



**Westfälische  
Hochschule**

Gelsenkirchen Bocholt Recklinghausen  
University of Applied Sciences

# Chancen und Risiken der → Digitalisierung

Prof. Dr. (TU NN)

**Norbert Pohlmann**

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

**if(is)**  
internet-sicherheit.

- **Digitalisierung** (*Chancen*)  
(Sichtweisen)
- **Generelle Herausforderungen** (*Risiken*)  
(Privatheit/Autonomie, Wirtschaftsspionage, Cyberwar)
- **Anwendungsbeispiele für Chancen/Risiken**  
(Smart Home, Mobilität, Soziale Netze, KI)
- **Digitale Modellstadt**  
(Der 7.Sinn, Bürger-ID, Blockchain)
- **Zusammenfassung und Ausblick**  
(Chancen und Risiken)

- **Digitalisierung** (*Chancen*)  
(Sichtweisen)
- **Generelle Herausforderungen** (*Risiken*)  
(Privatheit/Autonomie, Wirtschaftsspionage, Cyberwar)
- **Anwendungsbeispiele für Chancen/Risiken**  
(Smart Home, Mobilität, Soziale Netze, KI)
- **Digitale Modellstadt**  
(Der 7.Sinn, Bürger-ID, Blockchain)
- **Zusammenfassung und Ausblick**  
(Chancen und Risiken)

# Was ist Digitalisierung?

## → Einige Sichtweisen

### ■ Grundsätzliche Idee der Digitalisierung



- Prinzipiell: Von *analog* zu *digital*

- Allgemein: Digitalisierung beschreibt die **zunehmende Technisierung** sowie den **damit einhergehenden gesellschaftlichen Wandel**.

### ■ Industrie

- **Effizienzsteigerung** der Wertschöpfungsketten
- **Optimierung** der Produktionsprozesse, Logistikabläufe, ...

### ■ BürgerInnen

- Verbesserung der Lebensqualität
  - **Bequemlichkeit** („Alexa“: Lies ein Buch vor!)
  - **Effizienz** (Gewerbe, Parkberechtigung, ... on-line anmelden)

### ■ Politik

- Motor und Basis für **das Wohlergehen unserer** modernen **Gesellschaft**.

# Chancen und Risiken der Digitalisierung

## → Inhalt

- **Digitalisierung** (*Chancen*)  
(Sichtweisen)
- **Generelle Herausforderungen** (*Risiken*)  
(Privatheit/Autonomie, Wirtschaftsspionage, Cyberwar)
- **Anwendungsbeispiele für Chancen/Risiken**  
(Smart Home, Mobilität, Soziale Netze, KI)
- **Digitale Modellstadt**  
(Der 7.Sinn, Bürger-ID, Blockchain)
- **Zusammenfassung und Ausblick**  
(Chancen und Risiken)

# Generelle Herausforderungen

## → 1. Privatheit, Datenschutz, Autonomie

### Verschiedenen Sichtweisen

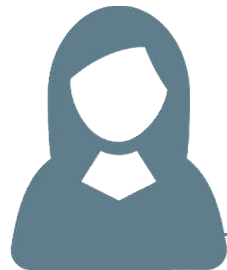
**Kulturelle Unterschiede**  
(Private Daten gehören den Firmen? US 76%, DE 22%)



**Geschäftsmodelle**  
„Bezahlen mit persönlichen Daten“



Privatheit / Autonomie



**Nutzer: Autonomie im Sinne der Selbstbestimmung**



**Staat (NSA, BND, ...): Identifizieren von terroristischen Aktivitäten**

# Generelle Herausforderungen

## → 2. Wirtschaftsspionage



ca. 54 Milliarden € Schaden pro Jahr

## Wirtschaftsspionage



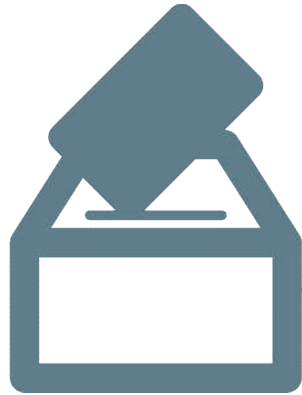
Zum Vergleich:

Internet-Kriminalität: ca. 100 Millionen € pro Jahr  
(Online Banking, DDoS, ...)



# Generelle Herausforderungen

## → 3. Cyberwar



Umsetzung von politischen Zielen  
→ „einfach“ und „preiswert“

Cyberwar



Angriffe auf Kritische Infrastrukturen  
z.B. Stromversorgung, Wasserversorgung, ...





