Betriebssysteme und Sicherheit

Einführung in Datenschutz & Datensicherheit

Elke Franz, Stefan Köpsell
(enthält Folien von: Andreas Pfitzmann, Thorsten Strufe)
TU Dresden, Fakultät Informatik, D-01062 Dresden
Nöthnitzer Str. 46, Raum 3070
Tel.: 0351/ 463-38247, E-Mail: stefan.koepsell@tu-dresden.de | elke.franz@tu-dresden.de
https://dud.inf.tu-dresden.de/

Datenschutz vs. Datensicherheit

- keine wirklich klaren Definitionen / Abgrenzungen vorhanden

- Datenschutz:
  - Schutz ***vor*** Daten

- Datensicherheit
  - Schutz ***von*** Daten

Betriebssysteme und Sicherheit

Einführung in Datenschutz & Datensicherheit

Themen:

1: Einführung, Schutzziele, Angreifermodelle
2: Datenschutz
3: Informationssicherheitsmanagement, Risikoanalyse
4: Zugriffskontrolle, Biometrie
5 & 6: Kryptographische Grundlagen: symmetrische/asymmetrische Systeme, Schlüsselaustausch, Verschlüsselung, Authentikation, Hashfunktionen
7: Anwendung kryptographischer Verfahren: Sicherheitsprotokolle
8: Hardware-basierte Sicherheit: TPM & Intel SGX

Elke Franz, Stefan Köpsell
(enthält Folien von: Andreas Pfitzmann)
TU Dresden, Fakultät Informatik, D-01062 Dresden
Nöthnitzer Str. 46, Raum 3070
Tel.: 0351/ 463-38247, E-Mail: stefan.koepsell@tu-dresden.de | elke.franz@tu-dresden.de
https://dud.inf.tu-dresden.de/

Vertiefungsmöglichkeiten
Sicherheit / technischer Datenschutz

Lehrveranstaltung	*Lehrende(r)*	*SWS*
Security & Cryptography I	Köpsell	2/2
Security & Cryptography II	Köpsell	2/2
Kryptographie und -analyse	Franz	2
Praktikum: Kryptographie und Datensicherheit	Köpsell	/4
Systemsicherheitslabor	Köpsell	2/2
Proseminar: Sicherheit in Computersystemen	Köpsell	/2
Proseminar: Entwicklung sicherer Anwendungen	Borcea-Pfitzmann	/2
Hauptseminar: Technischer Datenschutz	Osman et.al.	2
Datenschutzrecht	Wagner	2
Informatik und Gesellschaft	Köpsell	2
Informations- und Kodierungstheorie	Franz	2/1

Lehr- und Forschungsgebiete

- Mehrseitige Sicherheit, insbesondere Sicherheit durch verteilte Systeme
- Datenschutzfreundliche Technologien
- Kryptographie
- Multimedia-Forensik

- Sicherheit und Datenschutz
  - beim vernetzten Fahren
  - für IoT& Cyberphysikalische Systeme
  - industrielle Kommunikation
  - mit besonderem Fokus auf den Menschen : Social Engineering, Transparenz, Awareness

- SDN & Cloud Sicherheit

Ziele von Lehre an Universitäten

Wissenschaft soll u.a. klären

Wie etwas ist.

Vor allem aber auch

Warum etwas so ist

oder

Wie es alternativ sein könnte

(und vielleicht auch sollte).

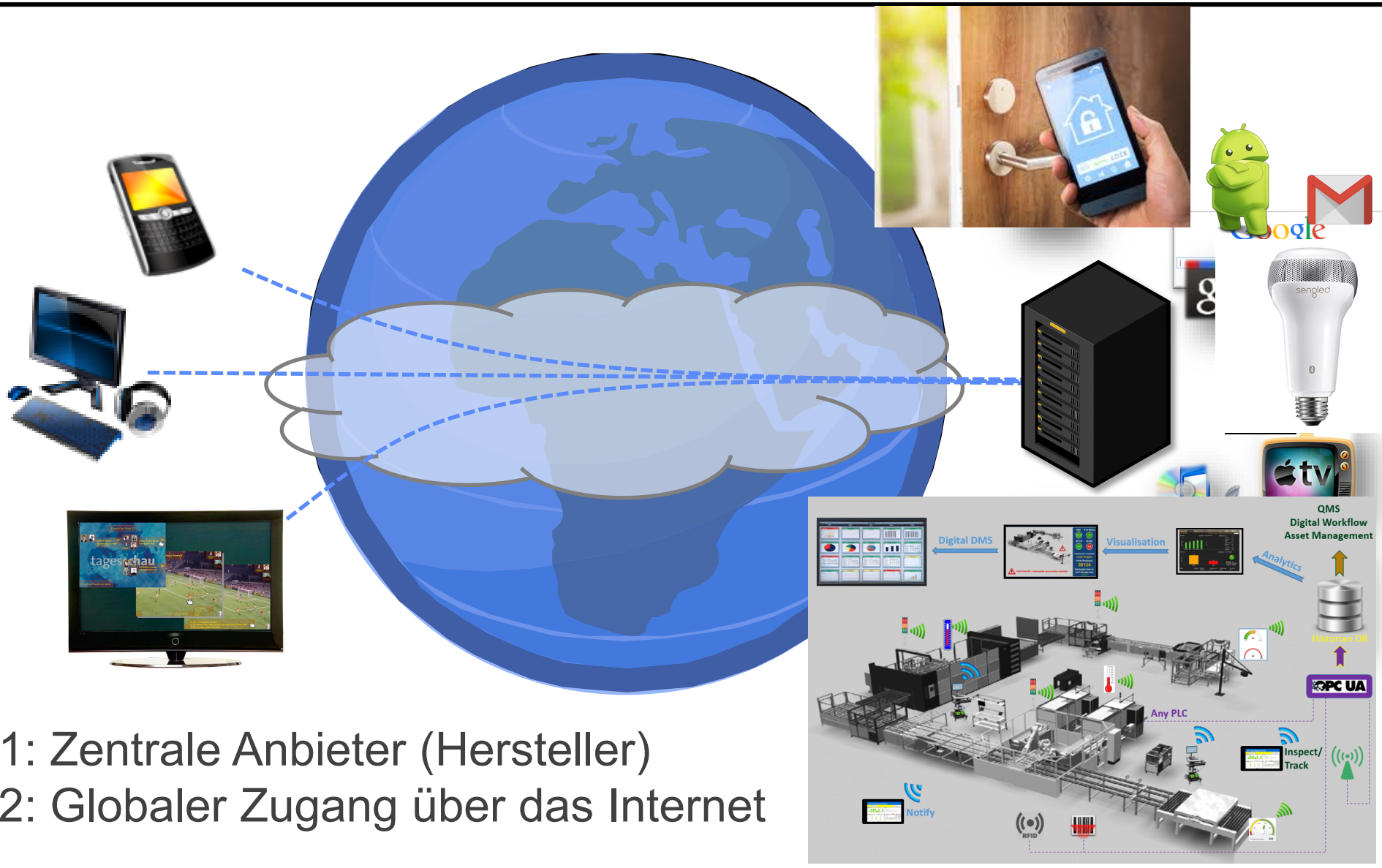
„**Ewige Wahrheiten**“ (d.h. Wissen mit großer Relevanzzeit) sollten an Universitäten mehr als 90% des Lehr- und Lernaufwands ausmachen.

Allgemeine Ausbildungsziele (nach Prioritäten)

1. Erziehung zu **Ehrlichkeit** und **realistischer Selbsteinschätzung**
2. Anregung zu realistischer **Fremdeinschätzung** von Personen, Firmen und Organisationen
3. **Sicherheits- und Datenschutzbedürfnisse** ermitteln
   - Realistische Schutzziele
   - Realistische Angreifermodelle / Vertrauensmodelle
4. **Validierung** und **Verifikation**, inkl. prinzipielle und praktische **Grenzen**
5. Sicherheits- und Datenschutz**mechanismen**
   - Kennen und verstehen sowie
   - Entwickeln können

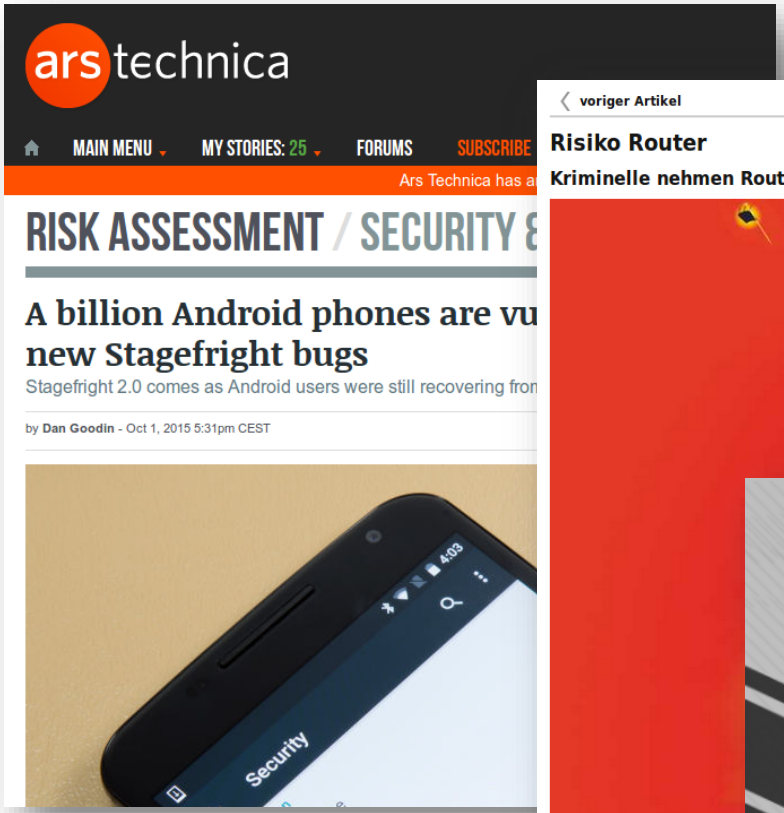
Kurzum: ***Integre IT-Sicherheitsexpert(inn)en mit eigenem Urteil und Rückgrat.***

