



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Einführung

Internet-Sicherheit A

Prof. Dr. (TU NN)

Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
<http://www.internet-sicherheit.de>

if(is)
internet-sicherheit.

- **Motivation**
- **IT-Sicherheit von 1990 bis heute**
- **Die Situation heute: Eine kritische Bewertung**
- **Ein Blick in die Zukunft**
- **Ausblick**

■ Motivation

- IT-Sicherheit von 1990 bis heute
- Die Situation heute: Eine kritische Bewertung
- Ein Blick in die Zukunft
- Ausblick

- **Veränderung, Fortschritt, Zukunft**
 - Entwicklung zur **vernetzten Informations- und Wissensgesellschaft.**
- **IT-Sicherheit / Datenschutz ist eine sich verändernde Herausforderung**
 - Das Internet geht über alle Grenzen und Kulturen hinaus!
 - **Zeit und Raum werden überwunden!**
 - Immer schnellere Entwicklung und Veränderung in der IT.
 - **Die Nutzer müssen immer wieder neues Wissen erwerben, wie sie sich angemessen verhalten können.**
 - Die zu schützenden Werte steigen ständig und ändern sich mit der Zeit.
 - **Die Angriffsmodelle innovieren und Angreifer werden professioneller.**
 - IT-Sicherheitsmechanismen werden komplexer, intelligenter und verteilter.
 - **Mit der Zeit werden die IT-Sicherheits- und Datenschutzprobleme immer größer!**

- Motivation
- **IT-Sicherheit von 1990 bis heute**
- Die Situation heute: Eine kritische Bewertung
- Ein Blick in die Zukunft
- Ausblick

Lage der IT Sicherheit

→ ~ 1990: Kommunikationssicherheit

■ IT-Trend:

- Mit dem PC kam eine Individualisierung und Dezentralisierung der IT.
- Der Wunsch, diese dezentralen IT-Systeme über Leitungen oder Daten-Netze, wie X.25-Netz zu verbinden.

■ IT-Sicherheitstrend:

- Mit **Leitungsverschlüsselung** (Modem, 2 MBit/s, ...) und **X.25-Verschlüsselungsgeräten** die neuen Sicherheitsprobleme lösen.



■ Unsere Einstellung:

- Wir müssen uns beeilen, sonst sind alle IT-Sicherheitsprobleme gelöst.

Lage der IT Sicherheit

→ ~ 2000: Perimeter Sicherheit

■ IT-Trend:

- Unternehmen haben sich ans Internet angeschlossen, um am **E-Mail-** und **Web-System** teilhaben zu können.
- Zusätzlich wurden Niederlassungen über das Verbundnetz Internet einfach angebunden.

■ IT-Sicherheitstrend:

- Abwehrmodell: Firewall- und VPN-Systeme
- Digitale Signatur, E-Mail-Sicherheit, PKI



■ Unsere Einstellung:

- Wir haben die IT-Sicherheitsprobleme im Griff!

Lage der IT Sicherheit

→ ~ 2010: Malware / Software-Updates

■ IT-Trend:

- Immer mehr PCs, Notebooks, SmartPhones zunehmend über GSM, UMTS, Hotspots, ... (an der zentralen Firewall vorbei) ins Internet
- Die Anzahl der Schwachstellen durch **Softwarefehler** wird immer größer (die Marktführer im SW-Bereich erkennen, dass es einen SW-Entwicklungsprozess gibt :-)

■ IT-Sicherheitstrend:

- **Verteilte Softwareangriffe** mit Hilfe von Trojanischen Pferden
- Anti-Malware, Software-Upgrades und Personal Firewalls
- Generierung der Sicherheitslage



■ Unsere Einstellung:

- Die IT-Sicherheitsprobleme wachsen uns über den Kopf!

- Motivation
- IT-Sicherheit von 1990 bis heute
- **Die Situation heute:
Eine kritische Bewertung**
- Ein Blick in die Zukunft
- Ausblick
- Buch: „Sicher im Internet“

Die IT-Sicherheitssituation heute

→ Eine kritische Bewertung (1/11)

■ Zu viele Schwachstellen in Software

- Die **Software-Qualität** der *Betriebssysteme* und *Anwendungen* ist **nicht gut genug!**
- **Fehlerdichte:**
Anzahl an Fehlern pro 1.000 Zeilen Code (Lines of Code - LoC).



Fehlerdichte	Klassifizierung der Programme
< 0,5	stabile Programme
0,5 .. 3	reifende Programme
3 .. 6	labile Programme
6 .. 10	fehleranfällige Programme
> 10	unbrauchbare Programme

Betriebssysteme haben mehr als 10 Mio. LoC

→ mehr als 3.000 Fehler
(Fehlerdichte 0,3)

→ und damit zu viele Schwachstellen

Die IT-Sicherheitssituation heute

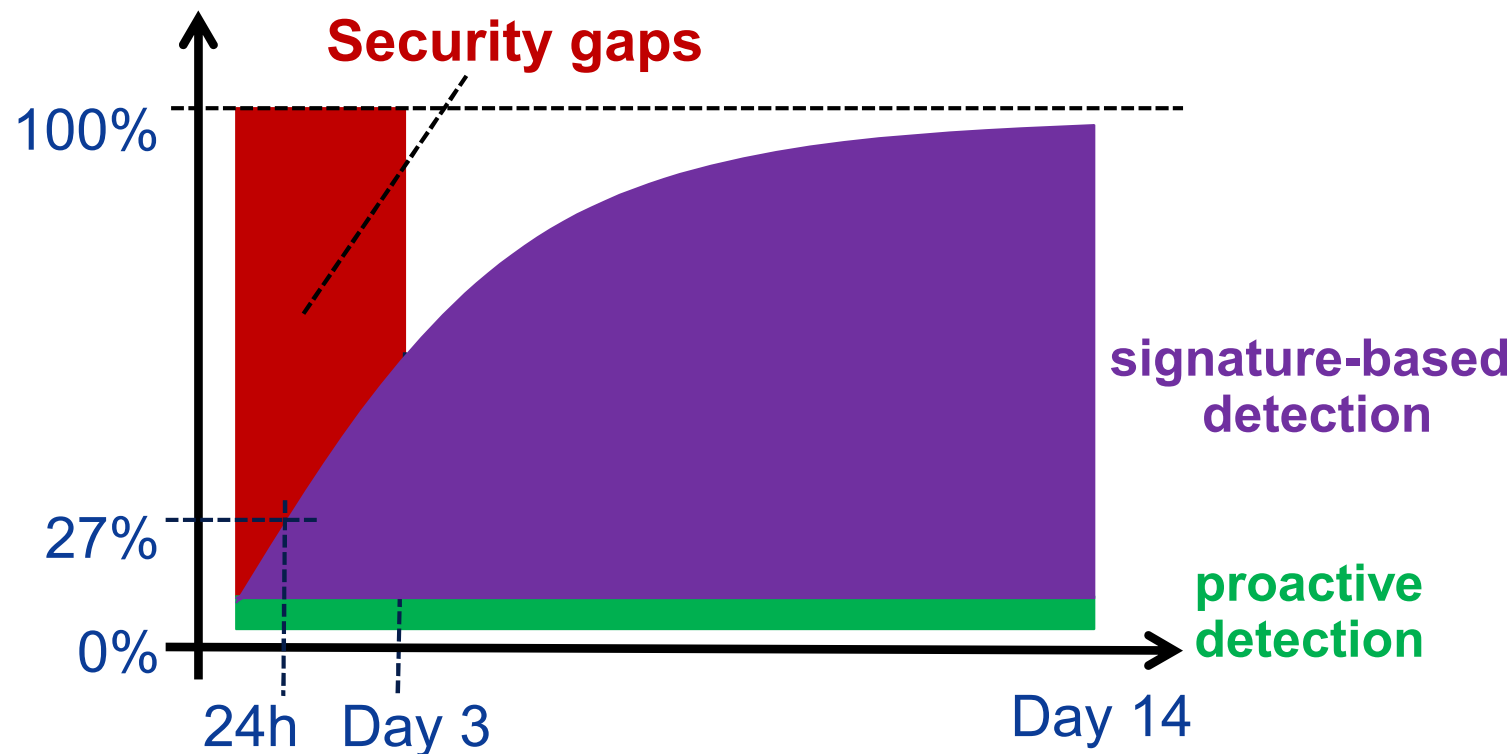
→ Eine kritische Bewertung (2/11)