# IT-Sicherheit

## → Die technischen Herausforderungen

### IT Sicherheitsprobleme

Smart Everything bringt neue Angriffsvektoren

Zu viele Schwachstellen in Software

Cloud Computing ist eine Herausforderung

Internet-Nutzer sind nicht sensibilisiert genug

# Risk

Manipulierte IT und IT Sicherheitstechnologie

Ungenügender Schutz vor Malware

Geschäftsmodell: „Bezahlen mit persönlichen Daten“

Unsichere Webserver im Feld

Ein zu hohes Risiko bei der E-Mail Kommunikation

heute

## Snowden

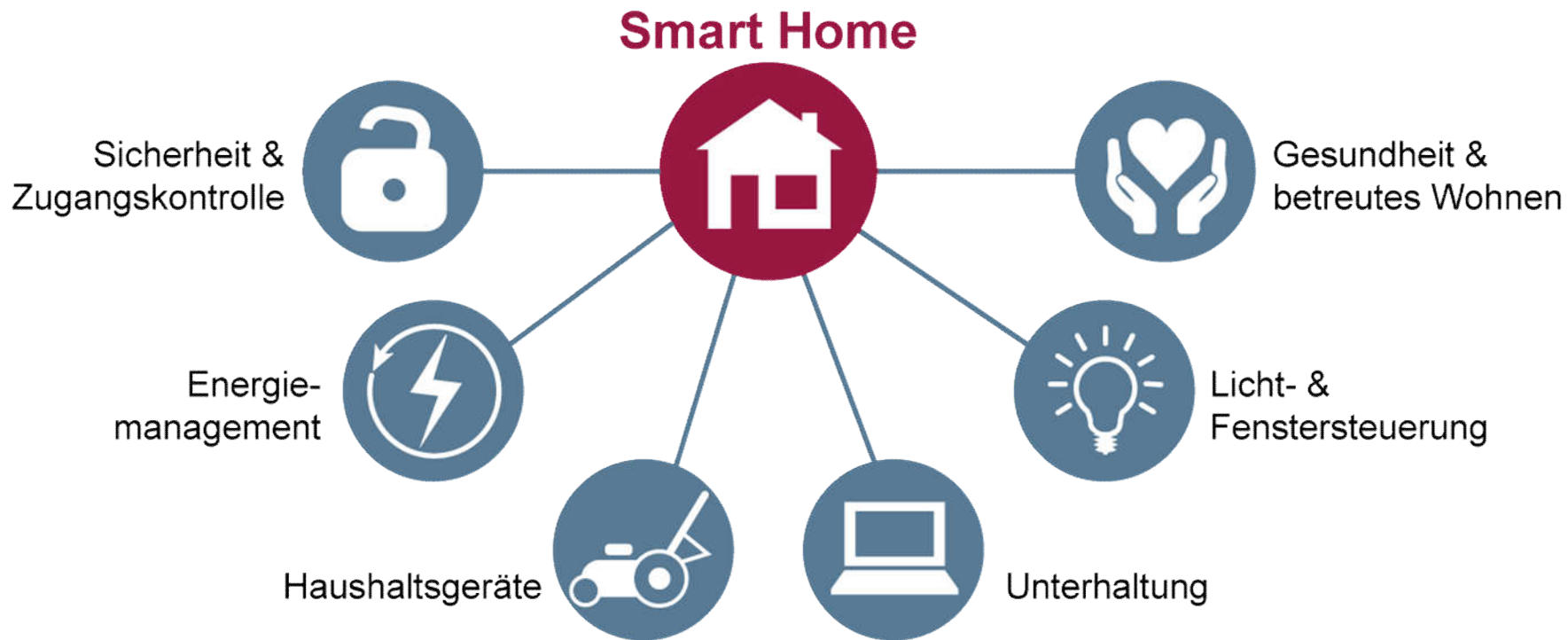
Gefahren durch mobile Geräte

Kein internationales Identity Management

- **Digitalisierung** (*Chancen*)  
(Sichtweisen)
- **Generelle Herausforderungen** (*Risiken*)  
(Privatheit/Autonomie, Wirtschaftsspionage, Cyberwar)
- **Anwendungsbeispiele für Chancen/Risiken**  
(Smart Home, Mobilität, Soziale Netze, KI)
- **Digitale Modellstadt**  
(Der 7.Sinn, Bürger-ID, Blockchain)
- **Zusammenfassung und Ausblick**  
(Chancen und Risiken)

# Smart Home

## → Chancen



## Innovative Interaktionskonzepte

Der Smart Home Sektor hat ein **Wachstum von 27%** jährlich!



