ulm university universität ulm

Grundlagen des Datenschutzes und der IT-Sicherheit

Ergänzungen zu den Vorlesungsfolien von Bernhard C. Witt

Tobias Schleinkofer | Sommersemester 2007
Fingerprint: CD0153D0FD997CC205C90A89C713A76B32E386AC

Nomenklatur von Gesetzen

- interessanter Link: http://bundesrecht.juris.de
- Beispiel BDSG:
- „§ 1 Abs. 2 Nr. 2 lit. b BDSG“

§ 1 Zweck und Anwendungsbereich des Gesetzes

(1) Zweck dieses Gesetzes ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezoger

(2) Dieses Gesetz gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch

1. öffentliche Stellen des Bundes,
2. öffentliche Stellen der Länder, soweit der Datenschutz nicht durch Landesgesetz geregelt ist und soweit sie
   a) Bundesrecht ausführen oder
   b) als Organe der Rechtspflege tätig werden und es sich nicht um Verwaltungsangelegenheiten handelt,
3. nicht-öffentliche Stellen, soweit sie die Daten unter Einsatz von Datenverarbeitungsanlagen verarbeiten, nutzen oder verarbeiten, nutzen oder dafür erheben, es sei denn, die Erhebung, Verarbeitung oder Nutzung der Daten erfolgt ausso

(3) Soweit andere Rechtsvorschriften des Bundes auf personenbezogene Daten einschließlich deren Veröffentlichung anzuwe Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die

Nomenklatur von Gesetzen

- Beispiel Grundgesetz:
- „Art. 72 Abs. 2 Nr. 2 GG“

Art 72

(1) Im Bereich der konkurrierenden Gesetzgebung haben die Länder die Befugnis zur Gesetzgebung, solange
Gebrauch gemacht hat.

(2) Auf den Gebieten des Artikels 74 Abs. 1 Nr. 4, 7, 11, 13, 15, 19a, 20, 22, 25 und 26 hat der Bund das Gesetz
Bundesgebiet oder die Wahrung der Rechts- oder Wirtschaftseinheit im gesamtstaatlichen Interesse eine bun

(3) Hat der Bund von seiner Gesetzgebungszuständigkeit Gebrauch gemacht, können die Länder durch Gesetz

1. das Jagdwesen (ohne das Recht der Jagdscheine);
2. den Naturschutz und die Landschaftspflege (ohne die allgemeinen Grundsätze des Naturschutzes, da
3. die Bodenverteilung;

Normenhierarchie

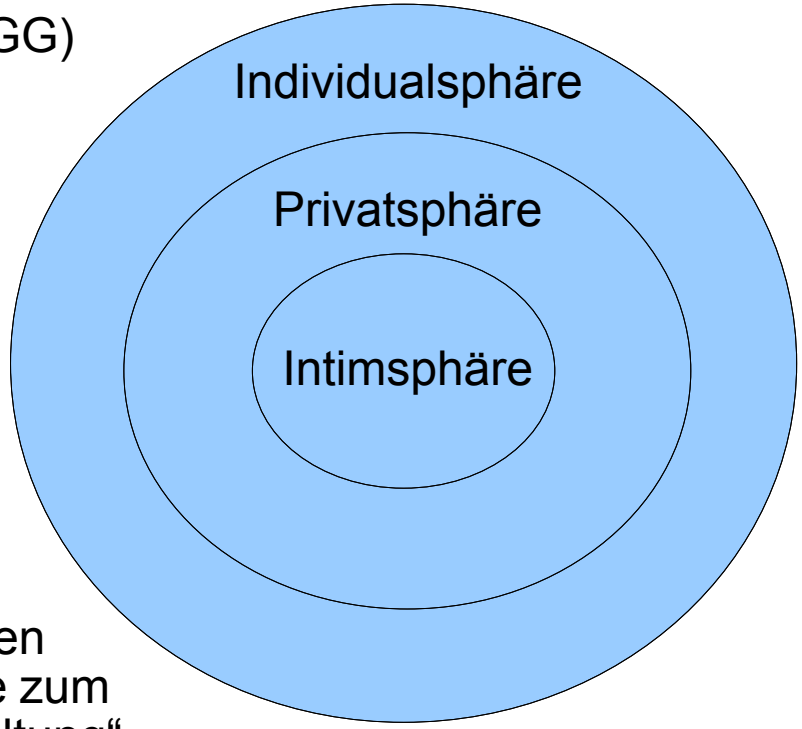
- interessanter Link: http://de.wikipedia.org/wiki/Normenhierarchie
- in D:
- Grundgesetz
  - Landesverfassungen
  - Bundesgesetze
    - Verordnungen
      - » Erlasse
- in EU:
- Verordnungen
  - „zwingende“ Richtlinien
  - Richtlinien mit „Spielraum“
- aber: Art. 23 GG => EU-Verordnungen höherwertig als GG

Begriffsbestimmungen

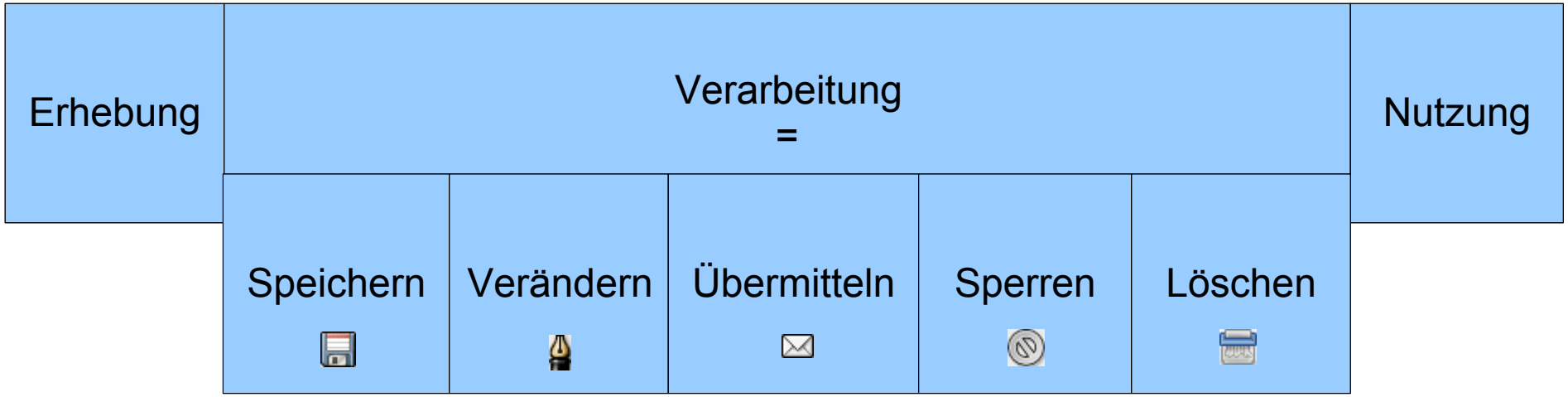
- bei „Datum“ nicht immer nur an eine Zeitangabe denken; im Datenschutzkontext auch Singular von „Daten“ ;-)
- also „Tobias, Schleinkofer, tobias.schleinkofer@uni-ulm.de, Student, männlich“ sind **Daten**, „Tobias“ ist ein **Datum**
- „0“ und „1“ sind **Zeichen**
- „010000100100001101010111“sind **Daten**
- „010000100100001101010111“sind **Informationen**, wenn sie als ASCII-Code interpretiert werden
- **Raster(fahnd)ung**: Aus einer Datenbank wird anhand von zuvor festgelegten Kriterien eine Teilmenge (i.d.R. Personen) aller Datensätze herausgefiltert – aktuellstes Beispiel „Operation Mikado“ vom Januar 2007 (welche jedoch von den Gerichten bis jetzt noch nicht als solche angesehen wird)
- Ein **Persönlichkeitsprofil** entsteht, indem (über einen längeren Zeitraum) Eigenschaften/Verhaltensmuster/Vorlieben einer Person mit Hilfe eines Identifikators angesammelt werden – Beispiele: Einkaufsposten auf dem Kassenbon + eindeutige Payback-ID; statische IP + angesurfte Webseiten

Sphären

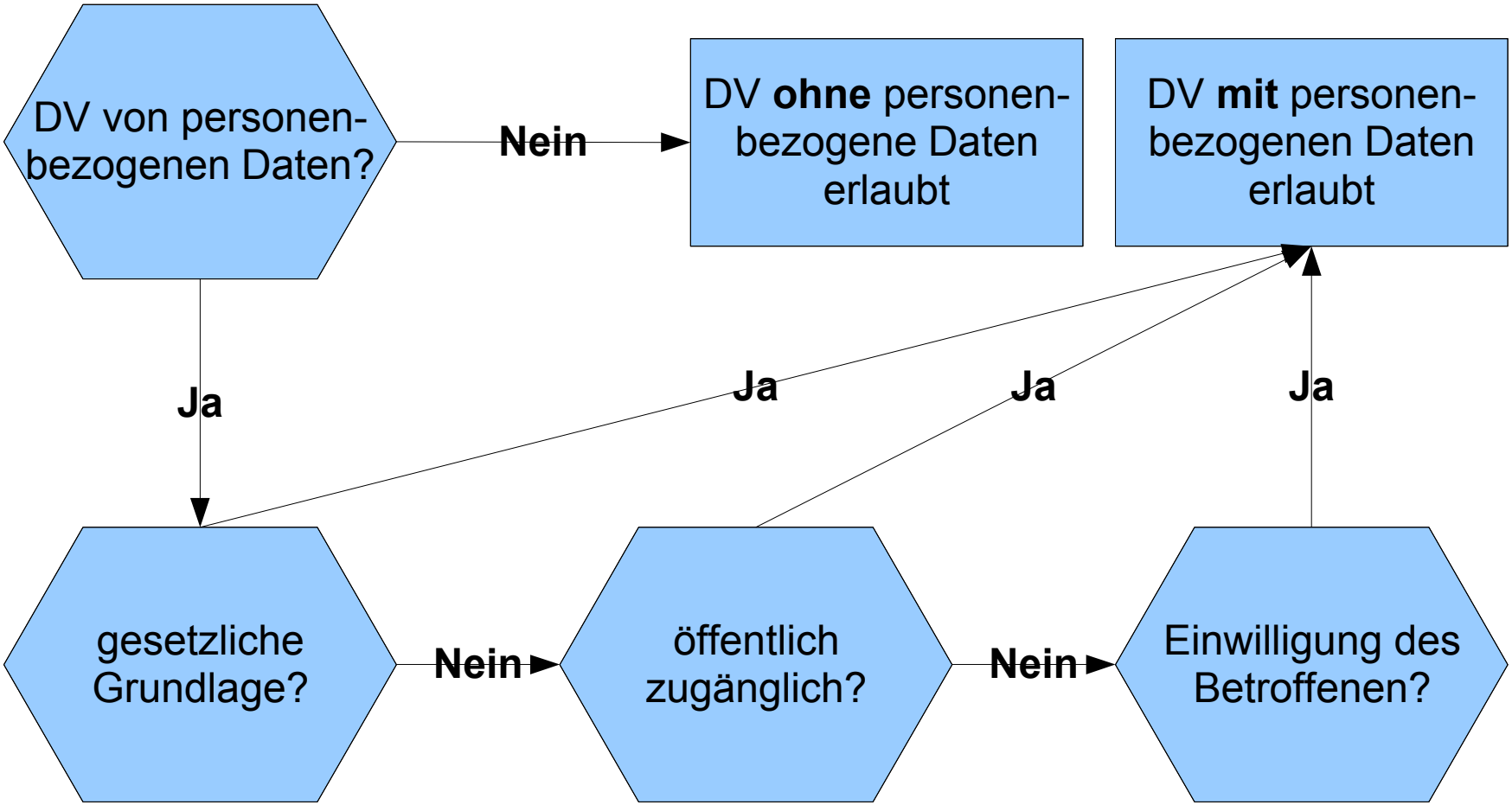
- Allgemeines Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG)
- informationelle Selbstbestimmung gehört bspw. zur Individualsphäre
- Aufnahmen ohne Zustimmung gehören bspw. zur Privatsphäre
- Sexualbereich gehört bspw. zur Intimsphäre
- seit dem Volkszählungsurteil werden jedoch diese Sphäre üblicherweise zum „Kernbereich privater Lebensgestaltung“ zusammengefasst
- interessanter Link: http://de.wikipedia.org/wiki/Allgemeines_Persönlichkeitsrecht



