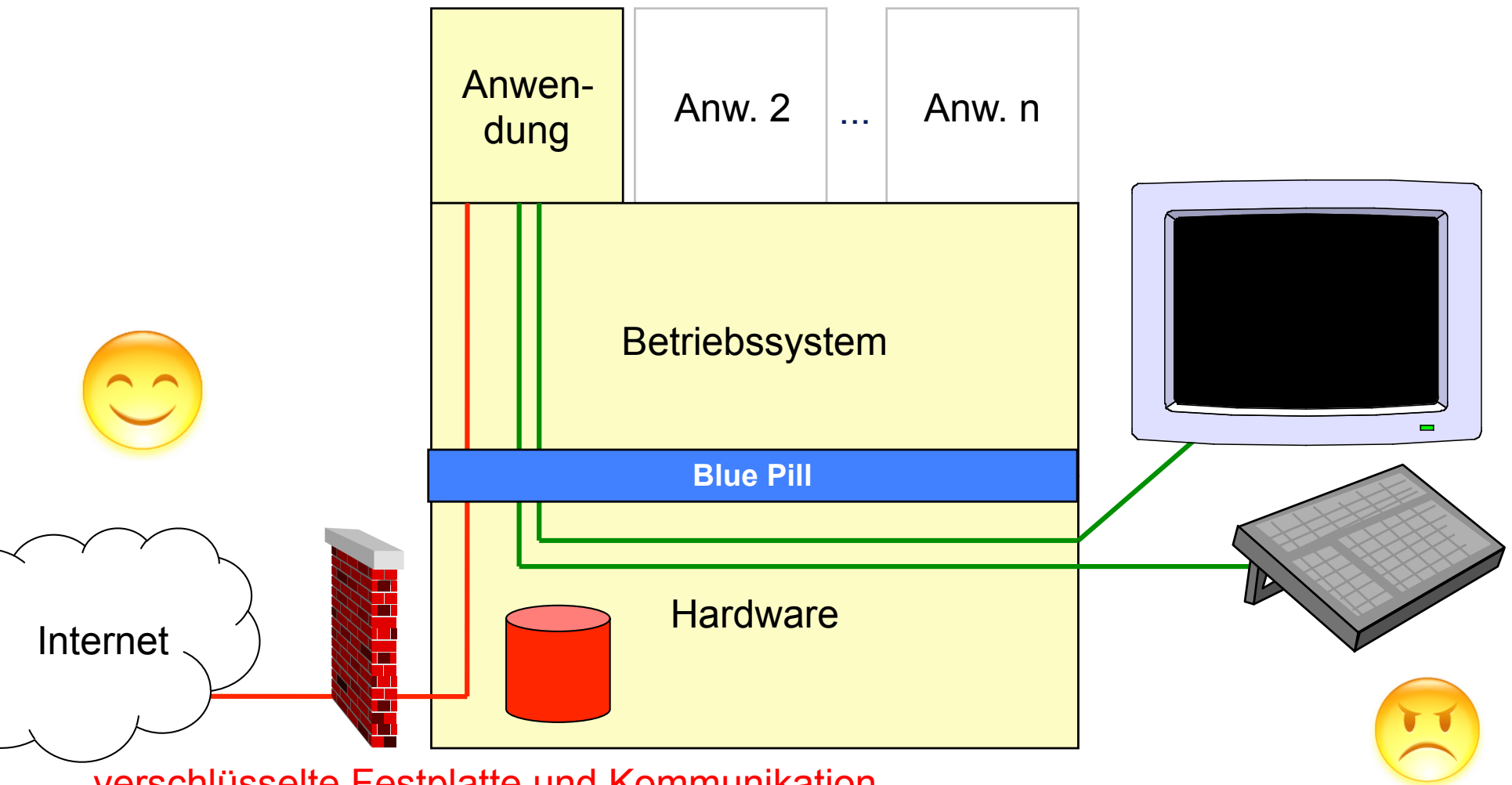
$C_0 = IV$
$M_i = E^{-1}(K, C_i) \oplus C_{i-1}$

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

Trojanisches Pferd greift von innen an

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



verschlüsselte Festplatte und Kommunikation

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

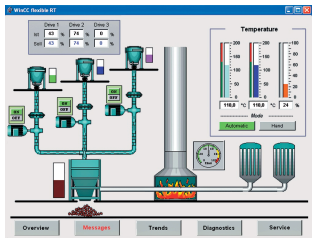
Stuxnet

- 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

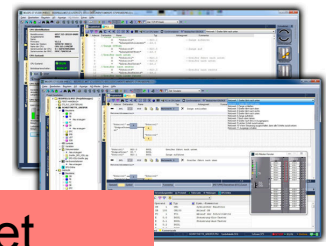

Bild von Natanz (Majid Saeedi/Getty Images)

Stuxnet - Szenario (Industrieanlage)

Intranet



IDE
(Siemens Step 7)



Stuxnet

Wechseldatenträger

isoliertes Netzwerk

Prozess-visualisierung (Siemens WinCC)

Programmierung (Siemens Field PG) Step 7

Stuxnet

Stuxnet

Speicherprogrammierbare Steuerung (Siemens Simatic SPS)