Sprachsteuerung

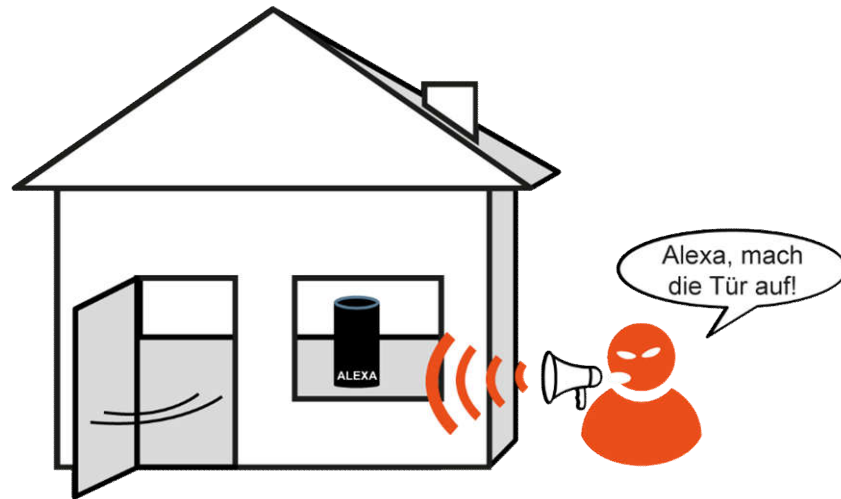


Gestensteuerung

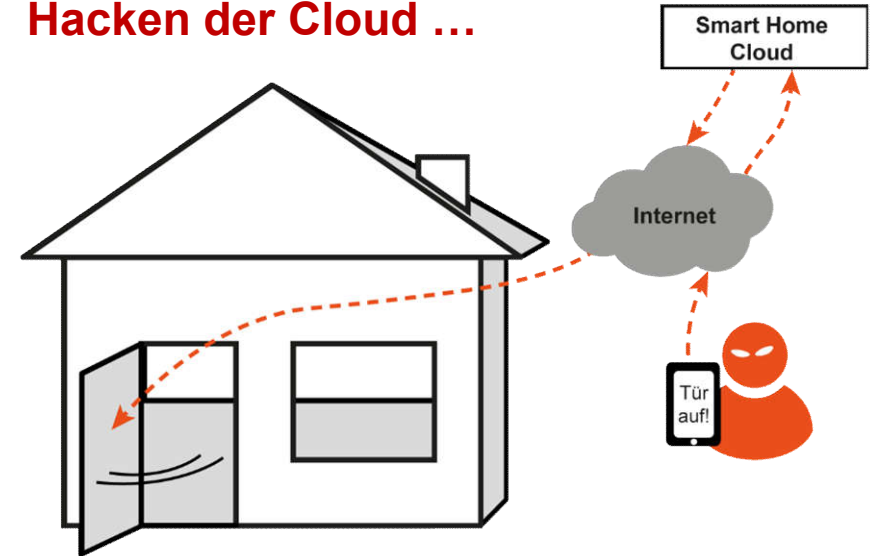
# Smart Home

## → Risiken

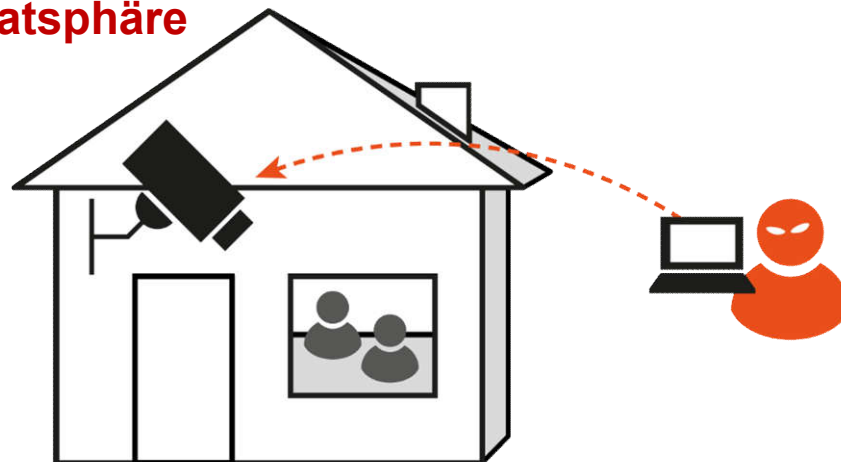
**Einbruch:**  
Sprachsteuerung durch das Fenster (Alexa), ...



**Einbruch:**  
Hacken der Cloud ...



**Risiko:**  
Privatsphäre



**"My home is my castle"**



# End-to-End Mobilität

## → Chancen

- **Ziel:**  
Von der Bonhoefferstraße in Aachen zur Reichenbergerstraße nach Berlin
- **Umsetzung:** Erster Schritt  
Mit einem autonom fahrenden Auto von der Bonhoefferstraße  
→ zum Hauptbahnhof Aachen *oder*  
→ Flughafen (Köln/Bonn, Düsseldorf, Maastricht, ...)
- **Umsetzung:** Zweiter Schritt  
Mit einem autonom fahrenden Auto vom Bahnhof / Flughafen  
in Berlin zur Reichenbergerstraße in Berlin
- **Im Problemfall** (Ausfall Zug oder Flug)  
→ automatische Auswahl einer Alternative  
→ einfache und klare Anweisung
- **Realisierung**  
→ Für den Nutzer: **App** (*alles in einer Verantwortung – Preis/Organisation/...*)  
→ Für die Mobilitätsanbieter: **Gemeinsame Mobilitätsplattform**

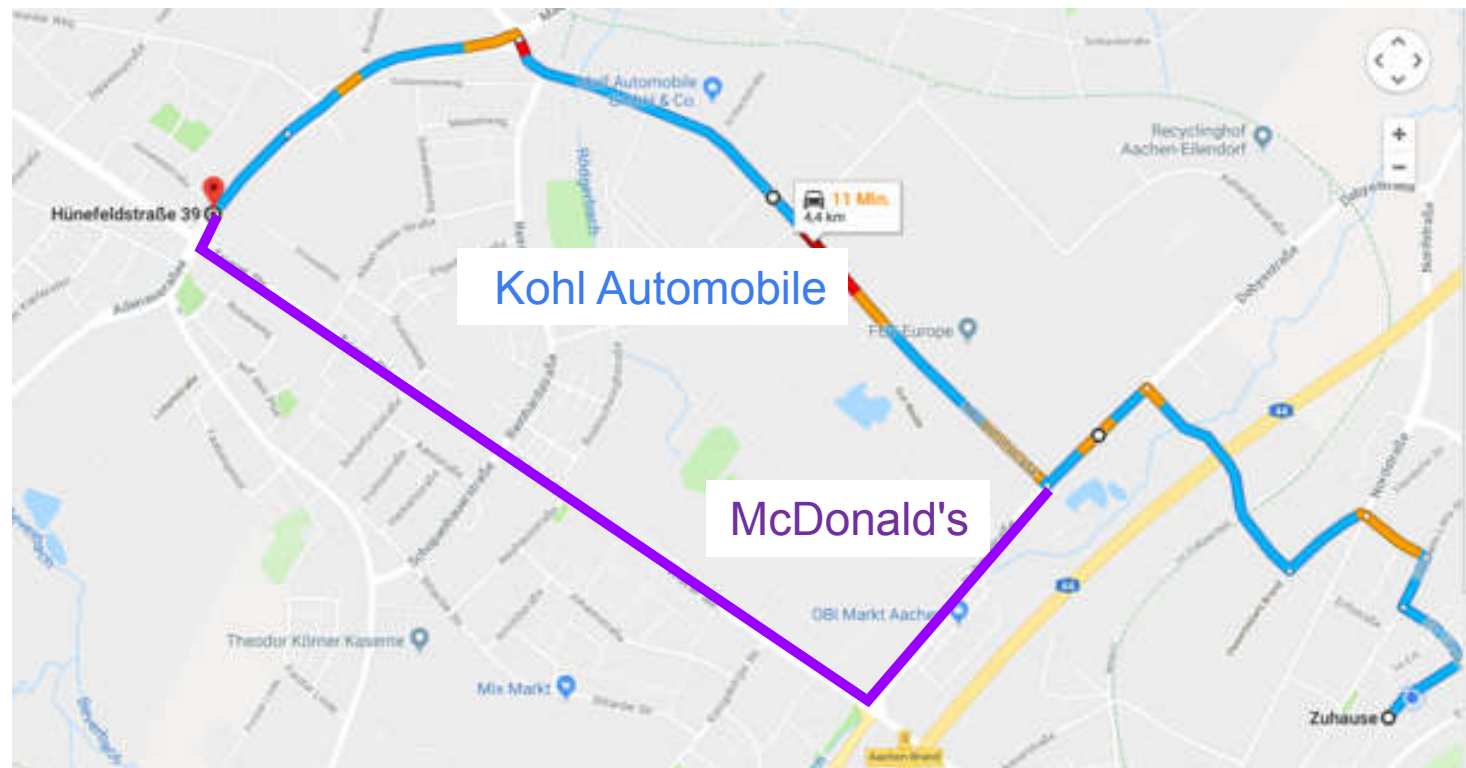


# End-to-End Mobilität

## → Risiken

- Wir verlieren die Fähigkeit, uns zu orientieren und zu organisieren.
- Wir können nicht mehr kontrollieren, ob der Weg für uns optimal ist.