■ Ungenügender Schutz vor Malware (1/2)

- Schwache Erkennungsrate bei Anti-Malware Produkten
→ nur 75 bis 95%!

Symantec erkennt nur noch 45 % der Malware!

- Bei direkten Angriffen weniger als 27%



Die IT-Sicherheitssituation heute

→ Eine kritische Bewertung (3/11)

■ Ungenügender Schutz vor Malware (2/2)

■ Jeder 10. Computer hat Malware!

- Datendiebstahl/-manipulation (Keylogger, Trojanische Pferde, ...)
- Spammen, Click Fraud, Nutzung von Rechenleistung, ...
- Datenverschlüsselung / Lösegeld, ...

■ Cyber War (Advanced Persistent Threat - APT)

- Eine der größten Bedrohungen zurzeit!
- Stuxnet, Flame, ...

→ CyberWar



Die IT-Sicherheitssituation heute

→ Eine kritische Bewertung (4/11)

■ Identity Management (2016)

- Passworte, **Passworte**, *Passworte*, ... sind das Mittel im Internet!
- **Identifikationsbereiche liegen im Unternehmens- und Kundenumfeld, nicht international!**
- Föderationen sind noch nicht verbreitet genug!



Identitätsdiebstähle

Phishing Angriffe

Dienste-Übernahmen



Die IT-Sicherheitssituation heute

→ Eine kritische Bewertung (5/11)

■ Webserver Sicherheit

- Schlechte Sicherheit auf den Webservern / Webseiten
- Heute wird Malware hauptsächlich über Webseiten verteilt
(ca. 2.5 % Malware auf den deutschen gemessenen Webseiten)

■ Gründe für unsichere Webseiten

- Viele Webseiten sind nicht sicher implementiert!
- Patches werden nicht oder sehr spät eingespielt
- Firmen geben **kein Geld für IT-Sicherheit** aus!
- **Verantwortliche kennen das Problem nicht!**



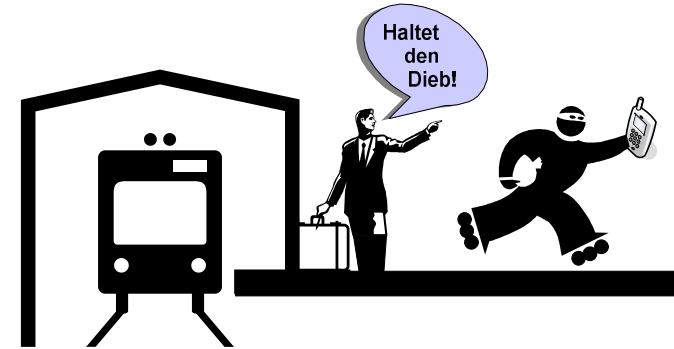
Die IT-Sicherheitssituation heute

→ Eine kritische Bewertung (6/11)

■ Gefahren mobiler Geräte

■ Verlieren der mobilen Geräte

Ständig wechselnde unsichere Umgebungen
(Flughäfen, Bahnhöfe, Cafés, ...) ...



... damit wird die Wahrscheinlichkeit des **Verlustes deutlich höher!**
(Handy-Statistik Taxis in London, Notebook-Statistik Flughäfen)

■ Bewegungsprofilbildung / Always-On

■ Apps als Spyware

■ Öffentliche Einsicht



■ Falsche oder manipulierte Hotspots (Vertrauenswürdigkeit)



■ Bring Your Own Devices / Consumerisation

Die IT-Sicherheitssituation heute

→ Eine kritische Bewertung (7/11)

- **Cloud Computing ist eine Herausforderung**
 - Dauerhafter und attraktiver zentraler Angriffspunkt
 - **Vernetzung bietet zusätzliche Angriffspunkte**
 - Identitätsdiebstahl, Session-Hijacking, ...
 - **Schwachstellen bei Shared Services, Abgrenzung der Unternehmensdaten**
 - Ich kenne die Orte, wo meine Daten gespeichert sind nicht!
 - **Wie kann ich sicher sein, dass die Daten noch existieren?**
 - Wie kann ich sicher sein, dass keiner meine Daten liest?
 - **Datenverlust (Platten-, Datenbank-, Anwendungsfehler, ...)**
 - Datenlecks (Datenbank, Betriebssystem, ...) – Hacker!
 - ...

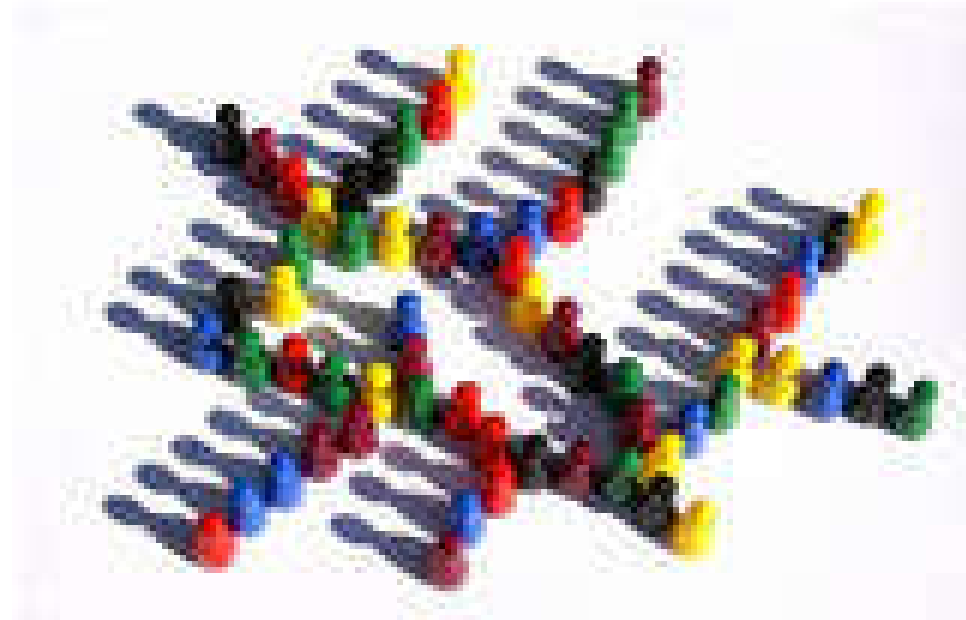
Die IT-Sicherheitssituation heute

→ Eine kritische Bewertung (8/11)

