Schutz der Privatsphäre im Internet

Prof. Dr. Hannes Federrath
Universität Regensburg
http://www-sec.uni-regensburg.de

Universität Regensburg

Vortrag an der Berufsschule B6,
Nürnberg, 18.1.2011

Schutzziele (Voydock, Kent 1983)

- Klassische IT-Sicherheit berücksichtigt im Wesentlichen Risiken, die durch *regelwidriges Verhalten* in IT-Systemen entstehen.

Vertraulichkeit	unbefugter Informationsgewinn
Integrität	unbefugte Modifikation
Verfügbarkeit	unbefugte Beeinträchtigung der Funktionalität

Schutzziele

Inhalte der Kommunikation	Kommunikationsumstände
Vertraulichkeit	**Anonymität** **Unbeobachtbarkeit** **Sender** **Ort** **Empfänger**

- 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

Angreifermodell: Datenschutzfördernde Technik

Inhalte der Kommunikation	Kommunikationsumstände
Vertraulichkeit	**Anonymität** **Unbeobachtbarkeit** **Sender** **Ort** **Empfänger**

- Outsider
  - Abhören auf Kommunikationsleitungen
  - Verkehrsanalysen
- Insider
  - Netzbetreiber oder bösartige Mitarbeiter (Verkehrsprofile)
  - Staatliche Organisationen (insb. fremde)

Prinzipien: Datenschutzfördernde Technik

Inhalte der Kommunikation	Kommunikationsumstände
Vertraulichkeit	**Anonymität** **Unbeobachtbarkeit** **Sender** **Ort** **Empfänger**

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

Historische Entwicklung

Jahr	Idee / PET system
1978	Public-key encryption
1981	MIX, Pseudonyms
1983	Blind signature schemes
1985	Credentials
1988	DC network
1990	Privacy preserving value exchange
1991	ISDN-Mixes
1995	Blind message service
1995	Mixmaster
1996	MIXes in mobile communications
1996	Onion Routing
1997	Crowds Anonymizer
1998	Stop-and-Go (SG) Mixes
1999	Zeroknowledge Freedom Anonymizer
2000	AN.ON/JAP Anonymizer
2004	TOR

Grundverfahren
Anwendung

Anonymität im Internet ist eine Illusion

- Wer ist der Gegner?
  - Konkurrenz
  - Geheimdienste fremder Länder
  - Big Brother
  - Systemadministrator
  - Nachbar ...
- Lesenswert: Interception Capabilities 2000
  - http://www.cyber-rights.org/interception/stoa/interception_capabilities_2000.htm

Funküberwachungsantenne (AN/FLR9) (aus Interception Capabilities 2000)

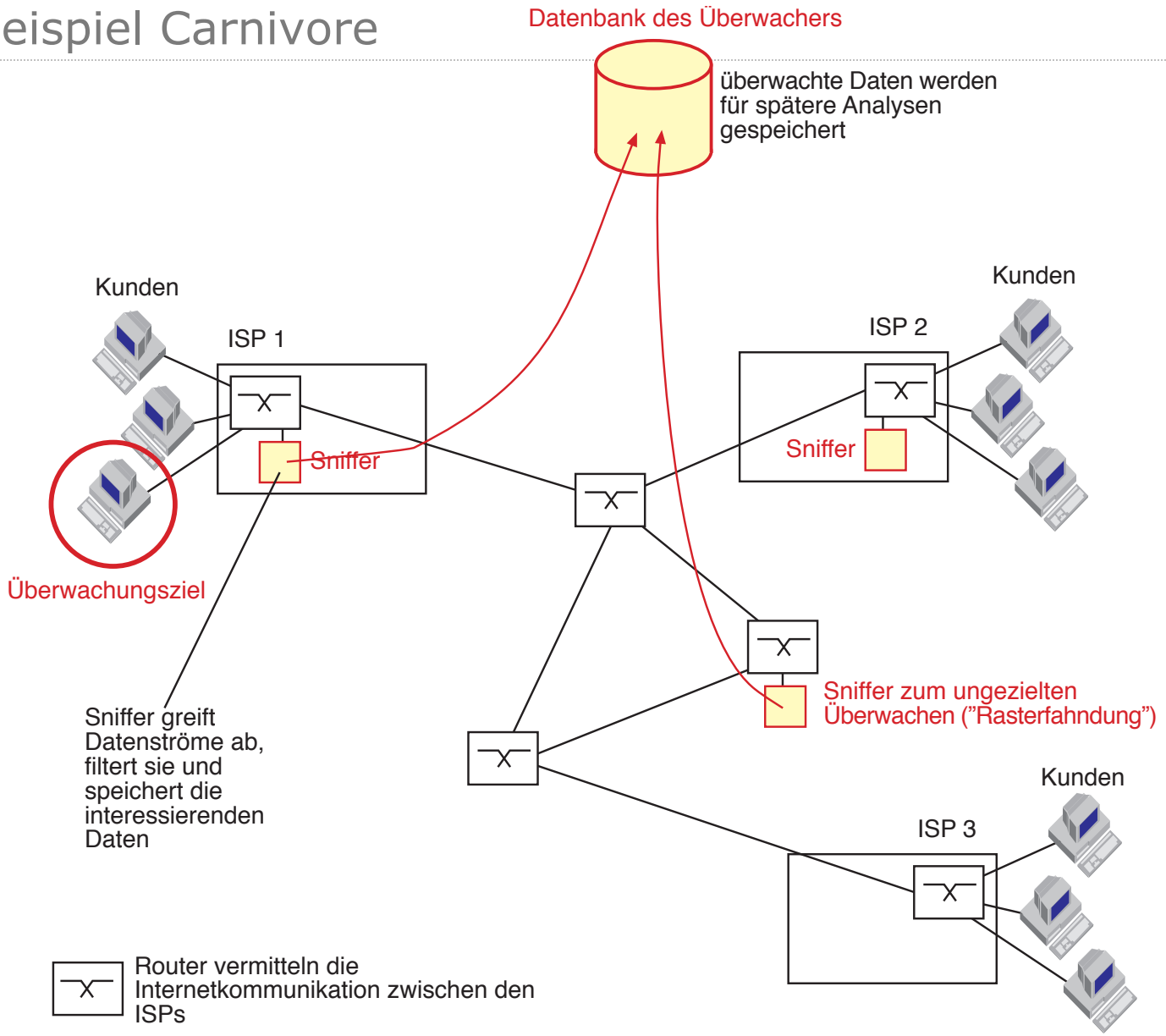
Anonymität im Internet ist eine Illusion

- Wer ist der Gegner?
  - Konkurrenz
  - Geheimdienste fremder Länder
  - Big Brother
  - Sys-admin
  - Nachbar ...

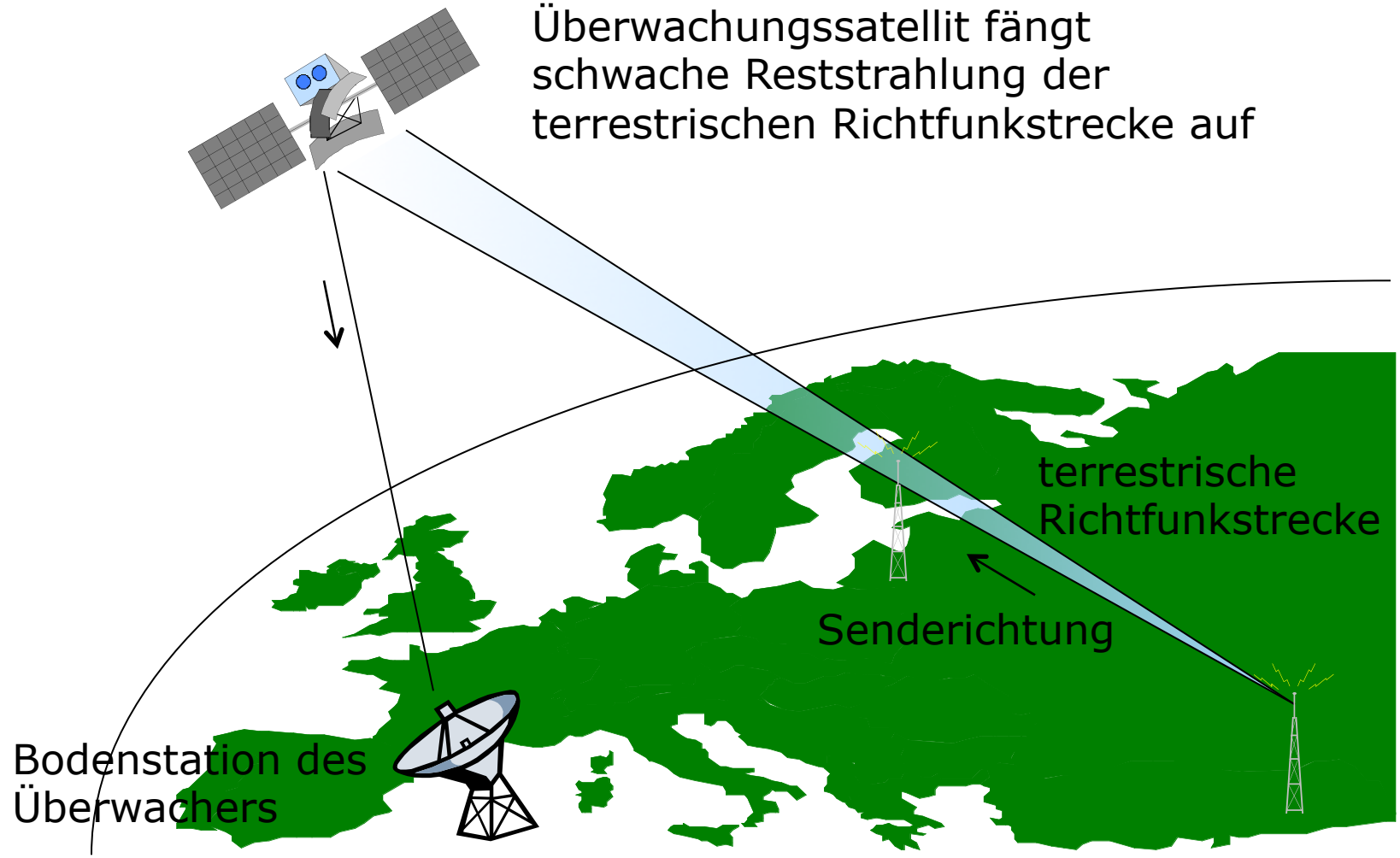
Bad Aibling Interception facility of the ECHELON system

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

Sniffing: Beispiel Carnivore



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.

Anonymität im Internet ist eine Illusion

Electronic Mail: Log-Dateien zeigen Kommunikationsbeziehungen

```
>tail syslog
Oct 15 16:32:06 from=<feder@tcs.inf.tu-dresden.de>, size=1150
Oct 15 16:32:06 to=<hf2@irz.inf.tu-dresden.de>
```

World Wide Web: Log-Dateien zeigen Interessensdaten

```
wwwtcs.inf.tu-dresden.de>tail access_log
amadeus.inf.tu-dresden.de - - [15/Oct/1997:11:50:01] "GET
/lvbeschr/winter/TechnDS.html HTTP/1.0" - "http://wwwtcs.inf.tu-
dresden.de/IKT/" "Mozilla/3.01 (X11; I; SunOS 5.5.1 sun4u)"
```

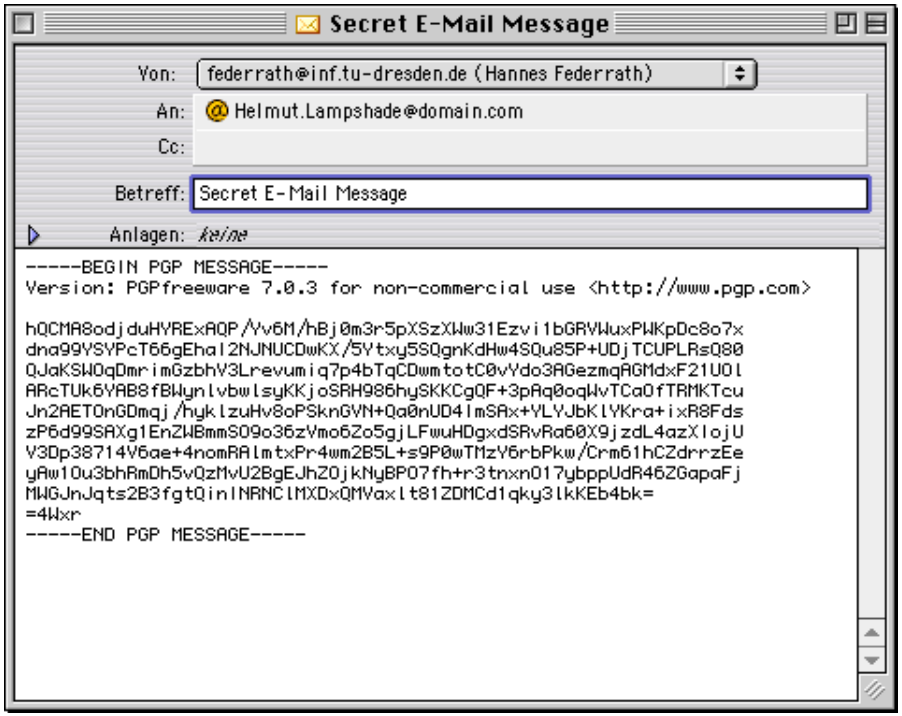
Referer

Finger: Die Ermittlung eines Rechnerbenutzers ist kein Problem

```
ithif19 logs 17 >finger @amadeus.inf.tu-dresden.de
[amadeus.inf.tu-dresden.de]
Login       Name                TTY         Idle    When
feder    Hannes Federrath       console             Wed 11:56
```

Hilft Verschlüsselung?

- Verschlüsseln hilft gegen Ausspähen der *Inhalte*



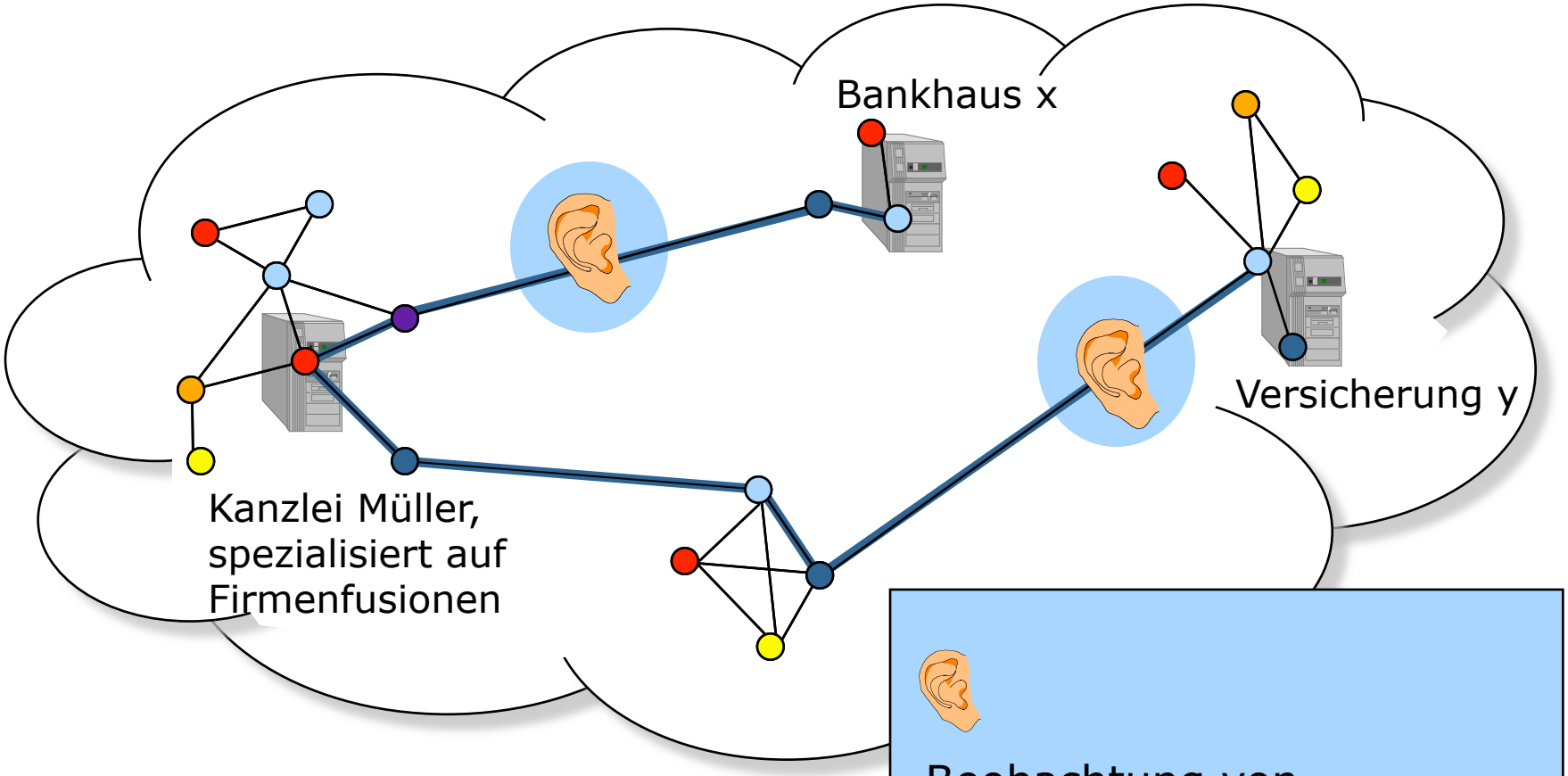
Trotzdem PGP verwenden!