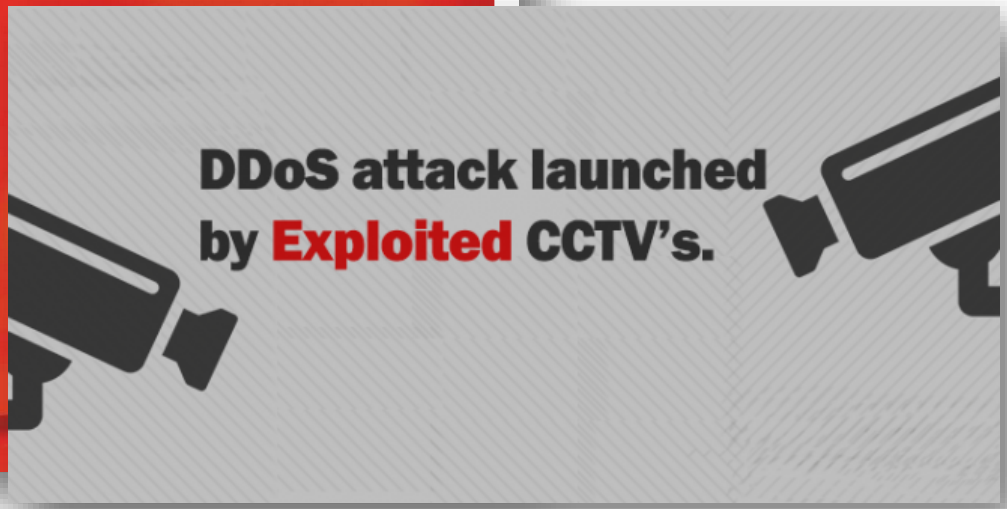
Vernetzte Dienste heute…



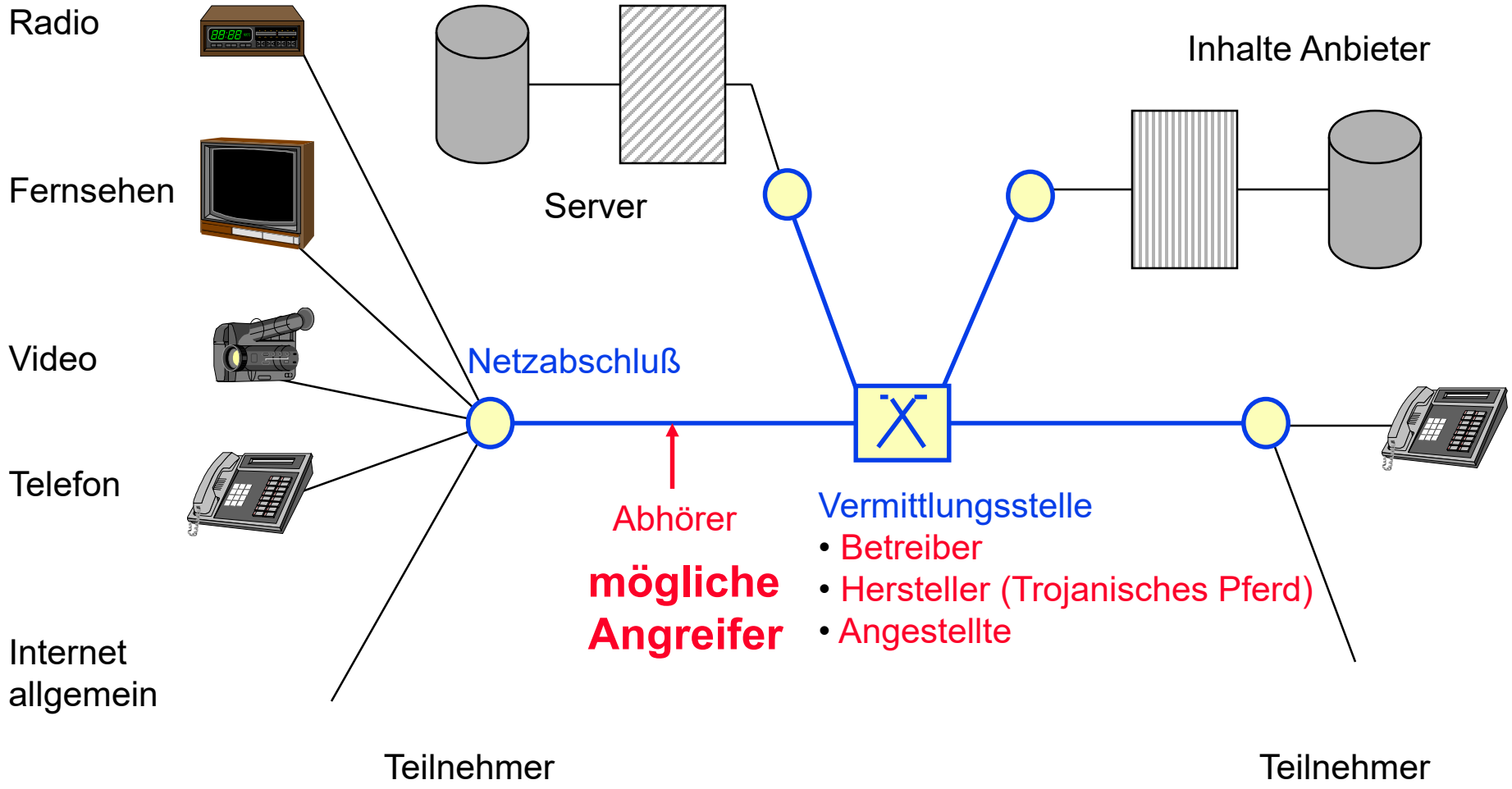
1: Zentrale Anbieter (Hersteller)
2: Globaler Zugang über das Internet

And the Dirty Realit



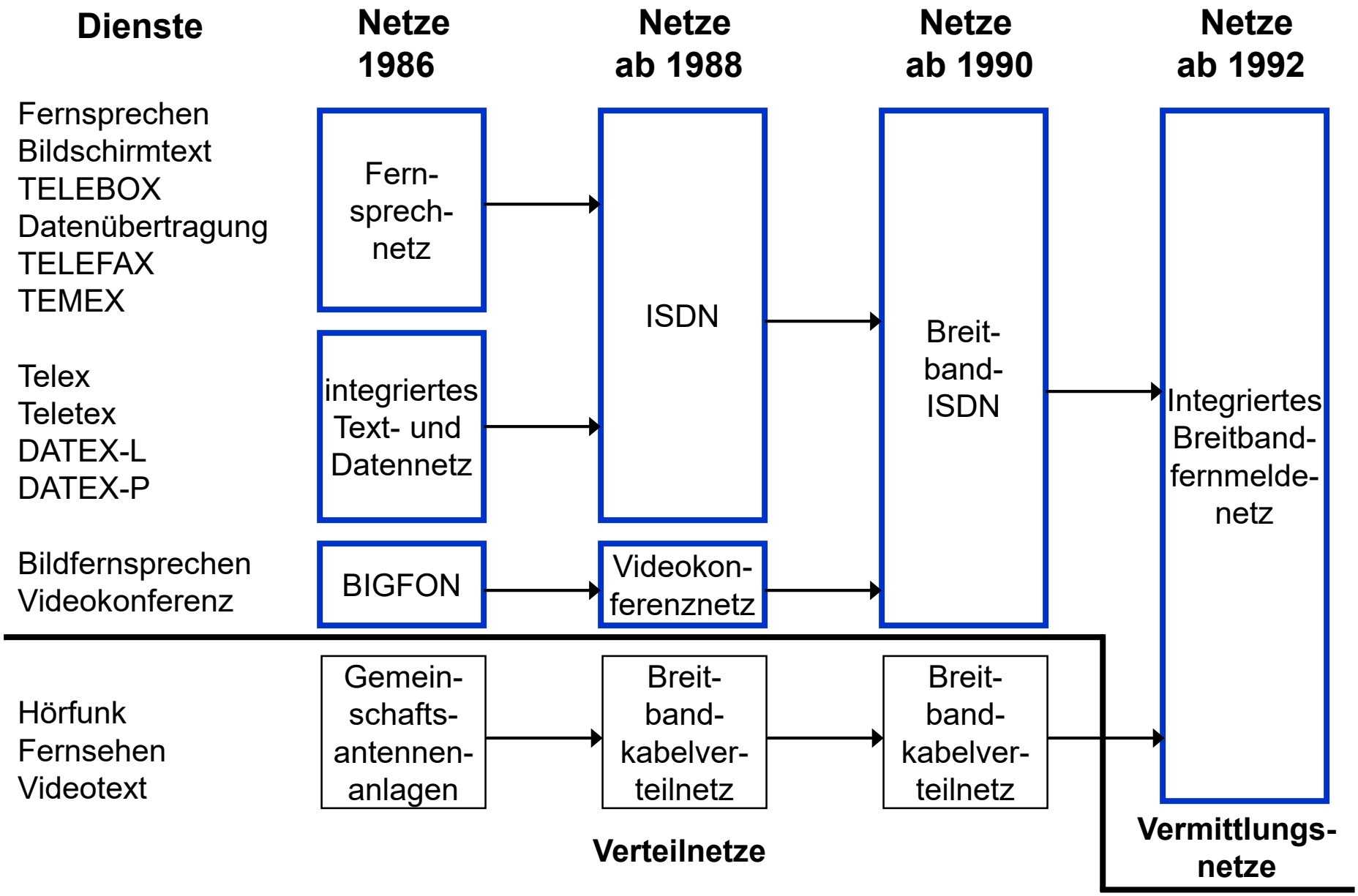


Ausschnitt eines Rechnernetzes



Warum reichen juristische Regelungen (für Rechtssicherheit und Datenschutz) nicht aus ?

Entwicklung der leitungsgebundenen Kommunikationsnetze der Deutschen Bundespost



Wichtige Begriffe

Rechner verbunden über **Kommunikationsnetz** = **Rechnernetz** (erster Art)

Prozeßrechner im **Kommunikationsnetz** = **Rechnernetz** (zweiter Art)

verteiltes System
- räumlich
- Kontroll- und Implementierungsstruktur

offenes System ≠ **öffentliches** System ≠ **Open Source** System

diensteintegrierendes System

digitales System

Was ist eine Bedrohung?

- Abstrakte Definition:
  - Bedrohungen sind mögliche *Ereignisse*, oder Reihungen von Ereignissen und Aktionen, die zu einer *Verletzung eines oder mehrerer Sicherheitsziele* führt
  - Eine Realisierung einer Bedrohung ist ein ***Angriff***

- Beispiele für Bedrohungen:
  - Unerlaubter Zugriff auf Firmendaten durch Hacker
  - Mutwillig manipulierte von Bank- oder Zeugnisdaten
  - Ausfall einer Webseite wegen Sabotage/temporäres Abschalten
  - Nutzung von Diensten im Namen einer anderen Partei

Bedrohungen - Klassen

- ***Maskerade***
  - Instanz gibt vor die Identität einer anderen Instanz zu haben
- ***Informationsverlust (Abgehört, Ausgespäht werden)***
  - Instanz liest Information, die nicht für sie bestimmt ist
- ***Authorisierungsverletzung***
  - Instanz nutzt Ressourcen ohne dazu autorisiert zu sein
- ***Zerstörung/Modifikation von Information***
  - Information wird zerstört oder verändert
- ***Fälschung von Information***
  - Instanz erzeugt Information in der Identität einer anderen Instanz
- ***Abstreiten von Ereignissen***
  - Instanz leugnet fälschlicherweise, an Ereignis beteiligt gewesen zu sein
- ***Sabotage***
  - Mutwillige/geplante (Zer-)Störung von Diensten oder Systemen

Bedrohungen und korrespondierende Schutzziele

Bedrohungen: Bsp.: medizinisches Informationssystem Schutzziele:

1) Informationsgewinn — Vertraulichkeit
   Rechnerhersteller erhält Krankengeschichten

2) Modifikation von Information
   unerkannt Dosierungsanweisungen ändern

3) Beeinträchtigung der Funktionalität
   erkennbar ausgefallen

≥ totale Korrektheit:
- Integrität ≅ partielle Korrektheit
- Verfügbarkeit für berechtigte Nutzer

keine Klassifikation, aber pragmatisch sinnvoll

Bsp.: Programm unbefugt modifiziert

1) nicht erkennbar, aber verhinderbar; nicht rückgängig zu machen
2)+3) nicht verhinderbar, aber erkennbar; rückgängig zu machen

Definitionen für die Schutzziele

Vertraulichkeit (confidentiality)

Informationen werden nur Berechtigten bekannt.