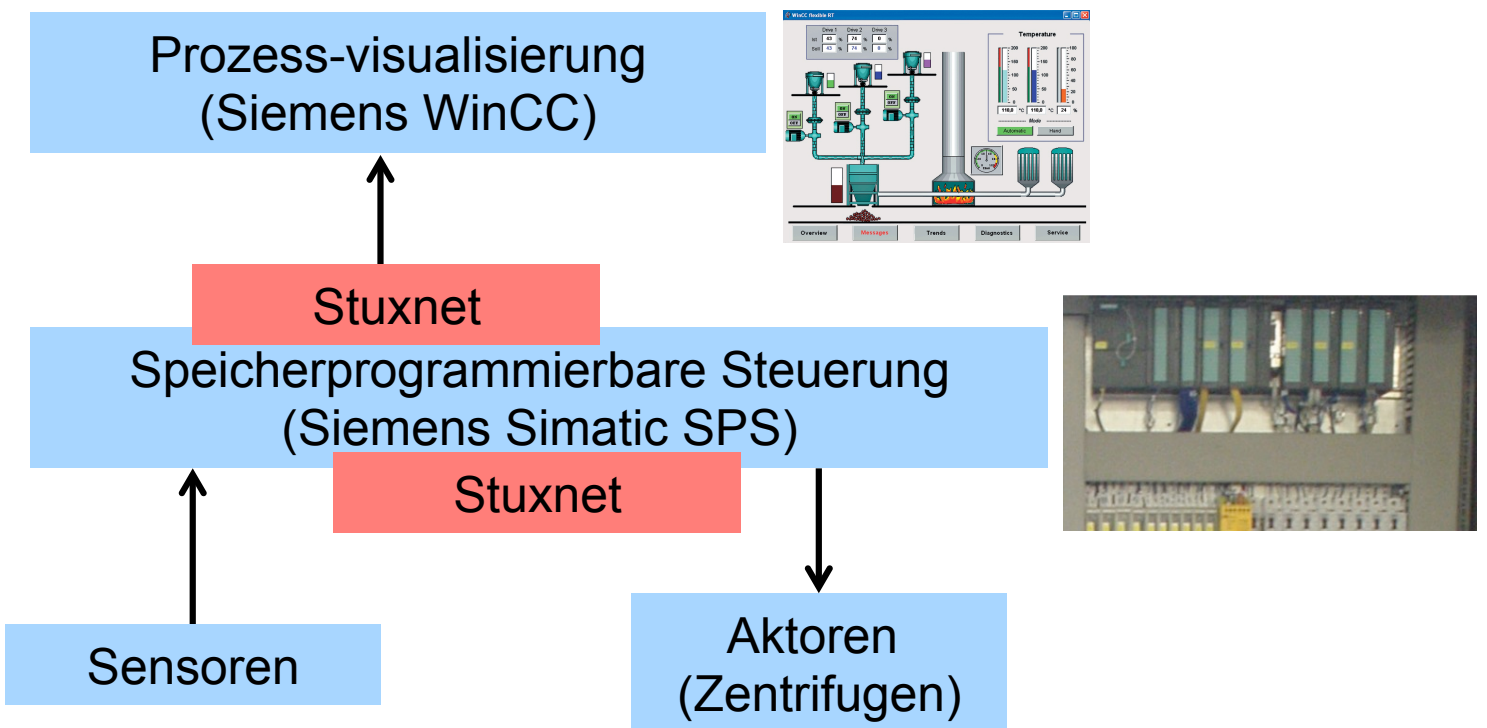
Stuxnet

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

Gliederung

- Einführung
- Angriff
  - »Bundestrojaner« und das neue Computergrundrecht
  - stattliche Angriffe auf IT-Systeme anderer Staaten
- Schutz
  - Gnu Privacy Guard
  - AN.ON – Anonymity Online
- Schlussbemerkungen

Gnu Privacy Guard (GnuPG)

- sehr bekanntes frei verfügbares Verschlüsselungsprogramm
- amerikanisches Vorbild Pretty Good Privacy (PGP)
- seit 1997 entwickelt

Open Source: Der Quellcode von GnuPG kann von Jedem geprüft, geändert und compiliert werden.

Pretty Good Privacy (PGP)

- ab 1991 von Phil Zimmermann als Open Source entwickelt
- 1997 kommerzialisiert

- Bereitstellung einer »internationalen« PGP-Version
  - US-Exportrestriktionen (starke Kryptographie gleichgesetzt mit Waffen) für digitale Version
  - Ausdruck und Ausfuhr des Quellcodes aus USA war jedoch erlaubt

- Ab Ende der 1990er Jahre gelockerte US-Exportrestriktionen
  - Ausfuhr auch für Programme mit >40 Bit Schlüssellänge erlaubt

Ab 1995 wurden die Quellcodes in Europa gescannt, compiliert und als PGPi bereitgestellt