### Beispiel





### Sinn und Zweck

- Darstellung (Image)
- Austausch von
  - Meinungen
  - Informationen
  - Erfahrungen

### Inhalte, die von den Nutzern von Sozialen Netzen eingestellt werden:

- Texte
- Bilder, Grafiken
- Videos, Filme
- Kommentare
- Musik, Audiodateien
- Quellcode

# Soziale Netzwerke

## → Zahlen Sozial Netze (2017)

### facebook

- Nutzer – ca. 2,07 Mrd.
- **Texte – ca. 4 Mrd. am Tag**
- Bilder – ca. 60 Millionen am Tag
- Videos – ca. 100 Millionen Stunden am Tag



- Nutzer – ca. 800 Millionen
- **Bilder – ca. 95 Millionen am Tag**
- Likes – ca. 4,2 Mrd. am Tag



- Nutzer – ca. 330 Millionen
- **Tweets – ca. 500 Millionen (800 gesehen) am Tag**



- Nutzer – mehr als 1 Mrd.
- Videos –  
3,25 Mrd. Std. angesehen (jeden Monat)  
**300 Std. Videomaterial (jede Minute)**



### Unerwünschte Inhalte (Rechtlich verboten, Hate Speeches, Fake News, ...)

- Volksverhetzung
- *Beleidigung*
- Verleumdung / Störung des öffentlichen Friedens (vortäuschen Straftaten ...)
- *Kinderpornographie*
- Gewaltverherrlichende Inhalte
- *Nackte Busen (USA, ...)*
- Hakenkreuz (DE, ...)
- ...



aber auch ...

- mit Rechten behaftete Objekte (Bilder, Filme Musik, ...)

### Weitere Aspekte (Inhalt)

- **Digitaler Narzissmus** (überzogene Selbstpräsentation auf der Suche nach Selbstbestätigung und Anerkennung macht anfällig für Kriminelle)
- ...

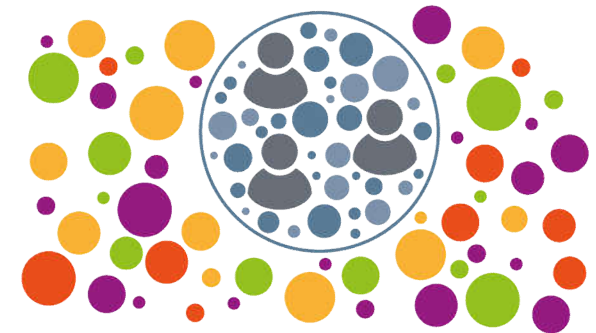
### Filterblasen

- Nutzer sehen tendenziell **nur Informationen, die mit ihren bisherigen Ansichten übereinstimmen.**
- **Verfahren:** Bestimmt durch das Like- und Klick-Verhalten.
- **Problem:** Nutzer bekommt keine Informationen, die den eigenen Standpunkt widersprechen und damit ist eine **objektive Selbstbestimmung nicht mehr möglich.**



### Echokammer

- Viele Menschen in den sozialen Netzwerken neigen dazu, sich **mit Gleichgesinnten** zu umgeben und sich dabei gegenseitig in der **eigenen Position verstärken.**
- **Problem:** Es erwächst der **Eindruck**, keine Minderheitsmeinung zu vertreten, sondern **eine gesellschaftlich relevante Mehrheit zu sein.**
- Soziale Netze unterstützen diesen Effekt!

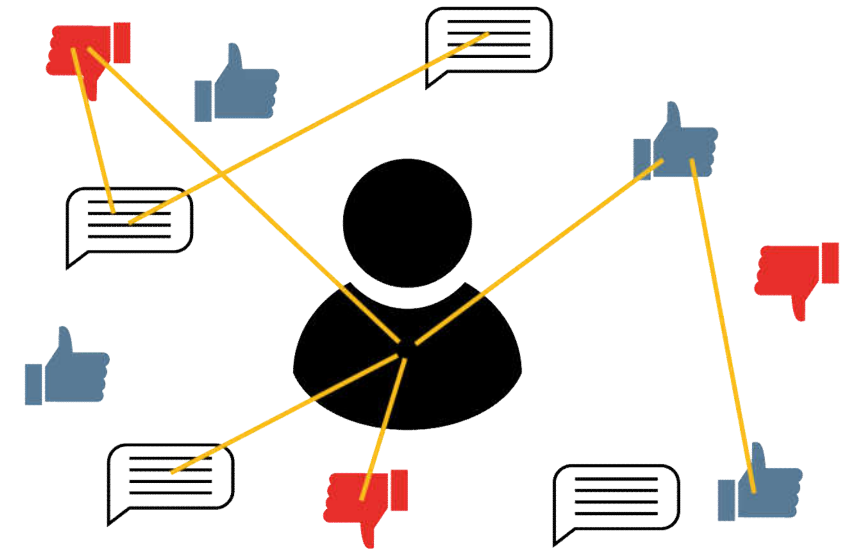


**Keine Diversität mehr!**

Die **Psychometrie** ist das Gebiet der Psychologie, das sich allgemein mit Theorie und Methode **des psychologischen Messens** befasst.

### Analyse auf Facebook (Cambridge Analytics)

- **Input:** Was haben Nutzer gelikt, geshared oder gepostet
- **Output:** Geschlecht, Alter, Wohnort, ...