Probleme:

■ Soziale Netzwerke

- Internet-Nutzer können sich über Soziale **Netzwerke sehr schnell neues Wissen aneignen und Informationen beschaffen.**
- **Vertrauliche Informationen sollen nicht eingestellt und besprochen werden!**
- Die Rechte der Betreiber sind nicht angemessen!
(siehe AGBs → können alles mit den eingestellten Inhalten machen!)
- Die angebotenen Schutzmechanismen sind nicht klar und qualitativ nicht gut genug!
- Von Sozialen Netzwerken in die reale Welt
→ **Freunde sind nicht immer Freunde**



Die IT-Sicherheitssituation heute

→ Eine kritische Bewertung (9/11)

Probleme:

■ E-Mail Sicherheit

- **Wenig verschlüsselte E-Mails** (<4 %)
(S/MIME, PGP, ...)
- **Wenig signierte E-Mails** (<6 %)
- **Spam**-Anteil größer als 95 %
(in der Infrastruktur – siehe ENISA-Studie)
- **Keine Beweissicherung**
- **Nicht zuverlässig** (Zustellung, E-Mail-Adresse,)



■ Was kommt in der Zukunft?

- **DE-Mail**
 - SSL-Verschlüsselung zwischen den Gateways, **Zustell-Garantie**
 - Verpflichtende Authentifizierung, Sichere Dokumentenablage
- **German Mail**
 - SSL, ...

Die IT-Sicherheitssituation heute

→ Eine kritische Bewertung (10/11)

■ Internet-Nutzer

- Internet-Nutzer müssen die Gefahren des Internets kennen, sonst **schaden sie sich und anderen!**
- **Umfrage BITKOM: (2012)**
Fast jeder dritte **Internet-Nutzer** **schützt sich nicht angemessen!**
 - **keine** Personal Firewall (30 %)
 - **keine** Anti-Malware (28 %)
 - gehen **sorglos** mit E-Mails und Links um
 - usw.
- **Studie „Messaging Anti-Abuse Working Group“:**
57 Prozent der Befragten haben schon einmal **Spam-Mails geöffnet** oder einen **darin enthaltenen Link angeklickt.**

Die IT-Sicherheitssituation heute

→ Eine kritische Bewertung (11/11)

**Der Level an
IT-Sicherheit, Datenschutz und Vertrauenswürdigkeit
unserer IT-Systeme ist heute ungenügend!**

Lösungsansätze:

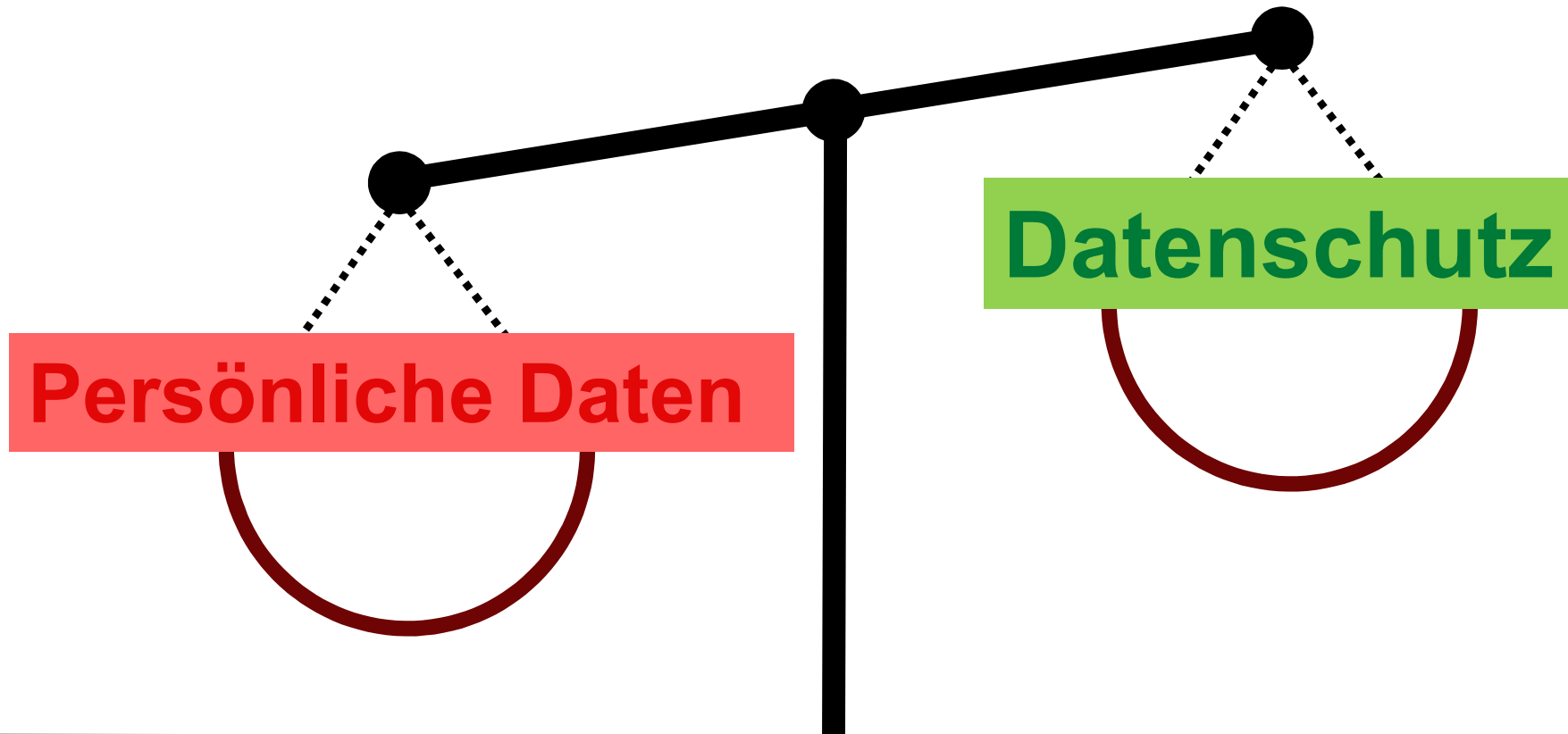


- **Herstellerverantwortung**
- **IT-Sicherheitsanspruch / IT-Sicherheitsbranche**
→ Chancen für die deutsche IT-Sicherheitsindustrie
- **Vertrauenswürdige Technologie, z.B. Trusted Computing**