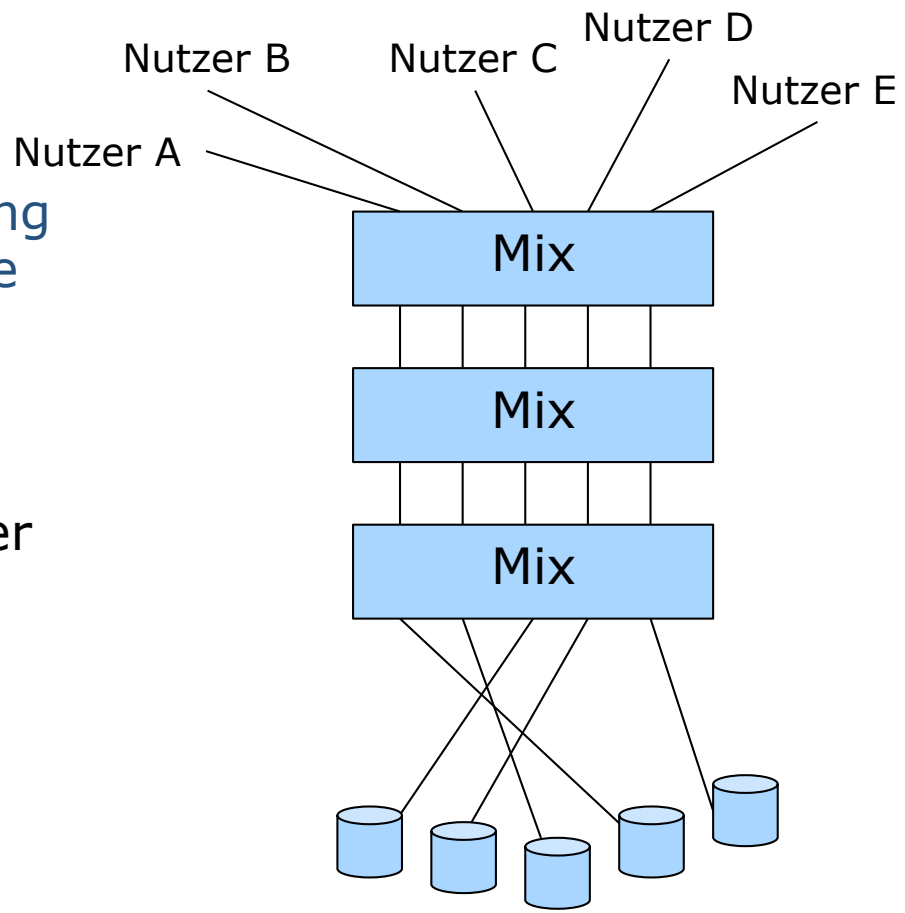
Gnu Privacy Project

- ab 2002 Bereitstellung einer Windows-Version
- Projektförderung durch BMWi und BMI
- Ziel: GnuPG somit für alle (relevanten) Plattformen verfügbar machen

Es sind bis heute keine ernsthaften Sicherheitslücken von GnuPG bekannt geworden.

AN.ON – http://www.anon-online.de

- Implementierung eines Dienstes zum anonymen Internetzugriff
- Schaffen einer praktikablen Lösung für anonyme und unbeobachtbare Basiskommunikation
  - beruht auf Erweiterungen des Mix-Verfahrens von Chaum
  - Schutz auch vor dem Betreiber des Dienstes (Schutz vor Insidern)
- Schutz des Einzelnen vor Überwachung und Profilierung seiner Internetaktivitäten auch durch private Organisationen



AN.ON/JAP

Förderer: BMWi, Projektpartner: TU Dresden, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, FU Berlin, HU Berlin, Universität Regensburg, Medizinische Universität Lübeck, Chaos Computer Club, Ulmer Akademie für Datenschutz und IT-Sicherheit, RWTH Aachen, New York University

Ziele:

Schaffen einer praktikablen Lösung für anonyme und unbeobachtbare Basiskommunikation

Schutz auch vor dem Betreiber des Dienstes (Schutz vor Insidern)