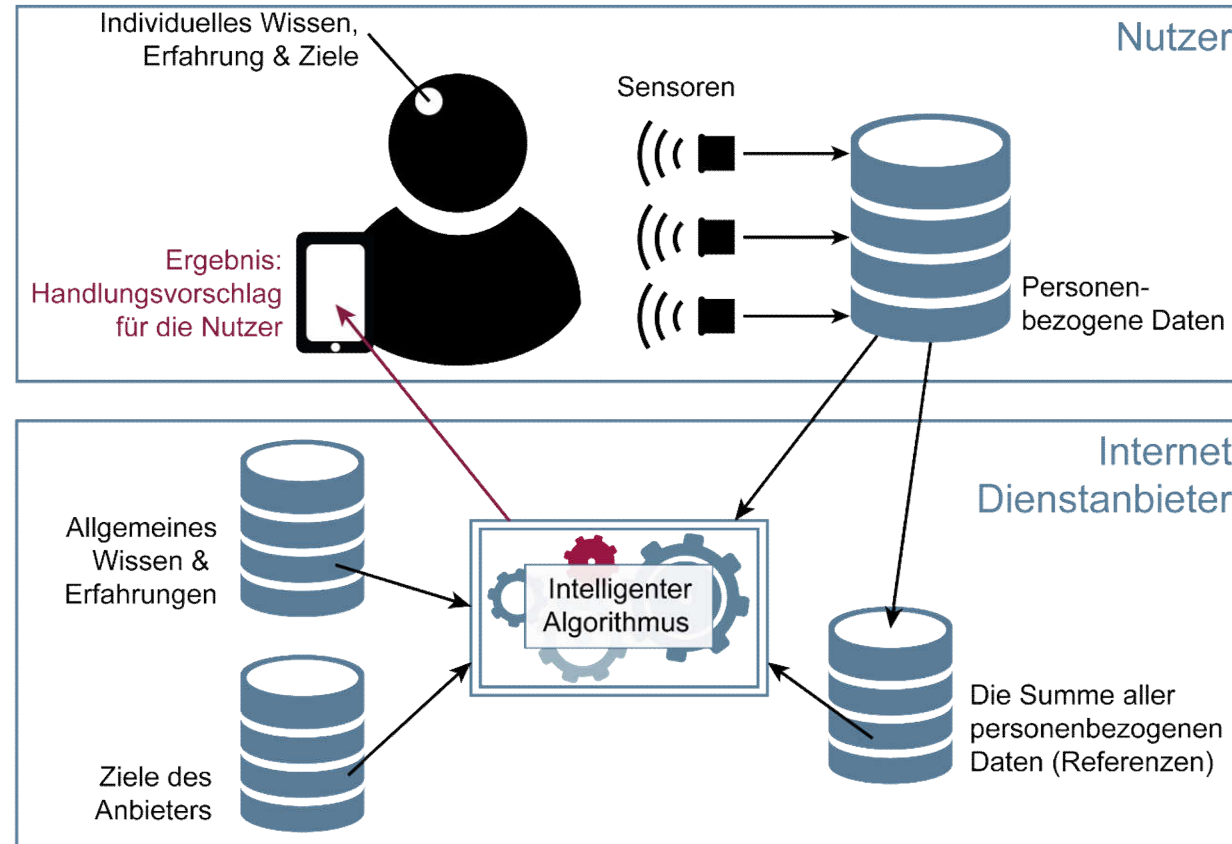
Welche **Zusammenhänge** sind berechenbar?

- Mit durchschnittlich 68 Facebook-Likes kann vorhergesagt werden:
  - Welche **Hautfarbe** der Nutzer hat (95-prozentige Treffsicherheit),
  - ob der Nutzer **homosexuell** ist (88-prozentige Wahrscheinlichkeit),
  - ob der Nutzer **Demokrat** oder **Republikaner** ist (85 Prozent).
- *Aber auch:*  
Intelligenz, Religionszugehörigkeit, Alkohol-, Zigaretten- und Drogenkonsum lassen sich berechnen.

# Intelligente Algorithmen

## → Chancen

- **Individuelles Wissen und Komplexität des denkenden Menschen** sind Algorithmen überlegen! +
- **Algorithmen können schneller Wissen aus vorhandenen Daten auswerten!** +
- Individuelles Wissen + Algorithmen Wissen = ++++



- **Praktische Probleme: Medizin / Watson**
  - Diagnostik (*Maschine*)
  - Haftung (*Mensch*)

### Anwendungsfall: Handlungsempfehlungen

- Dienste sind **nicht** kostenlos! (Server, Informatiker, Marketing, ...) *(Nutzer bezahlt mit seinen persönlichen Daten)*
- **Konsequenz:**  
Am Ende wird eine Entscheidung getroffen, die dem Anbieter Vorteile schafft und nicht dem Nutzer (Sponsoren, Pay2Win)

**Die IT soll dem Menschen dienen und nicht der Mensch den kommerziellen Dienste-Anbietern!**

### Allgemein

- Wir machen uns **abhängig, unwissend** und **verlieren Fähigkeiten**
- Arbeitsplätze fallen weg oder werden verändert