Integrität (integrity)

Informationen sind richtig, vollständig und aktuell oder aber dies ist erkennbar nicht der Fall.

Verfügbarkeit (availability)

Informationen sind dort und dann zugänglich, wo und wann sie von Berechtigten gebraucht werden.

- **subsumiert: Daten, Programme, Hardwarestrukturen**
- **es muss geklärt sein, wer in welcher Situation wozu berechtigt ist**
- **kann sich nur auf das Innere eines Systems beziehen**

Schutzziele: Sortierung

	Inhalte	Umfeld
Unerwünschtes verhindern	Vertraulichkeit Verdecktheit	Anonymität Unbeobachtbarkeit
Erwünschtes leisten	Integrität	Zurechenbarkeit
	Verfügbarkeit	Erreichbarkeit Verbindlichkeit

Schutzziele: Definitionen

Vertraulichkeit: Geheimhaltung von Daten während der Übertragung. Niemand außer den Kommunikationspartnern kann den Inhalt der Kommunikation erkennen.

Verdecktheit: Versteckte Übertragung von vertraulichen Daten. Niemand außer den Kommunikationspartnern kann die Existenz einer vertraulichen Kommunikation erkennen.

Anonymität: Nutzer können Ressourcen und Dienste benutzen, ohne ihre Identität zu offenbaren. Selbst der Kommunikationspartner erfährt nicht die Identität.

Unbeobachtbarkeit: Nutzer können Ressourcen und Dienste benutzen, ohne daß andere dies beobachten können. Dritte können weder das Senden noch den Erhalt von Nachrichten beobachten.

Integrität: Modifikationen der kommunizierten Inhalte (Absender eingeschlossen) werden durch den Empfänger erkannt.

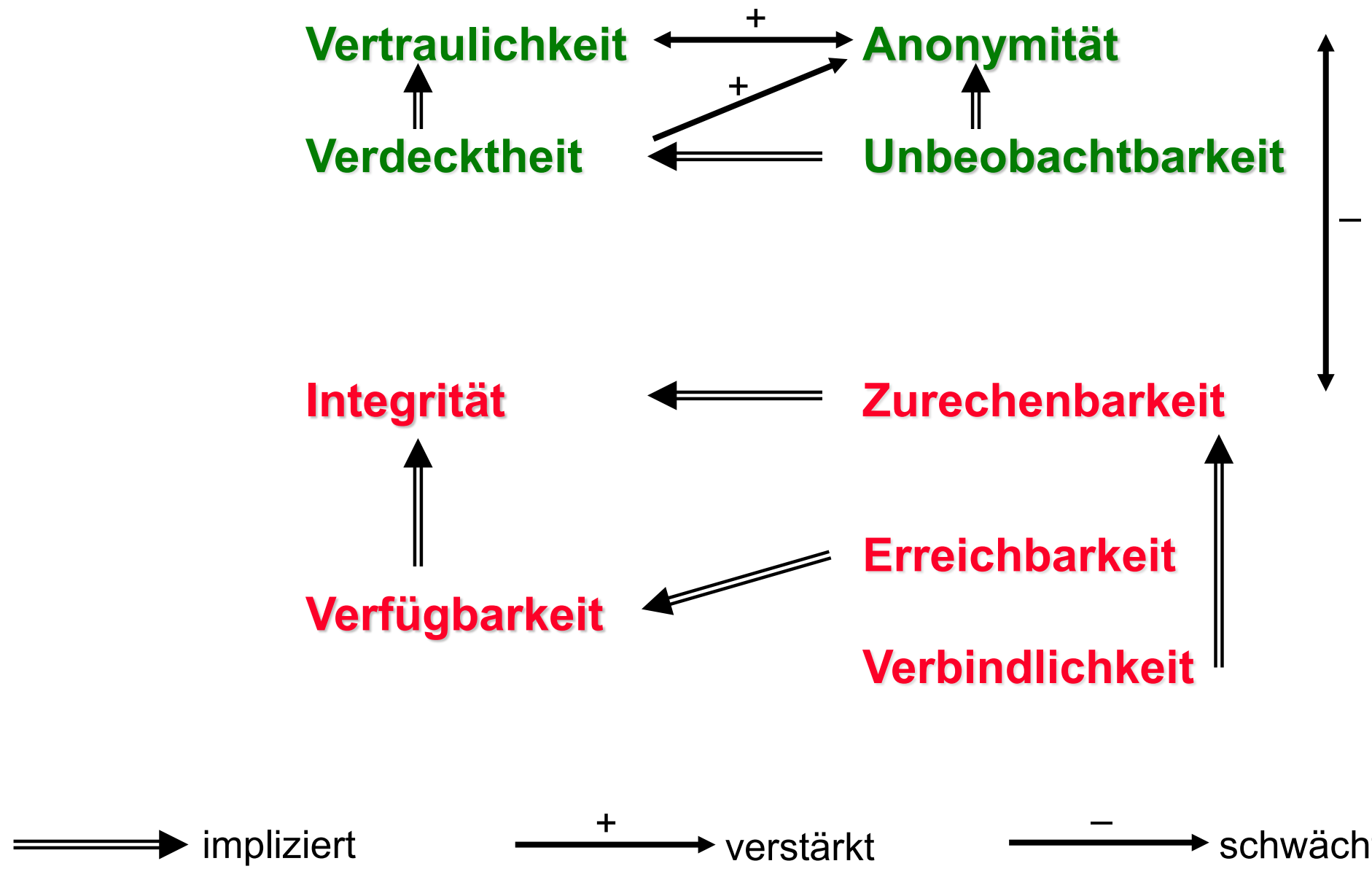
Zurechenbarkeit: Sendern bzw. Empfängern von Informationen kann das Senden bzw. der Empfang der Informationen bewiesen werden.

Verfügbarkeit: Nutzbarkeit von Diensten und Ressourcen, wenn ein Teilnehmer sie benutzen will.

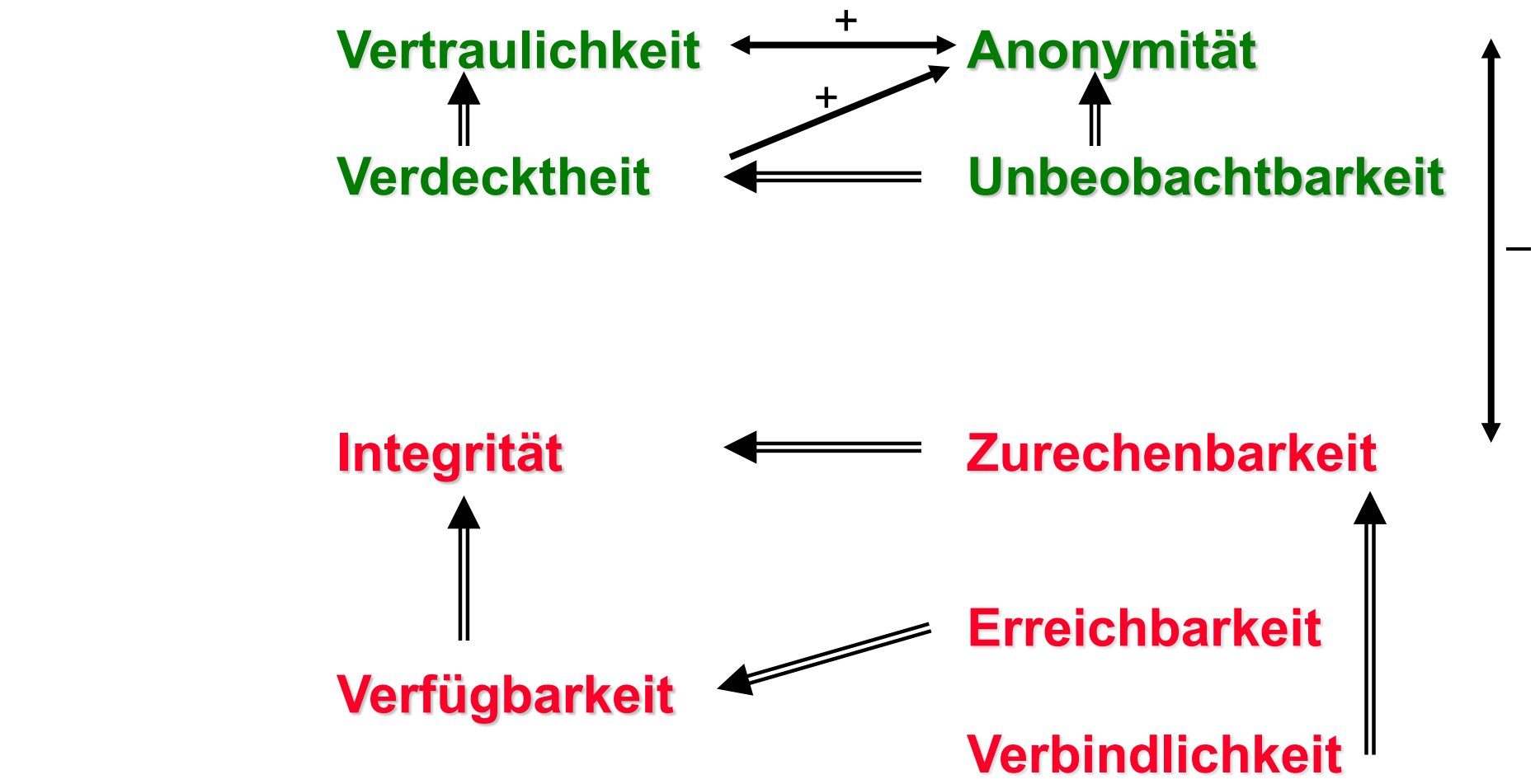
Erreichbarkeit: Zu einer Ressource (Nutzer oder Maschine) kann Kontakt aufgenommen werden, wenn gewünscht.

Verbindlichkeit: Ein Nutzer kann rechtlich belangt werden, um seine Verantwortlichkeiten innerhalb einer angemessenen Zeit zu erfüllen.