www.anon-online.de

Juristische Sicht

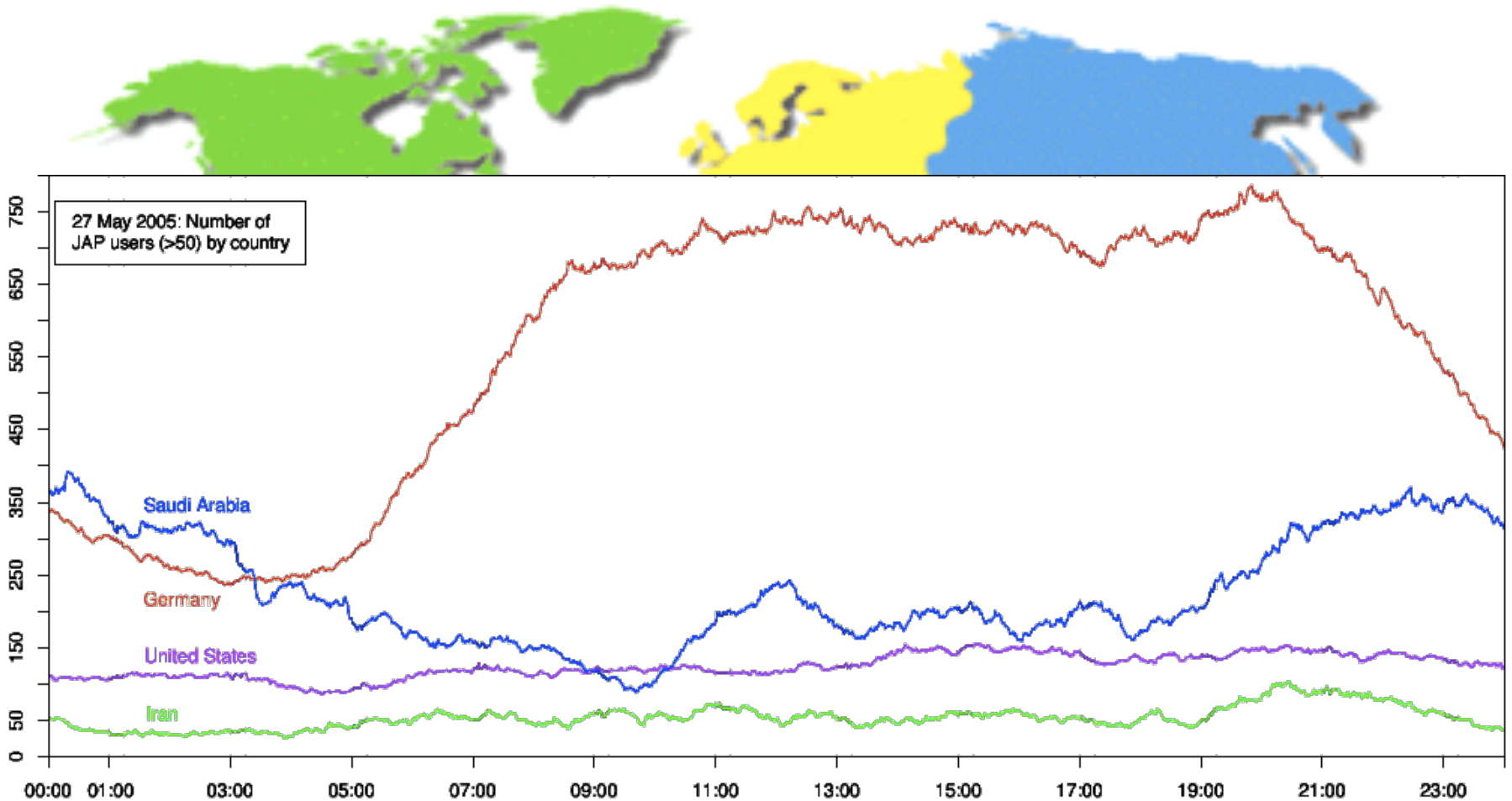
- Telemediengesetz (TMG, vormals Teledienstedatenschutzgesetz TDDSG)
  - § 13 Abs. 6 TMG: Der Diensteanbieter hat dem Nutzer die Inanspruchnahme von Telediensten und ihre Bezahlung anonym oder unter Pseudonym zu ermöglichen, soweit dies technisch möglich und zumutbar ist. Der Nutzer ist über diese Möglichkeit zu informieren.

Unerwarteter Sekundäreffekt:

Unterstützung der Meinungsfreiheit in Diktaturen

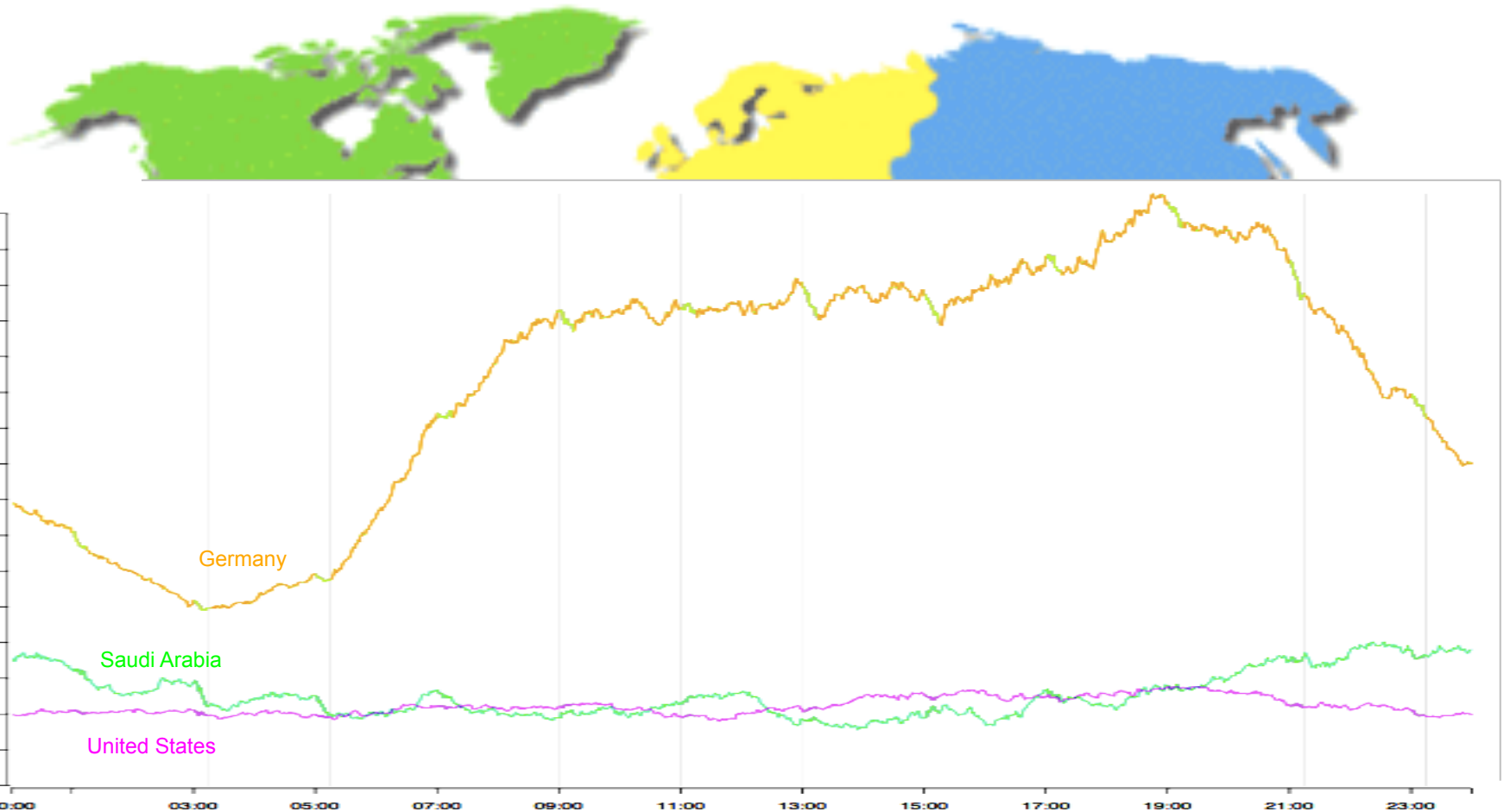
Wo kommen die JAP-Nutzer her?