Die Datenschutzsituation heute

→ Eine kritische Bewertung (1/7)

Persönlichen Daten sind ein Rohstoff
des Internetzeitalters



Die Datenschutzsituation heute

→ Eine kritische Bewertung (2/7)

Geschäftsmodell: „Bezahlen mit persönlichen Daten“

- **Soziale Netzwerke** (Facebook, ...), **E-Mail-Dienste** (Google , ...), ... **verdienen ihr Geld** vor allem **mit Werbung** !
- Je besser die Internet-Diensteanbieter die Internet-Nutzer kennen, desto mehr Geld können sie verdienen.
- Die Nutzer zahlen **kein Geld** für den Internet-Dienst!
- Die Nutzer stimmen über die AGBs zu, dass der Internet-Betreiber alle persönliche Daten für eine Profilbildung nutzen darf und damit Werbegeld einnehmen kann.
- Die Internet-Diensteanbieter verdienen mit **individualisierter Werbung** sehr viel Geld (**Google 2014 ca. 66 Milliarden US-Dollar!**).
- **aber**
individualisierte Werbung ist auch ein Feature,
was viele Internet-Nutzer sehr gut finden!

Die Datenschutzsituation heute

→ Eine kritische Bewertung (3/7)

Beispiel: Google (1/2)

Bei der Nutzung vieler Google-Dienste weiß Google:

- wer man ist und wo man wohnt (Buzz, Checkout, Gmail, Profiles etc.)
- welche sozialen Kontakte man pflegt (Buzz, Gmail, Orkut, Talk, Voice etc.)
- wo man sich gerade aufhält (Ortung per GSM-Zelle, GPS oder WLAN bei Google's mobilen Diensten wie Latitude, Navigation oder Near me now ...)
- wo man hin will (Earth, Maps, Navigation etc.)
- welche Termine man hat (Kalender, Sync etc.)
- welche Interessen man hat (diverse Suchdienste sowie weitere Dienste und Produkte wie Analytics, Blogger.com, Buzz, Chrome, Gmail, Groups, iGoogle, Knol, YouTube u.v.m.)
- wie die Bankverbindung lautet (Checkout)

Die Datenschutzsituation heute

→ Eine kritische Bewertung (4/7)

Beispiel: Google (2/2)

Bei der Nutzung vieler Google-Dienste weiß Google:

- wer die Partner bei Finanzgeschäften sind, was man kauft, wie viel man dafür ausgibt und wann Geschäfte abgewickelt werden (Checkout)
- welche und wie viele Aktien(-fonds) man besitzt und was man diesbezüglich für Transaktionen abwickelt (Finance)
- wie die eigene DNS aussieht und was für Krankheiten man hat oder hatte, einschließlich entsprechender Therapien (Health)
- wie man aussieht (Buzz, Gmail, Picasa, Profiles etc.)
- welche Daten man allgemein am eigenen Rechner bearbeitet (Chrome OS und weitere Cloud Computing-Angebote)

■ USW.

Studie: Google – die zwei Seiten des mächtigen Internet-Konzerns

www.internet-sicherheit.de/fileadmin/docs/publikationen/2011/Google-StudieV2.0.pdf

Die Datenschutzsituation heute

→ Eine kritische Bewertung (5/7)

Probleme:

```
91.51.162.241 - - [12/Sep/2009:11:41:32 +0200] „GET
/fileadmin/template/images/partner/logo-ifis-lehre.gif“
HTTP/1.1“ 200 2069 „http://www.internet-
sicherheit.de/forschung/aktuelle-
forschungsprojekte/internet-fruehwarnsysteme/“ „Mozilla/5.0
(X11;U;Linux i686; de-DE; rv:1.9.0.13) Gecko/2009082610
Gentoo Firefox/3.0.13“
```

- **Spuren des Users im Internet**
 - Browser (**Cookies**, **Browser-History**, spezielle Toolbars, ...)
 - Webserver (Log, Google-Analytics, Proxy-Server, ...)
 - Mail-, SIP-, DNS-Server, ...
 - Router, IDS, Firewalls, ... (Infrastrukturkomponenten)
 - **SmartPhones (IDs, Positionsbestimmung: GPS, GSM und WLAN)**
 - **Gefällt-Mir-Button**
 - ...

Die Datenschutzsituation heute

→ Eine kritische Bewertung (6/7)

Probleme:

- **IT-Branche**
 - Die praktische Umsetzung von Maßnahmen für die Aufrechterhaltung des Datenschutzes ist durch **mangelnde Vorgaben** eher zufällig gut oder schlecht
 - ...
- **Datenschutzorganisationen**
 - Strafverfolgung wäre möglich ...
 - Strafen könnten deutlich mehr verhängt werden ...
 - ...
- Usw.

Die Datenschutzsituation heute

→ Eine kritische Bewertung (7/7)