Erhebung, Nutzung, Verarbeitung



Zulässigkeit Datenverarbeitung von personenbezogenen Daten



Datenschutzaufsichtsbehörden in Deutschland

- oftmals Trennung der Zuständigkeit von öffentlichen und nicht-öffentlichen Stellen und Eingliederung in Innenministerien
- deswegen jedoch seit 2005 Vertragsverletzungsverfahren gegen Deutschland durch die EU wegen unzureichender Umsetzung der EU-Datenschutzrichtlinie (mangelnde Unabhängigkeit)
- interessante Links:
  EU-Datenschutzrichtlinie
  http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML

  Vertragsverletzungsverfahren
  http://www.heise.de/newsticker/meldung/62007

Datenschutzaufsichtsbehörden in Deutschland (Stand: 05-2007)

- **Baden-Württemberg:**
  Zuständigkeit für öffentliche Stellen des Landes:
  LfD Peter Zimmermann
  http://www.baden-wuerttemberg.datenschutz.de
  Zuständigkeit für nicht-öffentliche Stellen im Land:
  LMI Baden-Württemberg
  http://www.innenministerium.baden-wuerttemberg.de
- **Bayern:**
  Zuständigkeit für öffentliche Stellen des Landes:
  LfD Karl Michael Betzl
  http://www.baden-wuerttemberg.datenschutz.de
  Zuständigkeit für nicht-öffentliche Stellen im Land:
  Regierung von Mittelfranken
  http://www.regierung.mittelfranken.bayern.de
- **Berlin:**
  Zuständigkeit für öffentliche Stellen des Landes **und** für nicht-öffentliche Stellen im Land:
  LfDI Alexander Dix
  http://www.datenschutz-berlin.de

Datenschutzaufsichtsbehörden in Deutschland (Stand: 05-2007)

- **Brandenburg:**
  Zuständigkeit für öffentliche Stellen des Landes:
  LfDI Dagmar Hartge
  http://www.lda.brandenburg.de
  Zuständigkeit für nicht-öffentliche Stellen im Land:
  LMI Brandenburg
  http://www.mi.brandenburg.de
- **Bremen:**
  Zuständigkeit für öffentliche Stellen des Landes **und** für nicht-öffentliche Stellen im Land:
  LfDI Sven Holst
  http://www.datenschutz-bremen.de
- **Bund:**
  Zuständigkeit für öffentliche Stellen des Bundes:
  BfDI Peter Schaar
  http://www.bfdi.bund.de

Datenschutzaufsichtsbehörden in Deutschland (Stand: 05-2007)

- **Hamburg:**
  Zuständigkeit für öffentliche Stellen des Landes **und** für nicht-öffentliche Stellen im Land:
  LfD Hartmut Lubomierski
  http://www.datenschutz.hamburg.de
- **Hessen:**
  Zuständigkeit für öffentliche Stellen des Landes:
  LfD Michael Ronellenfitsch
  http://www.datenschutz.hessen.de
  Zuständigkeit für nicht-öffentliche Stellen im Land:
  Regierungspräsidium
  http://www.rp-darmstadt.hessen.de
- **Mecklenburg-Vorpommern:**
  Zuständigkeit für öffentliche Stellen des Landes **und** für nicht-öffentliche Stellen im Land:
  LfDI Karsten Neumann
  http://www.lfd.m-v.de/

Datenschutzaufsichtsbehörden in Deutschland (Stand: 05-2007)

- **Niedersachsen:**
  Zuständigkeit für öffentliche Stellen des Landes:
  LfD Joachim Wahlbrink
  http://www.lfd.niedersachsen.de
  Zuständigkeit für nicht-öffentliche Stellen im Land:
  LMI Niedersachsen
  http://www.mi.niedersachsen.de
- **Nordrhein-Westfalen:**
  Zuständigkeit für öffentliche Stellen des Landes **und** für nicht-öffentliche Stellen im Land:
  LfDI Bettina Sokol
  http://www.ldi.nrw.de
- **Rheinland-Pfalz:**
  Zuständigkeit für öffentliche Stellen des Landes:
  LfD Edgar Wagner
  http://www.datenschutz.rlp.de
  Zuständigkeit für nicht-öffentliche Stellen im Land:
  LMI Rheinland-Pfalz
  http://www.ism.rlp.de

Datenschutzaufsichtsbehörden in Deutschland (Stand: 05-2007)

- **Saarland:**
  Zuständigkeit für öffentliche Stellen des Landes:
  LfD Roland Lorenz
  http://www.lfdi.saarland.de
  Zuständigkeit für nicht-öffentliche Stellen im Land:
  LMI Saarland
  http://www.innen.saarland.de
- **Sachsen:**
  Zuständigkeit für öffentliche Stellen des Landes:
  LfD Andreas Schurig
  http://www.datenschutz.sachsen.de
  Zuständigkeit für nicht-öffentliche Stellen im Land:
  LMI Sachsen
  http://www.smi.sachsen.de

Datenschutzaufsichtsbehörden in Deutschland (Stand: 05-2007)

- **Sachsen-Anhalt:**
  Zuständigkeit für öffentliche Stellen des Landes:
  LfD Harald von Bose
  http://www.datenschutz.sachsen-anhalt.de
  Zuständigkeit für nicht-öffentliche Stellen im Land:
  LMI Sachsen-Anhalt
  http://www.mi.sachsen-anhalt.de
- **Schleswig-Holstein:**
  Zuständigkeit für öffentliche Stellen des Landes **und** für nicht-öffentliche Stellen im Land:
  LfDI Thilo Weichert
  http://www.datenschutzzentrum.de
- **Thüringen:**
  Zuständigkeit für öffentliche Stellen des Landes:
  LfD Harald Stauch
  http://www.datenschutz.thueringen.de
  Zuständigkeit für nicht-öffentliche Stellen im Land:
  LMI Thüringen
  http://www.thueringen.de/de/tim

Kontroll- vs Lizenzprinzip

- bspw. in D Kontrollprinzip: DV von personenbezogenen Daten ist unter Beachtung datenschutzrechtlicher Gesetze (wie BDSG) erlaubt. Aufsichtsbehörden und DSBs kontrollieren deren Einhaltung.
- bspw. in F Lizenzprinzip: DV von personenbezogenen Daten ist erst nach Erhalt einer Lizenz erlaubt. Lizenzgeber ist die Commission nationale de l'Informatique et des libertés (www.cnil.fr). Wer des Französischen mächtig ist, kann dort mal nach den offiziellen Unterlagen suchen ;-)

Datenschutz im nicht-öffentlichen Bereich

- Hilfe zur Selbsthilfe: Robinsonlisten, in die sich Verbraucher aufnehmen lassen können, um vor Werbung verschont zu bleiben
- für Briefpost: Robinsonliste beim deutschen Direktmarketingverband (www.dvv.de)
- für Fax: Robinsonliste bei Retarus GmbH (www.retarus.de) - Träger ist die Bitkom Servicegesellschaft (www.bitkom-service.org)
- für eMail, SMS, Telefon: Robinsonlisten beim Interessenverband deutsches Internet (www.idi.de)
- oder generell, falls möglich: „keeping a low profile“ - keine Aufnahme in Telefonbücher, Wegwerf-eMailadressen, ...

Vorratsdatenspeicherung (VDS)

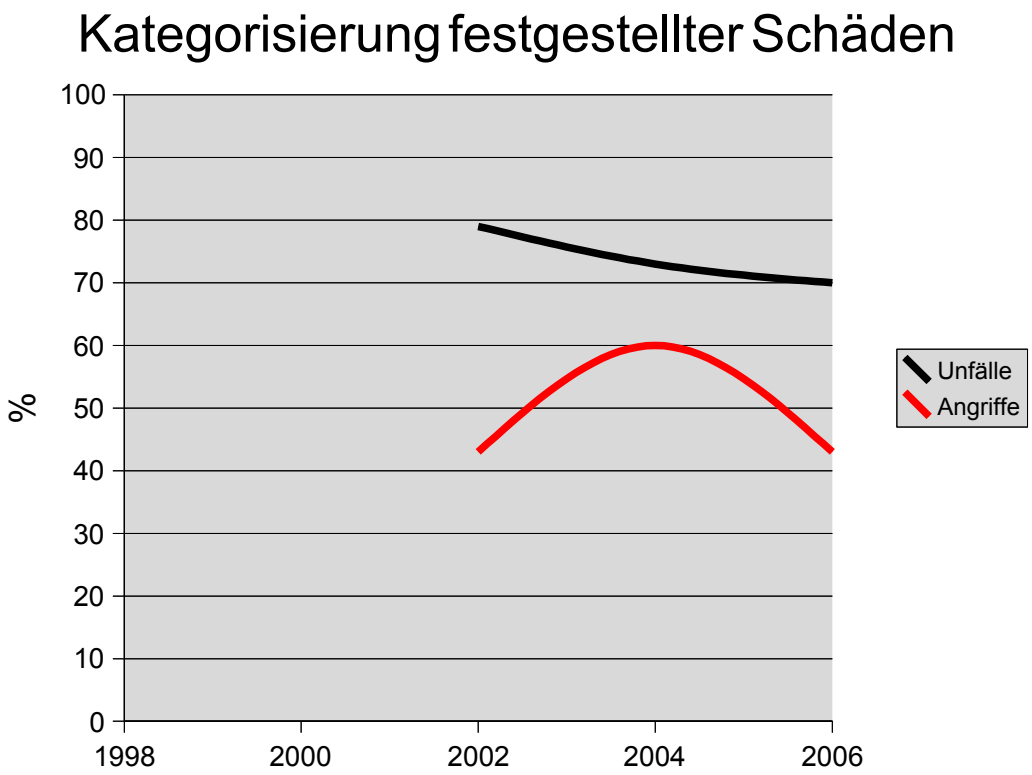
- http://de.wikipedia.org/wiki/Vorratsdatenspeicherung + http://www.vorratsdatenspeicherung.de
- träfe nicht auf Arbeitgeber zu, die ihren Mitarbeitern die Privatnutzung des Internets am Arbeitsplatz untersagt haben
- Zeitraum der Speicherung kann von EU-Mitgliedsstaaten gewählt werden (6 Monate bis 2 Jahre)
- Achtung (hypothetisches Beispiel: D -> 6 Monate, F -> 2 Jahre): Kommuniziert man via Internet mit einem französischen Server würde die Verbindung in D 6 Monate, in F 2 Jahre gespeichert – egal ob WWW, eMail, Usenet, VoIP, ...
- Speicherung „nur“ der Verkehrs- und Standortdaten – **nicht** der Inhaltsdaten (also „Wer mit wem wann“ nicht „Wer mit wem wann **was**“)