- Dayline of May 27, 2005



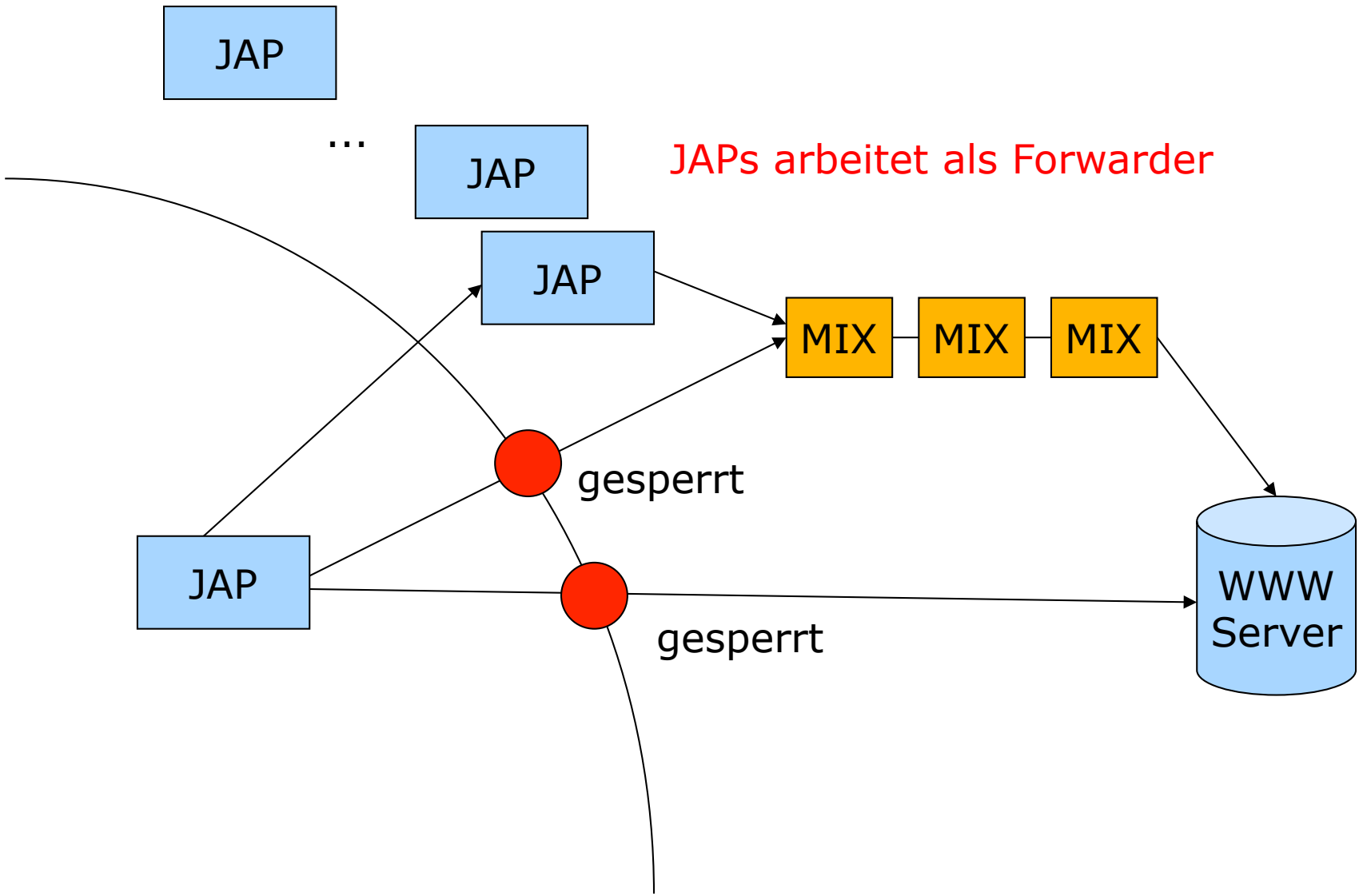
Wo kommen die JAP-Nutzer her?