Wechselwirkungen zwischen Schutzzielen



Wechselwirkungen zwischen Schutzzielen



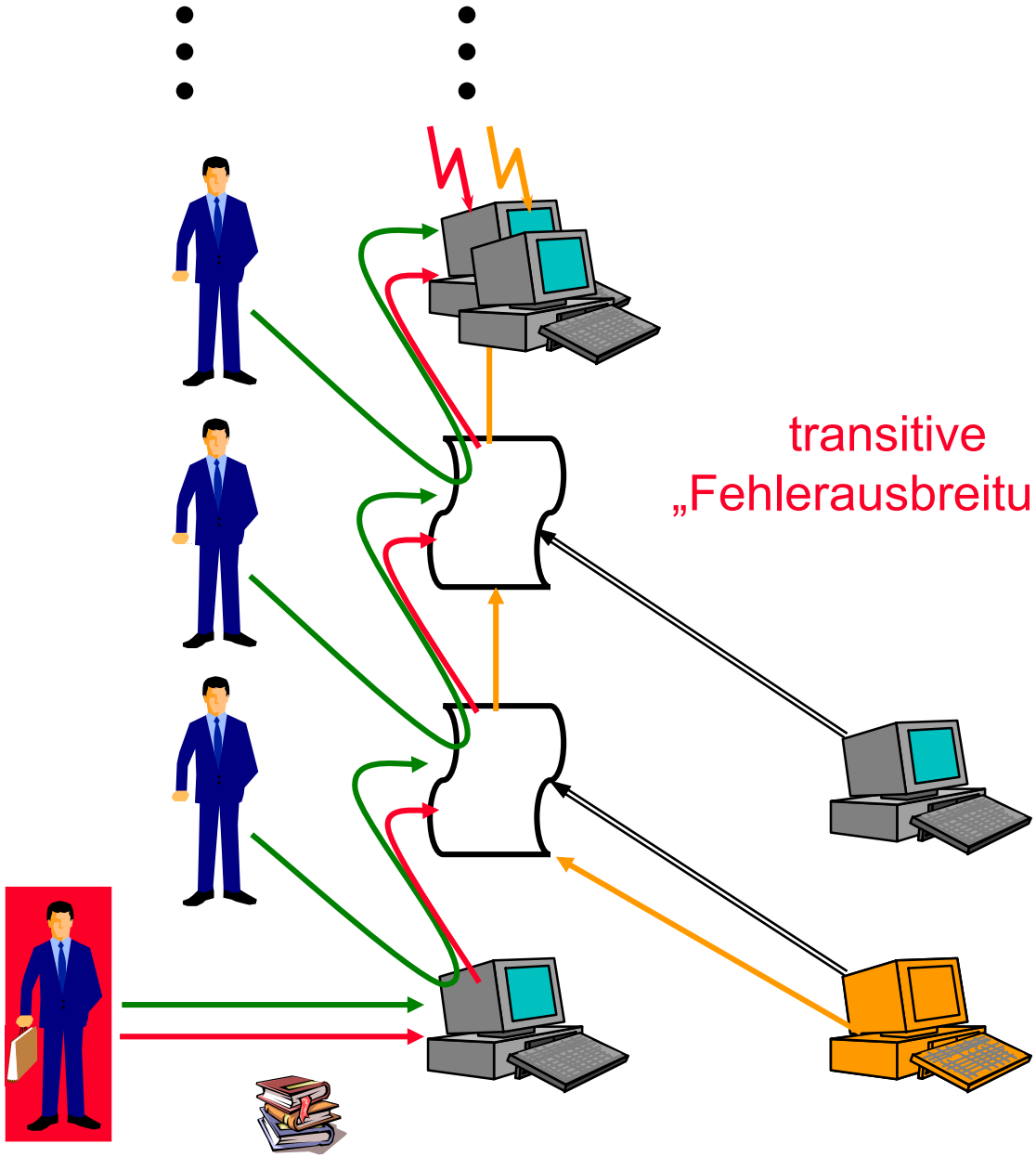
Transitive Hülle hinzufügen

impliziert

+ verstärkt

– schwächt

Transitive Ausbreitung von Fehlern und Angriffen

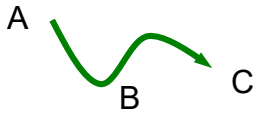


Symbolerklärungen

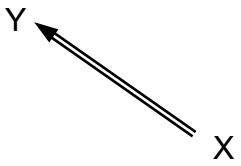
Rechner

Programm

A benutzt B, um
C zu entwerfen



Maschine X führt
Programm Y aus

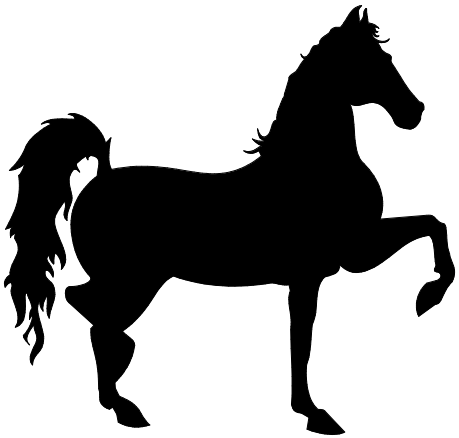


Universelles Trojanisches Pferd

Handlungs-
anweisungen

(verdeckter)
Eingabekanal

universelles



Trojanisches Pferd

(verdeckter)
Ausgabe-Kanal

Informationsgewinn

Schreibzugriff

unbefugte
Modifikation
von Informationen

Schreibzugriff
Nichtterminieren
Betriebsmittelverbrauch

Beeinträchtigung
der Funktionalität

Vor wem ist zu schützen ?

Naturgesetze und Naturgewalten

- Bauteile altern
- Überspannung (Blitzschlag, EMP)
- Spannungsausfall
- Überschwemmung (Sturmflut, Wasserrohrbruch)
- Temperaturänderungen ...

} Fehler-toleranz

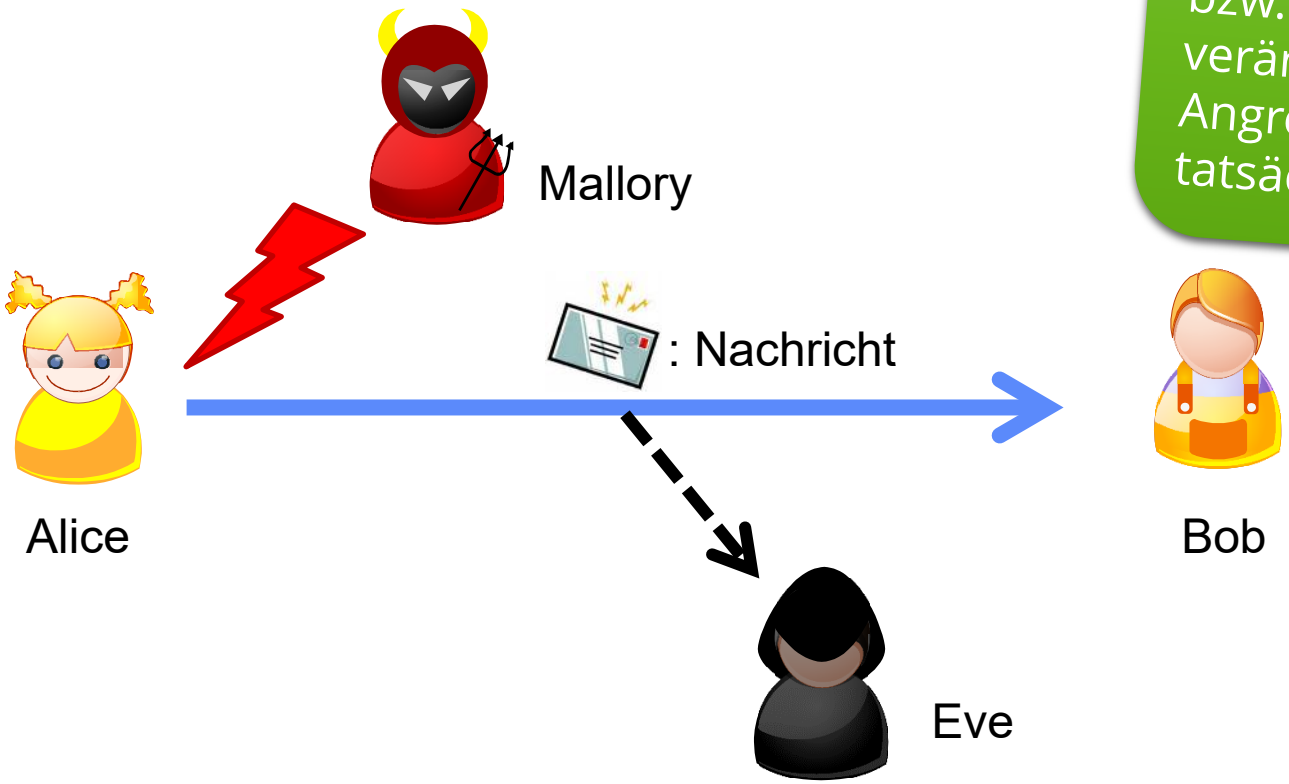
Menschen

- Außenstehende
- Benutzer des Systems
- Betreiber des Systems
- Wartungsdienst
- Produzenten des Systems
- Entwerfer des Systems
- Produzenten der Entwurfs- und Produktionshilfsmittel
- Entwerfer der Entwurfs- und Produktionshilfsmittel
- Produzenten der Entwurfs- und Produktionshilfsmittel der Entwurfs- und Produktionshilfsmittel
- Entwerfer ... jeweils auch Benutzer, Betreiber, Wartungsdienst ... des verwendeten Systems

} Trojanisches Pferd
- universell
- transitiv

Einige Akteure des Spiels

- Die klassischen Datensicherheits-Angreifer…



Was kann ein beobachtender (Eve) bzw. ein verändernder Angreifer (Mallory) tatsächlich tun?

Maximal berücksichtigte Stärke eines Angreifers

Angreifermodell

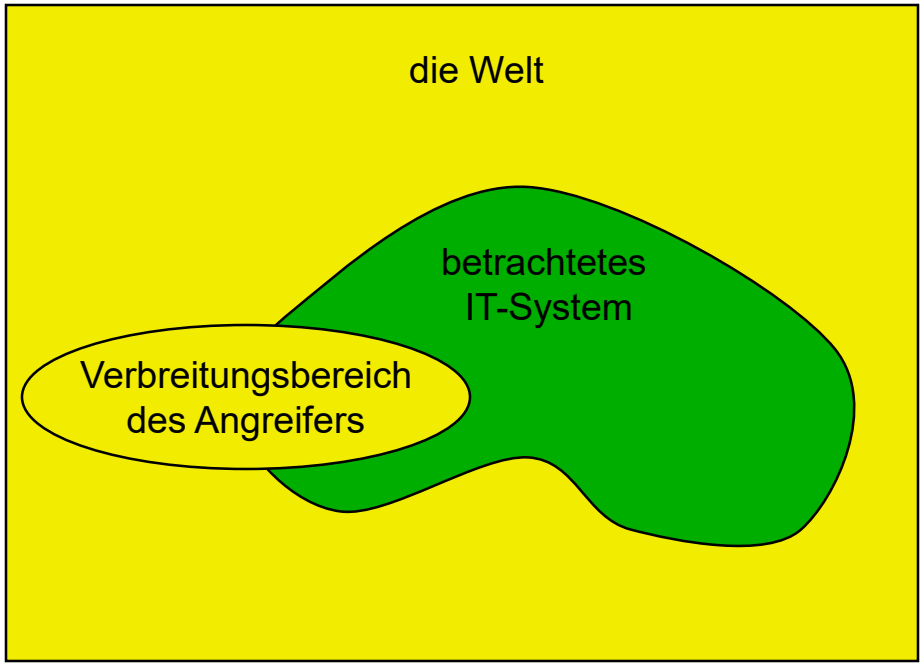
Schutz vor einem allmächtigen Angreifer ist unmöglich.