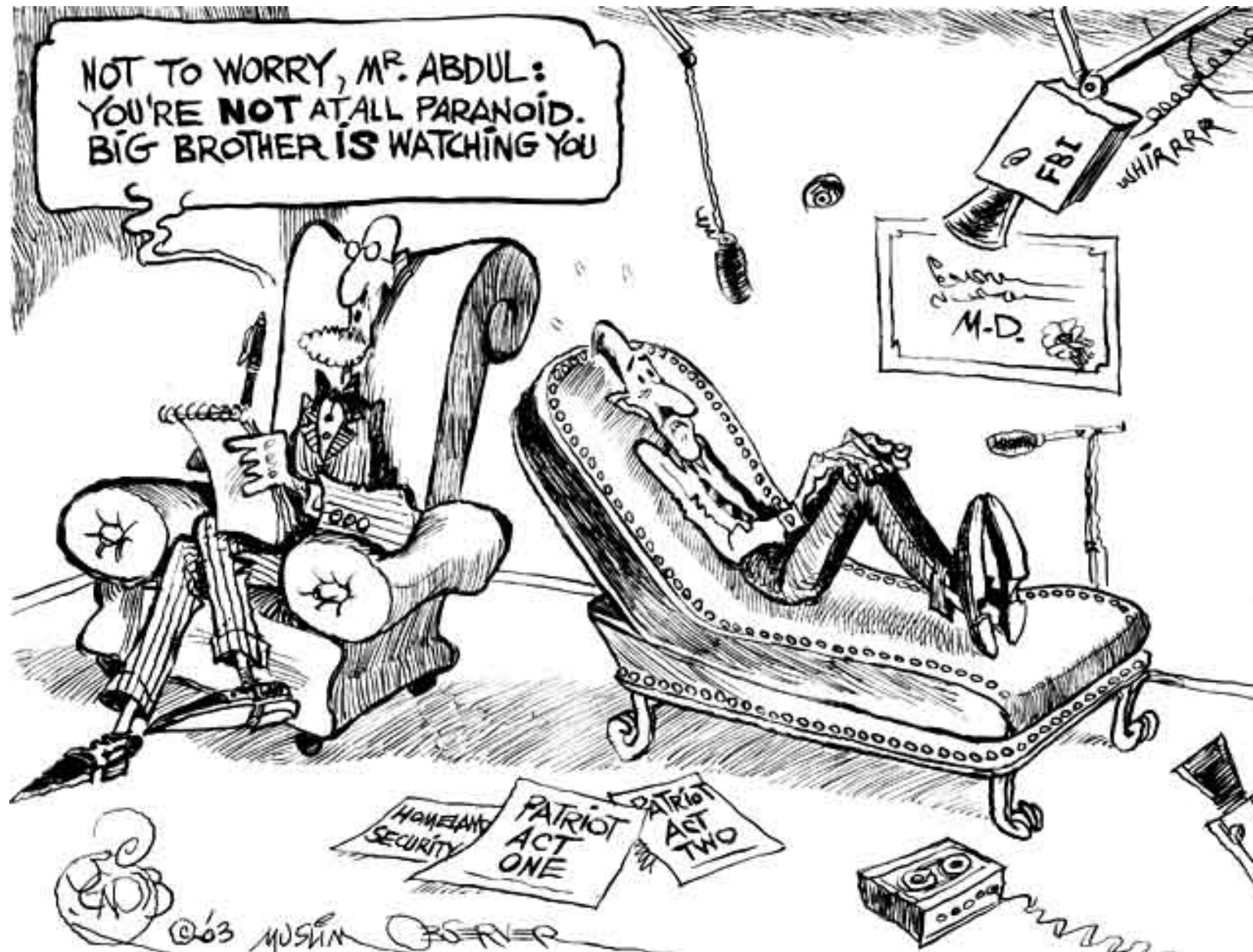
Beispiele und deren Bewertung

- **Sony** (Persönliche Daten von Millionen Sony-Kunden kopiert)
 - Kein Problembewusstsein (Technologie, Policy, Mitarbeiterschulung, ...)
 - Probleme: Zugangsdaten (Passwort für viele Dienste), Kreditkarten , ...
- **Apple** (Ortsbezogene Datenspeicherung)
 - Kein Problembewusstsein (Kultur, Policy, Mitarbeiterschulung)
 - Problem: Der gläserne Nutzer
- **Google** (WLAN-Aufzeichnung – StreetView)
 - Kein Problembewusstsein (Kultur, Policy, Mitarbeiterschulung)
 - Problem: TKG – Fernmeldegeheimnis
- ... *NPD-Google-Ranking* ... *Android-Schwachstelle* ...

Kulturelle Unterschiede

Privacy Paranoia

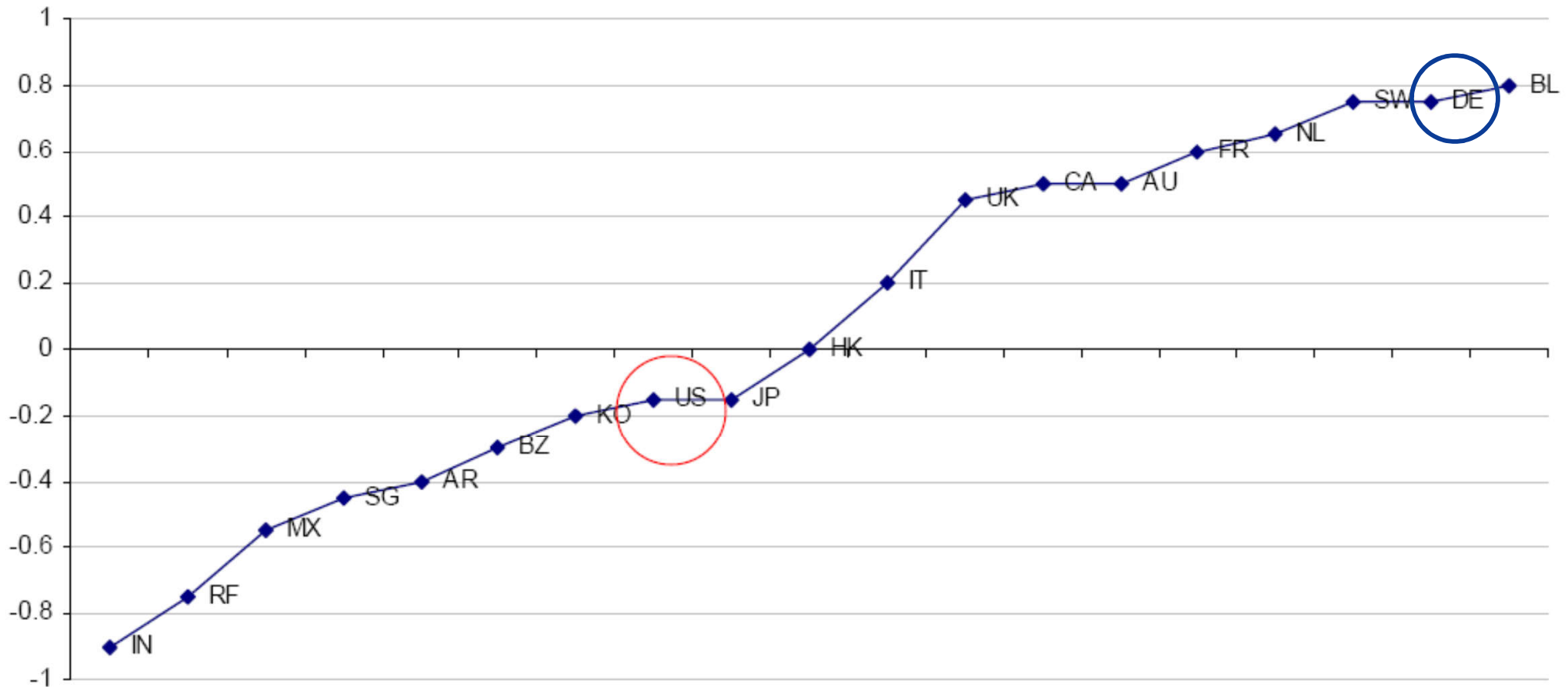
→ Different countries, different culture



Privacy Paranoia

→ Exkurs: Privacy Paranoia 1/4

Global Privacy Index
By ratio score (Max = +1, Min = -1)