- Dayline of Aug 1, 2005

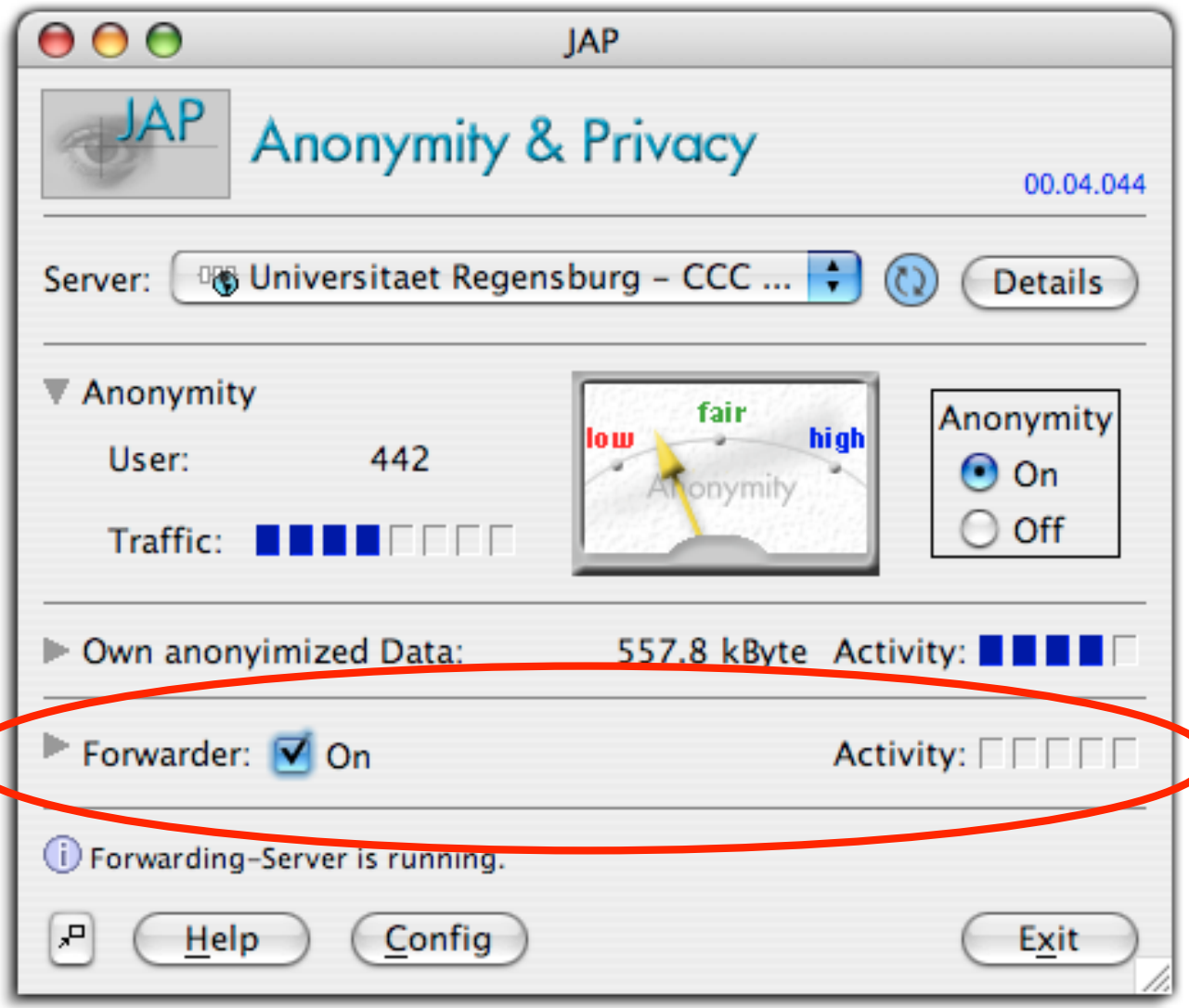


Iran?