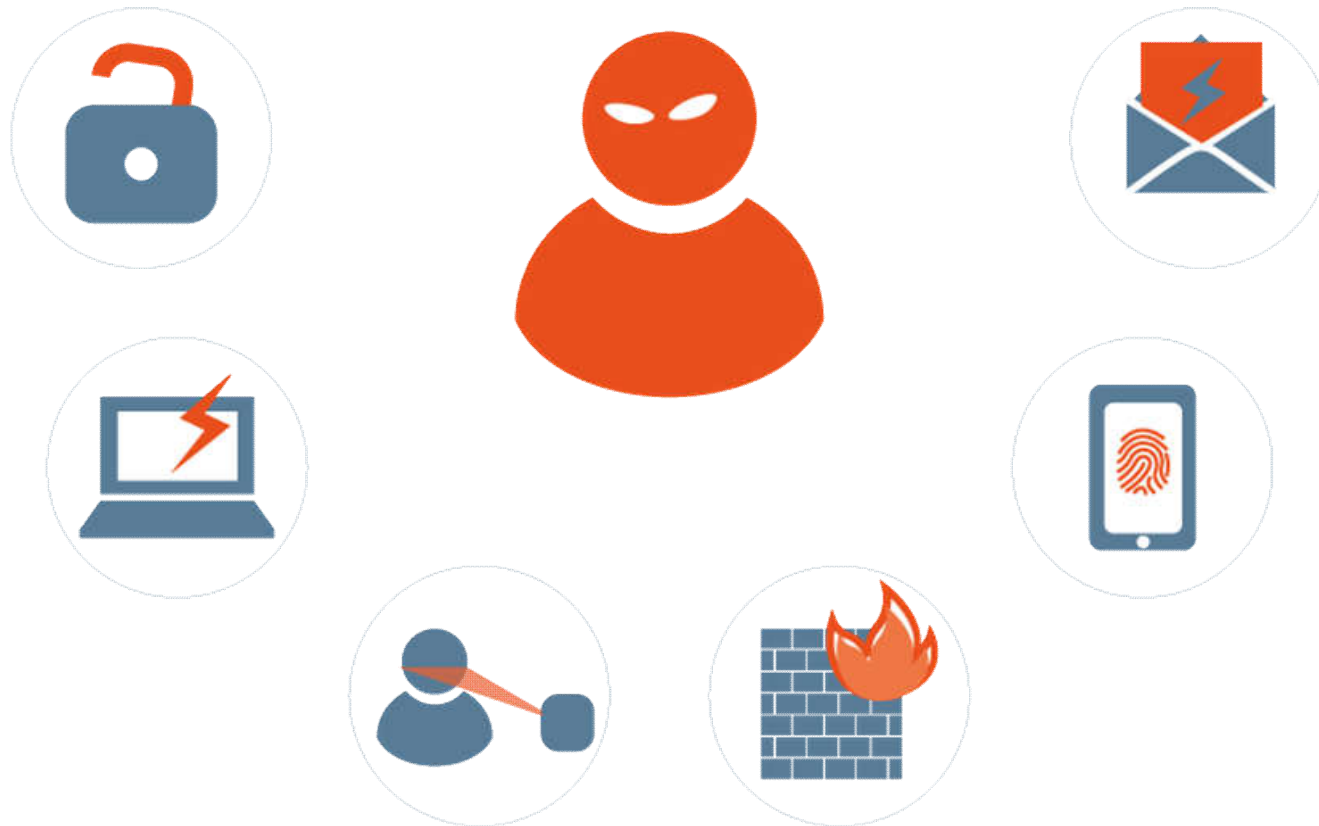
- **Digitalisierung** (*Chancen*)  
(Sichtweisen)
- **Generelle Herausforderungen** (*Risiken*)  
(Privatheit/Autonomie, Wirtschaftsspionage, Cyberwar)
- **Anwendungsbeispiele für Chancen/Risiken**  
(Smart Home, Mobilität, Soziale Netze, KI)
- **Digitale Modellstadt**  
(Der 7.Sinn, Bürger-ID, Blockchain)
- **Zusammenfassung und Ausblick**  
(Chancen und Risiken)

# Digitale Modellstadt

## → Der 7. Sinn der Digitalisierung

„Der 7. Sinn der Digitalisierung in Regionen“ versorgt BürgerInnen und Unternehmen (KMUs) in Aachen und Gelsenkirchen schnell, kostenlos und unkompliziert mit **Awareness-Videos** und **Ratgebern**, die helfen, **selbtsicher mit den neuen Digitalisierungsprozessen** in den Regionen **zurecht zu kommen**.