- Rollen des Angreifers (Außenstehender, Benutzer, Betreiber, Wartungsdienst, Produzent, Entwerfer …), *auch kombiniert*
- Verbreitung des Angreifers
- Verhalten des Angreifers
  - passiv / aktiv
  - beobachtend / verändernd (bzgl. seiner erlaubten Handlungen)
- dumm / intelligent
  - Rechenkapazität:
    - unbeschränkt: informationstheoretisch
    - beschränkt: komplexitätstheoretisch

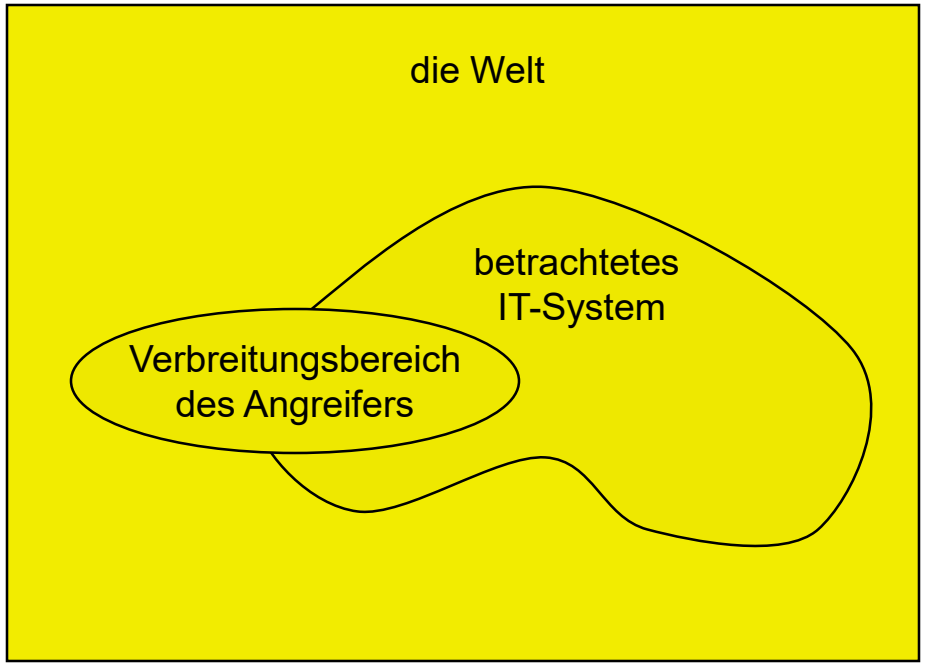
Geld

Zeit

Beobachtender vs. verändernder Angreifer



beobachtender Angreifer



verändernder Angreifer

nur erlaubtes Verhalten

auch verbotenes Verhalten

Stärke eines Angreifer(modell)s

Angreifer(modell) *A* ist stärker als Angreifer(modell) *B*, gdw. *A* in mindestens einer Hinsicht stärker ist als *B* und in keiner Hinsicht schwächer.

Stärker bedeutet:

- Menge der Rollen von *A* $\supset$ Menge der Rollen von *B*,
- Verbreitung von *A* $\supset$ Verbreitung von *B*,
- Verhalten des Angreifers
  - aktiv ist stärker als passiv
  - verändernd ist stärker als beobachtend
- intelligent ist stärker als dumm
  - Rechenkapazität: unbeschränkt ist stärker als beschränkt
- mehr Geld bedeutet stärker
- mehr Zeit bedeutet stärker

Definiert partielle Ordnung auf Angreifer(modelle)n.

Realistische Schutzziele/Angreifermodelle: Technische Lösung möglich?

Üblicherweise:

Je stärker der Angreifer des aufwendiger (teurer) die Sicherheitsmaßnahmen

Sicherheit in Rechnernetzen

Vertraulichkeit

- Nachrichteninhalte vertraulich — **Ende-zu-Ende-Verschlüsselung mit Konzelationssystem**
- **Ort**
  - Sender / Empfänger anonym — **Verfahren zum Schutz der Verkehrsdaten**

Integrität

- Fälschungen erkennen — **Authentikationssystem(e)**
- Empfänger kann Senden der Nachricht beweisen — **Nachrichten signieren**
- **Zeit**
  - Absender kann Senden beweis. — **Empfangsquittung**
- Nutzungsentgelte sichern — **während Diensterbringung mittels digitaler Zahlungssysteme**

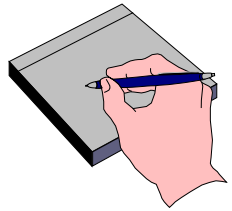
Verfügbarkeit

- Kommunikation ermöglichen — **Diversitäre Netze; faire Betriebsmittelaufteilung**

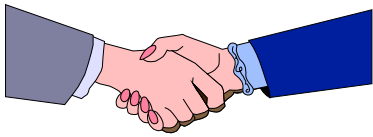
Mehrseitige Sicherheit

- Jeder Beteiligte hat eigene Sicherheitsinteressen.

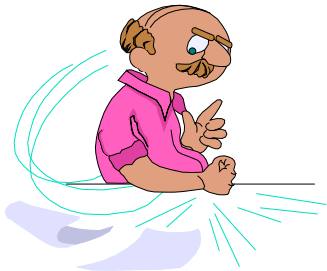
- Jeder Beteiligte kann seine Sicherheitsinteressen formulieren.



- Konflikte werden erkannt und Lösungen ausgehandelt.



- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen durchsetzen.

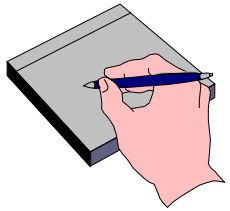


Sicherheit mit minimalen Annahmen über andere

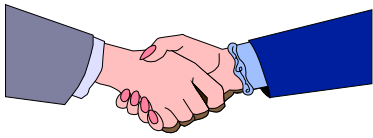
Mehrseitige Sicherheit (2. Version)

- Jeder Beteiligte hat eigene Interessen.

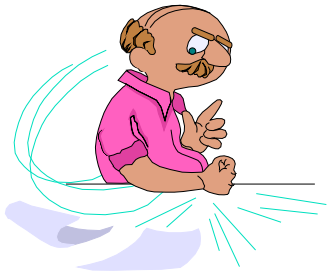
- Jeder Beteiligte kann seine Sicherheitsinteressen formulieren.



- Konflikte werden erkannt und Lösungen ausgehandelt.



- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen durchsetzen.

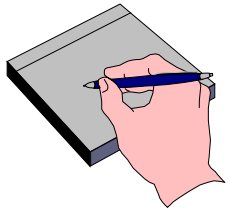


Sicherheit mit minimalen Annahmen über andere

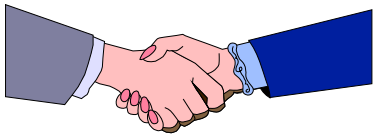
Mehrseitige Sicherheit (3. Version)

- Jeder Beteiligte hat eigene Interessen.

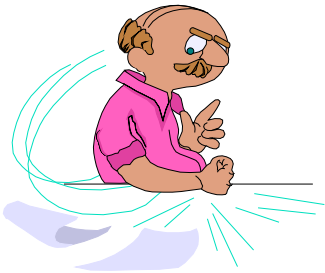
- Jeder Beteiligte kann seine Sicherheitsinteressen formulieren.



- Konflikte werden erkannt und Lösungen ausgehandelt.



- Jeder Beteiligte kann seine Sicherheitsinteressen in den ausgehandelten Lösungen durchsetzen. Grenzen der Durchsetzbarkeit betreffen alle Beteiligten in gleicher Weise.



Sicherheit mit minimalen Annahmen über andere

Physische Sicherheitsannahmen

Alle technischen Schutzmaßnahmen brauchen physische „Verankerung“ in einem Systemteil, auf den der Angreifer weder lesenden noch verändernden Zugriff hat.

Spektrum vom „Rechenzentrum X“ bis zur „Chipkarte Y“

Was kann man bestenfalls erwarten ?

Verfügbarkeit eines räumlich konzentrierten Systemteils ist gegen durchaus *vorstellbare* Angreifer nicht gewährleistbar

$\rightarrow$ **physisch verteiltes System**

und hoffen, dass Angreifer nicht an vielen Orten gleichzeitig sein kann.

Verteilung erschwert **Vertraulichkeit** und **Integrität.**

Physische Maßnahmen bzgl. Vertraulichkeit und Integrität jedoch wirkungsvoller: Schutz gegen *alle* derzeit *vorstellbaren* Angreifer scheint erreichbar. Gelingt dies hinreichend, steht physischer Verteilung nichts im Wege.