Pretty Good Privacy

http://www.pgp.com

Verschlüsseln hilft überhaupt nichts gegen Beobachtung von Kommunikationsbeziehungen

> Warum genügt Verschlüsselung nicht?



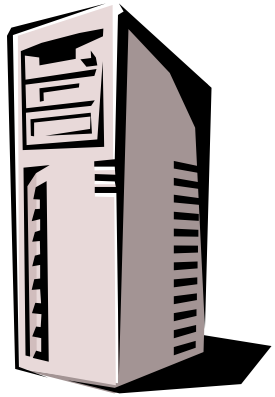
IP-Adressen zur Überwachung

- Statische IP-Adressen
  - stellen ein Personenpseudonym dar
  - sehr leichte Verkettbarkeit der Benutzeraktionen

Adresse:
123.86.9.5
(federrath.uni-regensburg.de)

GET www.buchshop.de
To: 195.66.15.4
From: 123.86.9.5

HTTP ...
To: 123.86.9.5
From: 195.66.15.4



Adresse:
195.66.15.4

  - fahrlässig:
    - DNS-Name mit Personenbezug
- Einschränkung:
  - Zuweisung dynamischer IP-Nummern bei Einwahlzugang

IP-Adressen zur Überwachung

- Überwachung durch Internet Service Provider (ISP)
  - selbst bei dynamischer Adressenvergabe kann eigener ISP problemlos Nutzeraktionen verketten

- Beispiel:
  - http://www.predictivenetworks.com/

Cookies

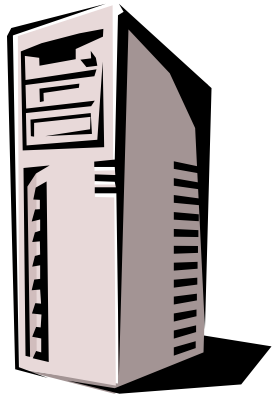
Cookies können zur Überwachung eingesetzt werden

- Funktionsweise von Cookies

Erster Besuch:

1. GET www.buchshop.de →

← 2. Set Cookie: id=12241235564



3. ggf. Warnung

4. Speichern auf Festplatte

Folgende Besuche:

GET www.buchshop.de
Cookie: id=12241235564 →

  - wird nur an zugehörigen Server zurückgesendet
  - hat ein vom Server definiertes Verfallsdatum
  - wird auch bei Abruf eingebetteter Objekte gesendet (z.B. Bilder)

Cookies

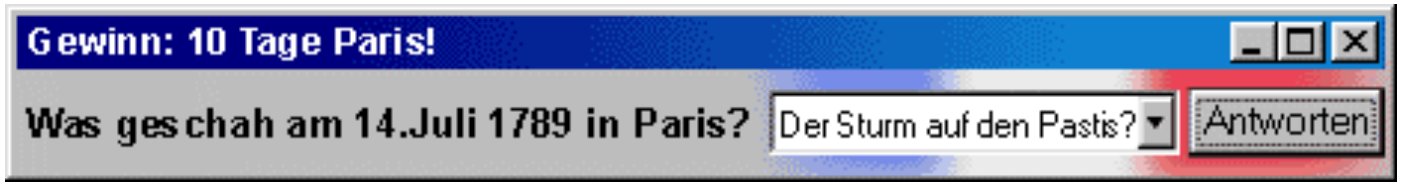
- Ungefährliche Kekse
  - Löschen nicht die Festplatte
  - Übertragen keine Viren
  - Verraten keine lokal gespeicherten Daten
    - Passwörter, geheime Schlüssel usw.

- Webserver erkennt Nutzer bei jedem Besuchen seiner Seite wieder
  - Positiv:
    - personalisierte Webseiten
  - Negativ:
    - Erstellung von Nutzerprofilen

- Cookie-Standards
  - RFC 2109 (HTTP State Management Mechanism)
  - RFC 2964 (Use of HTTP State Management)

Gefährliche Kekse ! Third-Party Cookies

- Laden eines eingebetteten Bildes (z.B. Werbebanner) von einem fremden Server (z.B. Werbering)
  - Werbering setzt Cookie
  - Referer verrät Herkunft des Requests
- Werberinge (z.B. Doubleclick.com):
  - Plazieren Banner auf Seiten vieler Anbieter
  - Banner von zentralem Server geladen, Cookie wird gesendet
  - Werbeserver erhält globales Nutzungsprofil
- Verschiedene Shops arbeiten mit demselben Werbering zusammen:
  - Website A (z.B. Bookshop)
  - Website B (z.B. Gesundheitsberatung)
  - Website C (z.B. Lebensversicherung)

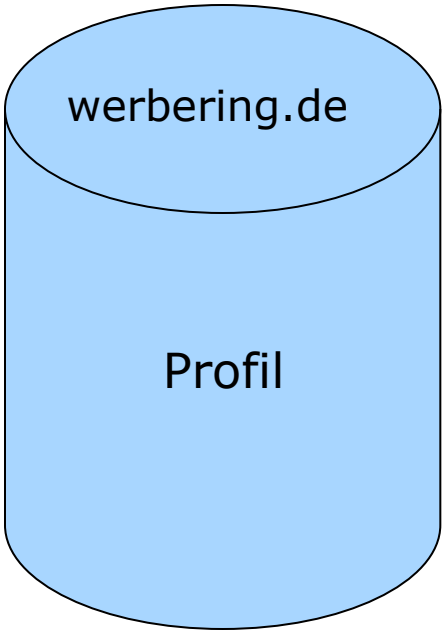


Third-Party Cookies

GET http://werbering.de/werbebanner1.gif
Cookie: guid=8867563
Referer: http://www.bookshop.de

GET http://werbering.de/werbebanner3.gif
Cookie: guid=8867563
Referer: http://www.gesundheitsberatung.de

GET http://werbering.de/werbebanner2.gif
Cookie: guid=8867563
Referer: http://www.lebensversicherung.de

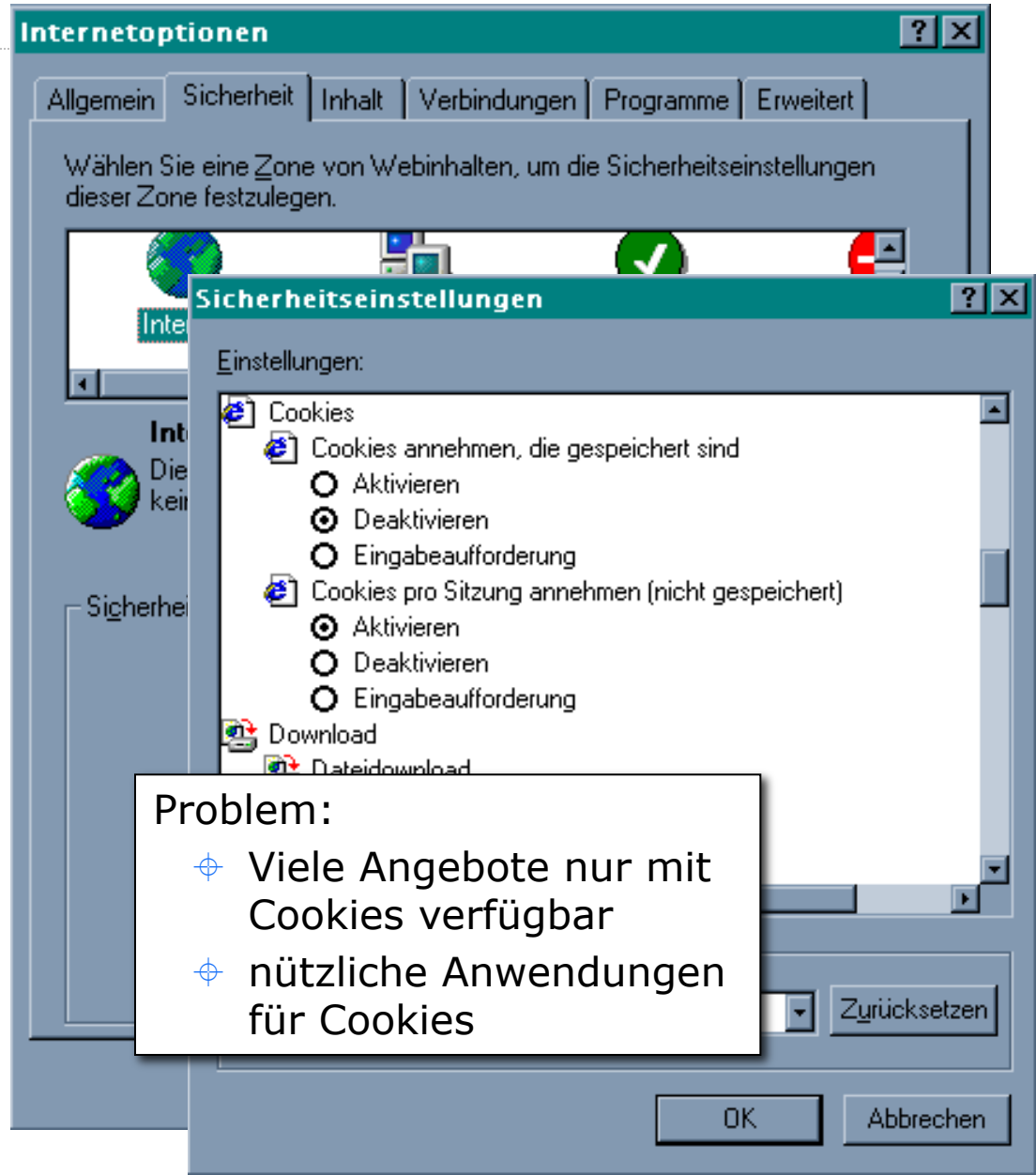


Gläserner Bürger? Legal?

Gegenmaßnahmen

Cookies

- deaktivieren
- nur bei ausgewählten Seiten speichern
- regelmäßig löschen
- filtern
- regelmäßig weltweit austauschen



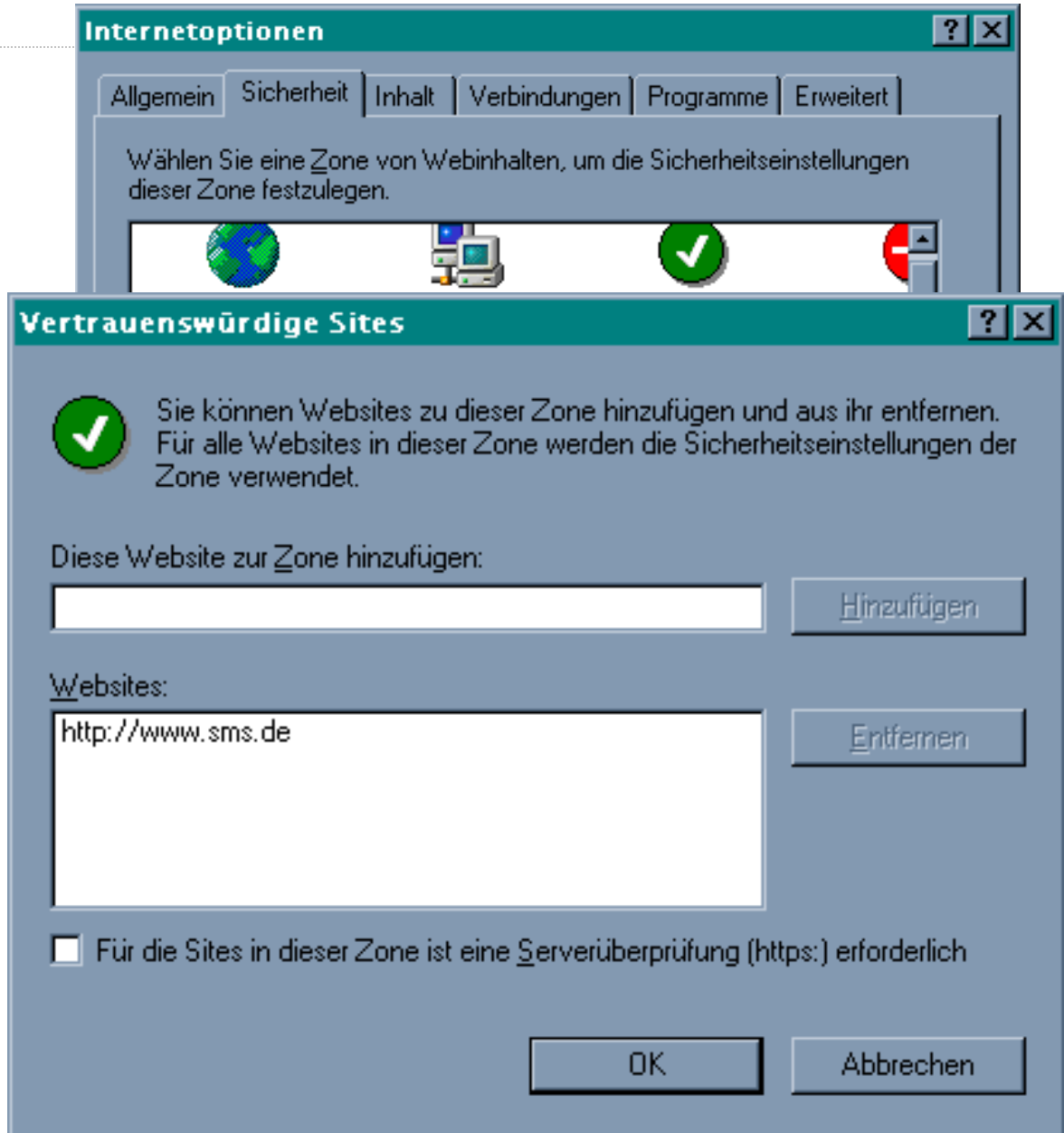
Problem:

- Viele Angebote nur mit Cookies verfügbar
- nützliche Anwendungen für Cookies

Gegenmaßnahmen

Cookies

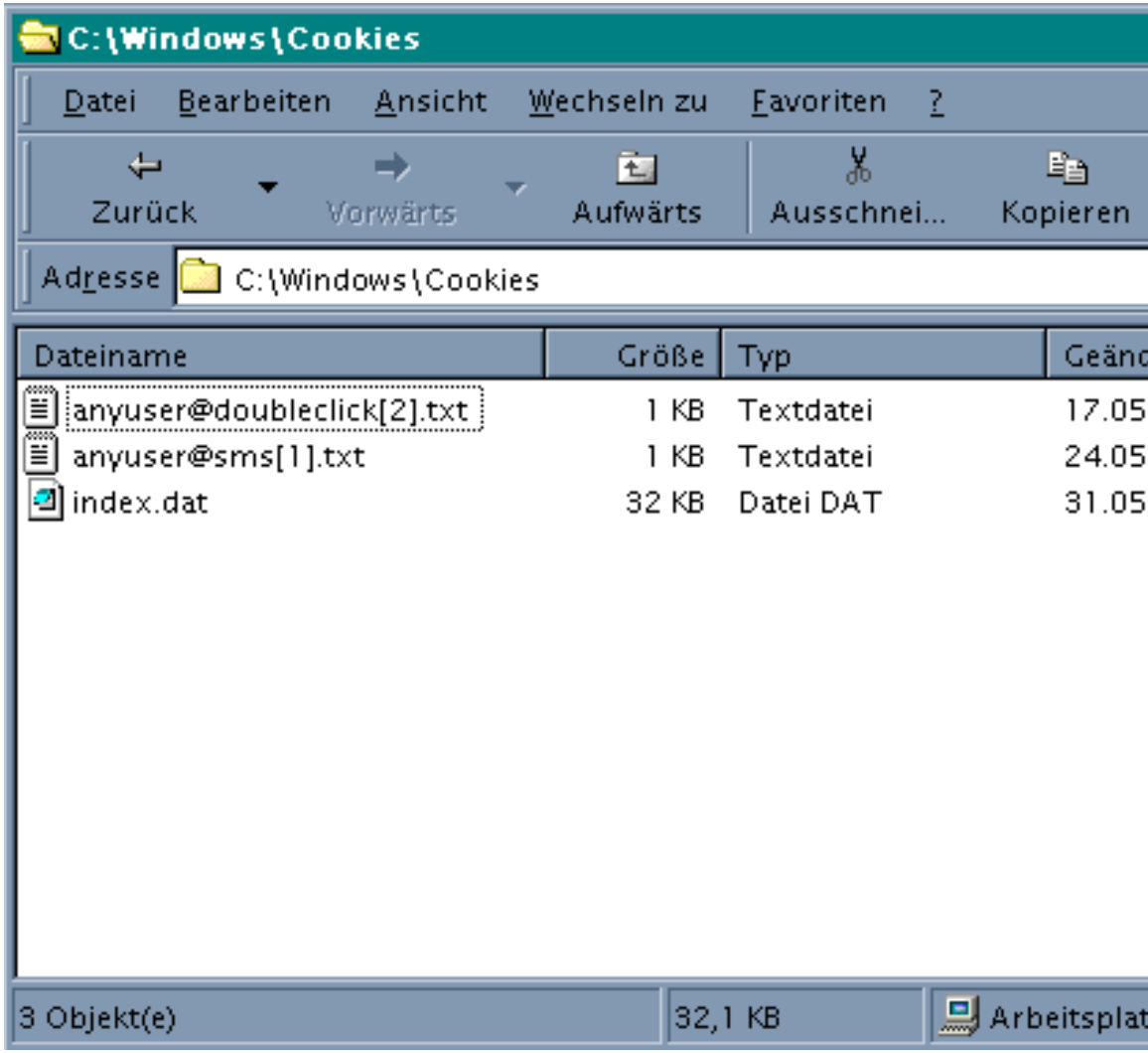
- deaktivieren
- nur bei ausgewählten Seiten speichern
- regelmäßig löschen
- filtern
- regelmäßig weltweit austauschen



Gegenmaßnahmen

Cookies

- deaktivieren
- nur bei ausgewählten Seiten speichern
- regelmäßig löschen
- filtern
- regelmäßig weltweit austauschen



Gegenmaßnahmen

Cookies

- deaktivieren
- nur bei ausgewählten Seiten speichern
- regelmäßig löschen
- filtern
- regelmäßig weltweit austauschen

http://www.junkbusters.com/

http://www.guidescope.com/

THE GUIDESCOPE MENU

http://www.webwasher.com

Gegenmaßnahmen

Cookies

- deaktivieren
- nur bei ausgewählten Seiten speichern
- regelmäßig löschen
- filtern
- regelmäßig weltweit austauschen

www.CookieCooker.de

CookieCooker

- Filter software für Cookies
  - ähnlich JunkBuster und WebWasher

- Aktiver Schutz durch Cookie-Austausch

- Identitätsmanager

www.CookieCooker.de

CookieCooker

- Idee:
  - Aktiver Schutz durch Cookie-Austausch zwischen Nutzern
  - Andere Personen surfen unter dem fremden Cookie
  - Verfälschung der Nutzerprofile

- Unterscheidung nötig zwischen nützlichen und ungewollten Cookies

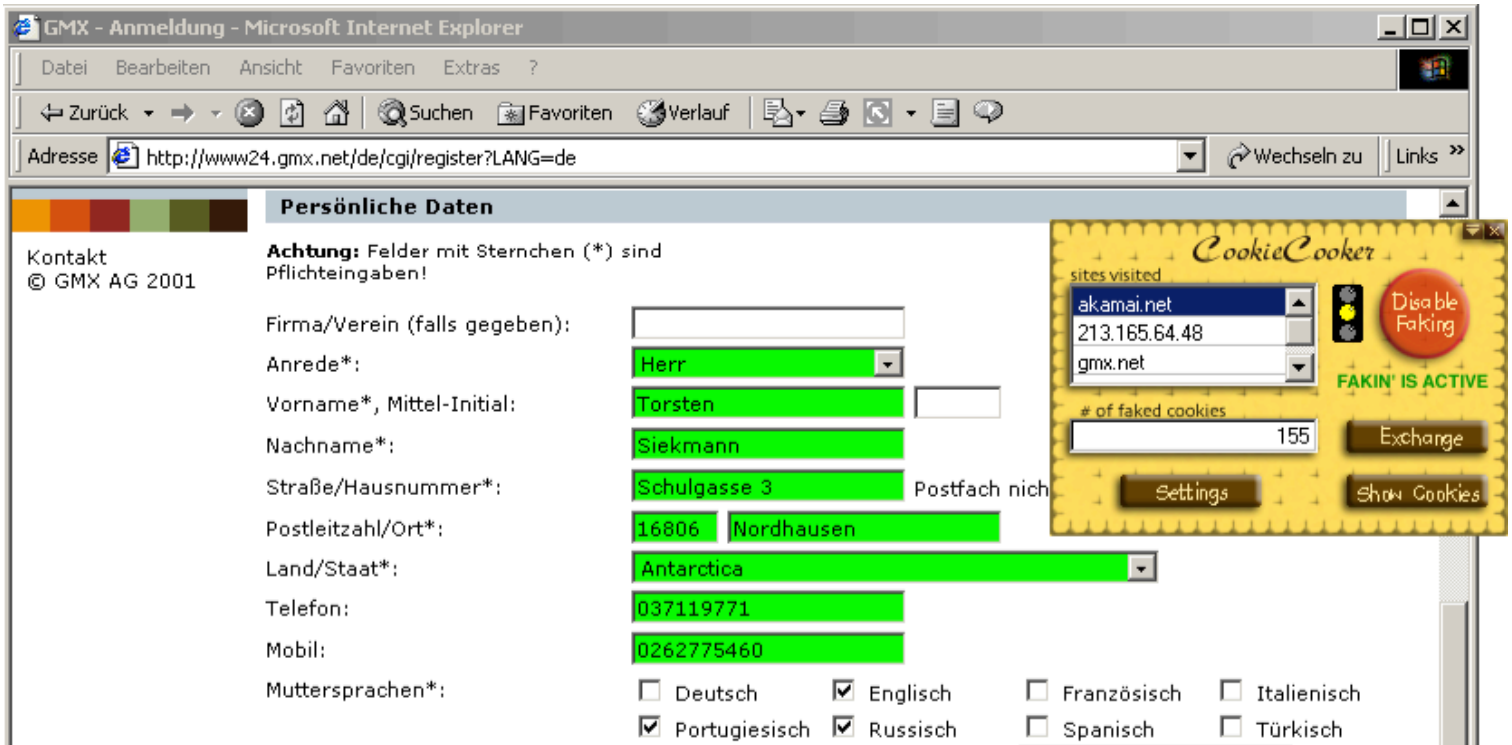
- Cookie-Austausch über Peer-to-Peer-Service

www.CookieCooker.de

CookieCooker

- Automatisiertes Ausfüllen von Web-Formularen
  - sehr schnelles Anlegen von Free-Mail-Accounts

- Identitätsmanagement
  - Cookie Cooker merkt sich (pseudonyme) Zugangsdaten (Name/ Passwort etc.)



Beispiele für Bausteine datenschutzfördernder Technik

- Verschlüsselung
- Schutz von Kommunikationsbeziehungen
  - Schutz vor Outsidern
    - Proxies
  - Schutz vor Insidern und Outsidern
    - Broadcast
    - DC network
    - 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

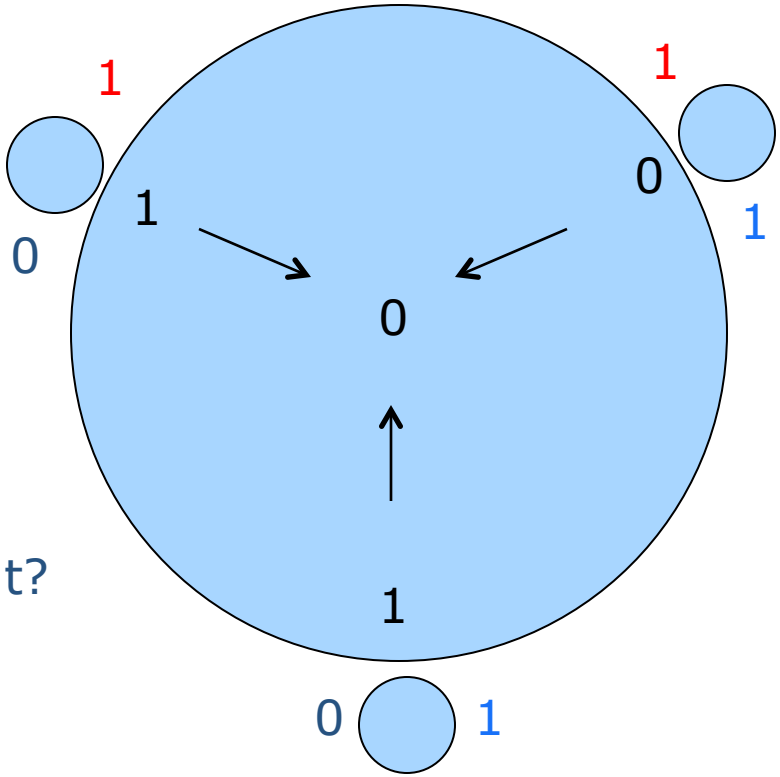
Vermittelter Zugang zu Inhalten

- Heute:
  - Video on Demand
  - Internet-Radio
  - Zeitungen online
  - Plötzlich stehen Nutzungsdaten zur Verfügung.
  - Der Kunde wird gläsern.
- Damals: (Broadcast)
  - Zeitung lesen
  - Radio über Antenne hören
  - Fernsehen über Breitbandverteilkabel

DC network (Chaum, 1988)

- Jeder für sich:
  1. Jeder wirft mit jeden eine Münze
  2. Berechnet das xor der beiden Bits
  3. Wenn bezahlt, dann xor mit 1 (Komplement des Ergebnisses aus Schritt 2)
  4. Ergebnis veröffentlichen

- Alle zusammen:
  1. Berechnen das xor der drei (lokalen) Ergebnisse
  2. Wenn globales Ergebnis 0, hat jmd. anderes bezahlt



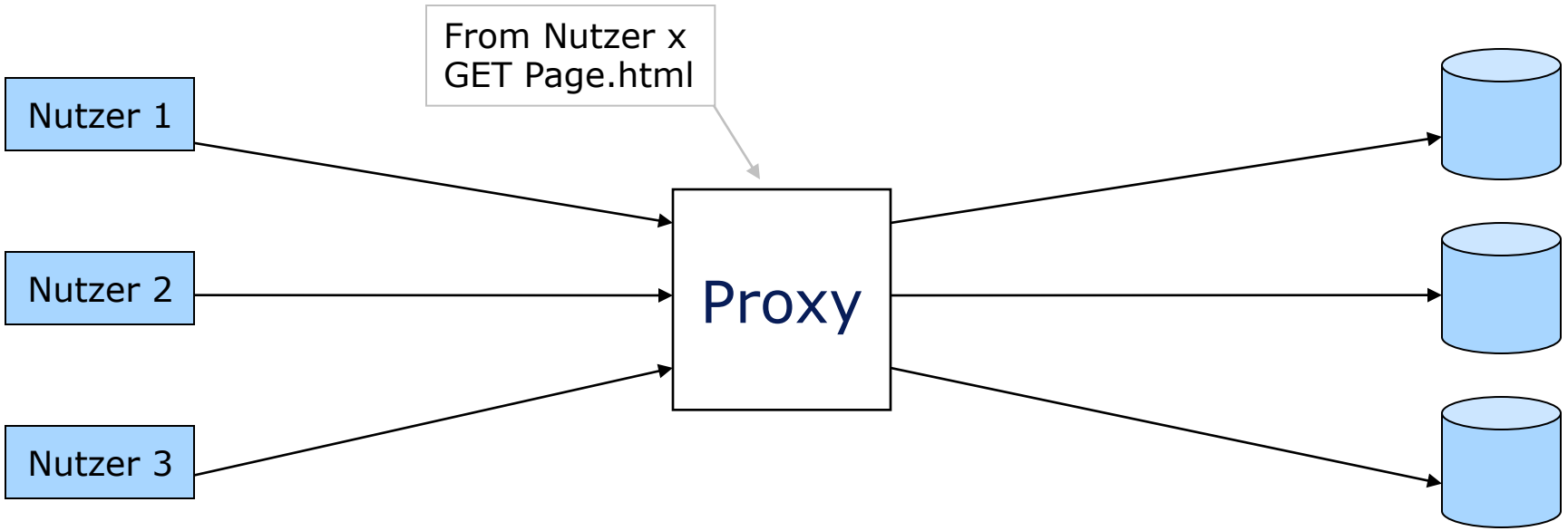
Wer hat bezahlt?

