Hochschule
Kaiserslautern
University of
Applied Sciences

Angewandte
Ingenieurwissenschaften
Kaiserslautern

IT-Sicherheit 2019

Tag des offenen Campus
06.04.2019, Kaiserslautern

Prof. Dr. Eva Maria Kiss

Informationssicherheit vor 25 Jahren

- Rechner werden für die elektronische Datenverarbeitung eingesetzt, der PC hat die Schreibmaschine schon abgelöst. Briefe werden am eigenen Arbeitsplatz ausgedruckt und per Fax verschickt, die Daten auf kleinen Disketten gespeichert.
- **Informationssicherheit vor 25 Jahren bedeutete:**
  - Physische Sicherheit
    - Datenspeicherung auf Papier
    - Datenhaltung hinter Schloss und Riegel
    - Datenübertragung durch sichere Transporte
  - Administrative Sicherheit
    - Zugangskontrollen
    - Personenüberwachung
    - Wirtschaftsprüfung

Jahr 1990

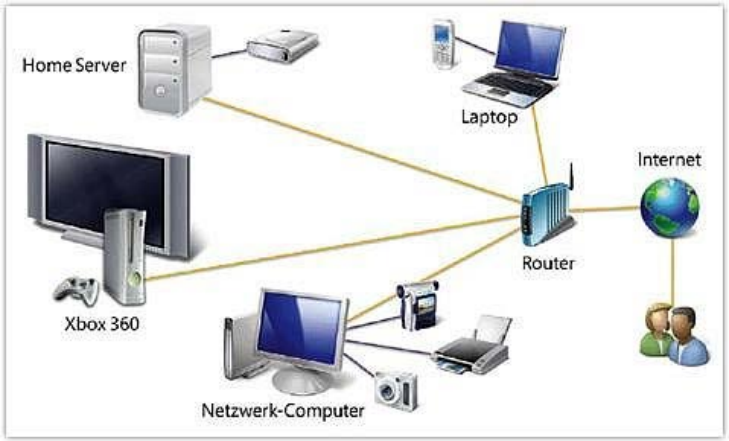
Informationssicherheit heute

- Zwischen 1990 und 2000 kam das Internet, zuerst mit Modems, ISDN, dann mit Breitband-DSL, zuerst an Hochschulen, dann in Unternehmen, dann überall.
- In den 2000er Jahren haben Laptops die PCs abgelöst, es werden keine Briefe mehr geschrieben, sondern E-Mails, das Faxgerät wird mit der Zeit vor allem zum Scannen benutzt. Nach 2005 kommen die mobilen Geräte hinzu.
- **Informationssicherheit heute bedeutet:**
  - Physische und administrative Sicherheit wird durch **IT-Sicherheit** ersetzt.
  - IT-Systeme müssen so entwickelt und betrieben werden, dass nur Berechtigte Zugriff haben.
  - Neue Herausforderungen durch
    - Mobilität
    - Vernetzung über das Internet
    - Miniaturisierung