Sicherheitsstandards

- ISO = International Organization for Standardization
- IEC = International Electrotechnical Commission
- ISO/IEC = Bezeichnung von Normen, die gemeinsam von ISO und IEC entwickelt werden
- ISO/IEC TR = Technical Reports, die von der ISO veröffentlicht werden

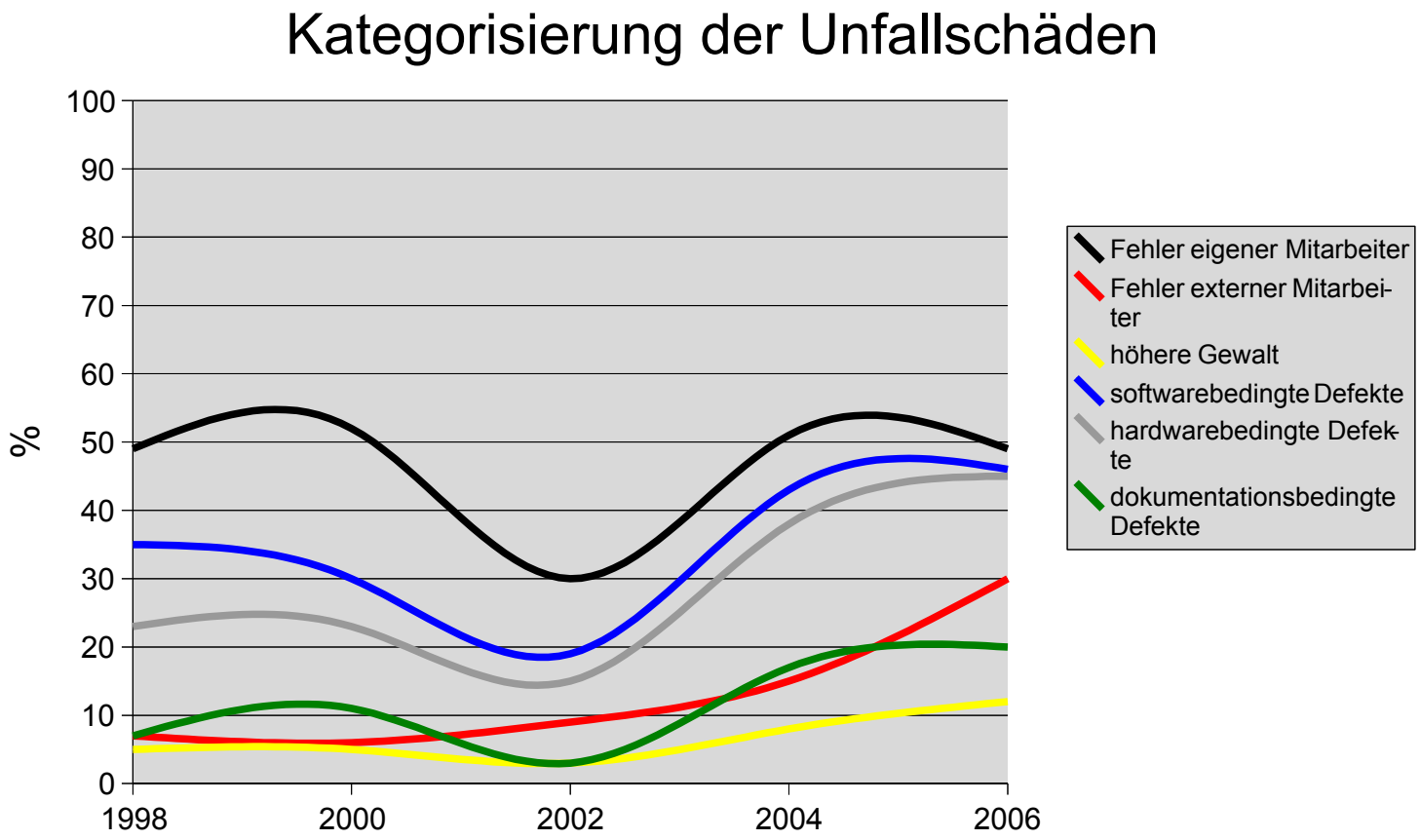
Mehrseitige IT-Sicherheit

– grafische Darstellung der <kes>-Statistiken



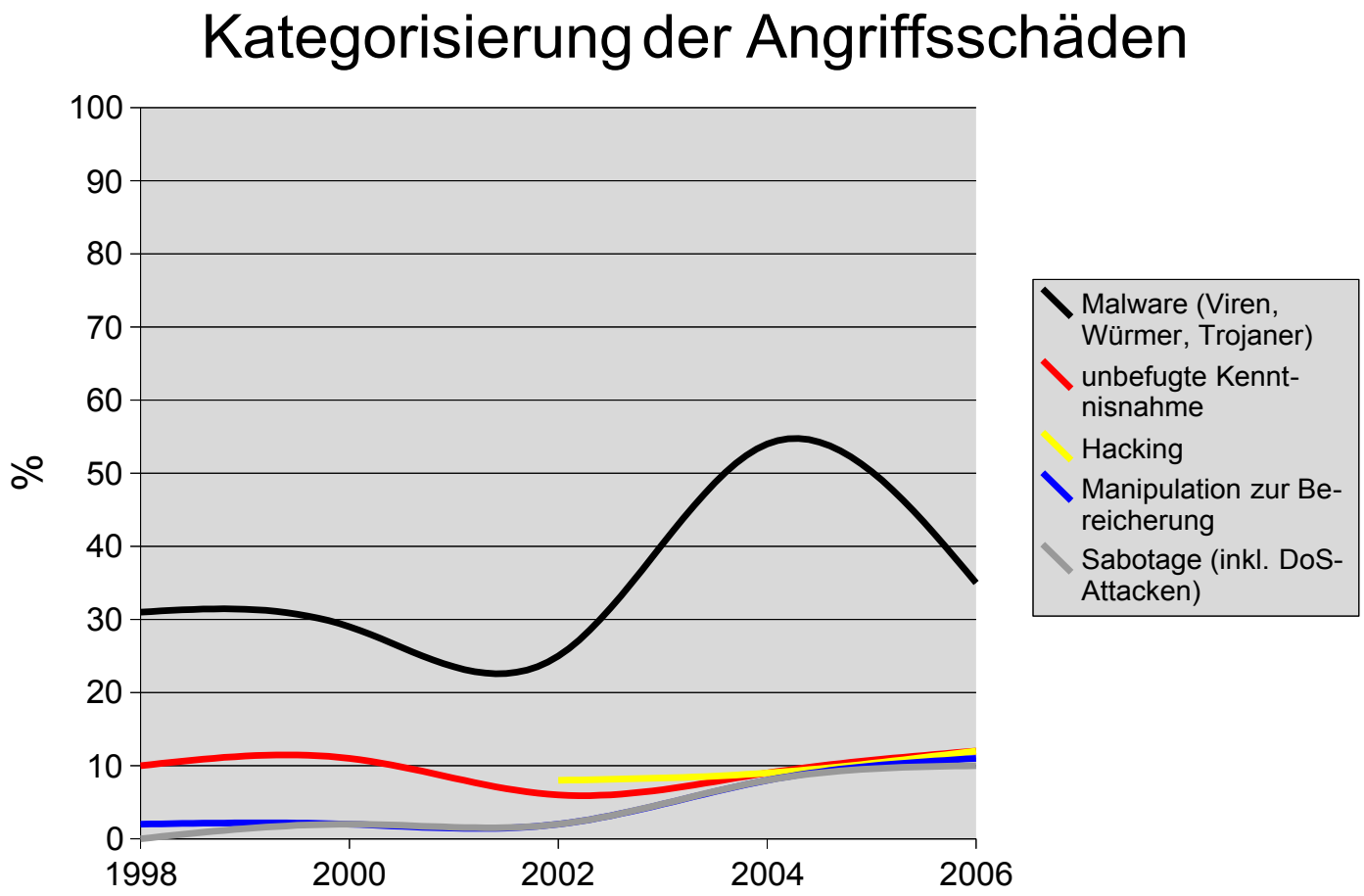
Mehrseitige IT-Sicherheit

– grafische Darstellung der <kes>-Statistiken



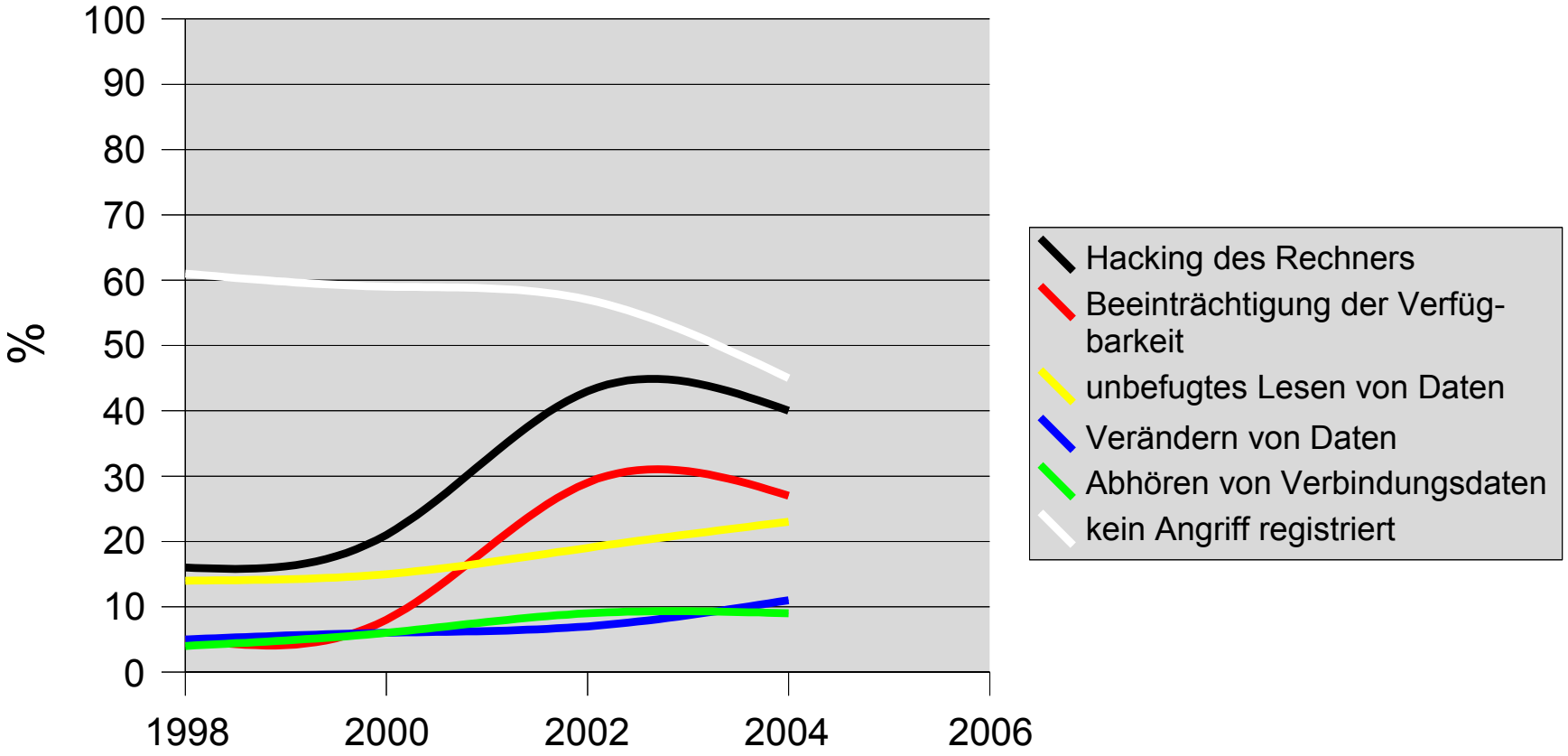
Mehrseitige IT-Sicherheit

– grafische Darstellung der <kes>-Statistiken



Mehrseitige IT-Sicherheit

- grafische Darstellung der <kes>-Statistiken
- „Ursachen von Angriffen aus dem Internet“



Mehrseitige IT-Sicherheit

- „Fehler eigener Mitarbeiter“: Entgegenwirken durch Schulungen oder Verbesserung der Bedienbarkeit durch Usability-Maßnahmen
- „höhere Gewalt“: hierzu zählen u.a. auch Streiks!
- „dokumentationsbedingte Defekte“: korreliert mit „Fehler eigener Mitarbeiter“
- „unbefugte Kenntnisnahme“: Feststellung u.U. mit zeitlicher Verzögerung

Berechnung der Verfügbarkeit

$$Verfügbarkeit = \frac{(\sum Betriebszeit - \sum Ausfallzeit)}{\sum Betriebszeit}$$

- Problem: „Ausfallzeit“ schwer bestimmbar, wenn das System, für welches die Verfügbarkeit errechnet werden soll, nicht ununterbrochen genutzt wird? Bspw. wird ein eMail-Server nur beim Abrufen und Senden von eMails in Anspruch genommen.
- daher die Intervalle zwischen Ausfällen mit den Reparaturen ins Verhältnis setzen:

$$Verfügbarkeit = \frac{MTBF}{(MTBF + MTTR)} = \frac{(\varnothing\ Ausfallintervall)}{(\varnothing\ Ausfallintervall + \varnothing\ Reparaturintervall)}$$