Beispiele für Bausteine datenschutzfördernder Technik

- Verschlüsselung
- Schutz von Kommunikationsbeziehungen
  - Schutz vor Outsidern
    - Proxies
  - Schutz vor Insidern und Outsidern
    - Broadcast
    - DC network
    - MIX network
- Schutz von Transaktionen
  - Pseudonyme
  - Credentials (an Pseudonyme gekettete Eigenschaften)

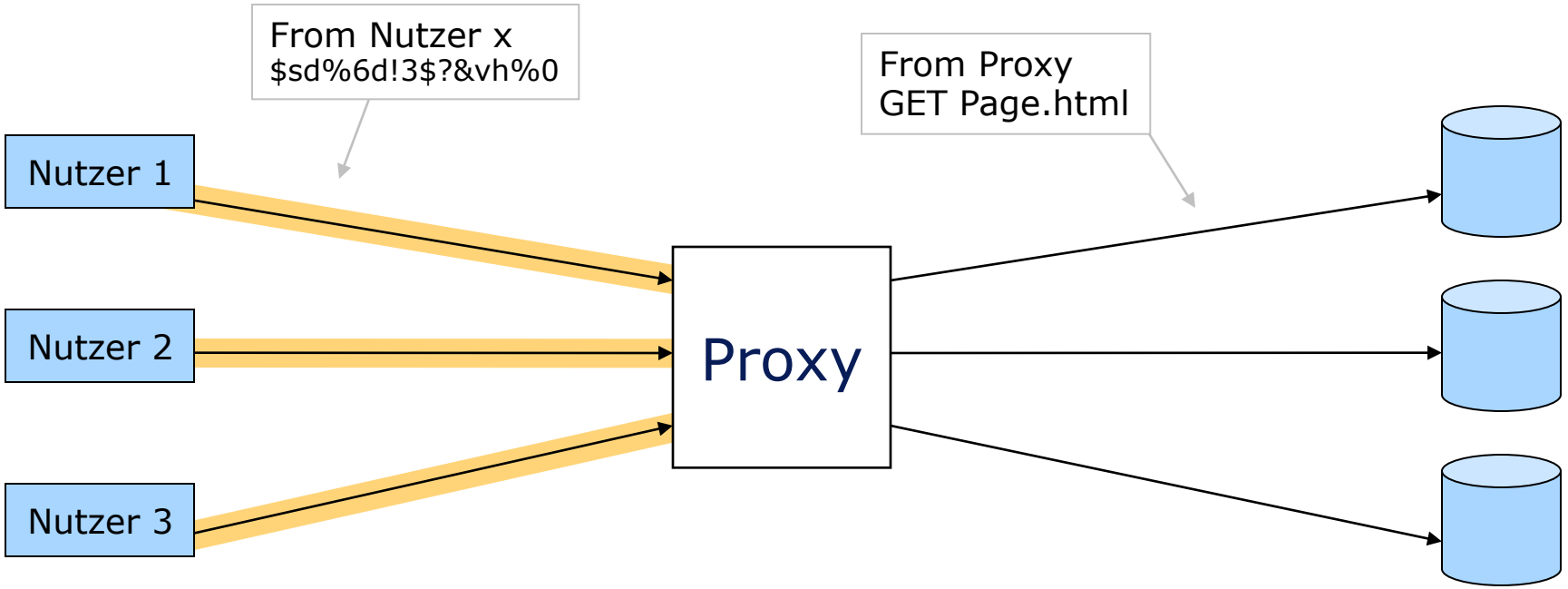
Proxies: Insider

- Erreichbare Sicherheit (Insider)
  - Kein Schutz gegen den Betreiber des Proxy



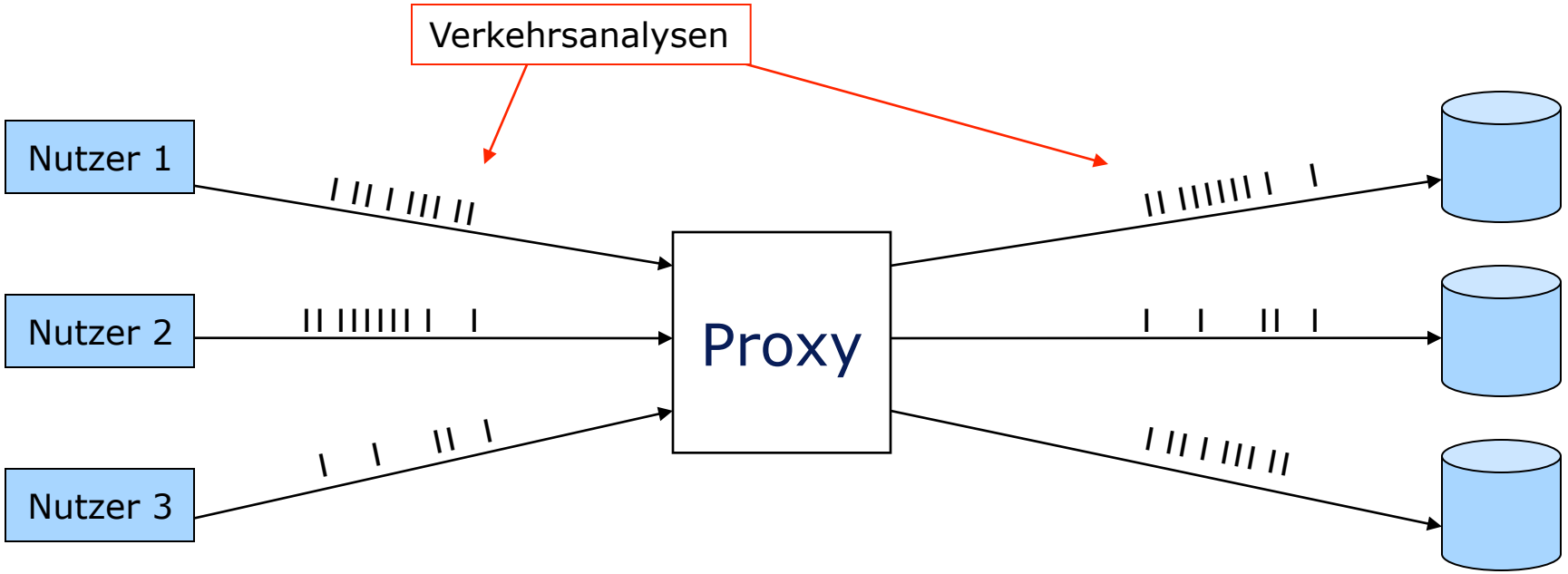
Proxies: Outsider

- 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



Mix-Netz (Chaum, 1981)

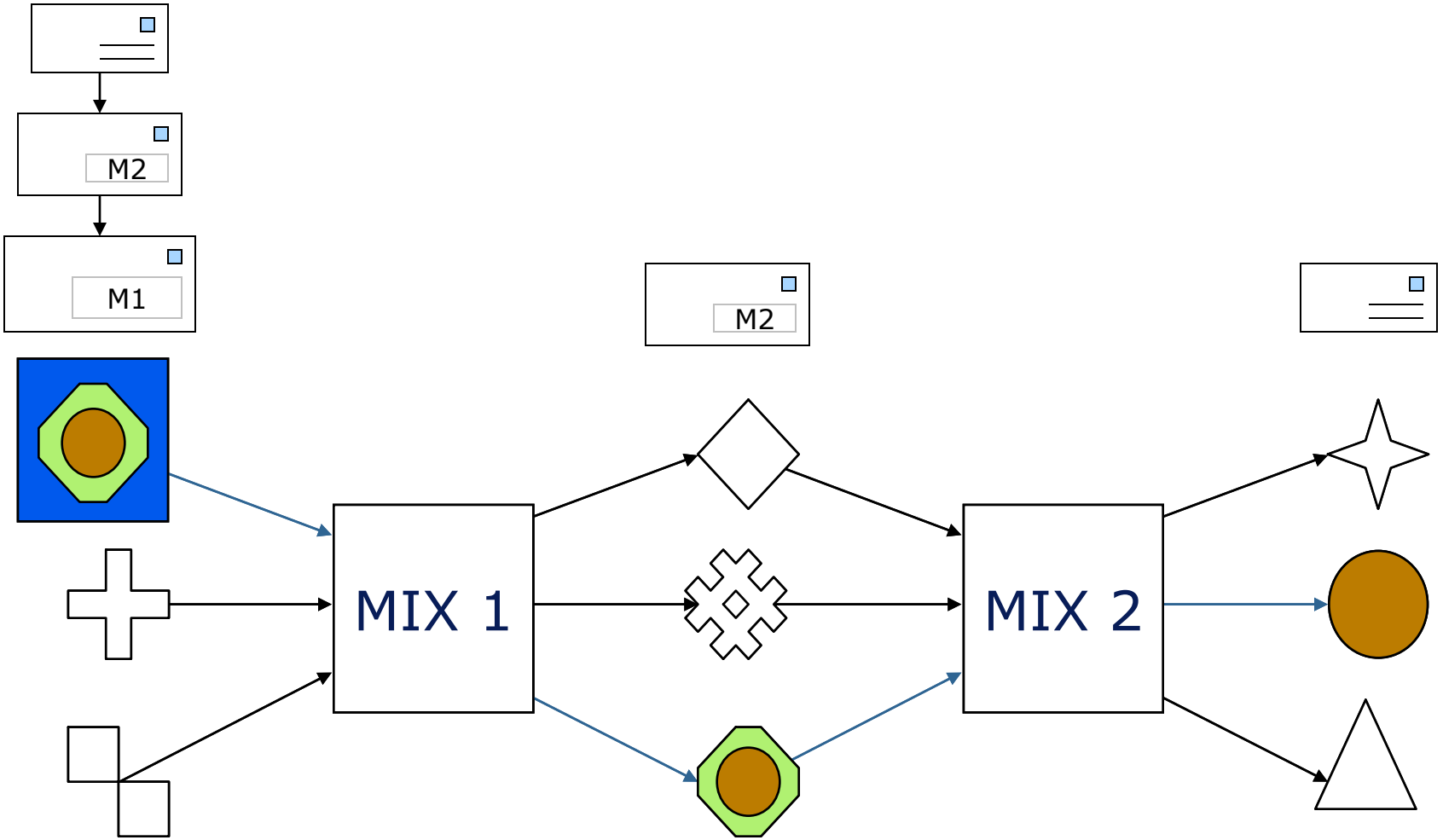
- System zum Schutz von Kommunikationsbeziehungen bei vermittelter Kommunikation

- 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

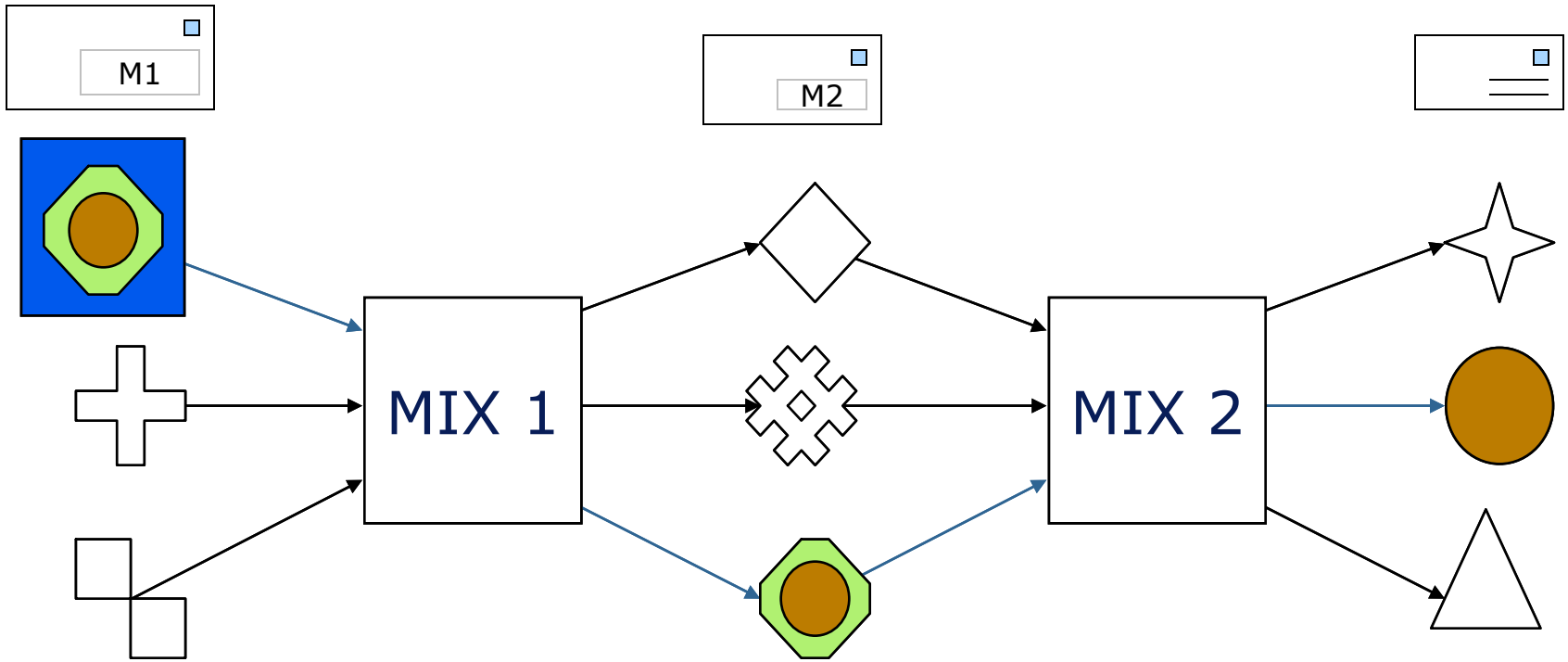
Mix-Netz (Chaum, 1981)

- System zum Schutz von Kommunikationsbeziehungen bei vermittelter Kommunikation



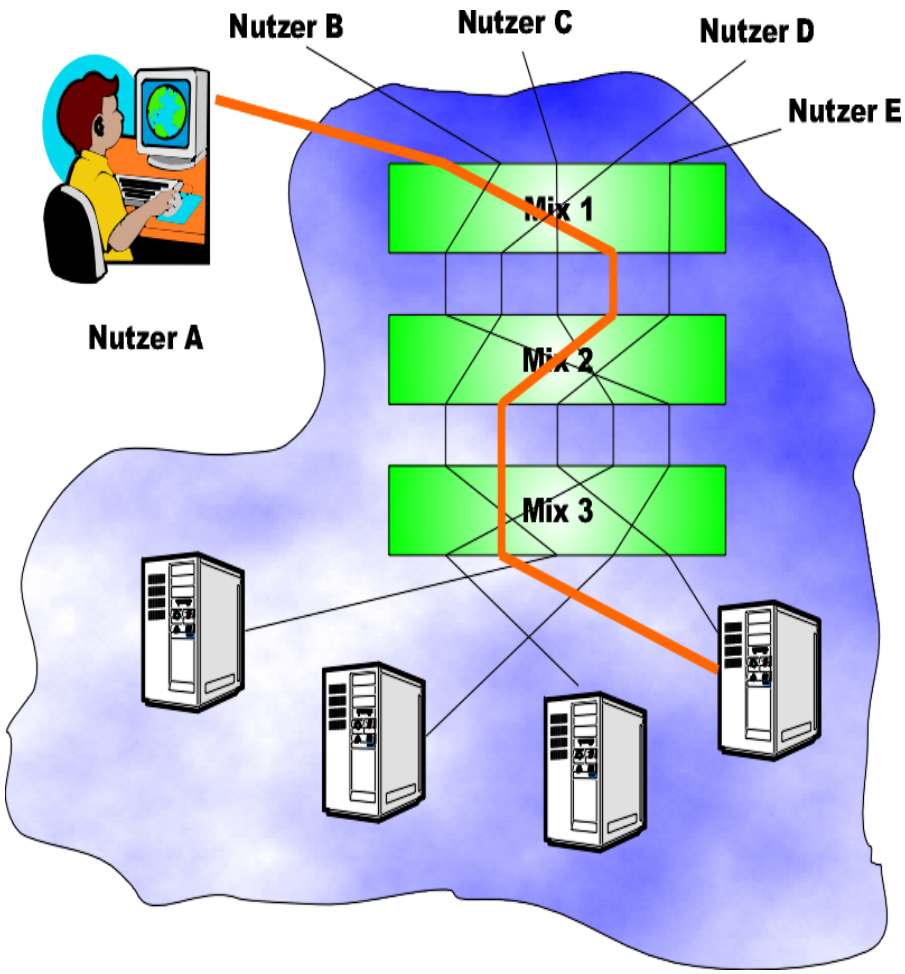
Mix-Netz (Chaum, 1981)

- 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.