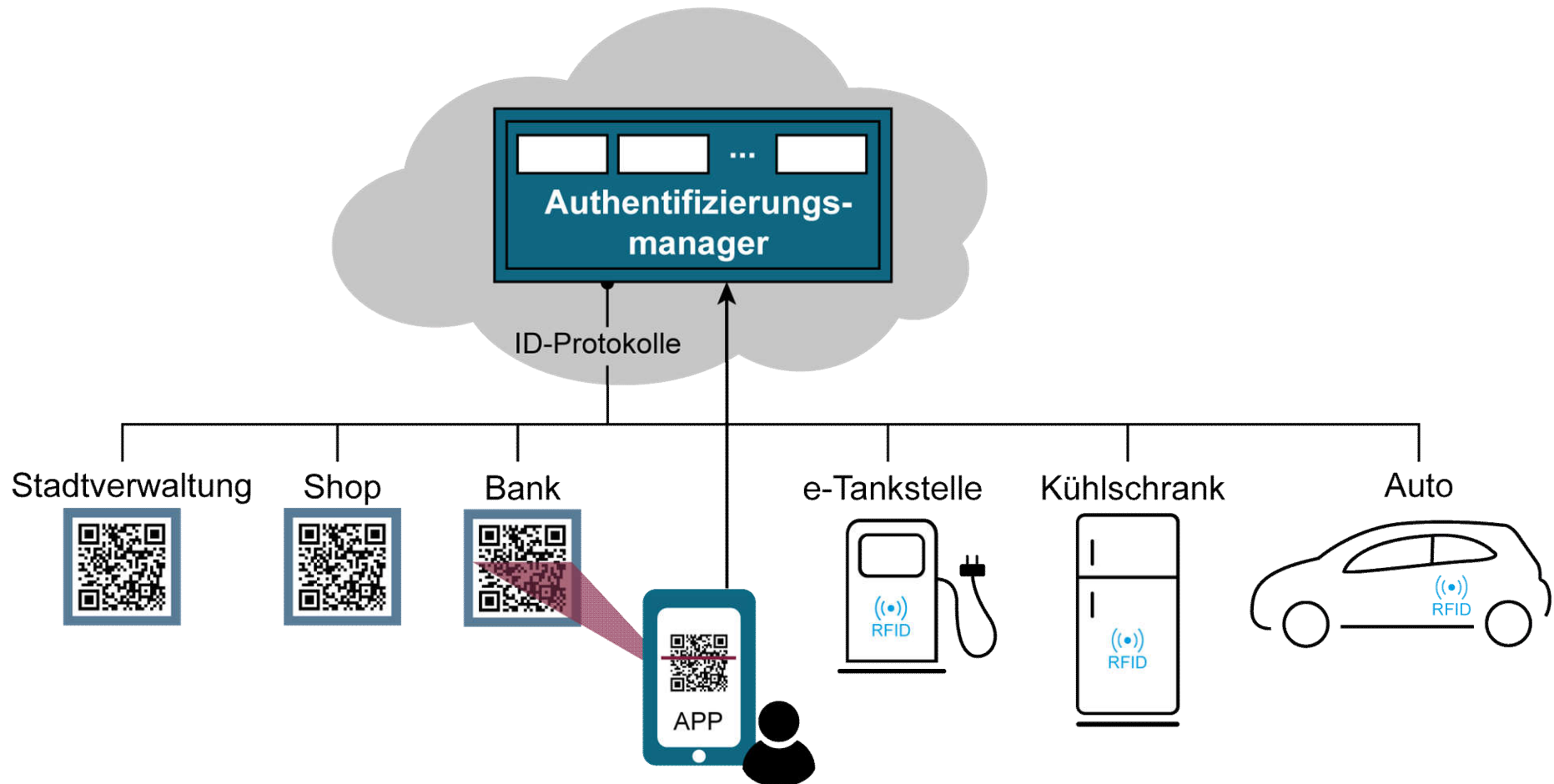
### Risiken



# Digitale Modellstadt

## → Bürger-ID

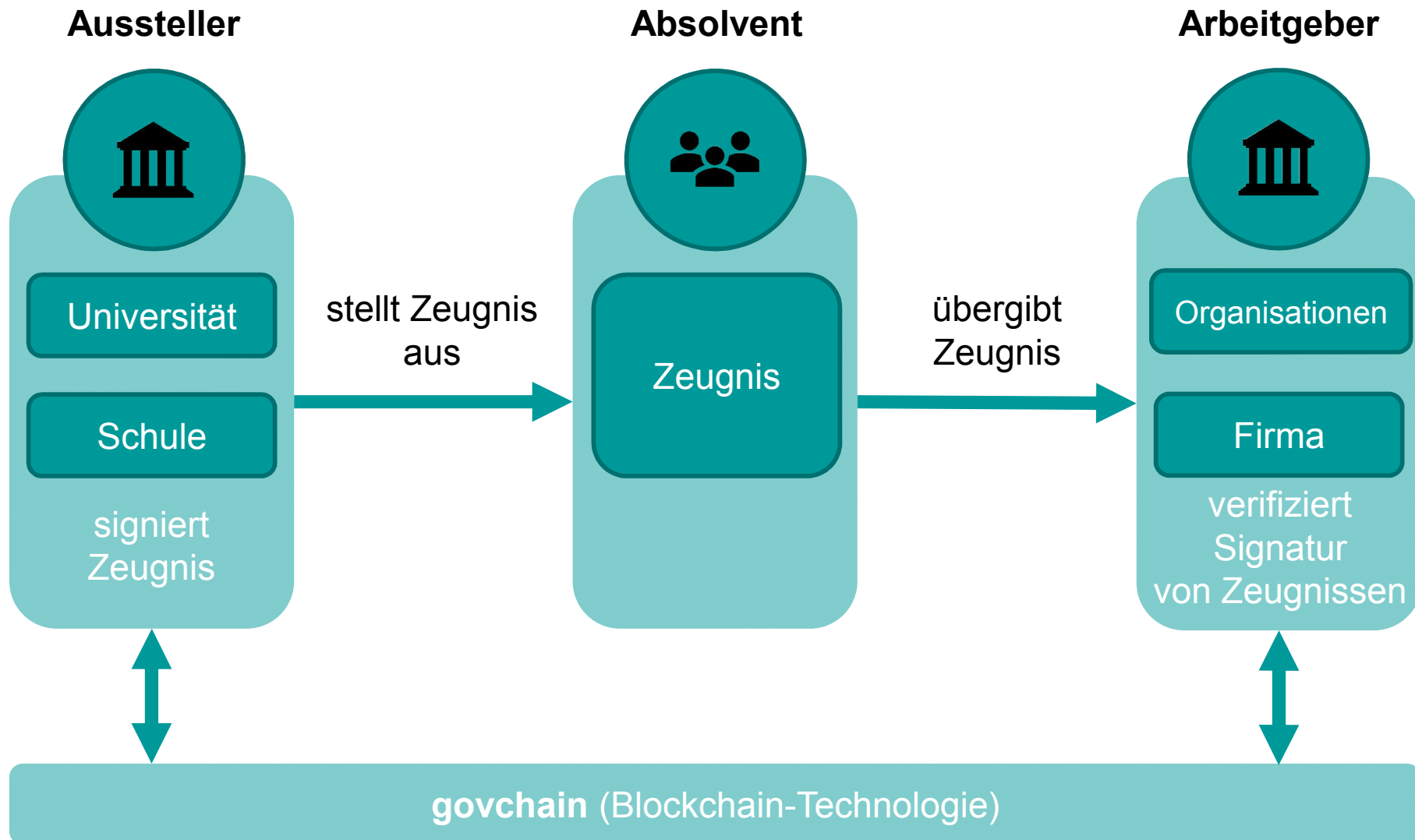
Die **starke Authentifizierung** des Bürgers per Smartphone, mit der **sicheren Erfassung der persönlichen Daten** und der flexiblen Nutzung der Bürger-ID, soll die Grundlage für alle zukünftigen personalisierten Anwendungen im **E-Government** und der **Smart City** bilden.





# Digitale Modellstadt → Blockchain

- Digital geprüfte Zeugnisse mit der **govchain** als ein Beispiel



- **Digitalisierung** (*Chancen*)  
(Sichtweisen)
- **Generelle Herausforderungen** (*Risiken*)  
(Privatheit/Autonomie, Wirtschaftsspionage, Cyberwar)
- **Anwendungsbeispiele für Chancen/Risiken**  
(Smart Home, Mobilität, Soziale Netze, KI)
- **Digitale Modellstadt**  
(Der 7.Sinn, Bürger-ID, Blockchain)
- **Zusammenfassung und Ausblick**  
(Chancen und Risiken)

# Digitalisierung

## → Chancen durch Gestaltung

- Effizienzsteigerung, Optimierung, Verbesserung (Bequemlichkeit, Effizienz)
- Sicherung des Wohlstandes unserer modernen Gesellschaft

*aber auch:*

- **Realisierung eigener IT-Technologien und IT-Infrastrukturen**
  - **Stand der Technik** im Bereich **IT-Sicherheit** umsetzen können.
  - Unabhängig von anderen Ländern sein (**Souveränität** in der IT)
  - ...
- **Wir sind besonders stark im Bereich Industrie 4.0**  
(Industrial Internet of Things)
- ...