$$= \frac{\left(\frac{\sum Betriebszeit}{\sum Ausfälle}\right)}{\left(\left(\frac{\sum Betriebszeit}{\sum Ausfälle}\right) + \left(\frac{\sum Reparaturzeit}{\sum Ausfälle}\right)\right)} = \frac{\sum Betriebszeit}{(\sum Betriebszeit + \sum Reparaturzeit)}$$

- Formel bezieht sich auf **ein einzelnes** System. Die Gesamtverfügbarkeit mehrerer Teilsysteme errechnet sich aus dem **Produkt** der einzelnen Verfügbarkeiten dieser Teilsysteme.

Berechnung der Verfügbarkeit

- Redundanz erhöht Verfügbarkeit

$$Verfügbarkeit_{Redundanz} = 1-(1-Verfügbarkeit)^{Anzahl\ Systeme}$$

- Beispiel:
  eMail-Server Verfügbarkeit ohne Redundanz 80%:

$$Verfügbarkeit = 1-(1-0{,}8)^{1} = 0{,}8$$

  eMail-Server Verfügbarkeit mit zwei redundanten Systemen:

$$Verfügbarkeit = 1-(1-0{,}8)^{2} = 0{,}96$$

  eMail-Server Verfügbarkeit mit vier redundanten Systemen:

$$Verfügbarkeit = 1-(1-0{,}8)^{4} = 0{,}9984$$

IPSec, VPN, Verschlüsselung

- Skript der Vorlesung Rechnernetze 1:
  http://www-vs.informatik.uni-ulm.de/teach/ws05/rn1/docs/RN1_k05_04_OSI_Referenzmodell.pdf
- IPSec erweitert IPv4; die Funktionalität von IPSec ist in IPv6 bereits integriert
- neben symmetrischen und asymmetrischen Verschlüsselungsverfahren, gibt es auch hybride Verfahren (bspw. SSL oder OpenPGP), bei denen mittels asymmetrischer Verschlüsselung ein Sitzungsschlüssel ausgetauscht und die übrige Kommunikation damit symmetrisch verschlüsselt wird
- Anzahl notweniger Schlüsseltauschvorgänge bei *n* Kommunikationspartnern:

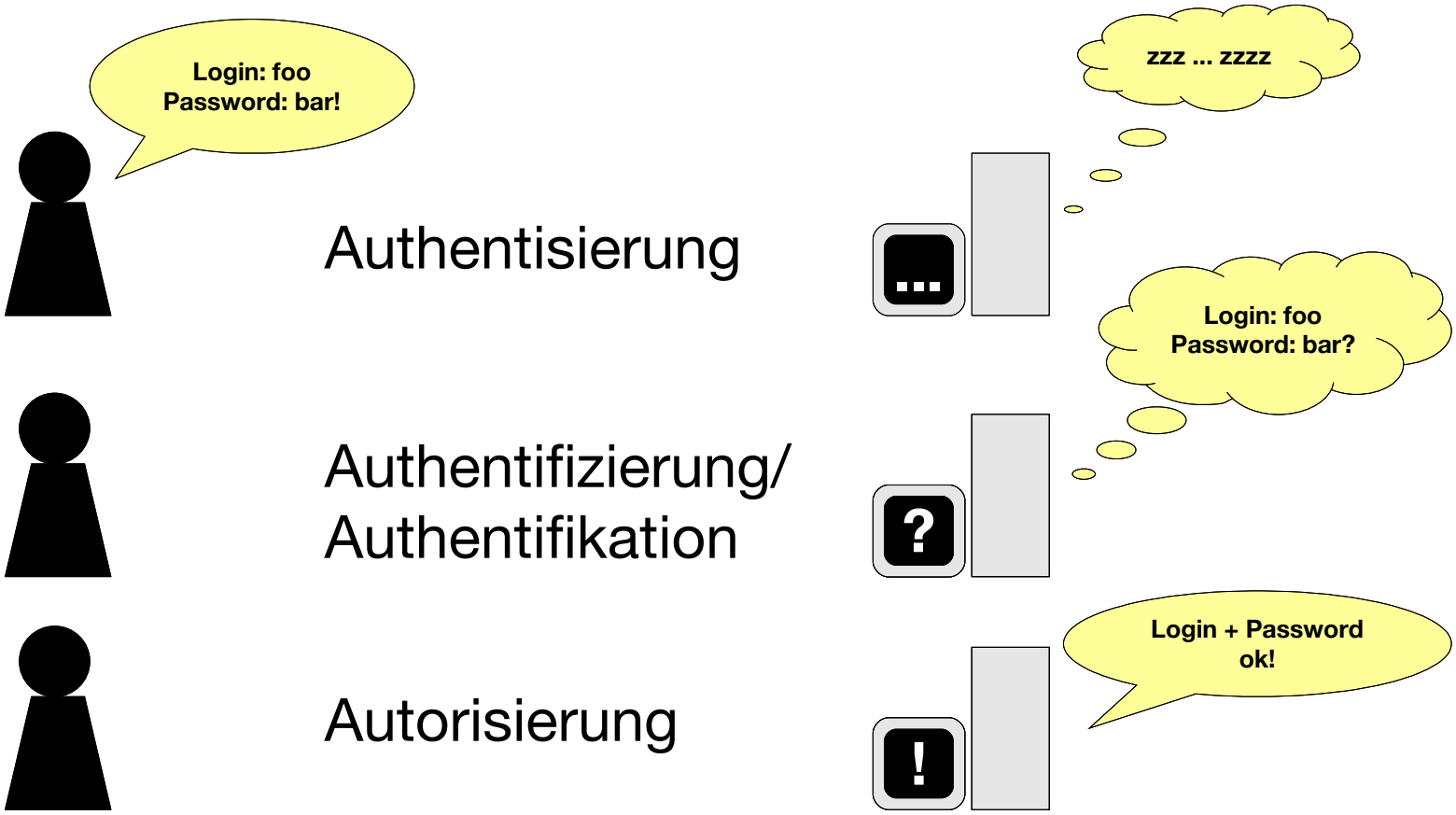
  symmetrisch: $\frac{n \cdot (n-1)}{2}$