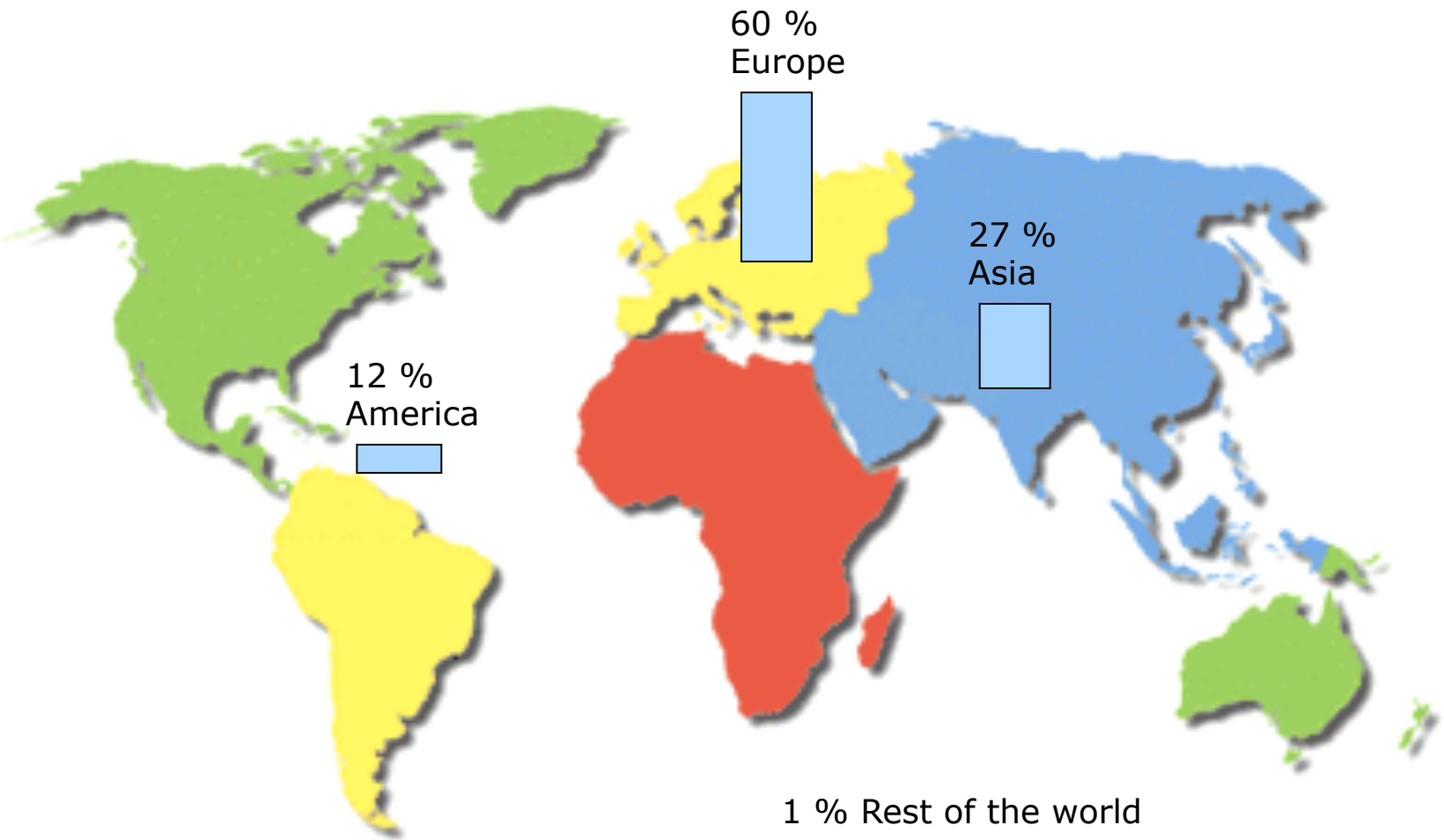
http://www.anon-online.de

- Wo kommen die Nutzer her?
- Wie ist die Zahlungsbereitschaft?
- Wofür verwenden sie den Dienst?
- Welche Möglichkeiten zur Strafverfolgung gibt es



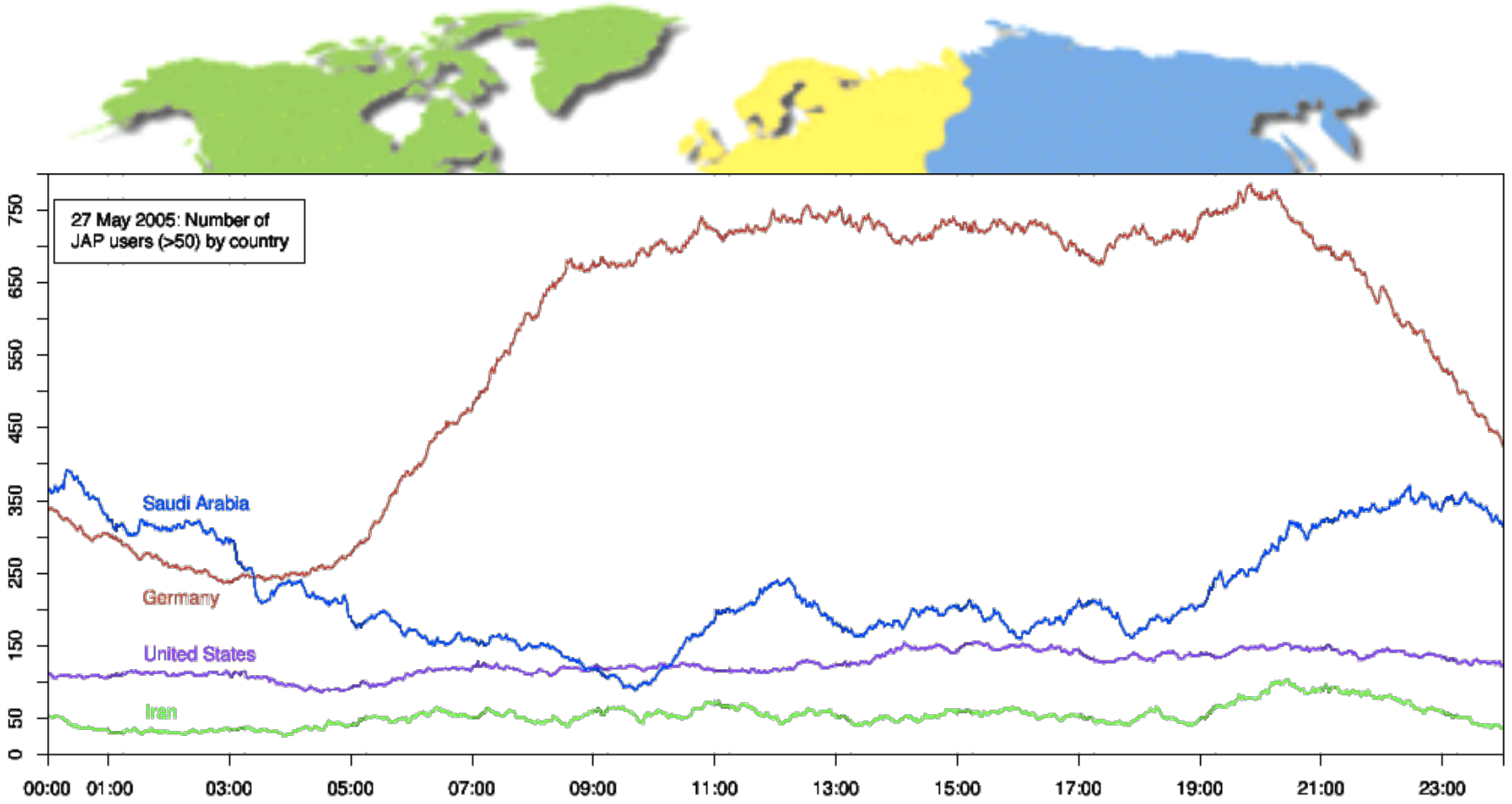
Wo kommen die JAP-Nutzer her?

- Eingehende Requests nach Regionen Mai-Juni 2005



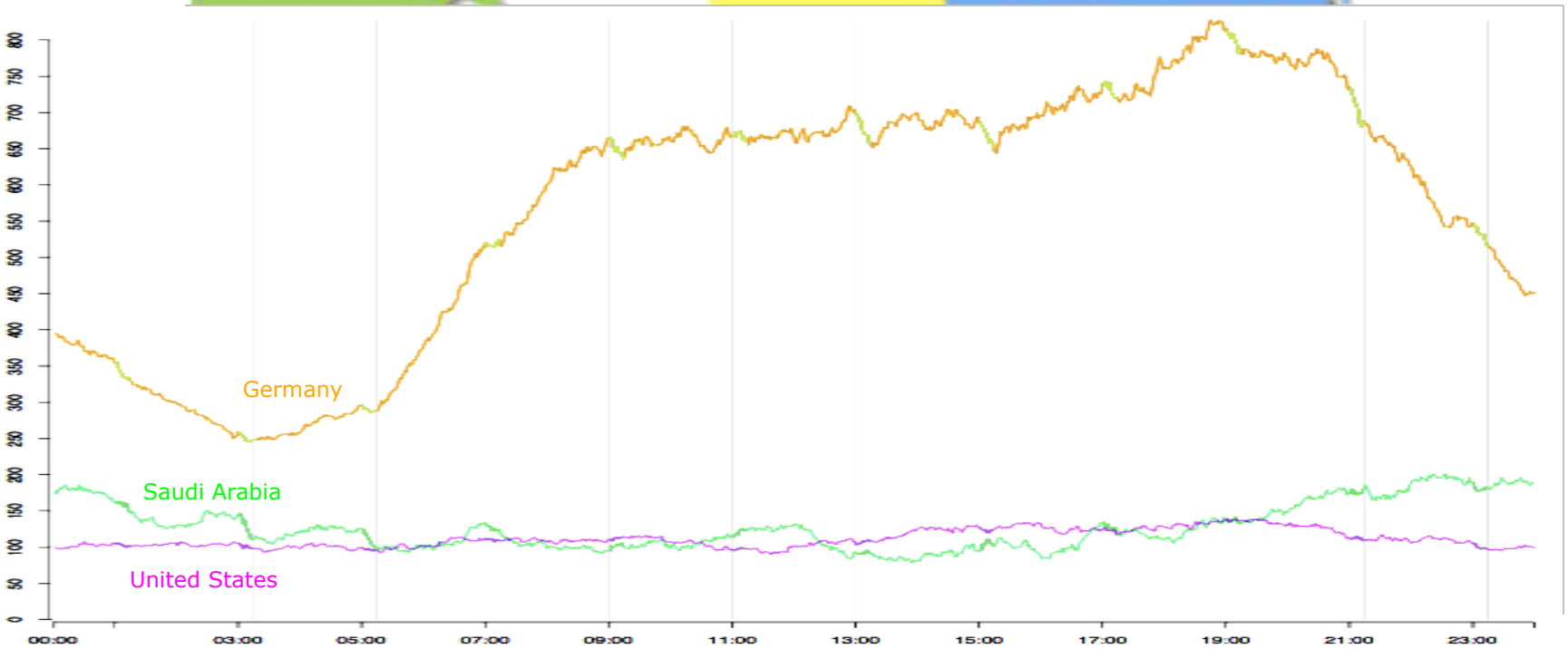
Wo kommen die JAP-Nutzer her?

- Dayline of May 27, 2005



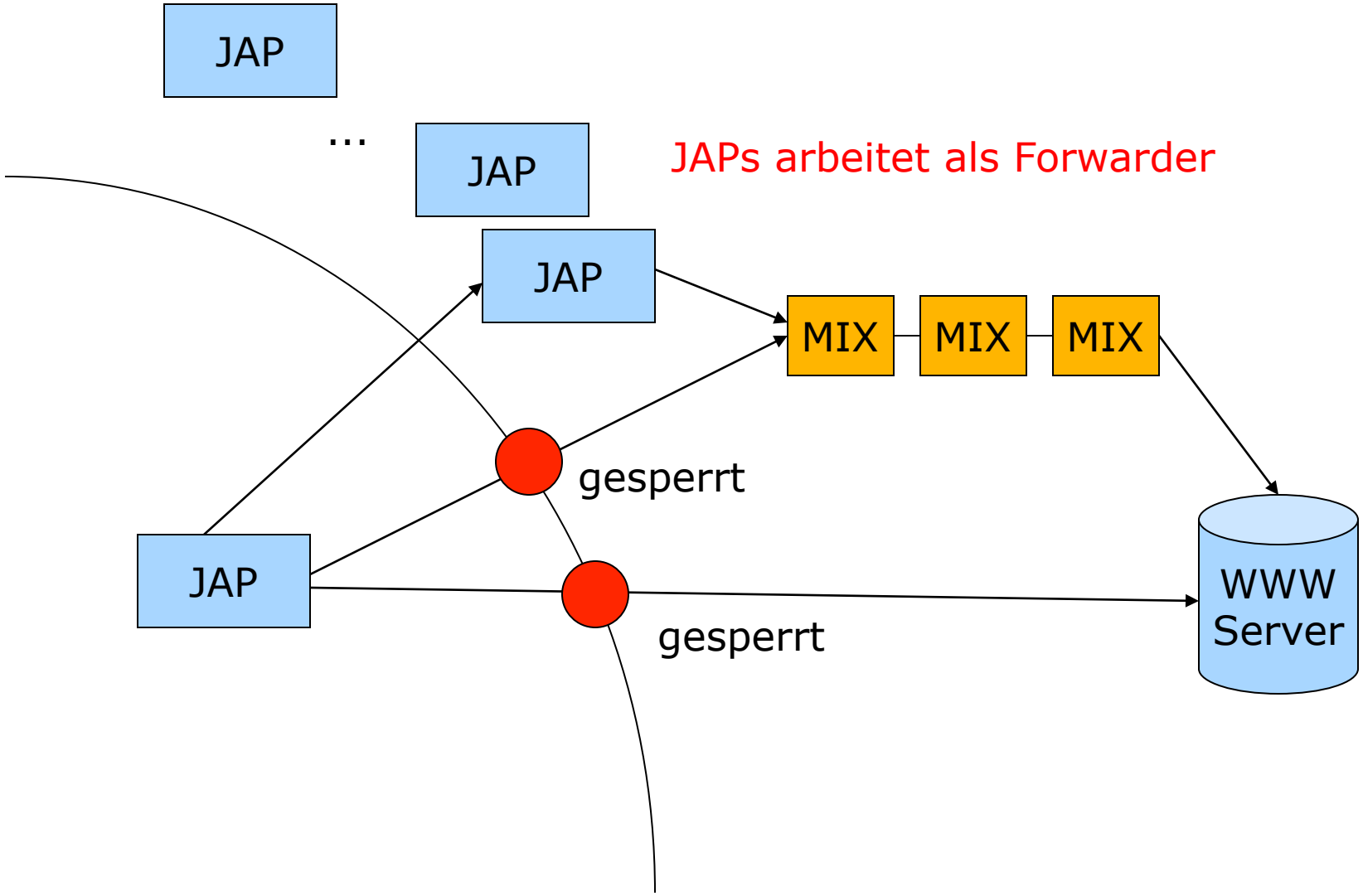
Wo kommen die JAP-Nutzer her?