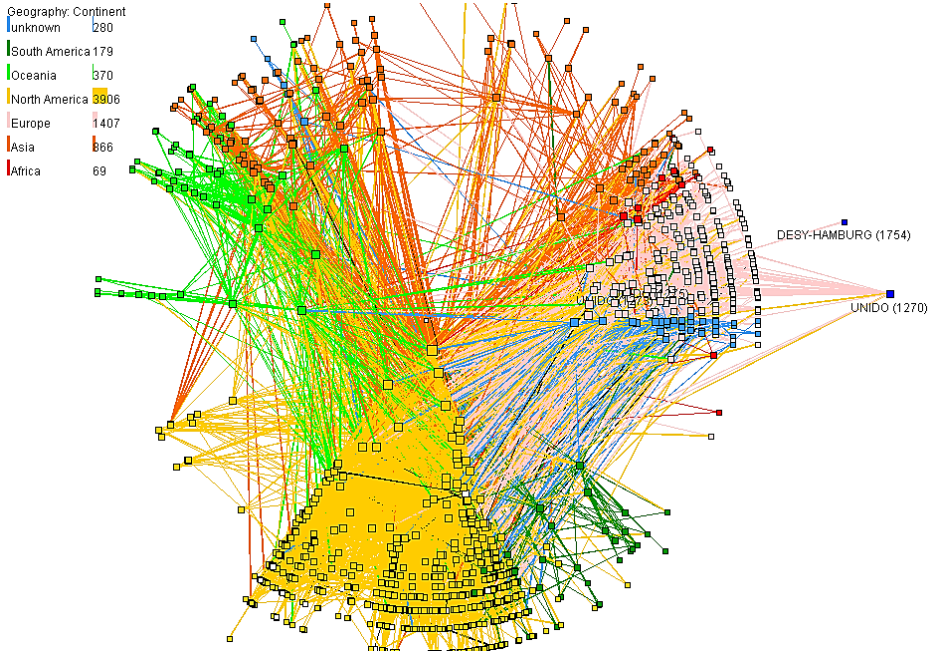
Jahr 2019

Vom Internet zum Internet der Dinge

- Im Jahr 2000 waren ca. 200.000 große Internet-Teilnehmer im Internet vernetzt, im Jahr 2015 sind es 42 Millionen.
- Ab 2010 kommen neue Teilnehmer hinzu: mechanische und elektronische Komponenten, die vernetzt das Internet der Dinge (Internet of Things, IoT) bilden. In der Industrie spricht man von Industrie 4.0, der vierten industriellen Revolution.



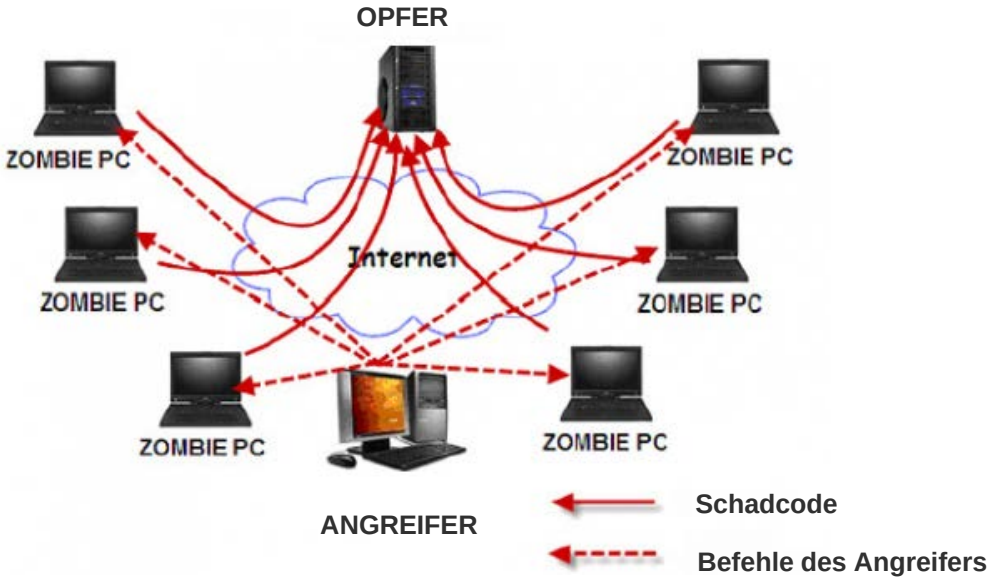
Firmen- und Heimnetzwerke sind über das Internet miteinander verbunden.



Internet-Graph im Jahr 2000
http://www.caida.org/projects/internetatlas/gallery/ascore/demo.xml