  asymmetrisch: n

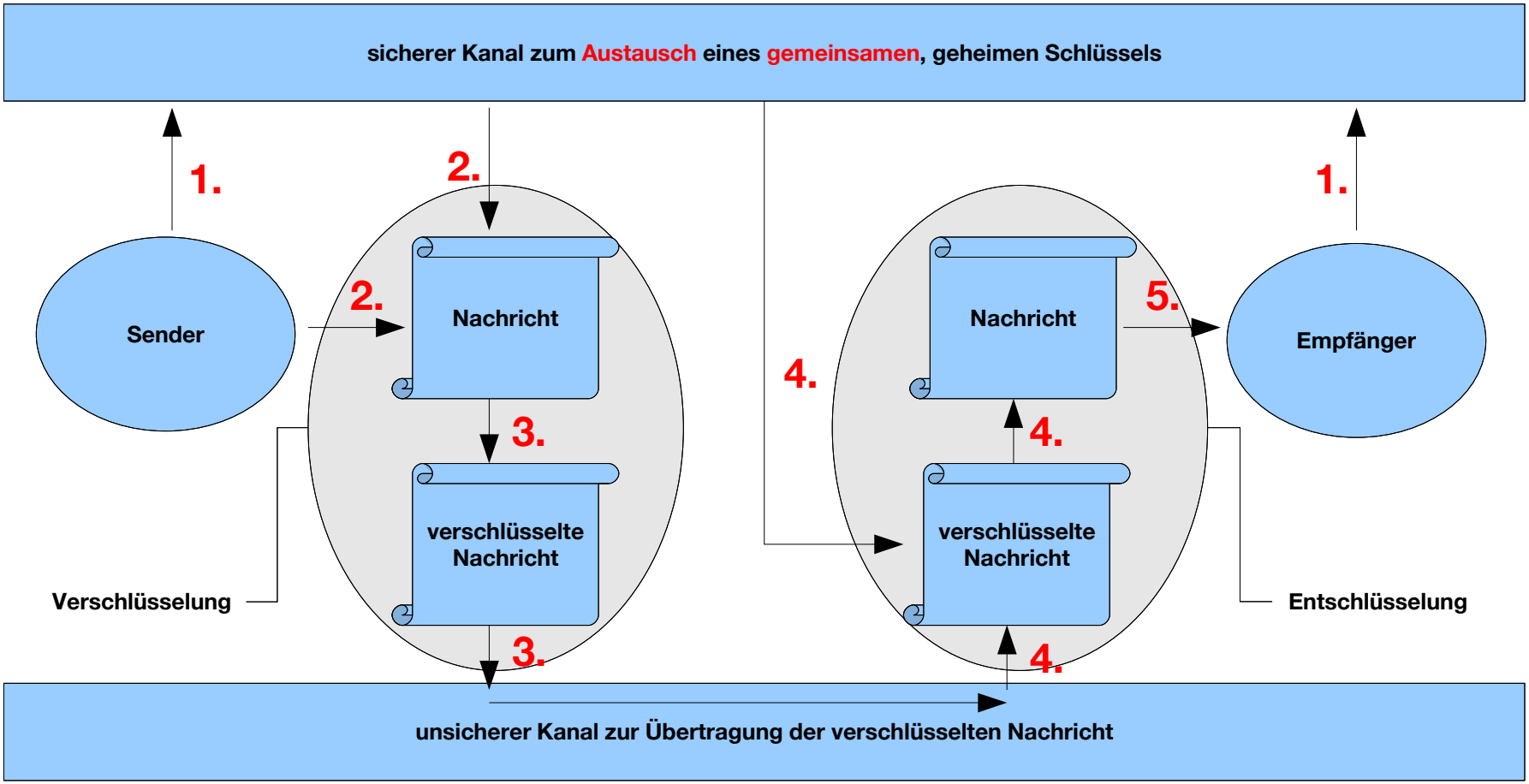
- OTP (one time pad): Ist das **einzigste** Verschlüsselungsverfahren, welches informationstheoretisch sicher ist (kann „wirklich nicht“ gebrochen werden)

Aut{ hentisierung | hentifizierung | orisierung}

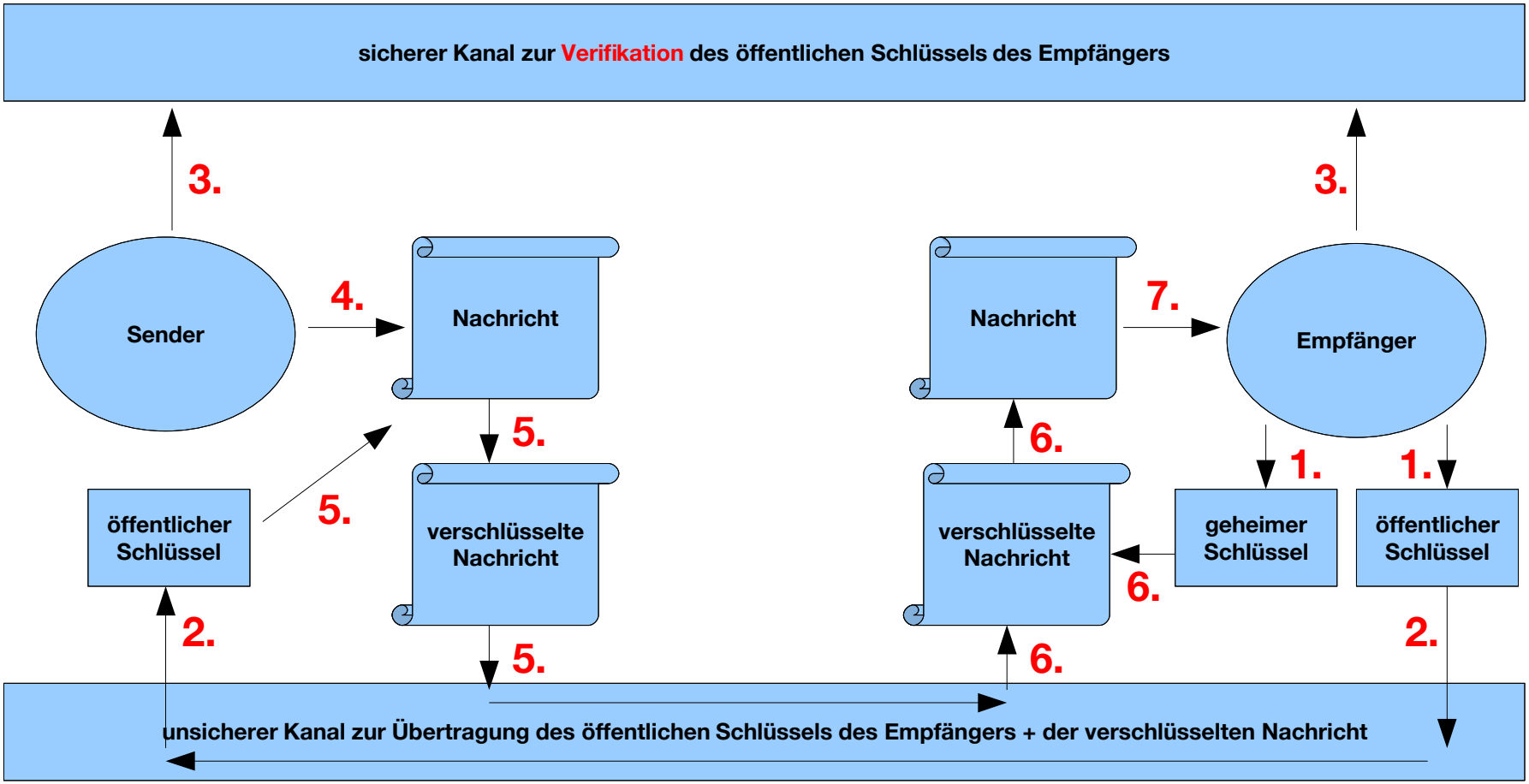
– Erläuterung anhand der Anmeldung an einem Computer



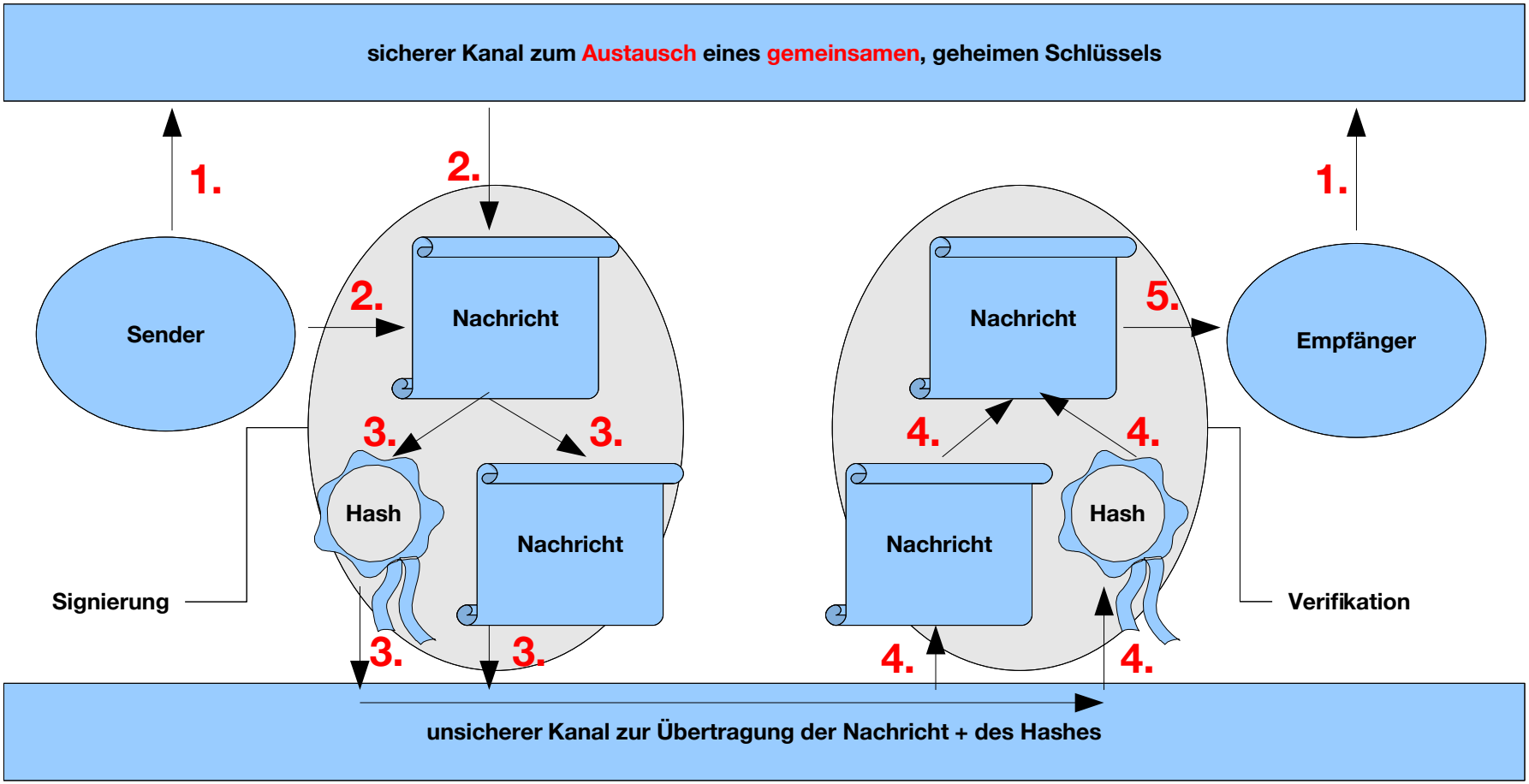
symmetrische / asymmetrische Verschlüsselung