Privacy Paranoia

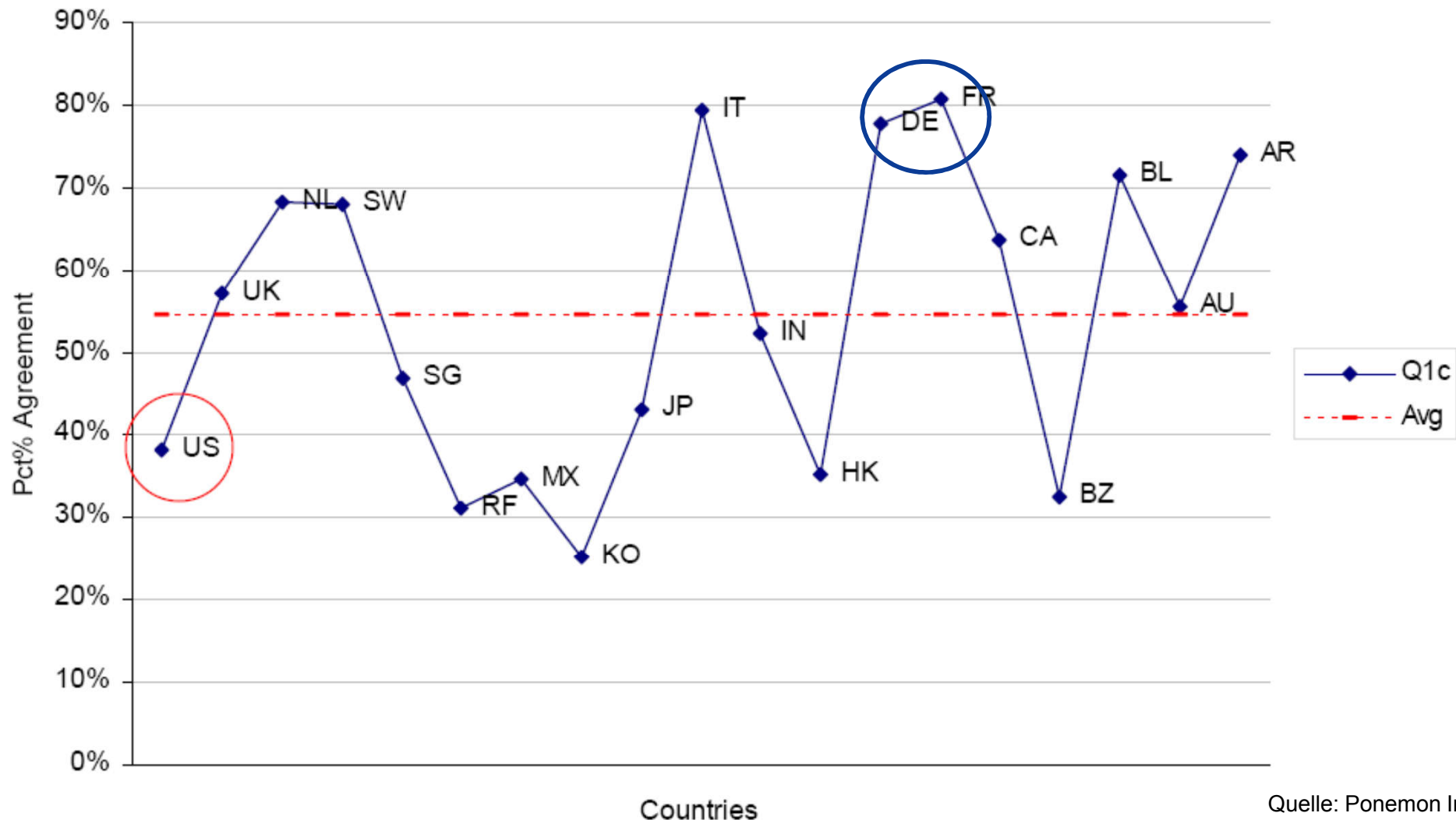
→ Exkurs: Privacy Paranoia 2/4

Country orientations	Lower privacy orientation	Higher privacy orientation
Higher data security orientation	<p>SG, KO, JP, HK</p>	<p>US AU UK</p> <p>DE, SW BL, NL CA</p>
Lower data security orientation	<p>IN</p> <p>RF</p> <p>BZ, AR MX</p>	<p>FR</p> <p>IT</p>

Privacy Paranoia

→ Exkurs: Privacy Paranoia 3/4

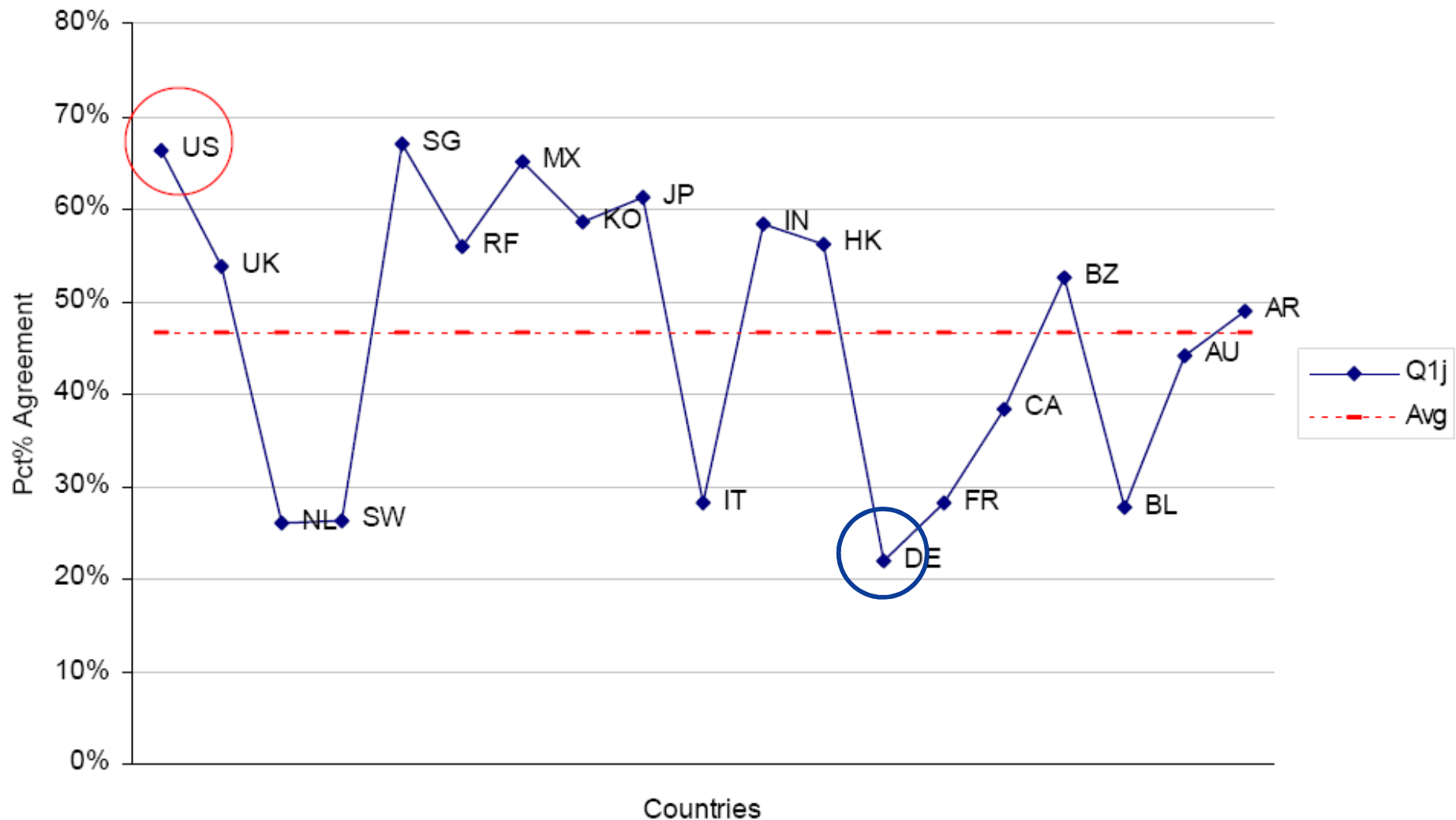
Q1c. Consumers have a right to access and review their personal information collected and used by organizations.