- Dayline of Aug 1, 2005

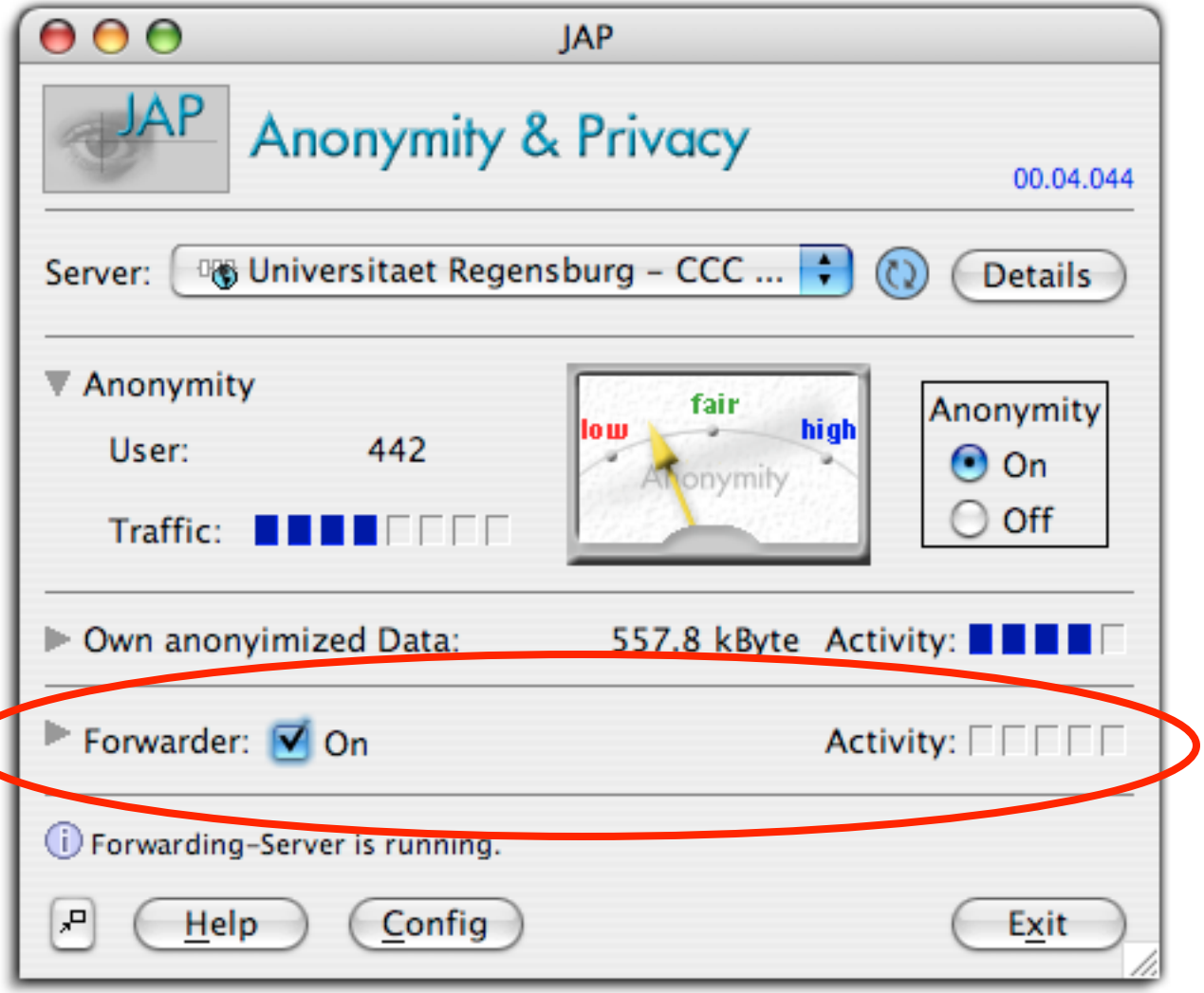


Iran?

Blockingresistenz



Blockingresistenz

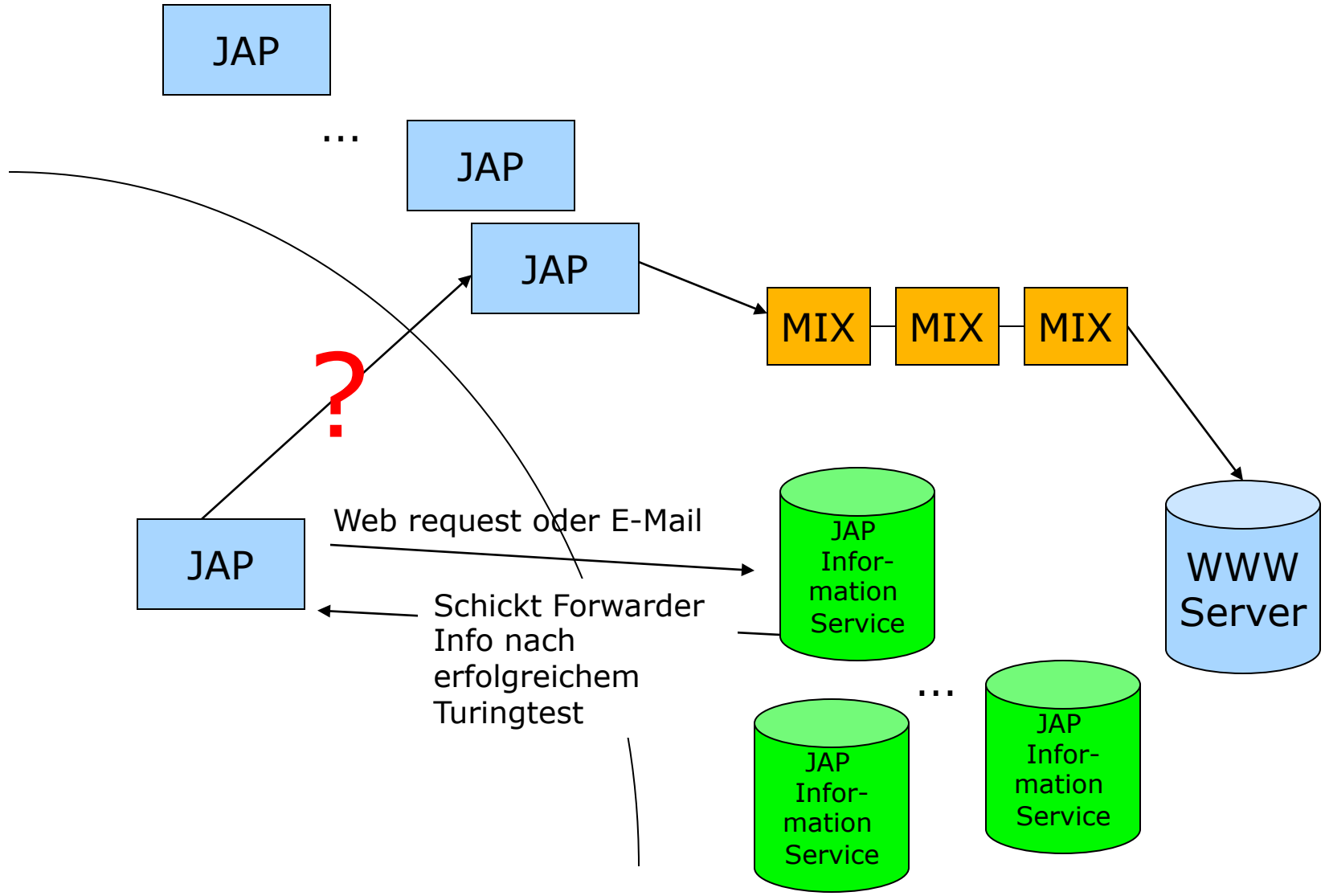


JAP-Nutzer stellen Teil ihrer Bandbreite zur Verfügung

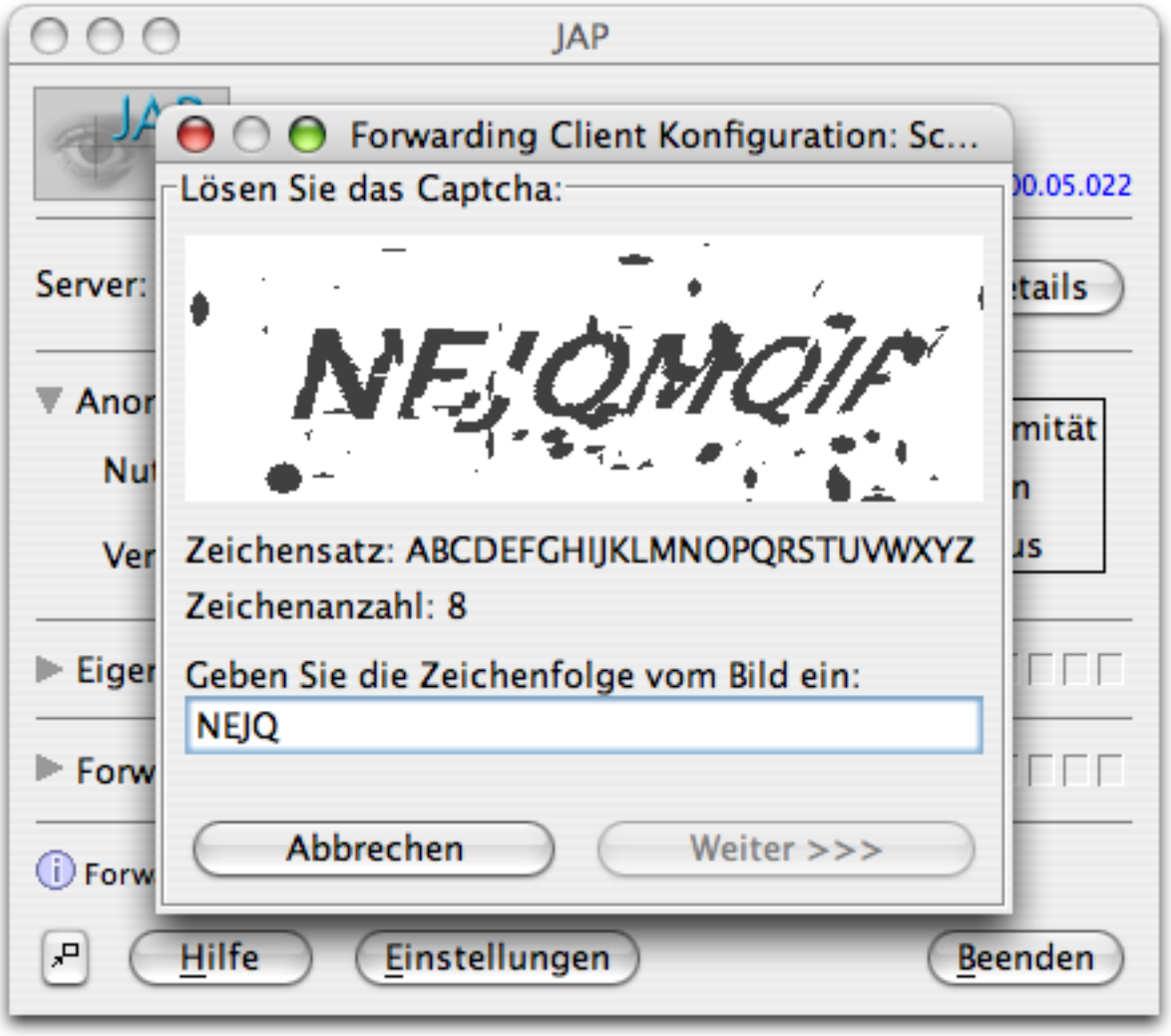
Zugriffe werden durch die Mixe anonymisiert