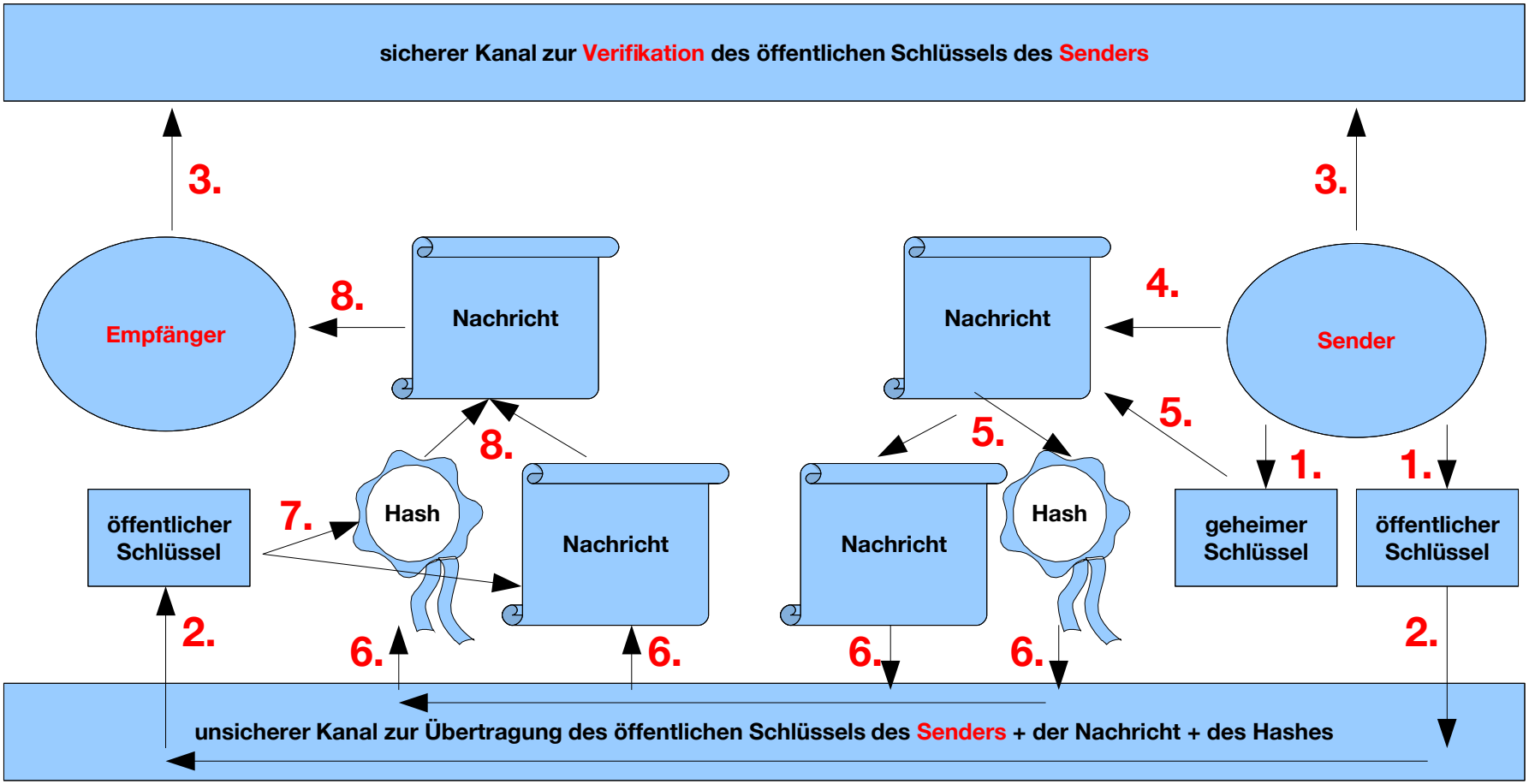
symmetrische / asymmetrische Verschlüsselung



symmetrische / asymmetrische Authentifizierung

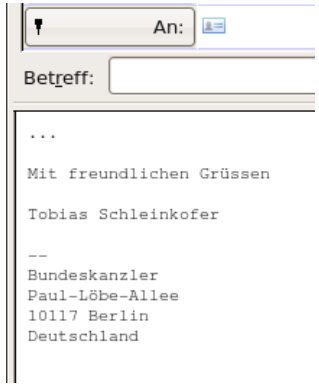


symmetrische / asymmetrische Authentifizierung



{ einfache | fortgeschrittene | qualifizierte } Signatur

– einfache Signatur



– fortgeschrittene Signatur

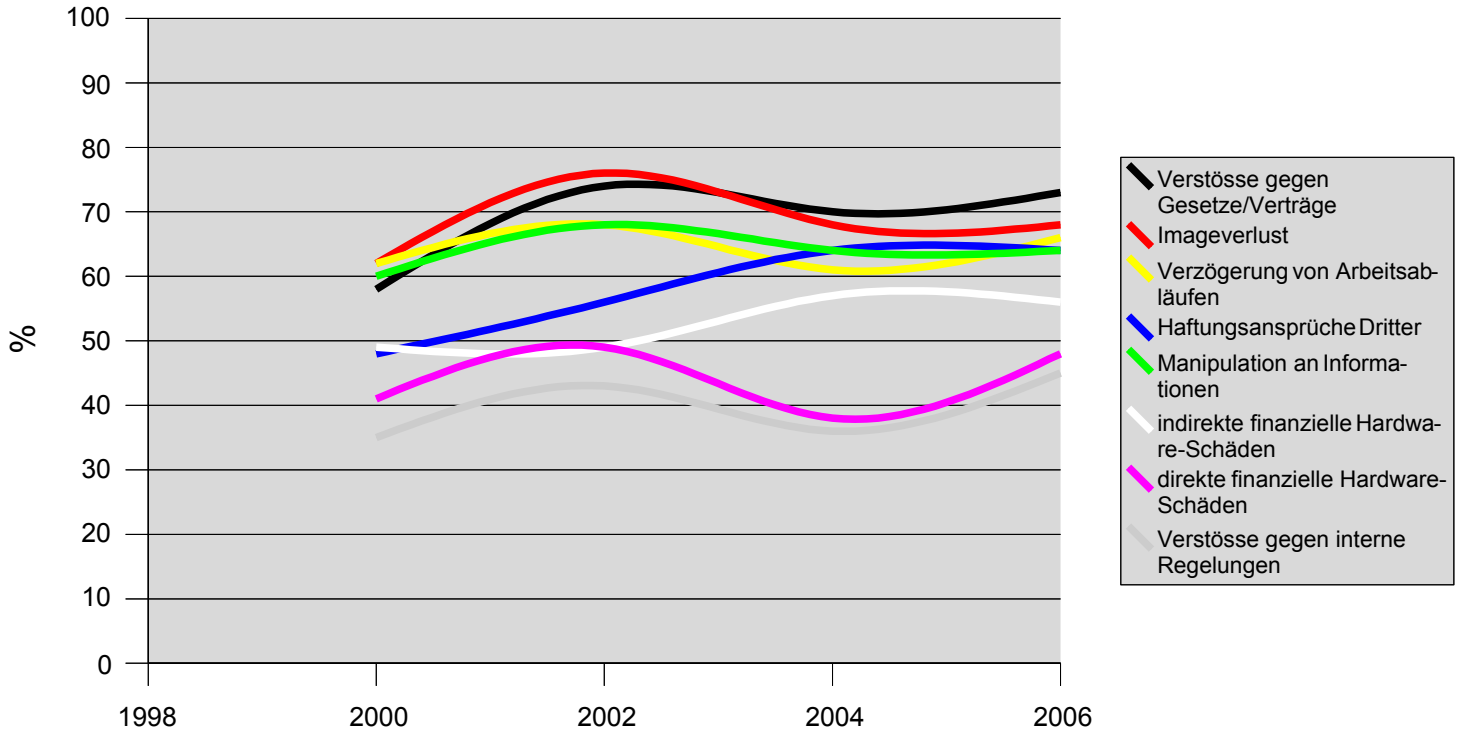
```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

...

-----BEGIN PGP SIGNATURE-----
Version: GnuPG v1.4.3 (GNU/Linux)
Comment: Using GnuPG with Mozilla - http://enigmail.mozdev.org
iD8DBQFGeRKhxxOnazLjhqwRAlzJAJ9n4oBcawOqBwhaCgqqB274v2loAwCeON
TF
WSuuBKLw00TAp1p0kimqlAE=
=gP9y
-----END PGP SIGNATURE-----
```

– qualifizierte Signatur (gleichgestellt mit Unterschrift)

http://bundesrecht.juris.de/sigg_2001/index.html
http://www.bundesnetzagentur.de/enid/Elektronische_Signatur/Zertifizierungsdiensteanbieter_ph.html