Privacy Paranoia

→ Exkurs: Privacy Paranoia 4/4

Q1j. The information consumers willingly share with business organizations is no longer owned by them.

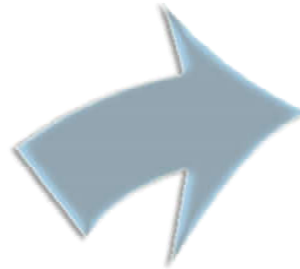
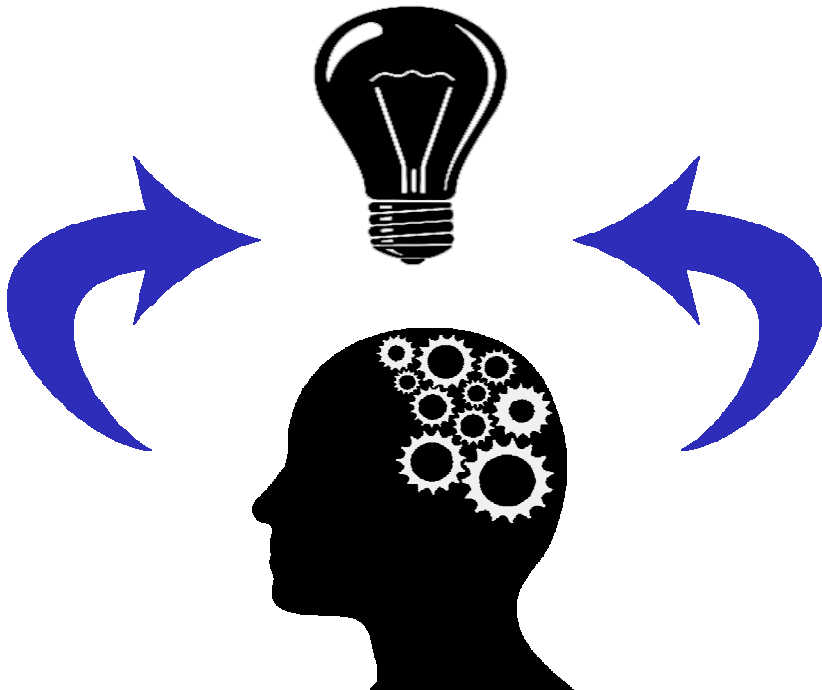


- Motivation
- IT-Sicherheit von 1990 bis heute
- Die Situation heute: Eine kritische Bewertung
- **Ein Blick in die Zukunft**
- Ausblick

Schnellere Innovation

→ Intelligente IT-Geräte und flexible IT Dienste

**Fähige Personen
für schnelle Innovationen**

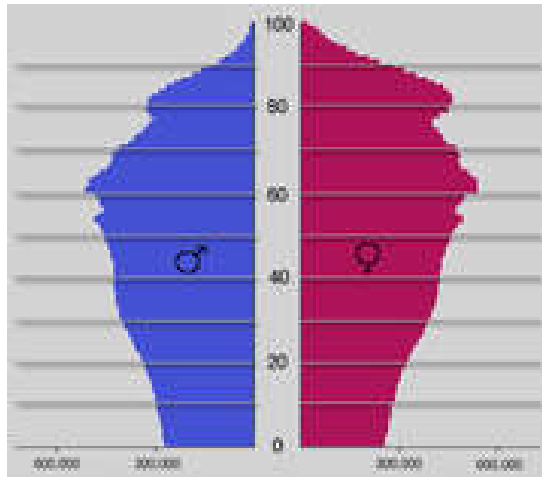


**Flexible IT Geräte und Dienste
für flexible Arbeitsverhältnisse**

Alterspyramide

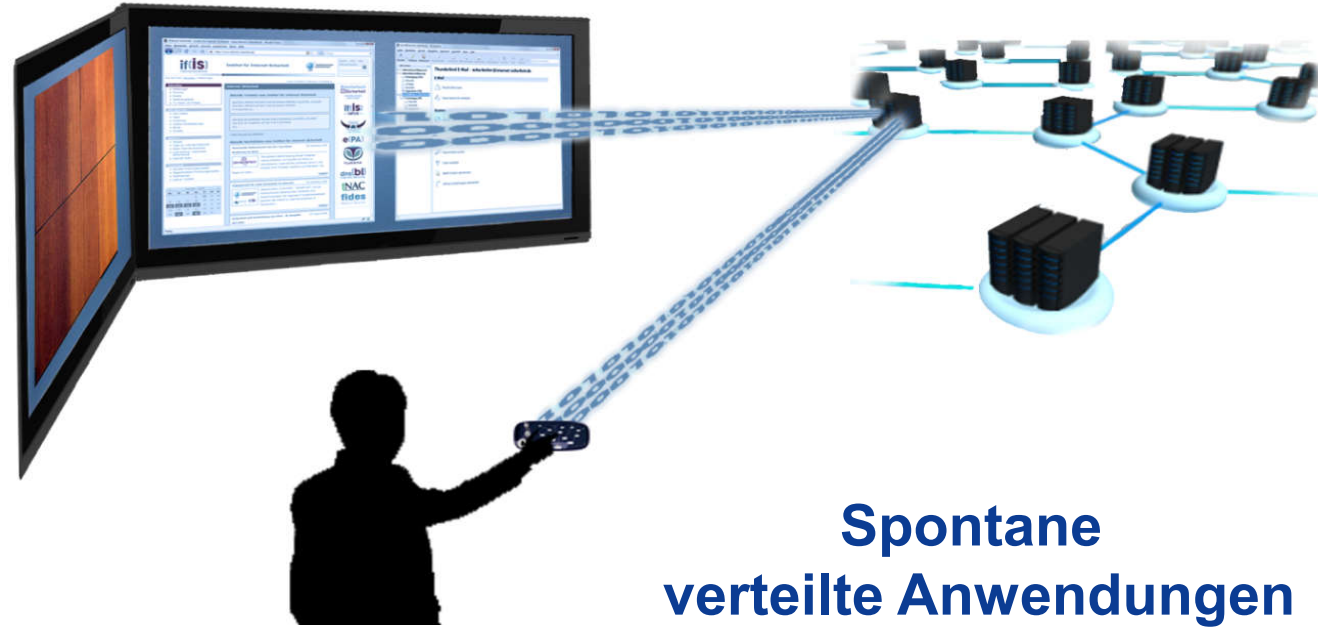
→ Sichere/vertrauenswürdige Zusammenarbeit