Forwarder erfahren nichts über die zugegriffenen Inhalte

Blockingresistenz



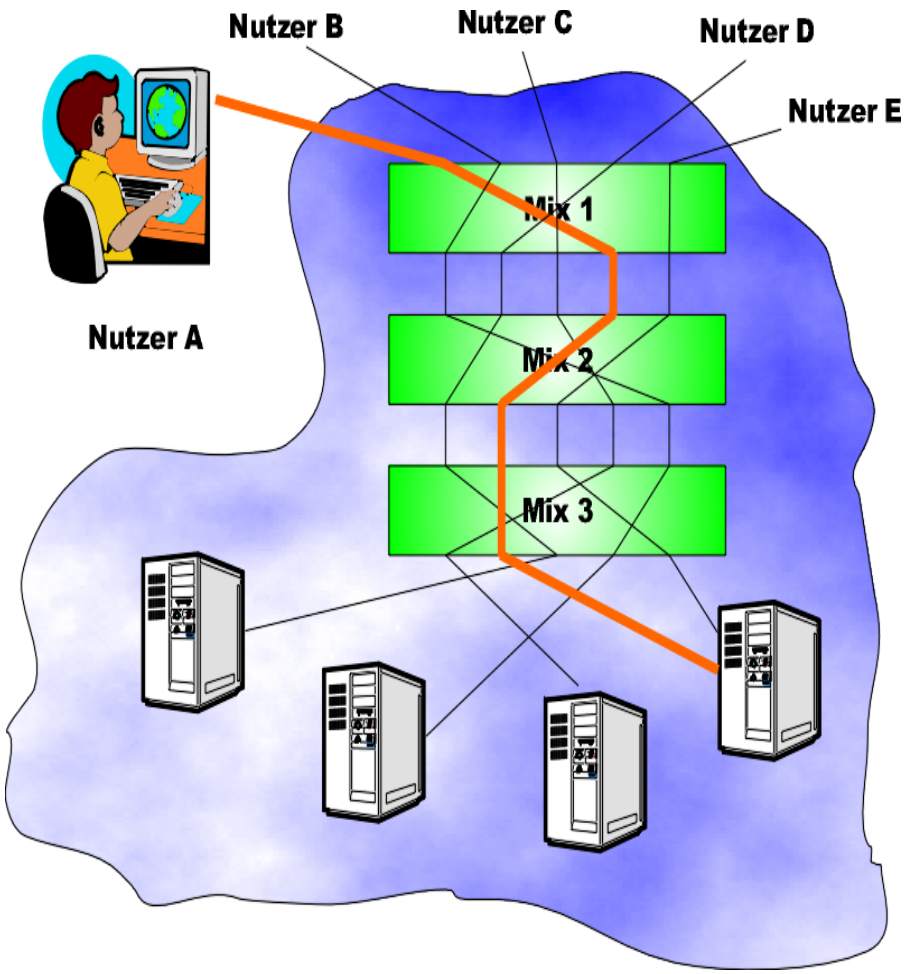
Blockingresistenz



InfoService schickt Forwarder Info nach erfolgreichem Turingtest

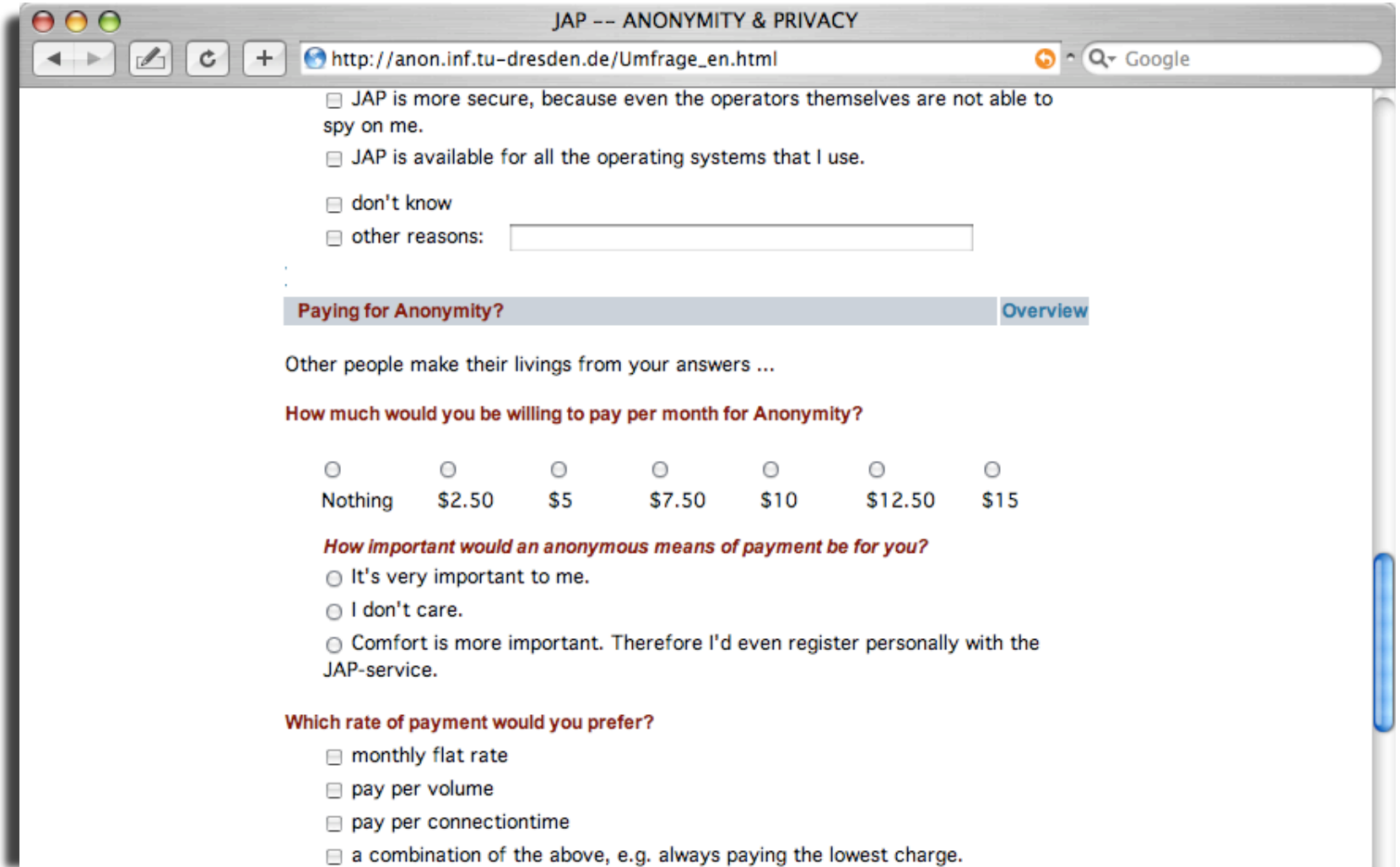
http://www.anon-online.de

- Wo kommen die Nutzer her?
- Wie ist die Zahlungsbereitschaft?
- Wofür verwenden sie den Dienst?
- Welche Möglichkeiten zur Strafverfolgung gibt es



Umfrage unter JAP-Benutzern (Spiekermann, 2003)

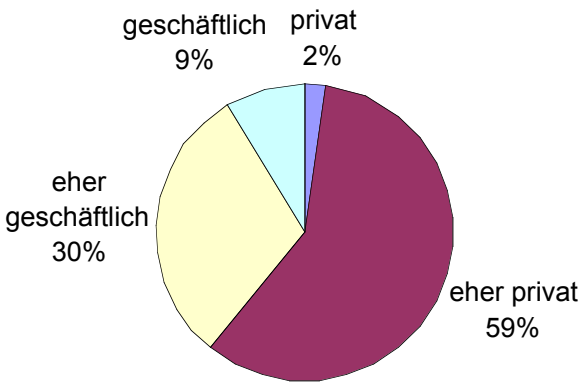
- Stichprobe:
  - 1800 JAP-Nutzer



Umfrage unter JAP-Benutzern

- Gründe für die Nutzung
  - ≈ 31% Free speech
  - ≈ 54% Schutz vor Geheimdiensten
  - ≈ 85% Schutz vor Profiling (Webnutzung)
  - ≈ 64% Schutz vor eigenem ISP

- Private oder geschäftliche Nutzung?
  - ≈ 2% ausschließlich privat
  - ≈ 59% überwiegend privat
  - ≈ 30% überwiegend geschäftlich
  - ≈ 9% ausschließlich geschäftlich



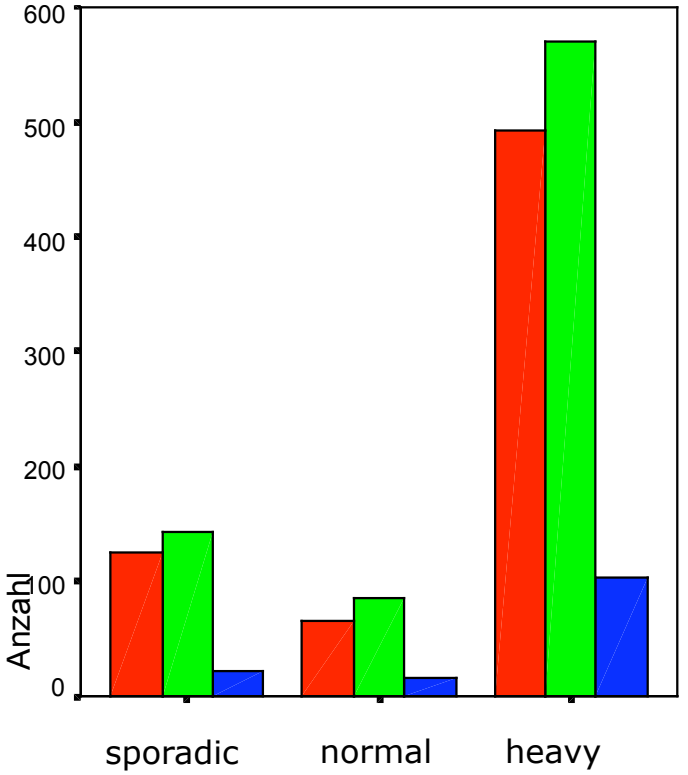
- Warum JAP?
  - ≈ 76% kostenlos
  - ≈ 56% schützt vor Betreibern
  - ≈ 51% einfach benutzbar

Umfrage unter JAP-Benutzern

- Zahlungsbereitschaft für Anonymität
  - ≈ 40% keine
  - ≈ 50% monatlich zwischen € 2,5 … € 5
  - ≈ 10% mehr als € 5 pro Monat

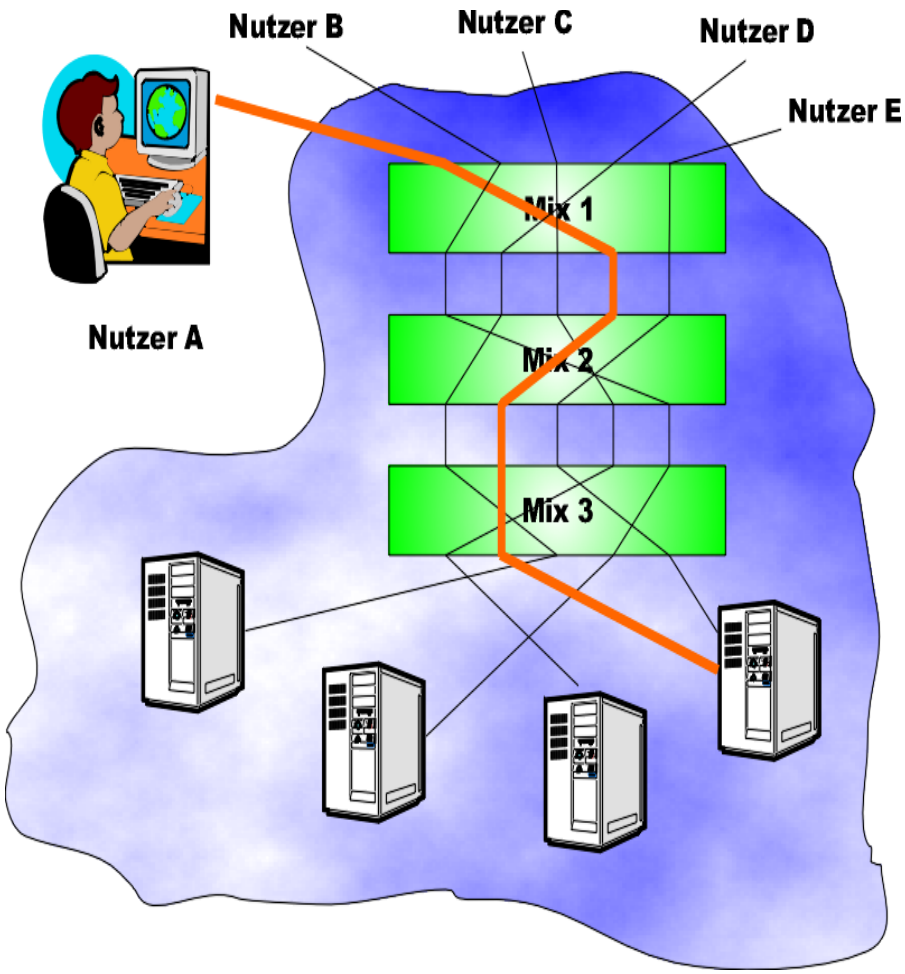
- Zahlungsbereitschaft korreliert nicht mit der Intensität der Nutzung

- Intensität der Nutzung
  - ≈ 73% heavy: tägliche Nutzung
  - ≈ 10% «normal»: ≥ 2x pro Woche
  - ≈ 17% sporadic: < 2x pro Woche



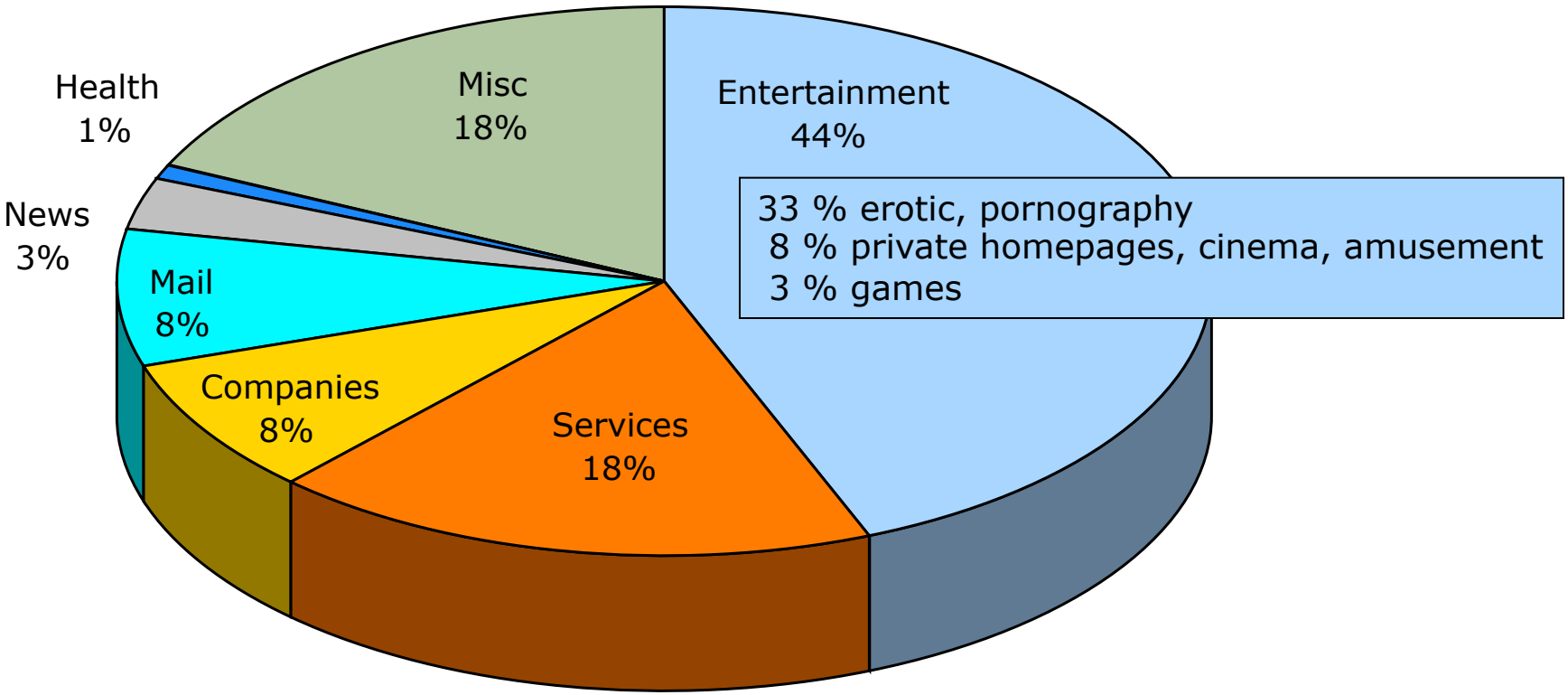
http://www.anon-online.de

- Wo kommen die Nutzer her?
- Wie ist die Zahlungsbereitschaft?
- Wofür verwenden sie den Dienst?
- Welche Möglichkeiten zur Strafverfolgung gibt es



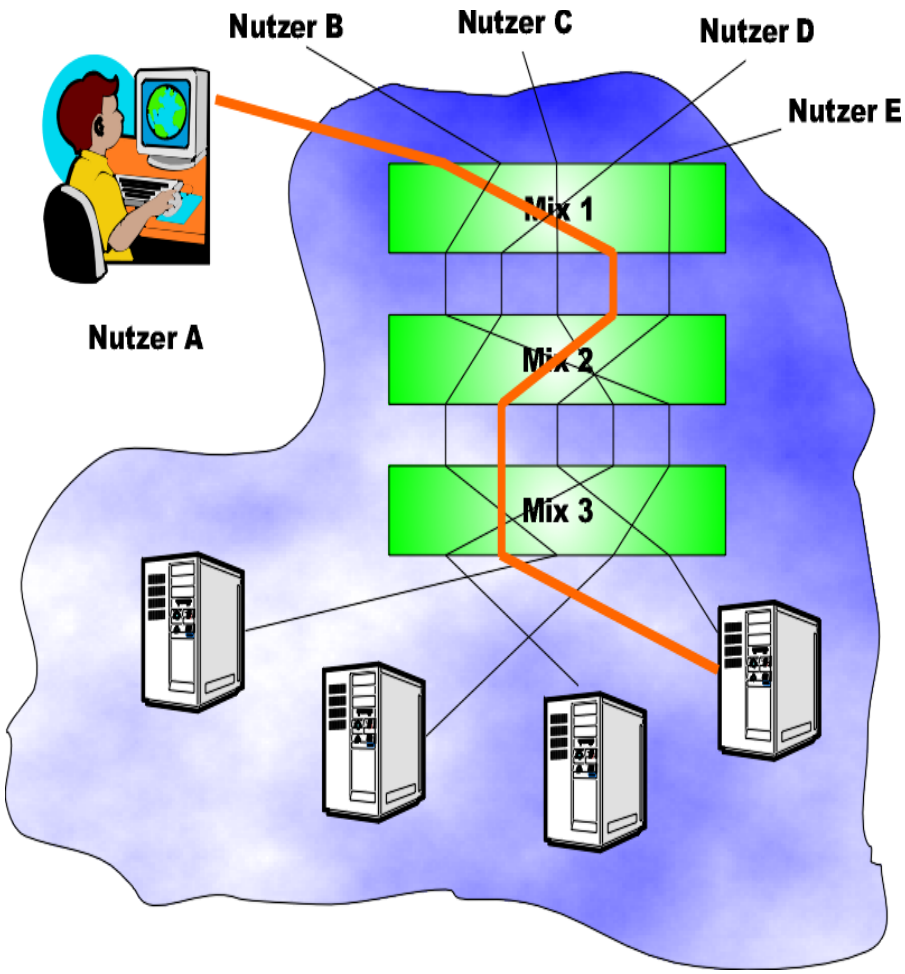
Anonymisierte Inhalte

- Zuordnung von 150 zufällig ausgewählten Requests aus mehreren Millionen Zugriffen im Juni 2005



http://www.anon-online.de

- Wo kommen die Nutzer her?
- Wie ist die Zahlungsbereitschaft?
- Wofür verwenden sie den Dienst?
- Welche Möglichkeiten zur Strafverfolgung gibt es