Bedrohungen der IT-Sicherheit

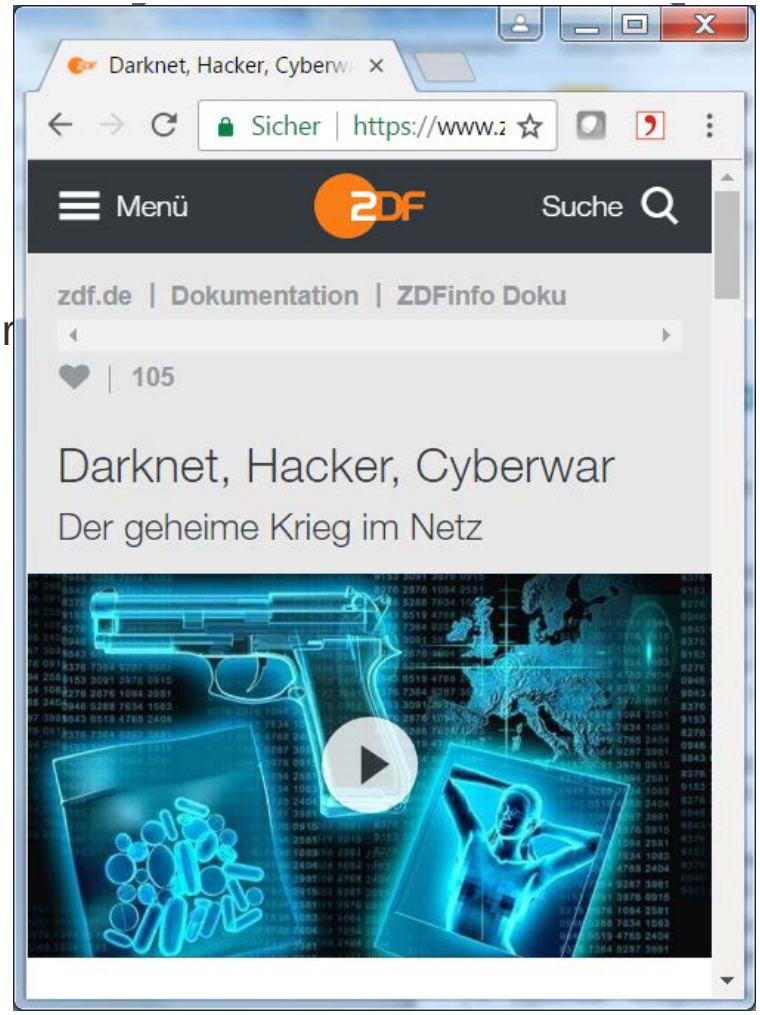
- Die ersten Bedrohungen der IT-Sicherheit bestanden in kleinen Schadprogrammen, die man noch relativ einfach mit dem Einsatz von Virenscannern, Spamfiltern und Firewalls bekämpfen konnte.
- Die neuen Bedrohungen sind kombinierte Angriffe, die viele Rechner und Geräte einbeziehen und sich sowohl gegen Privatpersonen als auch gegen Organisationen richten. Einem aktiven Angriff geht oft eine monatelange Beobachtungsphase voraus, während der die Angreifer unbemerkt Daten sammeln.



Bedrohungen der IT-Sicherheit

Aktuelle Bedrohungen:

- Social Engineering: Ausnutzen menschlicher Schwächen, z.B. Phishing
- Ransomware (ransom = Lösegeld): Schadprogramme, die Daten verschlüsseln, um für die Freigabe ein „Lösegeld“ zu fordern.
- Scareware: Schadprogramme, die Benutzer verängstigen und so zu bestimmten Handlungen bewegen sollen.
- Denial of Service: Server und Dienste werden künstlich mit Anfragen überlastet.
- Cyberspionage: Nachrichtendienste betreiben Informationsgewinnung im Internet.
- Cyberwar: Kriegsführung via Internet, das Internet eines Landes wird manipuliert und torpediert.
- Sicherheitslücken in Prozessoren (Meltdown)



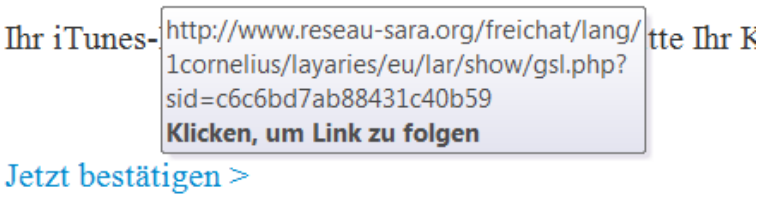
Beispiel: Phishing

Bei **Phishing** handelt es sich um eine E-Mail, die einem Internet-Nutzer Daten (Passwort, Kreditkartendaten) entlocken soll, indem er durch Anklicken eines Links auf eine präparierte Website geführt wird, die optisch sehr ähnlich aussieht wie die Website eines Anbieters (Apple, Paypal).

Sicherheitsmaßnahme:

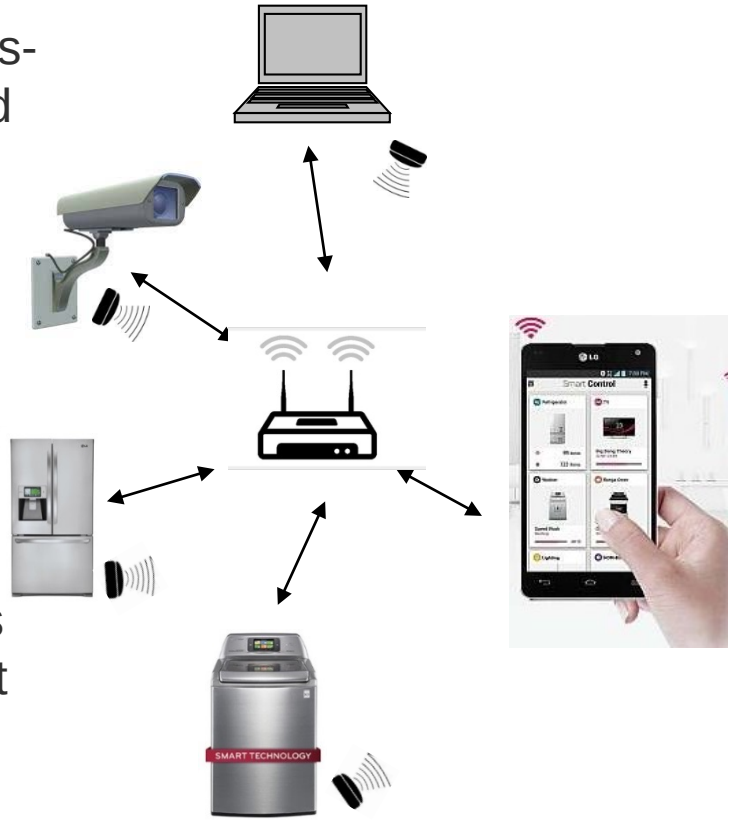
Phishing-E-Mails erkennen

1. Grammatik- und Orthografie-Fehler
2. Fehlende persönliche Anrede
3. Dringender Handlungsbedarf, Drohung
4. Aufforderung, einen Link anzuklicken.



Beispiel: Schadprogramm Mirai

- Oktober 2016: Mirai sucht nach schlecht geschützten IoT-Geräten (Router, Überwachungs-kameras, TV-Recorder, Industrie-Controller) und schließt sie an Botnets an.
- Die betroffenen Anwender merken lediglich, das ihr Internet-Anschluss langsamer wird und schließlich ausfällt.
- 900.000 Speedport-Router der Telekom werden lahmgelegt.

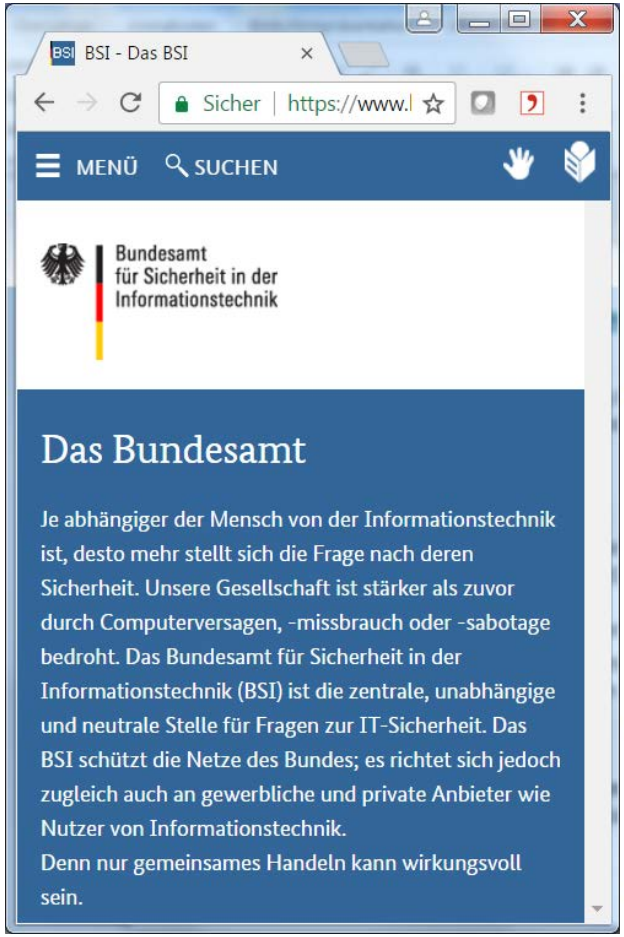


- Hacker bieten Überlastungsangriffe wie Mirai als kostenpflichtige Dienste im Darknet an. Misslingt der Verkauf, wird der Sourcecode online gestellt um Spuren zu verwischen.
- Februar 2017: 29jähriger Verdächtiger, ein britischer Hacker mit dem Codenamen BestBuy, wird in London verhaftet.