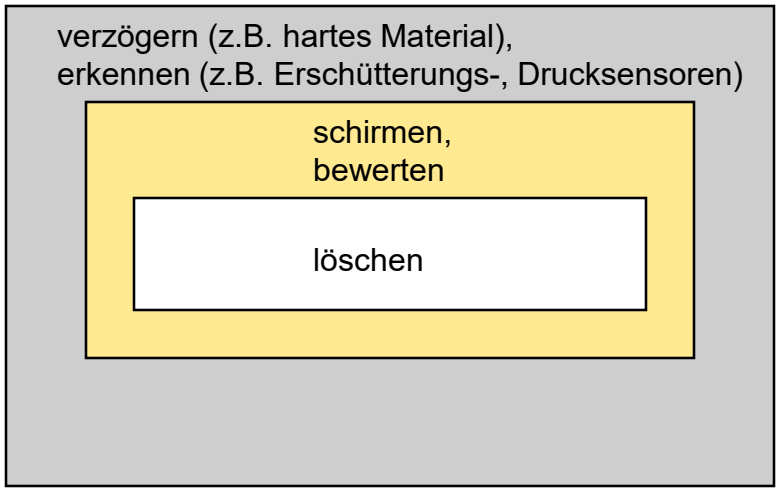
Unmanipulierbare Gehäuse

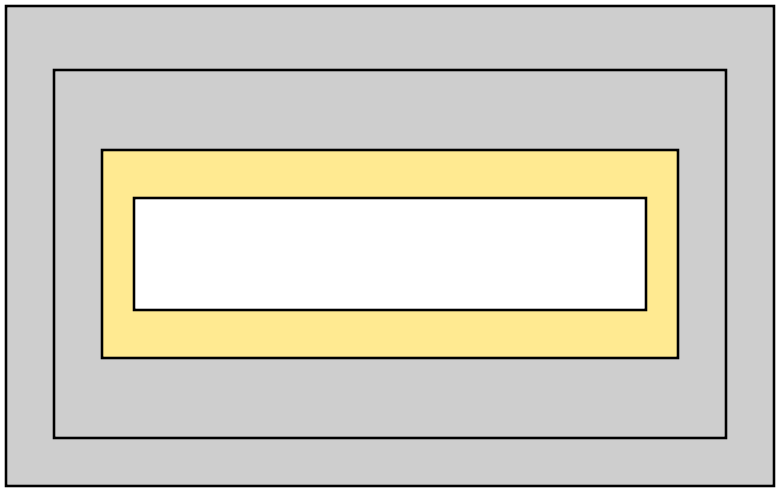
Eingriff: Erkennen
Bewerten

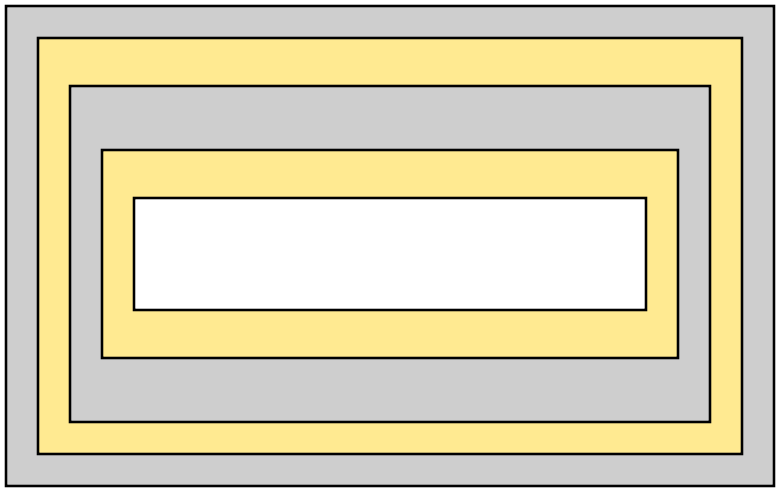
Angriff: Verzögern
Daten (etc.) löschen

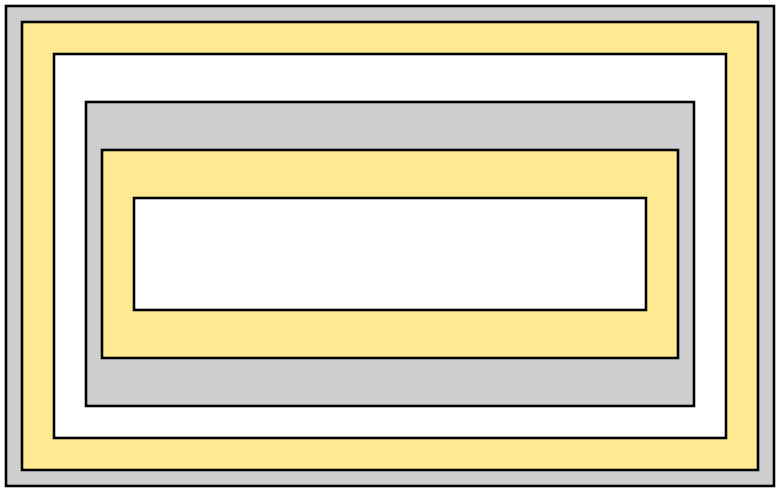
Möglichkeit: mehrere Schichten, Schirmung →

Schalenförmige Anordnung der fünf Grundfunktionen









Unmanipulierbare Gehäuse

Eingriff: Erkennen
Bewerten

Angriff: Verzögern
Daten (etc.) löschen

Möglichkeit: mehrere Schichten, Schirmung

Problem: Validierung ... Glaubwürdigkeit

Negativ-Beispiel: Chipkarten

- kein Erkennen (u.a. Batterie fehlt)
- Schirmung schwierig (Karte dünn und biegbar)
- kein Löschen vorgesehen selbst bei Strom-versorgung

Goldene Regel

Übereinstimmung zwischen organisatorischen und informationstechnischen Strukturen

Datenschutz: Risiken

- Risiken für den Datenschutz durch IKT
  - Schnelle Erfassung und Auswertung von Daten möglich
  - Möglichkeit der unbemerkten Datenerhebung
  - Kontrolle schwierig

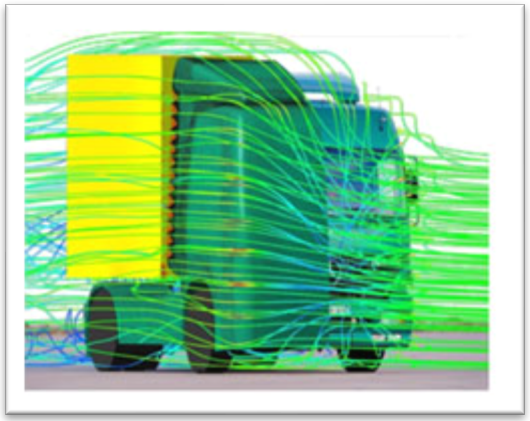
→ Notwendigkeit des Datenschutzes

- Datenschutz

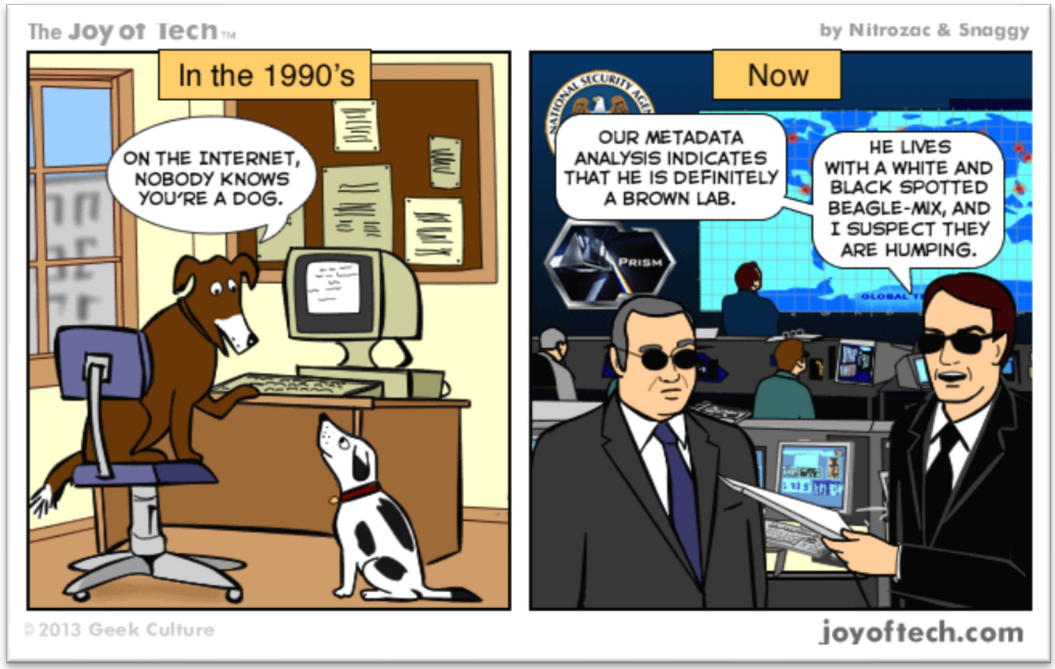
  = Schutz der Privatsphäre

Aber welche Daten denn?

- Daten ohne ***Personenbezug***
  - Simulationsdaten
  - Messungen in Experimenten



- Daten ***mit Personenbezug***
  - Arten
    - Inhalte
    - Verkehrsdaten
  - Veröffentlichung
    - Bewusst
    - Unbewusst



Beobacht- und Ableitbare Information

- Bewußt veröffentlicht
  - Texte, Bilder
  - Kommentare
  - Beziehungen (Freunde, Kontakte, Likes)

- Unbewußt veröffentlicht / abgeleitet
  - Name (Gesichtserkennung)
  - Krankheiten (Bild, Text, Videoanalyse)
  - Alter (Bild, Name)

- „Metadaten“
  - *Zeitpunkt / Dauer von Aktivitäten*
  - *Ort*
  - *Kommunikationspartner*
  - *genutzte Programme/Geräte*
  - *Clickstream*

Identifizierung von Menschen– auch ohne Gesichtserkennung

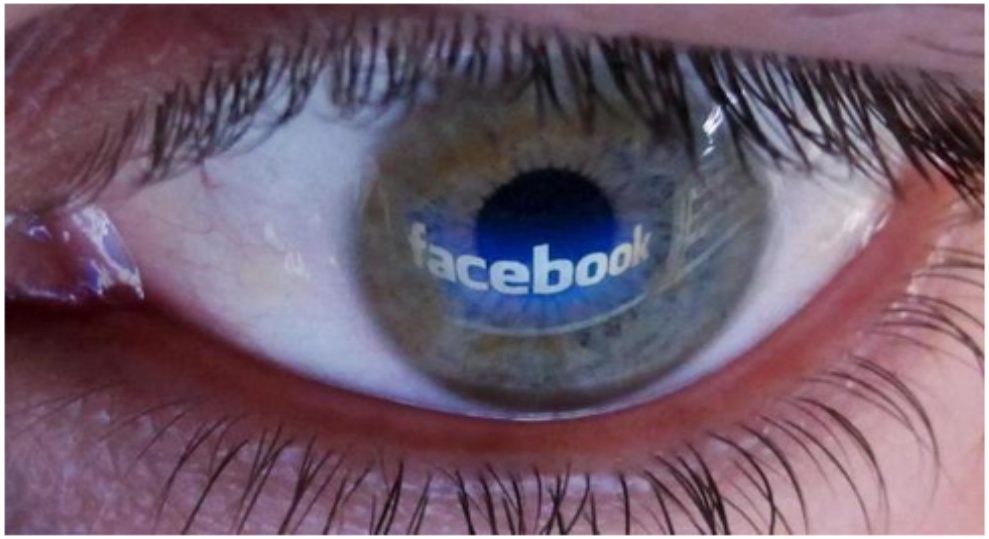
Facebook erkennt Gesicht

www.heise.de/newsticker/meldung/Facebook-erkennt-Gesichter-und-Frisuren-2722422.html

heise online > News > 2015 > KW 26 > Facebook erkennt Gesichter – und Frisuren

23.06.2015 15:40 « Vorige | Nächste »

Facebook erkennt Gesichter – und Frisuren



(Bild: dpa, Jochen Lübke)

Facebook hat einen experimentellen Algorithmus entwickelt, der Menschen an ihrer Körperhaltung, Kleidung und ihrer Frisur identifizieren kann.