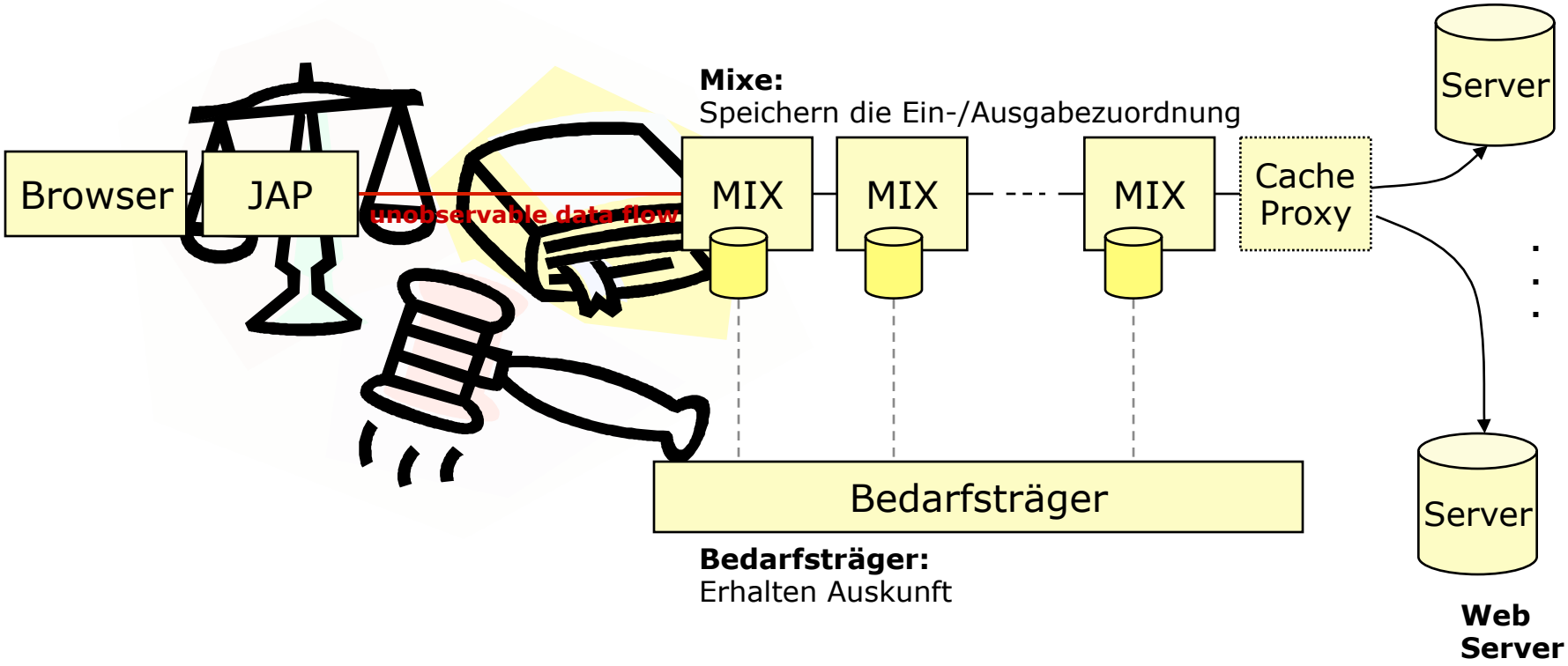


Anonyme Kommunikation ist legal

- Telemediengesetz (TMG)
  - § 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.

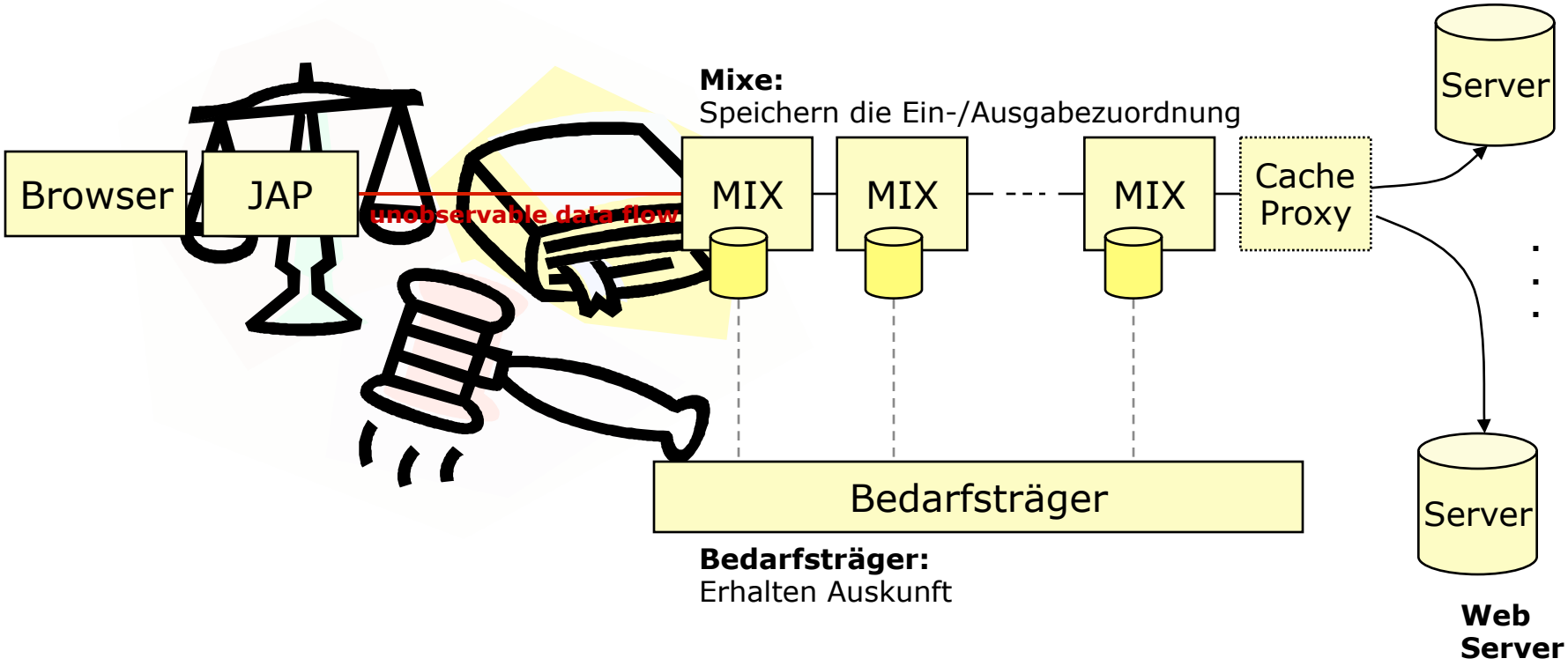
Strafverfolgung bei schweren Straftaten

- Voraussetzung: Anordnung nach § 100a,b StPO
  - Aktivieren der Funktion nach richterlicher Anordnung
  - auf 3 Monate begrenzt
  - nur für Zukunft
  - wird erfasst in Überwachungsstatistik



Vorratsdatenspeicherung

- Mixe speichern Ein-/Ausgabezuordnung für 6 Monate
  - Problem: Ziel-URLs dürfen nicht gespeichert werden
  - Auskunftsersuchen bezieht sich auf ausgehende IP (Cache-Proxy) und Uhrzeit



Website-Fingerprinting

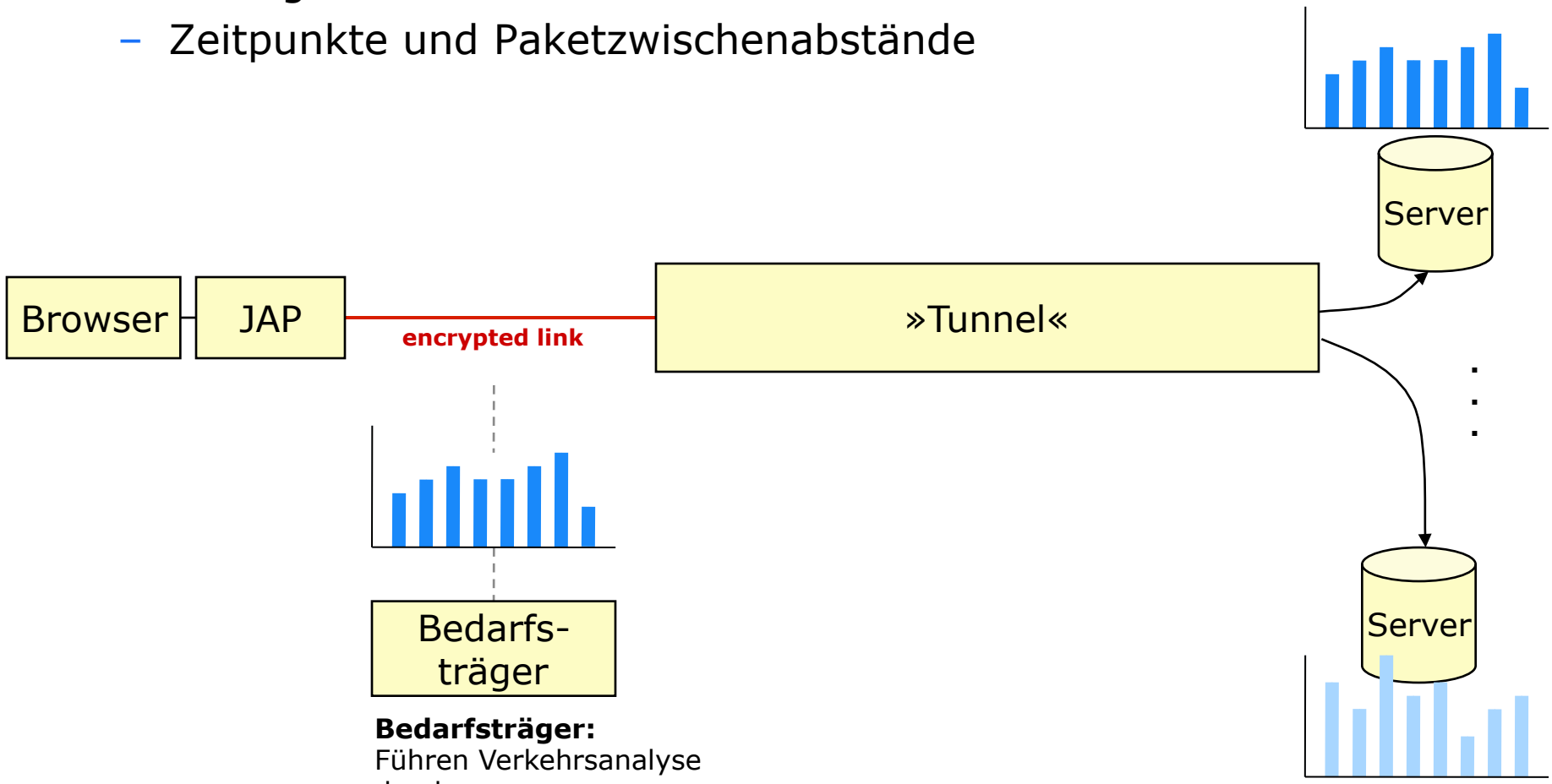
- Entschlüsselung des Datenstroms meist aussichtslos

- Alternativen:
  - Online-Durchsuchung: Direkter Zugriff auf Klartexte durch Installation einer Software auf dem Rechner eines Verdächtigen.
  - Traffic-Analyse: Durch Analyse charakteristischen Eigenschaften des Datenverkehrs kann ein passiver Beobachter auf Inhalts und/oder Adressdaten schließen.

- Beobachtbare Merkmale:
  - Auftretenshäufigkeit von Paketen/Verbindungen
  - Paketgröße und Datendurchsatz
  - Zeitpunkte und Paketzwischenabstände

Website-Fingerprinting

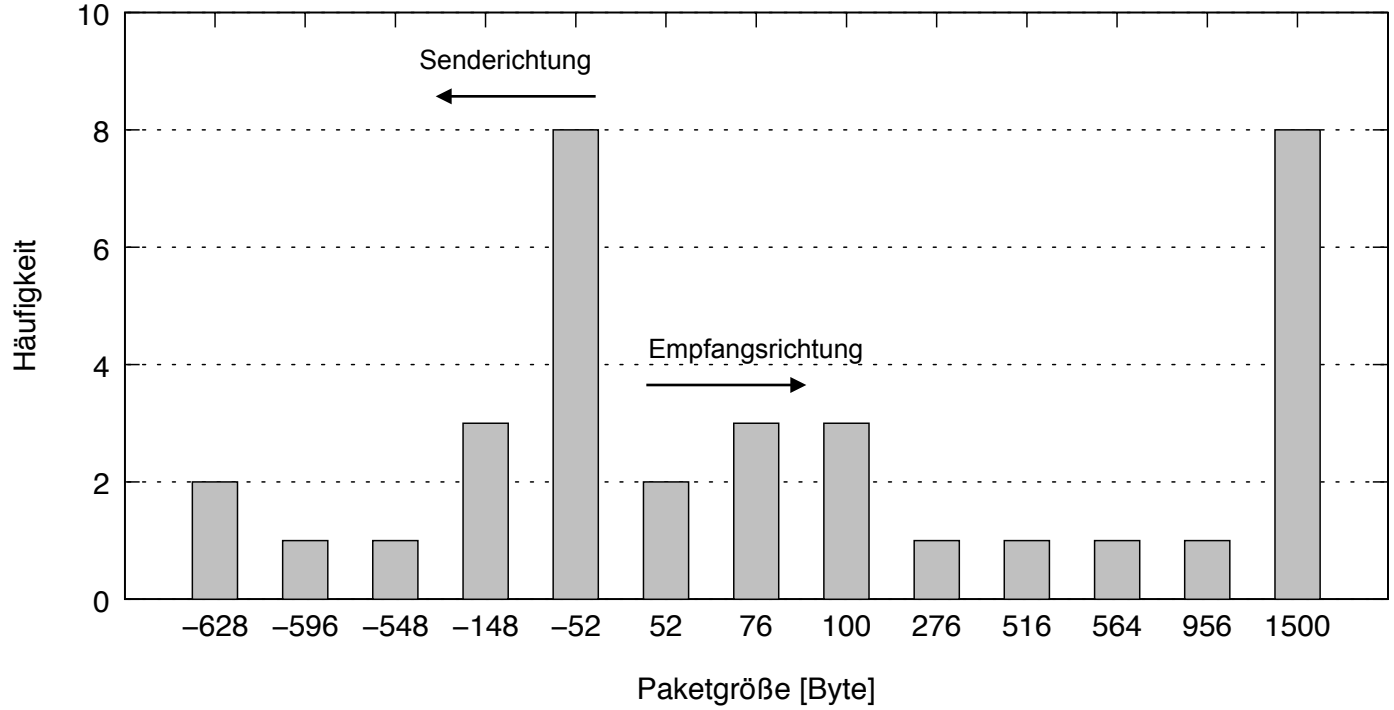
- Beobachtbare Merkmale:
  - Auftretenshäufigkeit von Paketen/Verbindungen
  - Paketgröße und Datendurchsatz
  - Zeitpunkte und Paketzwischenabstände



Bedarfsträger:
Führen Verkehrsanalyse durch

Verbessertes Website-Fingerprinting-Verfahren

- Analyse der charakteristischen Häufigkeitsverteilung der IP-Paketgrößen



- Schutz durch datenschutzfreundliche Systeme?
  - gering: SSH-Tunnel und VPNs; Erkennungsrate: 90-97%
  - moderat: Anonymisierer wie Tor und JAP/JonDonym; Erkennungsrate: < 20%

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