IT-Sicherheit in der Industrie

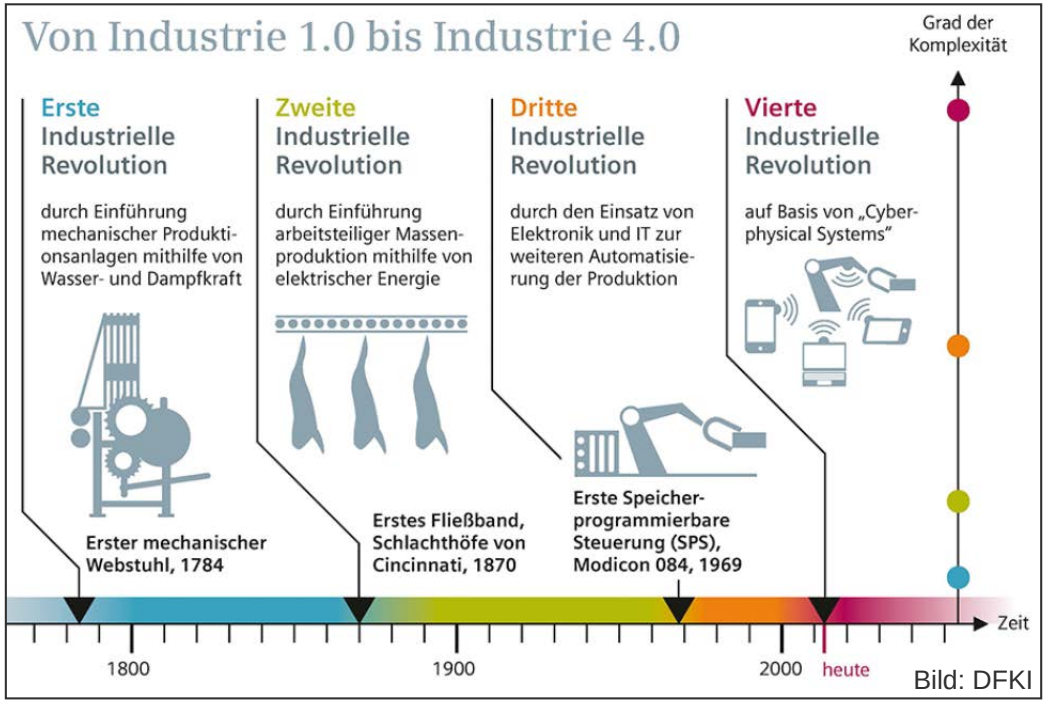
- Für Unternehmen kann eine Bedrohung der IT-Sicherheit teuer, geschäftsschädigend oder sogar existenzgefährdend sein.
- Viele Industrie-Unternehmen betreiben zertifiziertes Sicherheitsmanagement nach geltenden Standards (ISO 27001 oder BSI IT-Grundschutz) und müssen ggf. auch branchenspezifische Standards einhalten.
- Die Standards und Handlungsempfehlungen werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) vorgegeben.

- Viele Unternehmen kämpfen vor dem Hintergrund von Industrie 4.0 trotz Sicherheitsmanagement verstärkt mit Angriffen auf ihre IT-Sicherheit.



Industrie 4.0, die vierte industrielle Revolution

Nach Dampfmaschine, Fließband, Elektronik und IT bestimmen intelligente Fabriken („Smart Factories“) die vierte industrielle Revolution.



Der wesentliche Unterschied von Industrie 4.0 zu Industrie 3.0 ist die Anwendung von **Internettechnologien** zur Kommunikation zwischen Menschen, Maschinen und Produkten.

IT-Sicherheit in der Industrie 4.0-Landschaft

- Die digitale Aufrüstung und Vernetzung durch Industrie 4.0 bringt neue Anforderungen an die IT-Sicherheit, aber auch Fragen des Datenschutzes und der Haftung müssen geklärt werden.