Beobacht- und Ableitbare Information

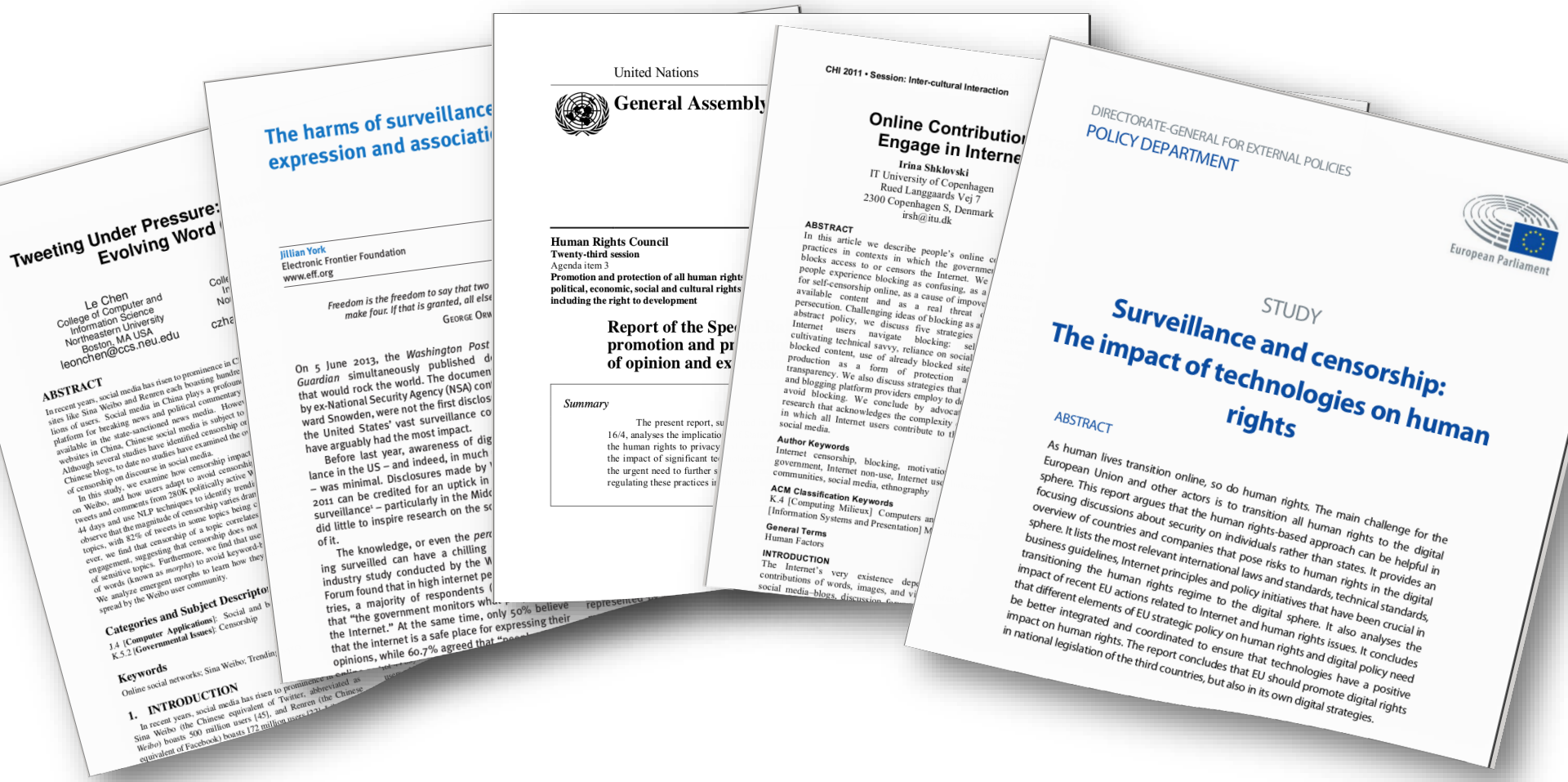
- Bewußt veröffentlicht
  - Texte, Bilder
  - Kommentare
  - Beziehungen (Freunde, Kontakte, Likes)

- Unbewußt veröffentlicht / abgeleitet
  - Name (Gesichtserkennung)
  - Krankheiten (Bild, Text, Videoanalyse)
  - Alter (Bild, Name)

- „Metadaten“
  - *Zeitpunkt / Dauer von Aktivitäten*
  - *Ort*
  - *Kommunikationspartner*
  - *genutzte Programme/Geräte*
  - *Clickstream*

- Extern verkettet
  - Profilbildung in Werbe-Netzen

„Ich hab nichts zu verbergen“



Tweeting Under Pressure: Evolving Word

Le Chen
College of Computer and Information Science
Northeastern University
Boston, MA USA
leonchen@ccs.neu.edu

ABSTRACT

Categories and Subject Descriptor

Keywords

1. INTRODUCTION

The harms of surveillance expression and associati

Jillian York
Electronic Frontier Foundation
www.eff.org

Freedom is the freedom to say that two make four. If that is granted, all else

GEORGE ORW

On 5 June 2013, the Washington Post Guardian simultaneously published d that would rock the world. The documen by ex-National Security Agency (NSA) con ward Snowden, were not the first disclos the United States' vast surveillance co have arguably had the most impact.

Before last year, awareness of dig lance in the US – and indeed, in much – was minimal. Disclosures made by 2011 can be credited for an uptick in surveillance – particularly in the Mid did little to inspire research on the sc of it.

The knowledge, or even the perc ing surveilled can have a chilling industry study conducted by the W Forum found that in high internet pe tries, a majority of respondents the Internet." At the same time, only 50% believe that the internet is a safe place for expressing their opinions, while 60.7% agreed that

United Nations

General Assembly

Human Rights Council
Twenty-third session
Agenda item 3
Promotion and protection of all human rights political, economic, social and cultural rights including the right to development

Report of the Spe promotion and pr of opinion and ex

Summary

The present report, su 16/4, analyses the implicatio the human rights to privacy the impact of significant te the urgent need to further s regulating these practices i

CHI 2011 • Session: Inter-cultural Interaction

Online Contributio Engage in Interne

Irina Shklovski
IT University of Copenhagen
Rued Langgaards Vej 7
2300 Copenhagen S, Denmark
irsh@itu.dk

ABSTRACT

Author Keywords

ACM Classification Keywords

General Terms

INTRODUCTION

DIRECTORATE-GENERAL FOR EXTERNAL POLICIES
POLICY DEPARTMENT

European Parliament

STUDY

Surveillance and censorship: The impact of technologies on human rights

ABSTRACT

As human lives transition online, so do human rights. The main challenge for the European Union and other actors is to transition all human rights to the digital sphere. This report argues that the human rights-based approach can be helpful in focusing discussions about security on individuals rather than states. It provides an overview of countries and companies that pose risks to human rights in the digital sphere. It lists the most relevant international laws and standards, technical standards, business guidelines, Internet principles and policy initiatives that have been crucial in transitioning the human rights regime to the digital sphere. It also analyses the impact of recent EU actions related to Internet and human rights issues. It concludes that different elements of EU strategic policy on human rights and digital policy need be better integrated and coordinated to ensure that technologies have a positive impact on human rights. The report concludes that EU should promote digital rights in national legislation of the third countries, but also in its own digital strategies.

Privatheitsverständnis: Right to be let alone

- Samuel Warren, ***Louis Brandeis***: "**The Right to Privacy**", Harvard Law Review, Vol. IV, No. 5, 15th December **1890**

- **Grund:** "snapshot photography" (technische Neuerung)
  - Ermöglichte Zeitungen Bilder von Personen ohne deren Einwilligung zu veröffentlichen
  - Privatpersonen wurden in ihrer Individualität verletzt
  - Befürchtung, dass "moralische Standards" in Gefahr seien

- **Überlegung:**
  - Grundprinzip des Gewohnheitsrechts: Schutz von Person und Besitz des Individuums
  - *"it has been found necessary from time to time to define anew the exact nature and extent of such protection"*
  - *"Political, social, and economic changes entail the recognition of new rights"*

- **Schlussfolgerung:**
  - "**right to be let alone**"
  - Konsequenz hier: Opt-out

Vs.: Informationelle Selbstbestimmung

- Europäisches Grundverständnis (Volkszählungsurteil 1983, BRD)

- Vorletzter Zensus in Deutschland (1981 geplant, stark verzögert)
- Starke öffentliche Opposition
  - Angst vor der Überwachungsgesellschaft
  - Diskussion des „gläsernen Menschen“
  - Öffentliche Aufforderungen zum zivilen Ungehorsam
  - Durchgeführt 1987
  - Resultat war Anfangsfehler von 25%

*…für die Preisgabe minimaler Informationen, dem **Staat** gegenüber*

Grundidee der Kontrolle des Individuums über die es betreffenden Daten
Konsequenz: das BDSG von ‘90, Opt-in und anschließende Kontrolle*(!)*

Recht auf "informationelle Selbstbestimmung"

- Volkszählungs-Urteil (BVerfGE 65,1 - 15. Dezember 1983)

„Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffende Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden. Mit dem ***Recht auf informationelle Selbstbestimmung*** *wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß."*

„Ein Zwang zur Angabe personenbezogener Daten setzt voraus, daß der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und daß die Angaben für diesen Zweck geeignet und erforderlich sind. Damit wäre die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken nicht zu vereinbaren "

Ihr Recht auf Datenschutz

- *„Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.“* (Art 8, Eur. Menschenrechtskonvention)

- Recht auf informationelle Selbstbestimmung im BDSG:
- *„Recht des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.“*

- Für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten gilt:
- ***Verbot mit Erlaubnisvorbehalt***

- Erforderlich: rechtliche Grundlage durch (noch):
  - Gesetzliche Grundlage (BDSG) (DSGVO ab 5/18) oder
  - andere Rechtsvorschrift (z.B. Betriebsvereinbarung)
  - Einwilligung des Betroffenen
    - Ausreichende Information
    - Freiwilligkeit
    - Widerruflichkeit

Was ist Personen-beziehbar?

- Legal: ***P***ersonally ***I***dentifiable ***I***nformation / ***PII***
  - ***US:*** *Name, address (Phone, Email), national identifiers (tax, passports), IP address, driving (vehicle registration, drivers licence), biometrics (face, fingerprints), credit card numbers, date/place of birth (age, login name(s), gender, "race", grades, salary, criminal records)*
  - ***EU:*** *'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;* [Art. 4, GDPR]

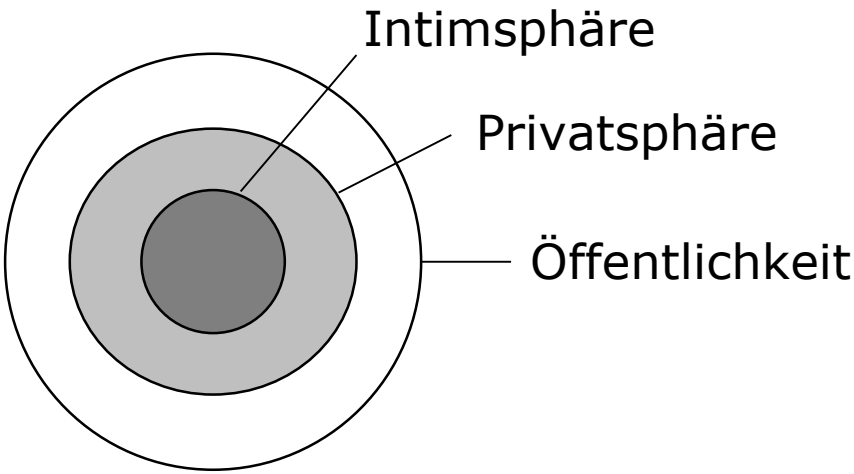
Bei welcher Verarbeitung?