Doppelt so viele Menschen verlassen das Berufsleben



Offene „Objekt-Sicherheit“
weniger „Perimeter-Sicherheit“

Mehr CPUs, mehr Leistung → Trusted Computing in allen Dingen



**Spontane
verteilte Anwendungen**

Internet der Dinge

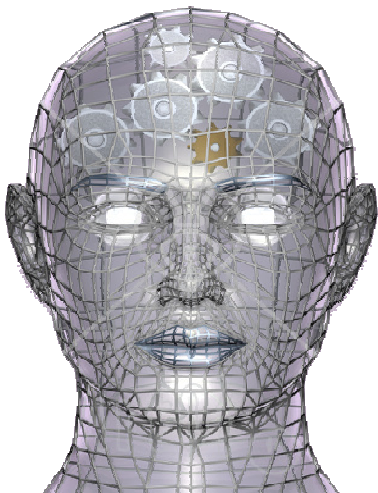


Mehr künstliche Intelligenz → IT Fee – Software Assistent

© Prof. Norbert Pohlmann, Institut für Internet-Sicherheit - if(is), Westfälische Hochschule, Gelsenkirchen



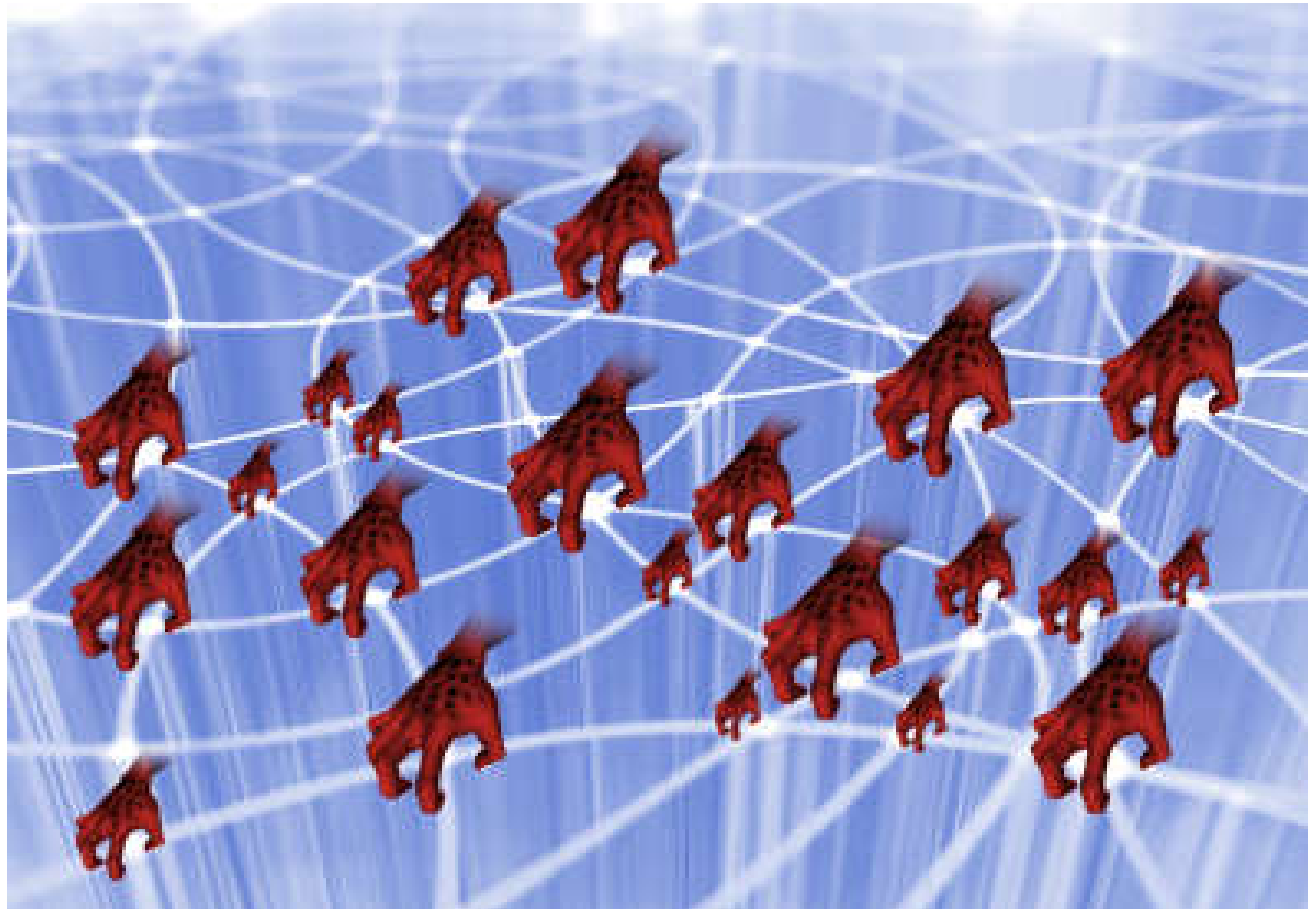
Mehr Power,
mehr Intelligenz



Für jeden eine „Gute IT Fee“

Cleverer und komplexerer → Angriffsmodelle

Die digitale Welt ist so gefährlich,
wie die Hilfsmittel, die sie verwendet!



- Motivation
- IT-Sicherheit von 1990 bis heute
- Die Situation heute: Eine kritische Bewertung
- Ein Blick in die Zukunft
- **Ausblick**

Aktuelle IT-Sicherheitslage

→ Zusammenfassung

- Wir müssen etwas tun, um unsere Zukunft **sicherer** und **vertrauenswürdiger** zu gestalten.
- Dazu brauchen wir einen **Quantensprung**
 - in der **Sicherheitstechnologie**,
 - in der **Vorgehensweise** und
 - in der **Zusammenarbeit** mit anderen.
- Die Zukunft beginnt jetzt, also lassen Sie uns anfangen!



**Westfälische
Hochschule**

Gelsenkirchen Bocholt Recklinghausen
University of Applied Sciences

Einführung

Internet-Sicherheit A

Vielen Dank für Ihre Aufmerksamkeit
Fragen ?

Prof. Dr. (TU NN)

Norbert Pohlmann

Institut für Internet-Sicherheit – if(is)
Westfälische Hochschule, Gelsenkirchen
<http://www.internet-sicherheit.de>

if(is)
internet-sicherheit.