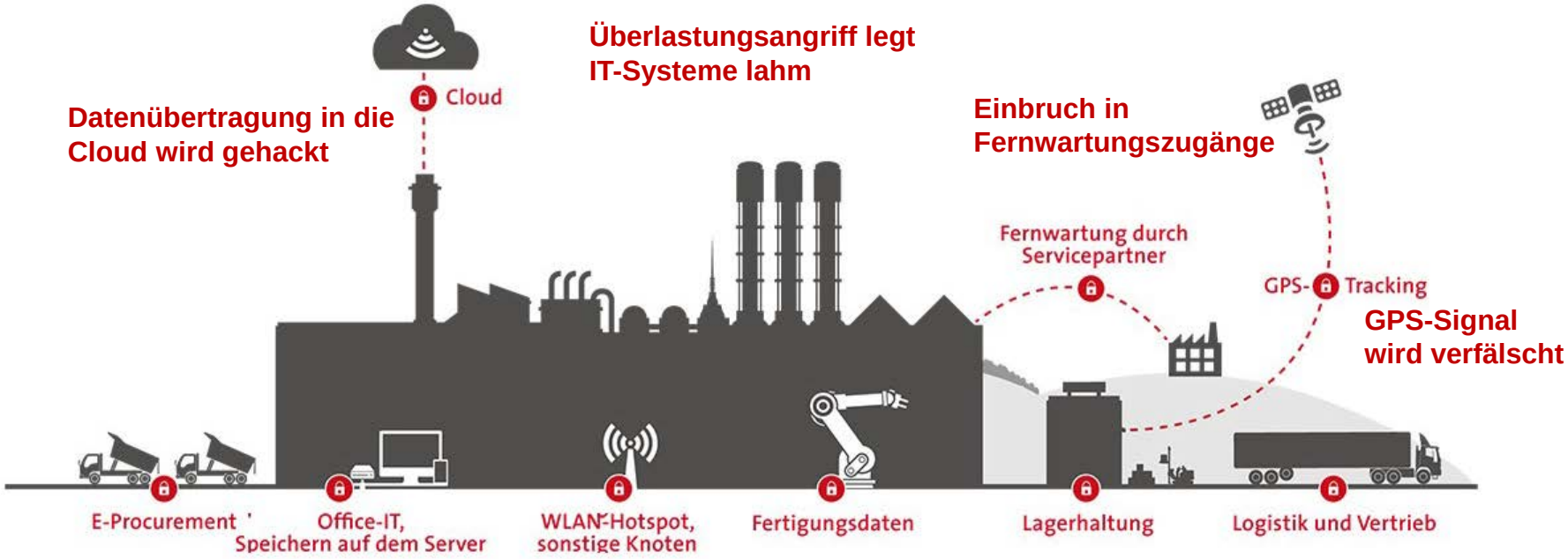


Bild: Consileon

Neue Bedrohungen der IT-Sicherheit

In neuen Industrie 4.0-Produktionsprozessen oder -Anwendungsszenarien entstehen neue Bedrohungen der IT-Sicherheit.

- **Neue Technologien sind nicht ausgereift**
  - Beispiel Smartphones: Virenscanner und Firewalls für Smartphones gab es in den ersten Jahren noch nicht (inzwischen schon).
- **Industrielle Anlagen werden unsicher vernetzt**
  - Einerseits sollen Objekte möglichst vernetzt werden, andererseits gibt es hochsichere Anlagen (z.B. Steuerungsanlage eines Windparks), die nur über sichere Verbindungen vernetzt werden dürfen.
- **Rechtliche Aspekte, Datenschutz**
  - Wenn große Datenmengen gespeichert werden, müssen die rechtlichen Grundlagen (wem gehören die Daten?) vorab geklärt werden.

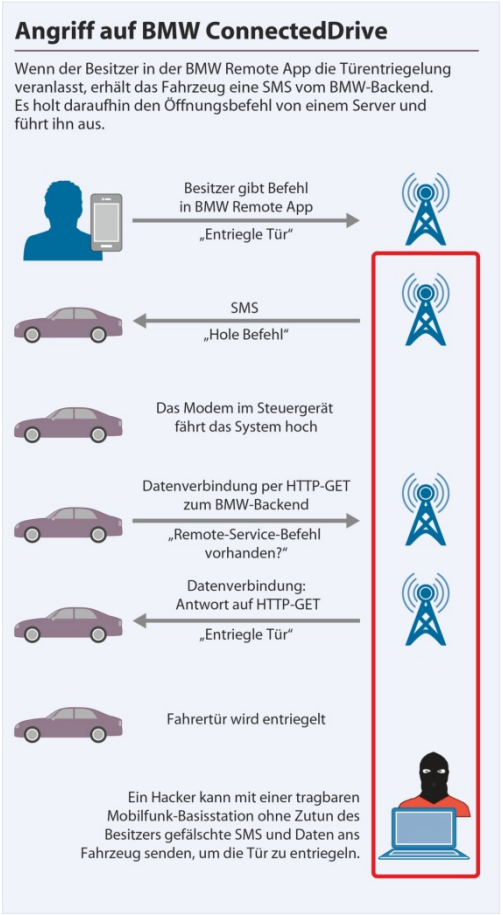


Bild: c't

Neue Fragen zum Datenschutz

Datenschutz gilt nur für personenbezogene Daten im Sinne von § 3 des Bundesdatenschutzgesetzes (BDSG). Datenschutzrecht folgt dem Prinzip des Verbots mit Erlaubnisvorbehalt: alles ist verboten, was nicht explizit erlaubt ist.
Wie legt man fest, was personenbezogene Daten sind?