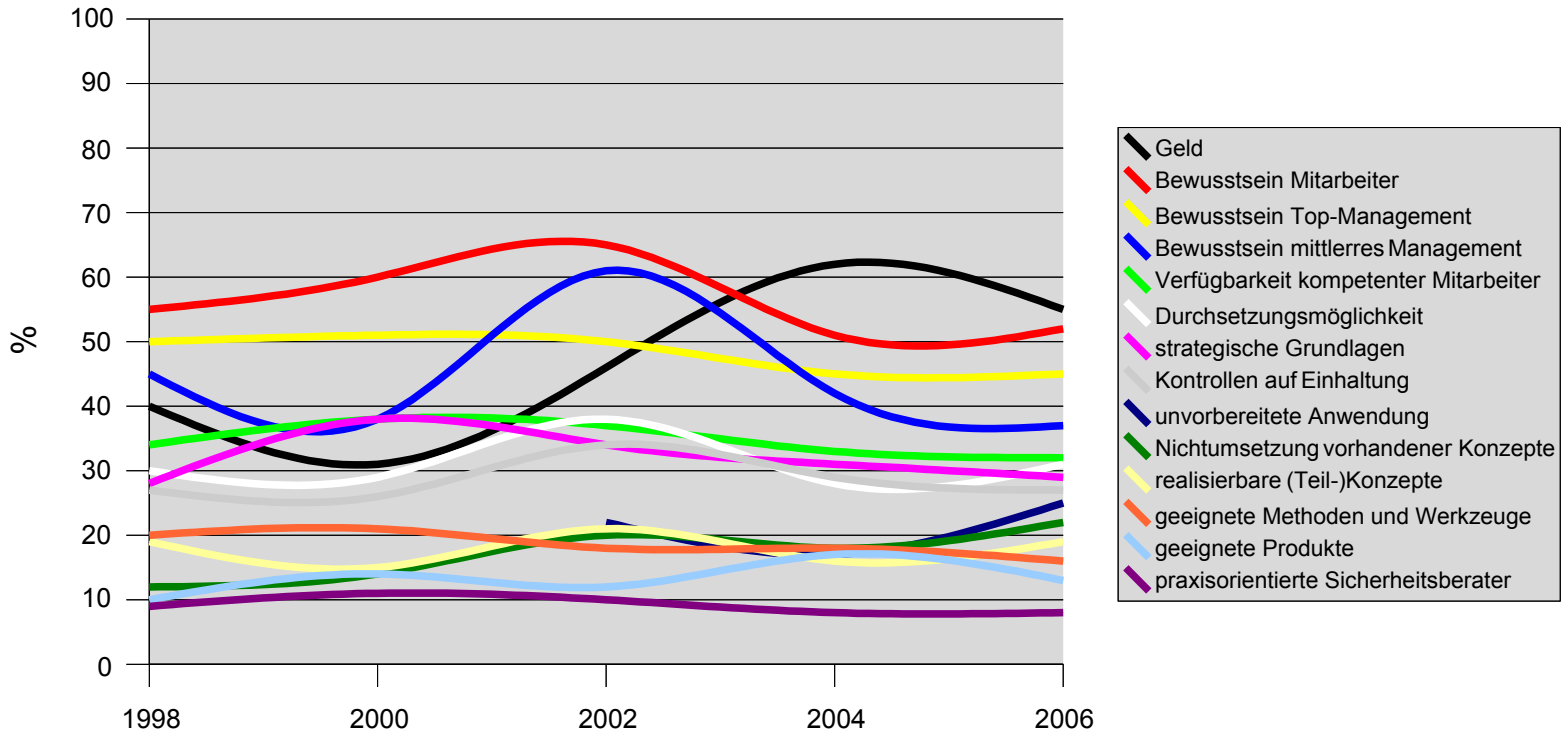
Kriterien zur Einordnung identifizierter Risiken

– grafische Darstellung der <kes>-Statistiken



Gründe für fehlende IT-Sicherheit

– grafische Darstellung der <kes>-Statistiken



Risikomatrix

- Beispiel anhand der Risken in einer Vorlesung
- nicht repräsentativ ;-)
- individuelle Festlegung: Werte von 1 bis 6

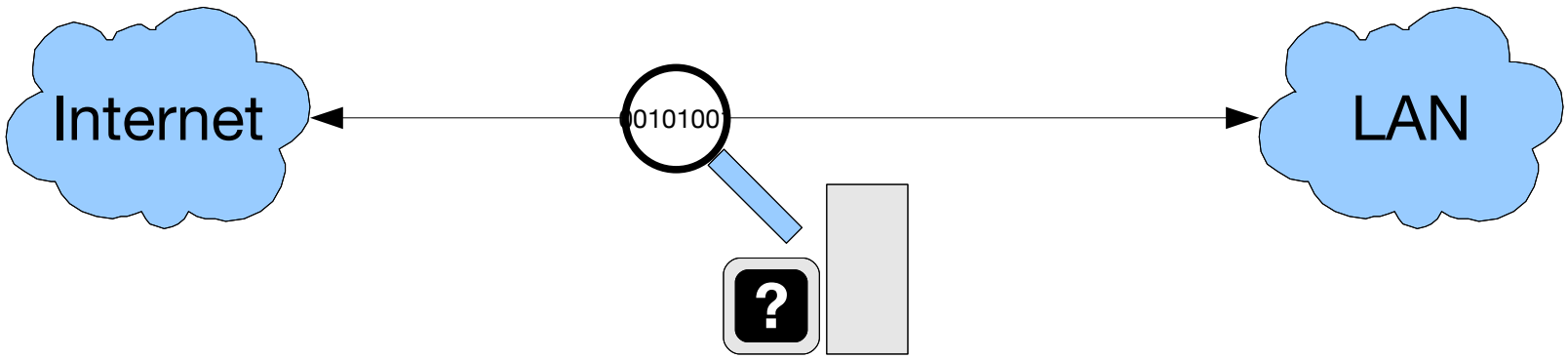
Risikorang	Risiko-Kategorie	Auswirkung	Eintrittswahrscheinklichkeit	Risikofaktor
1.	Erwischt werden beim Abschreiben	6	6	36
2.	Verpassen der Übungsblattabgabe	4	4	16
3.	Verpassen einer Übung	3	5	15
4.	Prüfungstermin verpassen	5	1	5
5.	Verpassen einer Vorlesung	2	2	4
6.	Während der Vorlesung einschlafen	1	3	3

Konzeption von IT-Sicherheit

- teilweise Interessenskonflikte mit dem Datenschutz (bspw. Protokollierung und Überwachung von Datenströmen)
- Penetrationstest werden rechtlich erschwert(/unmöglich?) 6.7.2007: Bundesrat billigt Novelle des StGBs (http://www.heise.de/newsticker/meldung/92334)
- Vulnerability Management: Suche nach Exploits und deren Behebung
- Firewalltypen: Packet Filter, Screened Host, Dual Homed Host, ...
- mehr dazu: Vorlesung „Sicherheit in IT-Systemen“ von Frank Kargl

Firewallarchitekturen

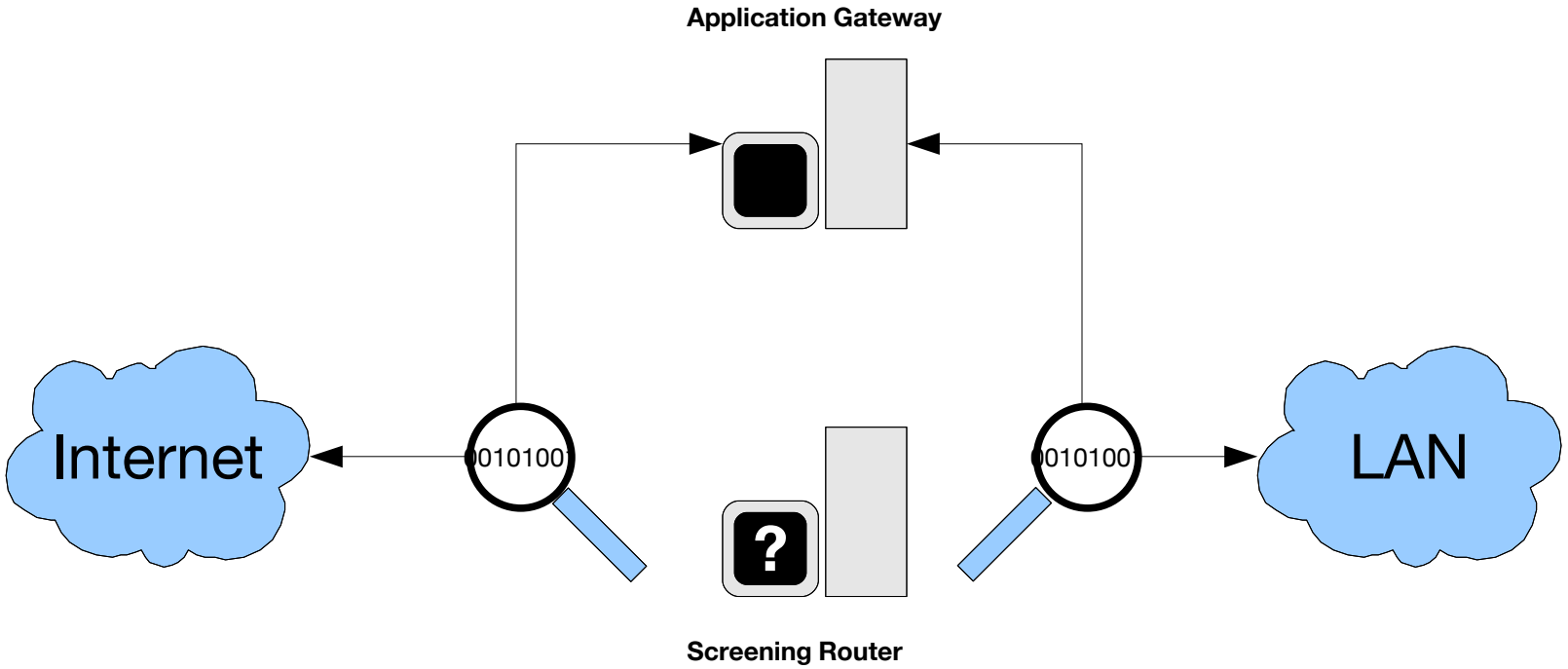
- siehe auch Vorlesung „Sicherheit in IT-Systemen“ von Frank Kargl im Wintersemester
- Packet Filtering Router, Screened Host, Dual-homed Host, Screened Subnet
- Packet Filtering Router:



Packet Filtering Router

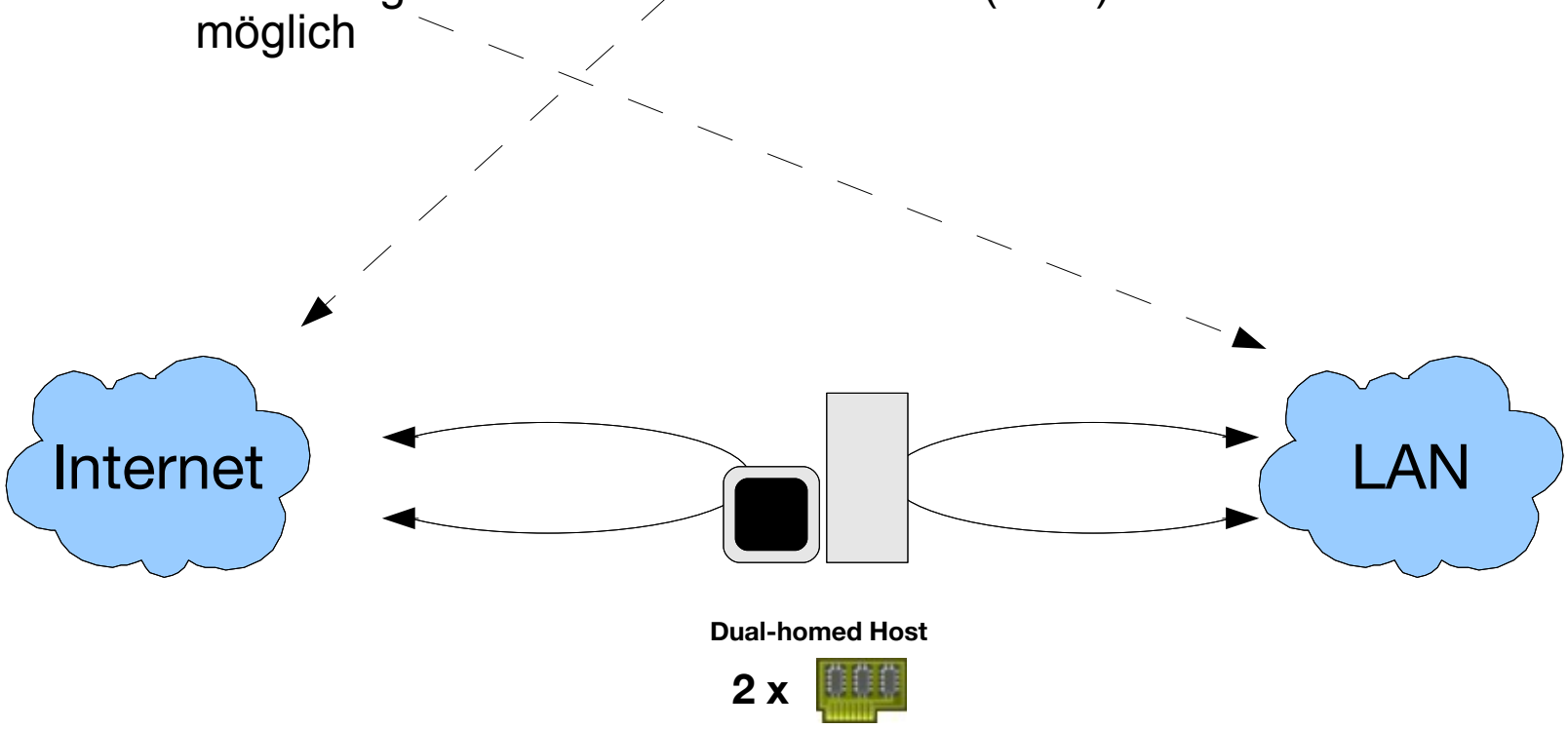
Firewallarchitekturen

– Screened Host:



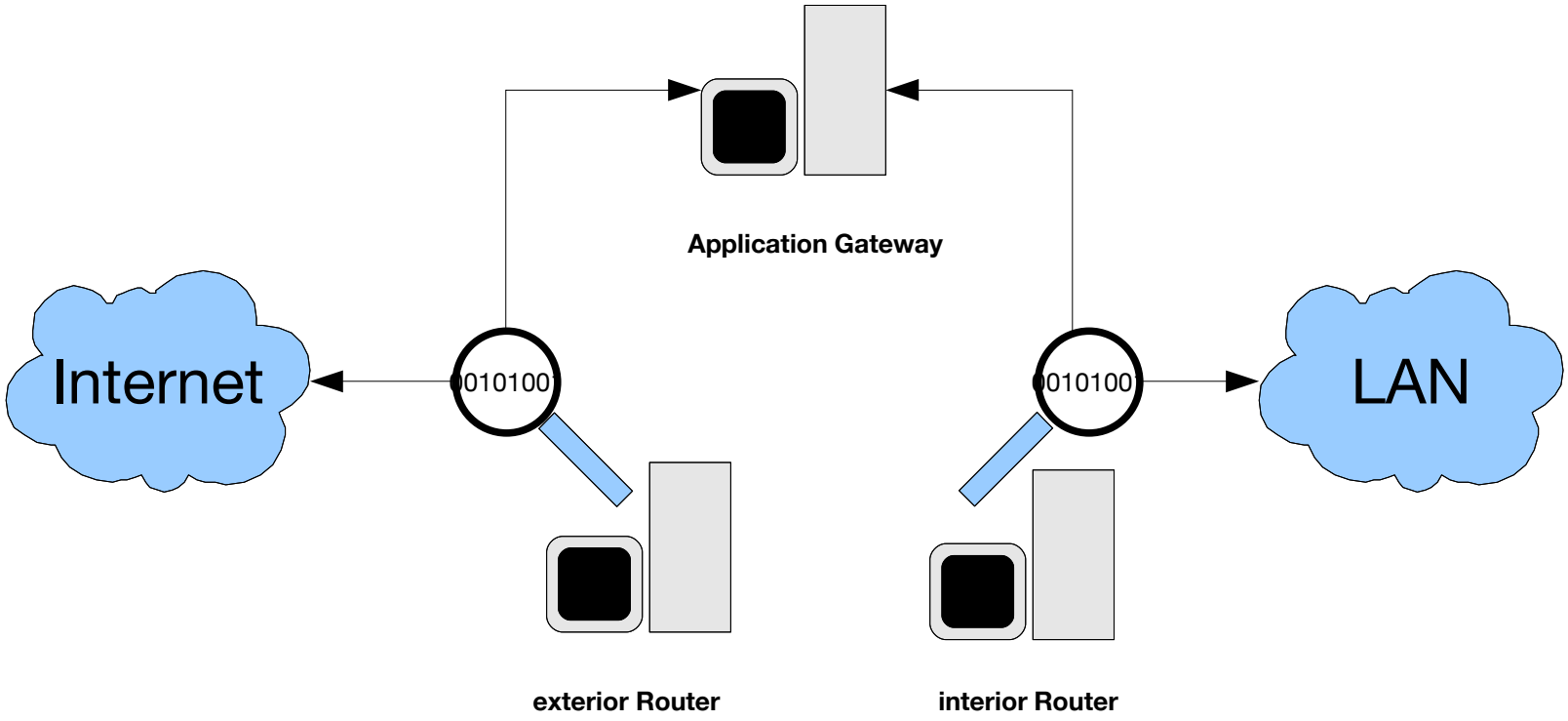
Firewallarchitekturen

- Dual-homed Host:
- konkretes Beispiel: Zugriff auf Unterlagen diverser Uni-Vorlesungen vom Internet aus nur via (Web)VPN oder SSH möglich

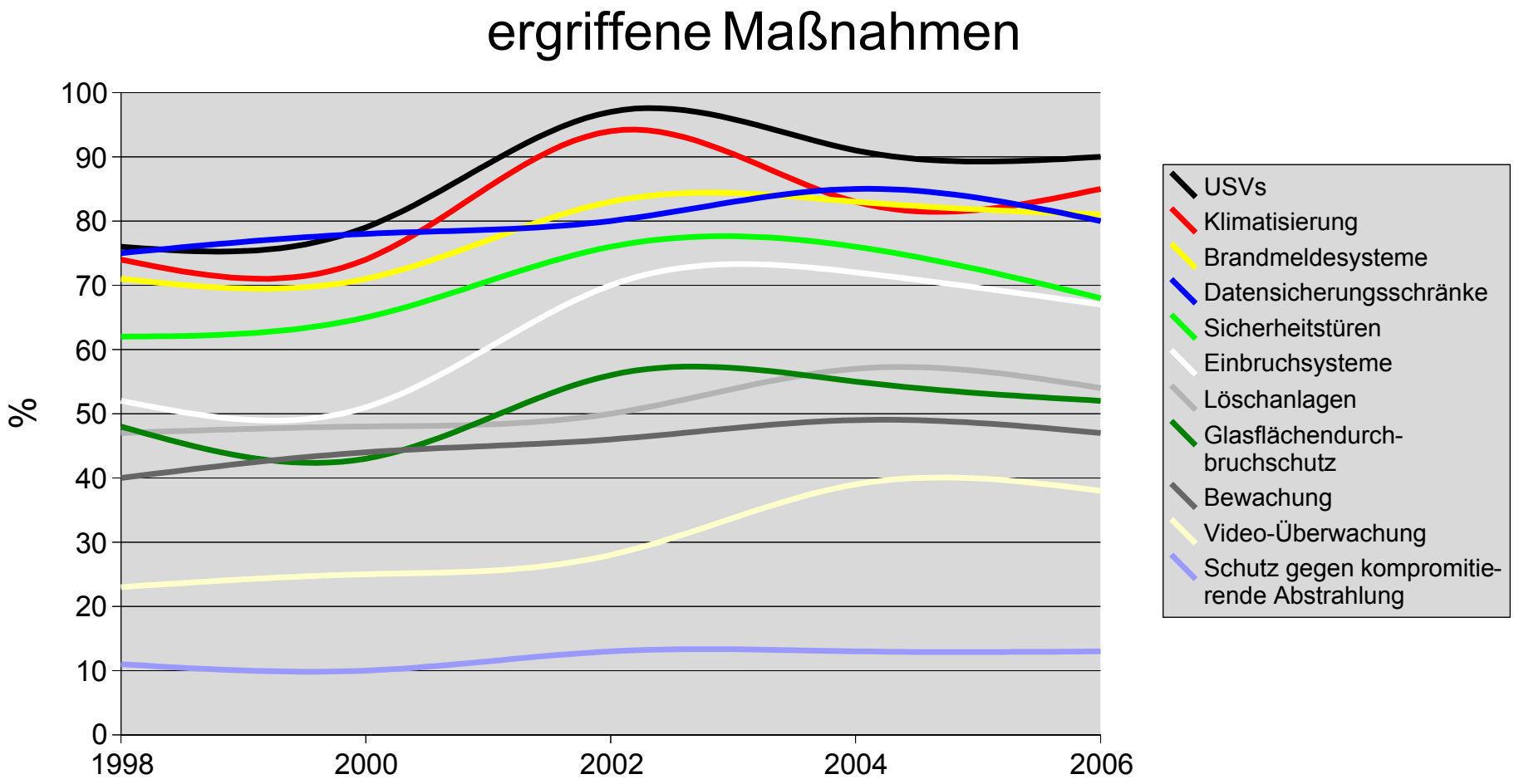


Firewallarchitekturen

– Screened Subnet:



Maßnahmen physischer Sicherheit



Passwörter

- via Brute-Force ein Passwort knacken (Beispielrechnung mit theoretischen Werten)
- Dualcore CPU mit 2 x 2,4 Ghz Takt
  C = ca. 20.000.000 Passwortkombinationen/Sekunde möglich
- Zeichenraum: z = { a-z, A-Z, 0-9 } = 62 Zeichen
- Länge des Passworts: L = 6 Zeichen
- Anzahl möglicher Passwortkombinationen: $K = z^L = 62^6 = 56.800.235.584$
- Anzahl Sekunden bis alle Kombinationen ausprobiert wurden:
  K / C = ca. 2840 Sekunden = ca. 45 min
- Mal spasseshalber für die PIN der EC-Karte ausrechnen
- http://www.1pw.de/brute-force.html +
  http://www.orange.co.jp/~masaki/rc572/fratee.php