- *'processing' means **any operation** or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as **collection**, **recording**, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, **disclosure by transmission**, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;* [ebd]

- Auch pseudonyme Daten:
- *'pseudonymisation' means the processing of personal data in such a manner that the personal data **can no longer be attributed to a specific data subject** without the use of **additional information**, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;* [ebd]

Datenschutz: Sphärenmodell

- Bereiche unterschiedlicher Schutzwürdigkeit durch konzentrische Kreise (z.B. 3) dargestellt, nach außen hin abnehmende Schutzwürdigkeit

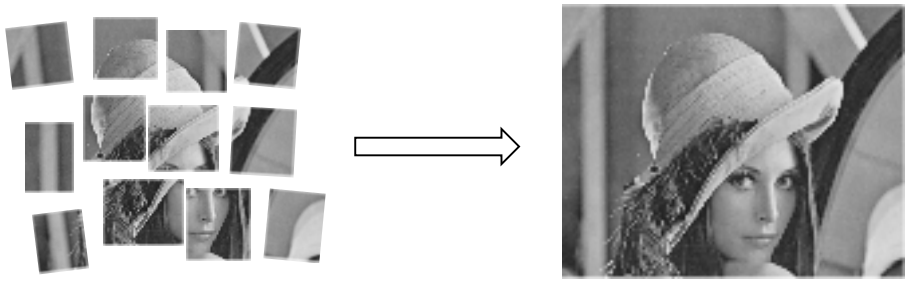


Information zu einer Person

- Zuordnung der Daten zu den Sphären individuell
- Zuordnung auch abhängig von Situation

Datenschutz: Mosaikmodell

- ***Idee:***
- Informationen über Menschen lassen sich in Teile zerlegen
- Zusammenfügen von Einzelteilen ergibt präzises Gesamtbild

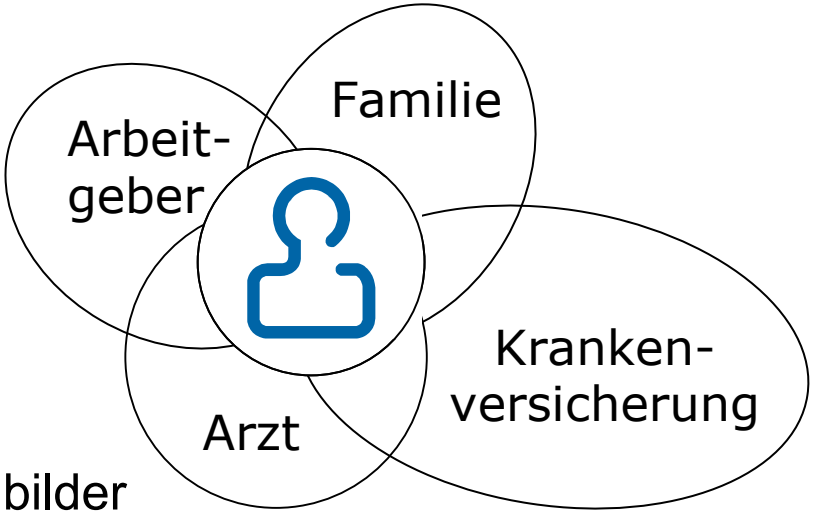


- Mosaikmodell berücksichtigt auch Schutz von Daten, die laut *Sphärenmodell* nicht zum absolut schützenswerten Bereich gehören
- Zugriff auf einzelnen Teile nicht dargestellt
- Überprüfung, welche Verknüpfungen kritisch sind, ist schwierig
- Nicht nur Datenerfassung, auch Datenverarbeitung berücksichtigen!

Datenschutz: Rollenmodell

- ***Idee:***
- Menschen agieren in Rollen
- Darlegung aller Informationen nicht notwendig zu deren Erfüllung

- Statt Trennung der Daten in Bereiche verschiedener Sensibilität:
- Erzeugung von Einzelbildern



- Beibehaltung der Trennung der Einzelbilder
- Selbstbestimmung der Datenweitergabe nur bedingt (problematisch z.B. gegenüber öffentlichen Behörden)

Datenschutzprinzipien

- Datensparsamkeit
- Datenminimierung
- Datenvermeidung
- Verhältnismäßigkeit

Mosaikmodell

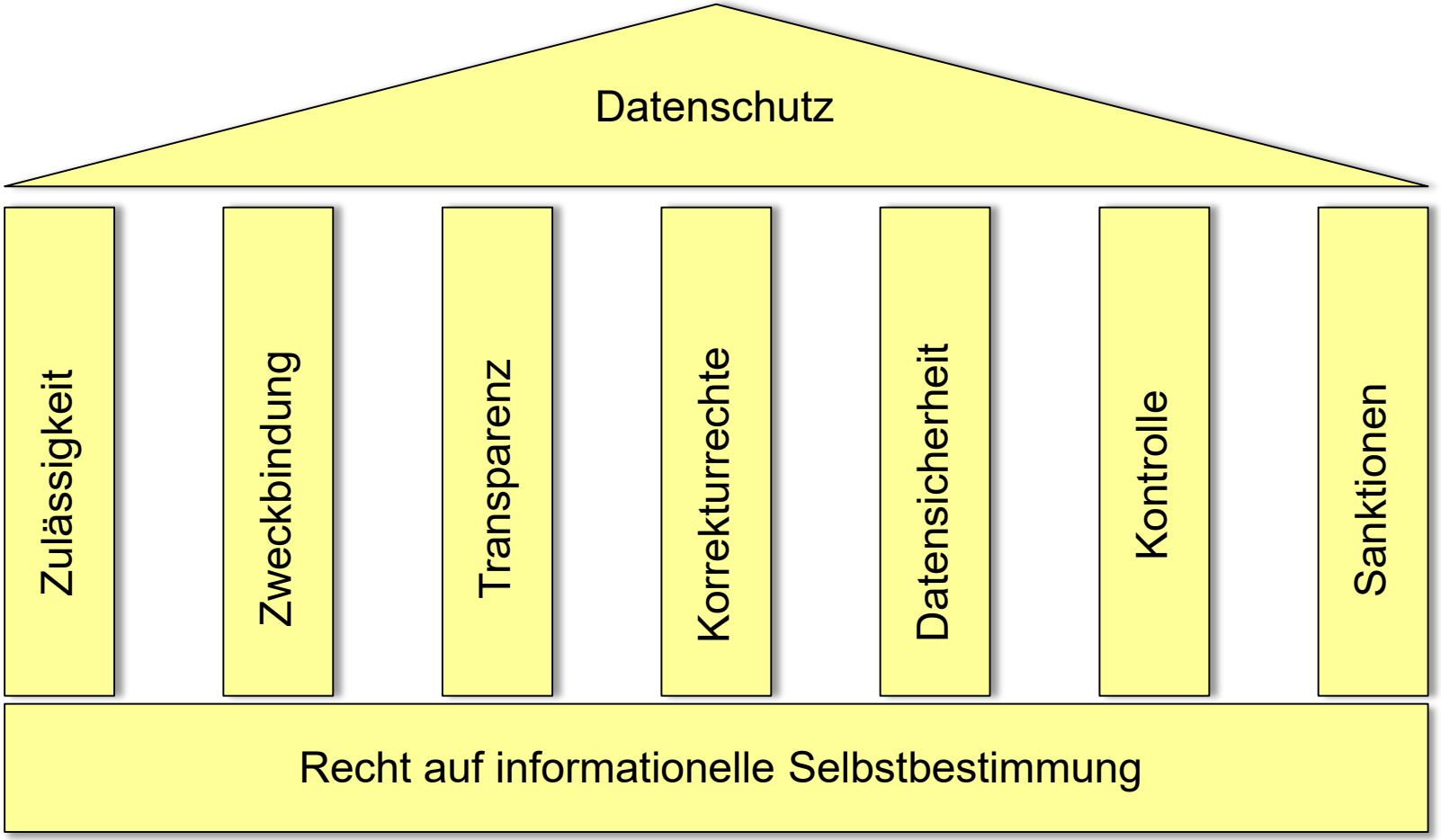
- Zweckbindung

Rollenmodell

- Transparenz
- Zustimmung
- Auskunftsrecht
- Recht auf Löschung und Berichtigung
- besonders geschützte Daten

Sphärenmodell

7 Säulen der Informat. Selbstbestimmung



Prinzipien des Datenschutzes (DSGVO)

1. Rechtmäßigkeit, Fairness, Transparenz
2. Zweckbindung
3. Datenminimierung
4. Richtigkeit („*unverzügliche Löschung oder Korrektur*“)
5. Speicherbegrenzung (für den Zweck notwendig)
6. Integrität und Vertraulichkeit
7. Rechenschaftspflicht (Accountability)

Datenschutz Prinzipien

- Rechtmäßigkeit, Fairness, Transparenz
- Informierte Einwilligung („informed consent“)
- Notwendigkeit für
  - Vertragserfüllung
  - legale Pflichten.

Datenschutz – Transparenz

- ***Informationspflicht***: verantwortliche Stelle muss aktiv werden
- ***Auskunftsanspruch:*** von Betroffenen geltend zu machen

- Erhebung erfolgt grundsätzlich beim Betroffenen
- → Unterrichtung des Betroffenen durch verantwortliche Stelle über
  - Identität der verantwortlichen Stelle
  - Zweck der Erhebung, Verarbeitung und Nutzung
  - Kategorien von Empfängern

- Auskunftsanspruch: zusätzlich Art und Umfang gespeicherter Daten, Herkunft und Empfänger
- Auskunft (grundsätzlich) unentgeltlich

Datenschutz Prinzipien

- Zweckbindung
- Verwendungszweck muss bei Erhebung festgelegt sein
- Information der Betroffenen notwendig
- Zweckänderung erfordert gesonderte Legitimation

- Datensparsamkeit:
  - Begrenzung auf die für den jeweiligen Zweck ***notwendigen*** Daten
  - Möglichkeiten der Anonymisierung bzw. Pseudonymisierung
  - Löschen nicht mehr benötigter Daten (bzw. Sperren)

Datenschutz – Korrektur, Kontrolle, Sanktion

4% Jahresumsatz 2016:

Facebook: 1.4 Mrd €
Apple: 2.6 Mrd €
Deutsche Telekom: 2.9 Mrd €
Google: 3 Mrd €
Amazon: 4.6 Mrd €
Daimler (Connected Cars): 5.2 Mrd €

Korrekturrechte

- Berichtigung
- Löschen bzw. Sperren
- Widerspruch

Kontrolle

- Intern: betrieblicher Datenschutzbeauftragter
- Extern: Aufsichtsbehörde

- Rechenschaftspflicht
- Datenverarbeitende Stelle muss über Verwendung Nachweis erbringen (wie?)

Sanktionen

- Bußgeld: 4% des Jahresumsatzes

Notions of Privacy: Contextual Integrity

- Helen Nissenbaum: *Privacy as Contextual Integrity*, Washington Law Review, 2004
- close relation to data protection principles:
  - purpose binding
- Idea:
  - privacy violation, if:
    - violation of **Appropriateness**
      - the context „defines“ if revealing a given information is appropriate
      - **violation:** usage of information disclosed in one context in another context (even if first context is a “public” one)
    - violation of **Distribution**
      - the context „defines“ which information flows are appropriated
      - **violation:** inappropriate information flows

Datenschutz und Datensicherheit

- Datenschutz ist sinnvoll, denn man sollte wissen, wer welche personenbezogenen Daten zu welchem Zweck speichert und nutzt.

- Man muß sich darüber klar sein, welche Daten man preisgeben will.

- Man sollte nur das für den jeweiligen Zweck erforderliche Minimum an personenbezogenen Daten preisgeben.

- *Wie sicher sind Ihre Daten, haben Sie darüber Kontrolle?*
- *Google play? App Store anybody?*

Principles of PETs

- Privacy-enhancing Technologies (PETs)
  - Information suppression tools (Opacity tools)
  - Transparency-enhancing tools (TETs)
- Opacity Tools:
  - Anonymization, pseudonymization, obfuscation
- Transparency-enhancing Tools:
  - Informing user about data collection, purpose etc.
  - Informing about impact of data collection (needed for „informed consent“)
  - Enables checks whether data collection is conform to legal regulation
  - Various techniques:
    Secure Logging, Audits, Quality Seals, Policies etc.

Transparency-enhancing Tool