- Beispiel Connected Car: Auto erfasst Straßen- und Wetterverhältnisse und sendet die Daten an Hersteller. Unterliegt das dem Datenschutzgesetz?

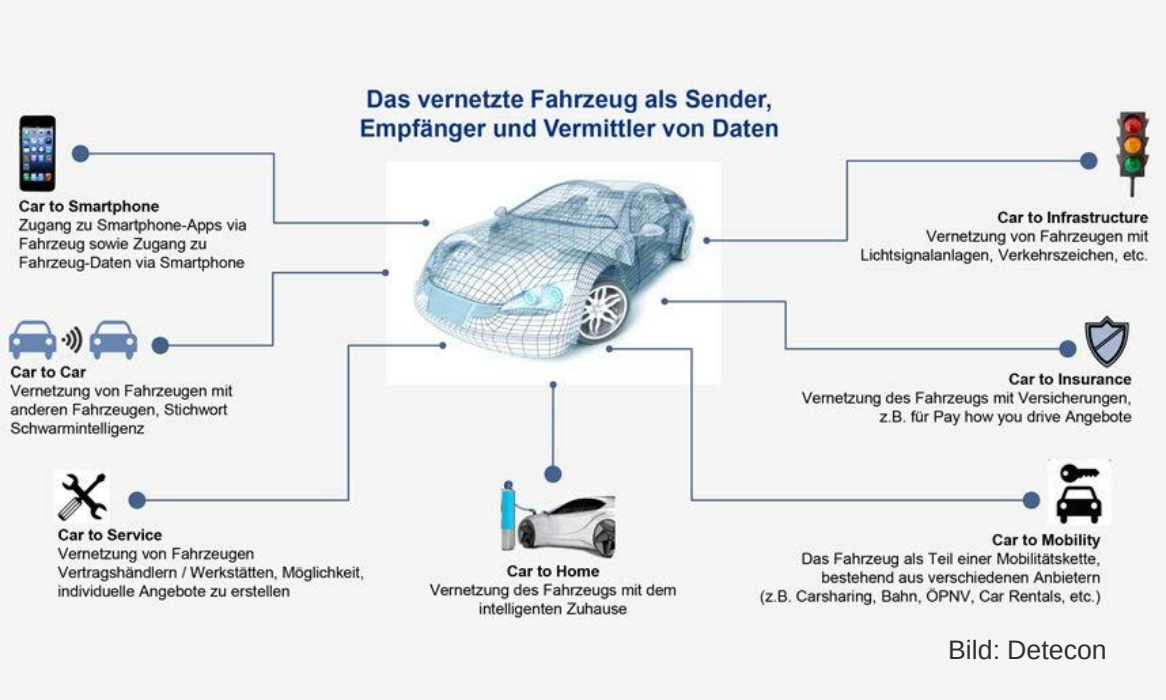


Bild: Detecon

Neue Fragen zur Haftung

Im deutschen Recht gilt der Grundsatz, dass nur natürliche Personen im rechtlichen Sinn verantwortlich sein können.

Industrie 4.0 und Digitalisierung bringen es mit sich, dass Maschinen miteinander kommunizieren und Prozesse automatisiert ablaufen.

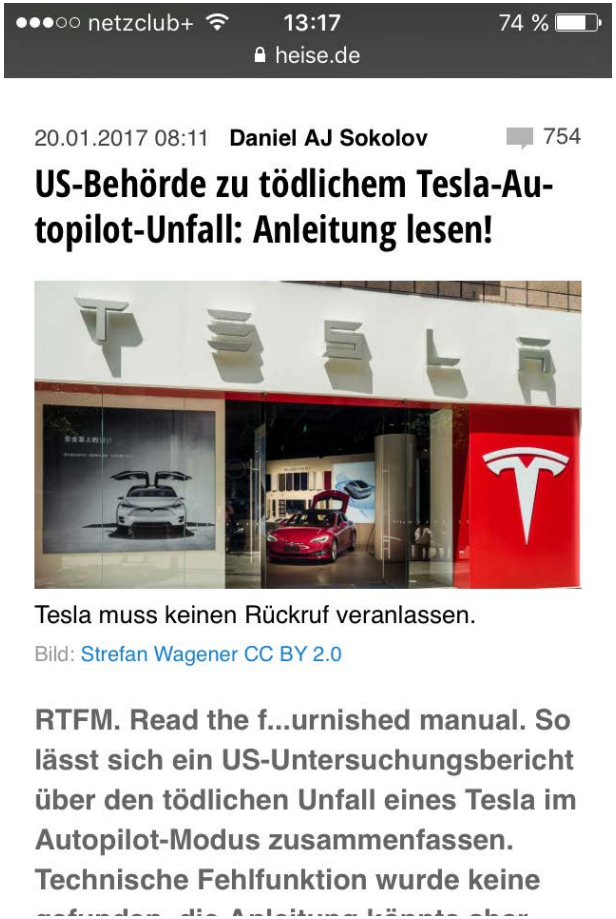
Wie findet man heraus, welche Person oder Firma im Schadensfall haftet?