Blockingresistenz



Blockingresistenz

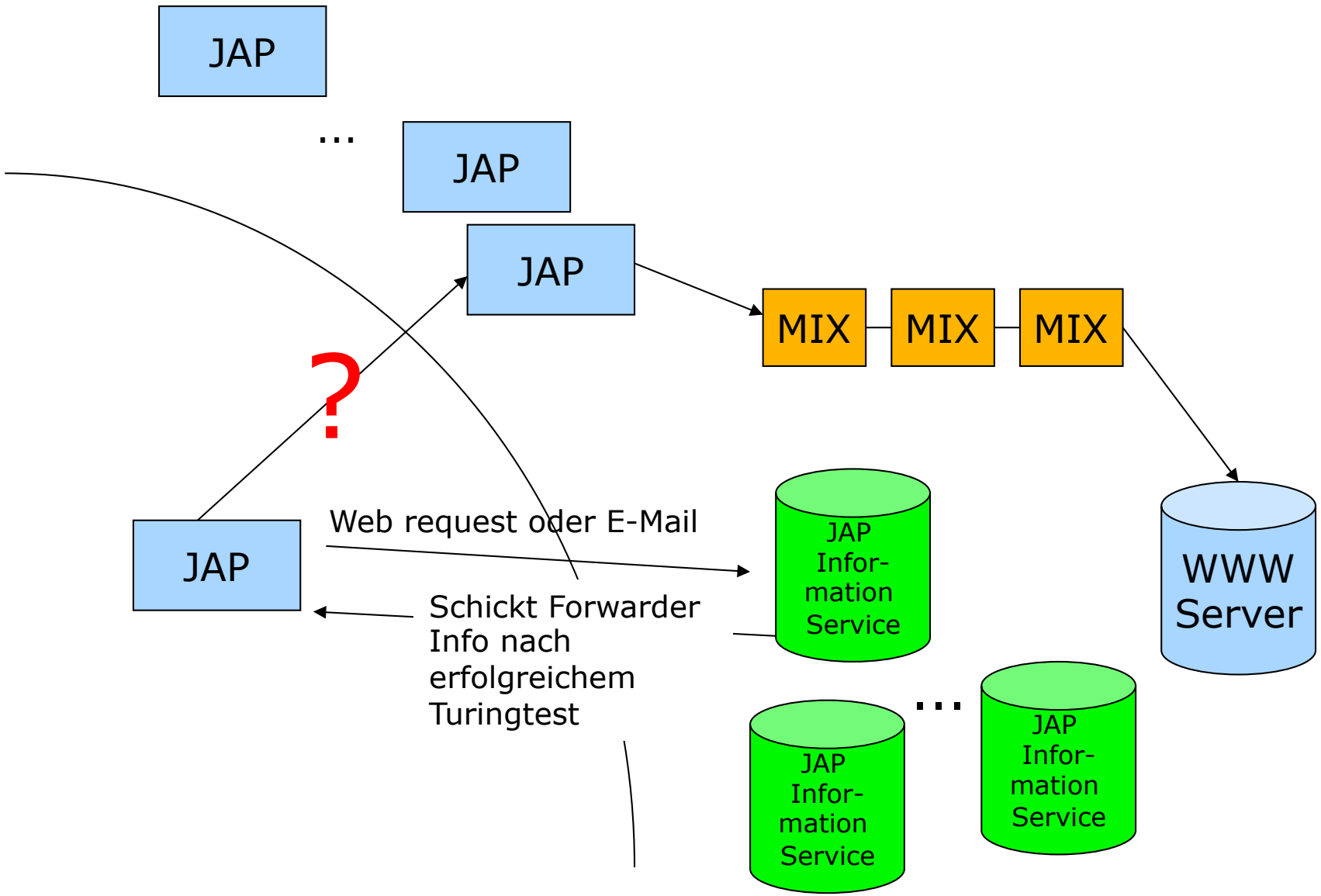


JAP-Nutzer stellen Teil ihrer Bandbreite zur Verfügung

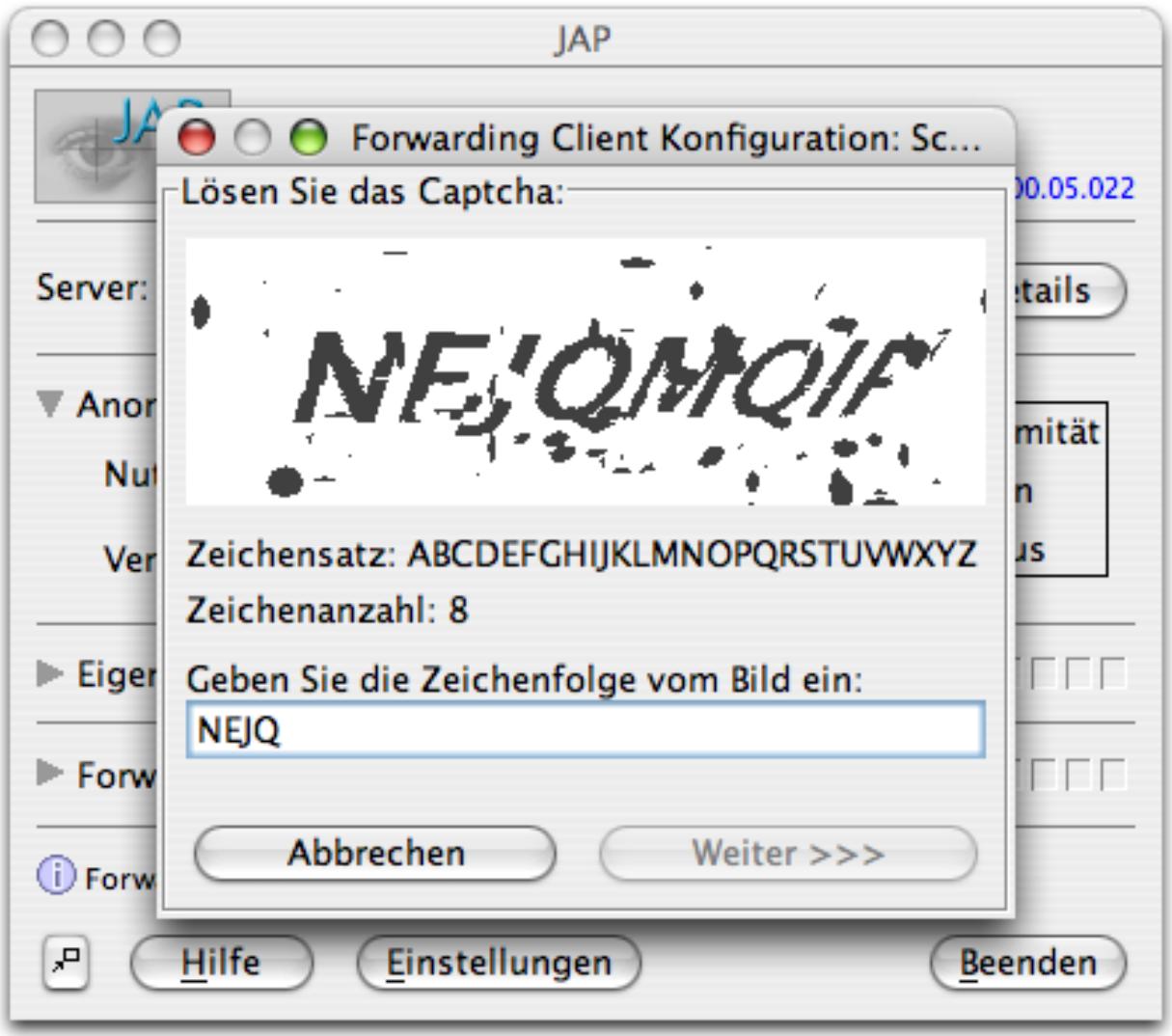
Zugriffe werden durch die Mixe anonymisiert