# Rahmenbedingungen Digitalisierung

## → Verantwortung der Politik

- Digitalisierung als Motor, aber nur, wenn die Weichen richtig gestellt werden.
  - Sicherstellen, dass **alle von der Digitalisierung profitieren** können
  - **Sicherstellung von wichtigen Aspekten**  
(Wissen kann nicht nur die Verantwortung von Google sein!)
  - **Bedingungsloses Grundeinkommen**, oder ähnliche Konzepte werden wir langfristig brauchen ...
- **Regulierungen**
  - Arbeit 4.0
  - Ethik-Themen (autonom fahrendes Auto, Killer-Roboter, ...)
  - ...

# Zusammenfassung und Ausblick

## → Chancen und Risiken

- **Kompetenzen aufbauen**
  - Wir brauchen Kompetenzen, um **an den Chancen erfolgreich partizipieren** zu können und die **Risiken** dabei aktiv zu **minimieren**.
- **Veränderung der Ausbildung**
  - Die IT ist dem Menschen in vielen Dingen voraus!
  - Daher sollten wir uns in Zukunft auf andere **Fähigkeiten konzentrieren** (Werte/Glauben, unabhängiges Denken, Kunst, Teamwork, Sport, ...)
  - **Konsequenzen für Lerninhalte** an Schulen/Hochschulen
- **Für Resilienz sorgen, damit die IT-Dienst verfügbar sind**
- **Selbstverpflichtungen** (Cyberwar, ...)
  - Wie Atomwaffensperrvertrag



**Westfälische  
Hochschule**

Gelsenkirchen Bocholt Recklinghausen  
University of Applied Sciences

# Chancen und Risiken der → Digitalisierung

**Mit Sicherheit in die Zukunft!**

Prof. Dr. (TU NN)

**Norbert Pohlmann**

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

**if(is)**  
internet-sicherheit.

## Wir empfehlen

- **Kostenlose App securityNews**



securityNews



- **7. Sinn im Internet (Cyberschutzraum)**  
[https://www.youtube.com/channel/UCEMkJW9dHcWfek\\_En3xhjg](https://www.youtube.com/channel/UCEMkJW9dHcWfek_En3xhjg)

- **Cybärcast – Der IT-Sicherheit Podcast**  
<https://podcast.internet-sicherheit.de/>



- **Master Internet-Sicherheit**  
<https://it-sicherheit.de/master-studieren/>



## Quellen Bildmaterial

Eingebettete Piktogramme:

- Institut für Internet-Sicherheit – if(is)

## Besuchen und abonnieren Sie uns :-)

### WWW

<https://www.internet-sicherheit.de>

### Facebook

<https://www.facebook.com/Internet.Sicherheit.ifis>

### Twitter

<https://twitter.com/ifis>

### Google+

<https://plus.google.com/107690471983651262369/posts>

### YouTube

<https://www.youtube.com/user/InternetSicherheitDE/>

### Prof. Norbert Pohlmann

<https://norbert-pohlmann.com/>

## Der Marktplatz IT-Sicherheit

(IT-Sicherheits-) Anbieter, Lösungen, Jobs, Veranstaltungen und Hilfestellungen (Ratgeber, IT-Sicherheitstipps, Glossar, u.v.m.) leicht & einfach finden.  
<https://www.it-sicherheit.de/>

## Artikel:

N. Pohlmann: „Cyber Security“, WISU – Das Wirtschaftsstudium, Lange Verlag, 2/2015

<https://norbert-pohlmann.com/app/uploads/2015/08/331-Cyber-Security-Die-Herausforderung-unserer-Gesellschaft-Prof.-Norbert-Pohlmann.pdf>

H.B. Dhia, N. Pohlmann: „Intelligente Helfer als persönliche Assistenten. Wie sicher und vertrauenswürdig sind Roboter?“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 4/2016

<https://norbert-pohlmann.com/app/uploads/2017/03/350-Intelligente-Helfer-als-persönliche-Assistenten-Wie-sicher-und-vertrauenswürdig-sind-Roboter-Prof.-Norbert-Pohlmann.pdf>

M. Hertlein, P. Manaras, N. Pohlmann: „Die Zeit nach dem Passwort - Handhabbare Multifaktor-Authentifizierung für ein gesundes Eco-System“, DuD Datenschutz und Datensicherheit – Recht und Sicherheit in Informationsverarbeitung und Kommunikation, Vieweg Verlag, 4/2016

<https://norbert-pohlmann.com/app/uploads/2016/05/345-Die-Zeit-nach-dem-Passwort-Handhabbare-Multifaktor-Authentifizierung-für-ein-gesundes-Eco-System-Prof.-Norbert-Pohlmann.pdf>

U. Coester, N. Pohlmann: „Verlieren wir schleichend die Kontrolle über unser Handeln? Autonomie hat oberste Priorität“, BI-SPEKTRUM Fachzeitschrift für Business Intelligence und Data Warehousing, 05-2015

<https://norbert-pohlmann.com/app/uploads/2015/12/341-Verlieren-wir-schleichend-die-Kontrolle-über-unser-Handeln-Autonomie-hat-oberste-Priorität-Prof-Norbert-Pohlmann.pdf>

J.-H. Frintrop, N. Pohlmann: „Alexa, wie sicher bist du? – Intelligente Sprachsteuerung unter der Lupe“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 6/2017

<https://norbert-pohlmann.com/app/uploads/2018/01/365-Alexa-wie-sicher-bist-du---Intelligente-Sprachsteuerung-unter-der-Lupe-Prof.-Norbert-Pohlmann.pdf>

N. Pohlmann „Fake-News in Sozialen Netzwerken – Das „Mitmach-Web“ hat seine Unschuld (endgültig) verloren“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 5/2017

<https://norbert-pohlmann.com/app/uploads/2017/10/363-Fake-News-in-Sozialen-Netzwerken---Das-Mitmach-Web-hat-seine-Unschuld-endgültig-verloren-Prof.-Norbert-Pohlmann.pdf>

N. Pohlmann: „Blockchain-Technologie unter der Lupe – Sicherheit und Vertrauenswürdigkeit kryptografisch verkettete Datenblöcke“, IT-Sicherheit – Fachmagazin für Informationssicherheit und Compliance, DATAKONTEXT-Fachverlag, 4/2018