Wenn etwas schief läuft, sind natürliche Personen als Auslöser einer Handlung schwer zu identifizieren, bzw. es ist schwieriger festzustellen, welche Komponente der Kette einen Fehler verursacht hat.

Beispiel: Tesla Autopilot-Unfall, haftet Fahrer oder Autohersteller?

Neue Fragen zur Haftung

- Denkbare Schadensfälle:
  - Verbindungsunterbrechungen in der Kommunikation zwischen Maschinen
  - Fehlerhafte Steuerung im Smart Home führt zu Brandschäden
  - Mangelnde Medikamentenverfügbarkeit durch fehlerhaft erhobene Daten
  - Verkehrsunfälle durch Autopilot-Modus
- Wer haftet?
  - Hersteller und Betreiber von IT-Systemen und Anwendungen?
  - Bei mehreren Teilnehmern muss die vertragliche Haftung vorab festgelegt werden.



Antworten? Maßnahmen?

- Das Gewährleisten der IT-Sicherheit erfordert, dass Sicherheitsmaßnahmen laufend auf den aktuellen Stand der Technik gebracht und dabei alle möglichen Querverbindungen berücksichtigt werden müssen.
  - Virenscanner und Spamfilter sollten laufend aktualisiert werden.
  - Firewalls müssen richtig konfiguriert werden.
  - Verschlüsselungsverfahren müssen laufend auf den neuesten Stand gebracht werden.
  - Software muss "By Design" sicher entwickelt werden.

  . . .
- Problem: IT-Sicherheit wird in vielen Unternehmen noch von IT-Administratoren nebenher mit betreut. Es fehlt an Expertise.
- Um ein Sicherheitsmanagement entsprechend der neuen Sicherheits-anforderungen umsetzen zu können, benötigt man IT-Sicherheitsexperten, die sich im Rahmen eines Studiums oder auch durch Zertifizierungen qualifiziert haben und laufend weiter qualifizieren.

IT-Sicherheit@aing.hs-kl.de

- IT-Sicherheit wird im Fachbereich Angewandte Ingenieurwissenschaften als Wahlpflichtfach angeboten und wird auch in den regulären Vorlesungen (Kommunikationsnetze . . .) berücksichtigt.
- Themen:
  - Grundlegende Begriffe der IT-Sicherheit
  - Internet-Sicherheit, Aufbau des Internets, Internet-Protokollfamilie, Bedrohungen und Maßnahmen
  - Sicherheitsmanagement, Sicherheitsprozess nach BSI-IT-Grundschutz
  - Einführung in Basistechnologien (Kryptografische Grundlagen, Public-Key-Infrastrukturen, Authentifizierung)
  - Anwendungssicherheit (E-Mail, Soziale Netze, Mobile Anwendungen)
  - Industrie 4.0-Sicherheit (Sicherheit im Engineering-Bereich, was ist Industrie 4.0, was sind die neuen Sicherheitsprobleme)

Weitere Informationen

Weitere Informationen zum Studium der Elektrotechnik an der Hochschule Kaiserslautern finden Sie auf der Website des Fachbereiches Angewandte Ingenieurwissenschaften.

Fragen zu Studium und Vorpraktikum:

Dekanat Angewandte Ingenieurwissenschaften
Tel: 0631 - 3724 - 2201 / - 2301
E-Mail: dekanat-aing@hs-kl.de
Web: http://www.aing.hs-kl.de/

Studiengangsleitung Elektrotechnik:
Prof. Dr. rer. nat. Eva Maria Kiss

Hochschule Kaiserslautern
University of Applied Sciences

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!