Forwarder erfahren nichts über die zugegriffenen Inhalte

Blockingresistenz

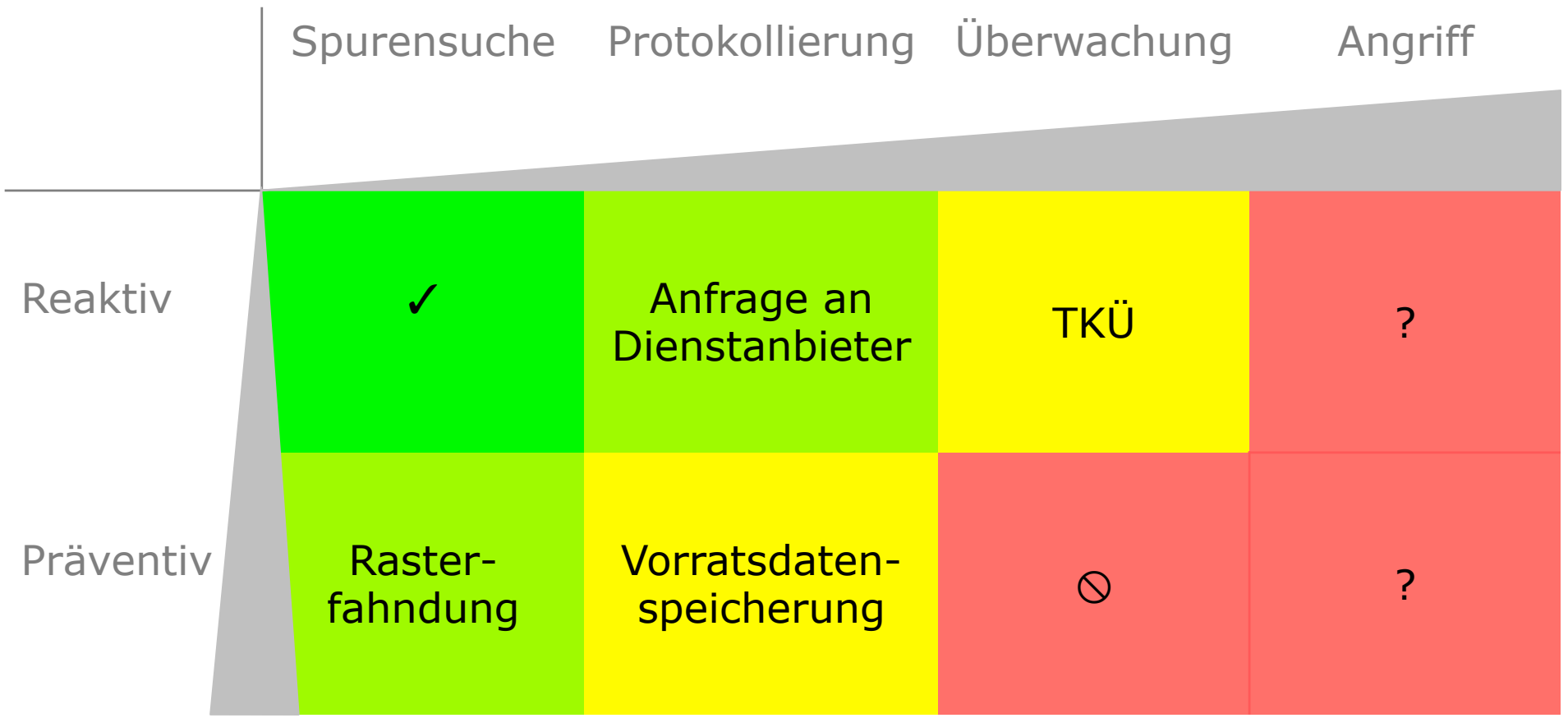


Blockingresistenz



InfoService schickt Forwarder Info nach erfolgreichem Turingtest

Eingriffstiefe in die Freiheit



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