Jahresthema 2018 „Gestern gehörten meine Daten mir - gehören sie morgen meinen Feinden? Eine längst fällige gesellschaftliche Diskussion“

Fünfter Vortrag des Jahres 2018 am 10. September 2018 in der Hanns-Seidel-Stiftung

PROF. DR. GABI DREO RODOSEK, UNIVERSITÄT DER BUNDESWEHR MÜNCHEN, LEITENDE DIREKTORIN CODE (CYBERDEFENCE)

VOM APOKALYPTISCHEN SUPER-GAU ZUM SICHEREN UNTERNEHMENSALLTAG

Vorbemerkung:

IT – wir leben in einer digitalen Gesellschaft, das ist unsere Zukunft; wie schnell können wir derartige Produkte entwickeln – die USA haben Google, die Volksrepublik China hat Alibaba und Alphabet und Europa?

Google hat machine learning: wer nach etwas sucht, das lernt auch Google kennen + weiß woran er arbeitet.

Unser Leben im Cyberraum

- 2020 wird es 50 Mrd. vernetzte Geräte geben: diese Geräte tauschen sich untereinander aus;
  das Smarthome schaltet sich selbst aus, fährt selbst herunter und erkennt die „Besitzer“.
- Bis 2025 wird es 163 Zettabyte Daten geben (heute sind es acht)
- D. H. **Daten sind das Öl der Zukunft**

Silicon Valley produziert Hardware,

Asien produziert Software,

Europa kauft.

- Europa braucht eigene Infrastruktur dieser Art!
- Was passiert in einer Minute im Netz/weltweit?
  exponentielle Zunahme der Daten!

Algorithmen brauchen das: die Systeme werden „smarter“ und autonomer; KI (künstliche Intelligenz) für Autos; Alexa oder Siri (Sprachassistenten) – hören immer mit

- -> kein Schutz der Privatsphäre durch diese „coolen Sachen“

- Alles miteinander vernetzt: man kann gut leben von gestohlenen Passwörtern – siehe die Angriffe auf Amazon, New York Times, GitHub, Twitter (über Subprovider wie Dyn)
- Finanzsektor ist attraktiv für Kriminelle:
  ebenso Energieversorgung, Automobilindustrie, Gesundheitswesen, Produktionssteuerung, militärische (vernetzte) Operationen
- d.h.: IT ist die Schlüsseltechnologie der vernetzten Gesellschaft und die **digitale Souveränität haben wir nicht!**

Unsere ethischen Werte stehen auf dem Spiel <-> ca. 100 Leute (Europäer), die wirklich wichtig sind, sind in den USA tätig für die führenden Firmen in Forschung und Entwicklung.

- 2010 „Stuxnet“ – ist nach Internetzeit ewig her, weil ein Internetjahr drei Monate dauert – es ging nicht ums Internet, sondern die dortigen Schwachstellen (200.000 Euro im Darknet) wurden ausgenutzt;
- 2012 Spionage-Software „Flamer“ und „Miniflamer“;
- Bankraub durch „High-Roller“ - Angriff 2012: von großen Geschäftskonten wurde wenig abgehoben;
- „Wannacry“, „Petya“, „Notpetya“: zerstören Hardware, verschlüsseln Daten – zeigt die Wichtigkeit von Backups/Sicherungen, auch für Private!
- Qualität und Quantität steigern sich nicht mehr im Internet (Internet of Things, IoT), stattdessen: „Ambient Internet“ übernimmt die Führung – wir werden die IT nicht mehr sehen, Sensorik im Raum steuert die Umgebung des Menschen, Objekte werden immer „intelligenter“.

Die deutsche Entwicklung „Olli“ erkennt unsere Emotionen (von sechs Personen, mehr als „Alexa“ oder „Siri“) und lernt gleichzeitig -> es tut sich sehr viel im Bereich Lernen + IT.

Mobiles Eco-System: das Handy integriert viele Dienste wie Social Media, Ticketkauf, Carsharing und auch Zahlung.

Daten

Die „Battle For Data“ – from Big Data to Smart Data – hat Europa verloren, aber den Kampf um die Algorithmen noch nicht, hier herrscht Goldgräberstimmung:

- Descriptive Analytics: was ist passiert;
- Analytics: sind die Algorithmen, z. B: IBM Watson oder SAP Hanna.

China will die Nr. 1 in Künstlicher Intelligenz (KI) werden, es werden Milliarden investiert.

Korrelationen und komplexe Zusammenhänge ergeben den Menschen oder KI, während der Rechner eine einfache Sache ist.

KI sind Algorithmen; heute entwickeln Algorithmen Algorithmen – wie stelle ich sicher, dass meine KI etwas Gutes lernt? (Ethik und Algorithmen, siehe dazu Telekom)

Digitale Identitäten

Die Benutzung von Username + Passwort ist Standard der 60er/70er Jahre, aus Sicherheitsgründen nie von Google oder Facebook dorthin übergehen – das ultimative für Passwörter ist der „Passwordmanager" (nur mehr ein (komplexes) Passwort statt vieler).

Wir haben mehrere (digitale) Identitäten – in der Arbeit, im Sport, durch Auto und Smartphone … alles ist vernetzt mit mir. Das Smartphone beispielsweise lernt, wo ich zuhause bin.

Eine einzelne Information ist uninteressant, aber die gesamte Profilbildung durch viele, umfangreiche Daten ist interessant.

Wir sind weiter durch die **Blockchain-Technologie**:
Bitcoin basiert darauf, es gibt nichts Neutrales mehr, sondern die Transaktion wird dem gesamten Netz mitgeteilt – jeder weiß alles und es gibt keine zentralen Komponenten im System mehr.

Quantencomputing: stammt aus der Quantenphysik (Qubits),
kann gleichzeitig in unterschiedlichen Zuständen sein, heutige Rechner sind dazu noch zu langsam. Problem: die asymmetrische Verschlüsselung wird dann leicht zu knacken sein, die Verschlüsselung muss Quantenresistent werden.

Daher ist die Uni BW Teil von IBM GitHub (50 Qubits), um zu verstehen was, welche Technologie dahinter steckt.

Angriffe entwickeln sich ebenso: sie werden immer mehr „smart attacks" – eigentlich haben wir verloren: denn der Angreifer braucht nur eine Schwachstelle finden, während der Verteidiger alles verteidigen muss. Beispiel dafür ist ein Tresor: der bleibt an einem Ort, sobald er gefunden ist, ist er zu knacken. Daher müssen wir es anders machen: **Moving Target**

Defence – der Angreifer weiß nicht, wo das Ziel zu finden ist, sondern wir verschieben unsere Daten, was den Angriff immens erschwert für potentielle Angreifer – er muss suchen und wir sind im Vorteil.

=> **Cyber Resilience**: der Wettlauf hat gerade begonnen; wir müssen immer die (Cyber-) Architektur so bauen, dass bei einem Ausfall nicht alles an Daten weg ist oder alles zusammenbricht.

EVA DITTRICH, ASS. JUR.

Zum Weiterlesen:

- Wie funktioniert ein Quantencomputer? (Nora Kusche, Welt der Physik, 26.02.2016), zu finden unter https://www.weltderphysik.de/gebiet/technik/quanten-technik/einfuehrung-quantencomputer/, eingesehen am 11.09.2018;
- Der Hype um die Quantencomputer (Ralf Krauter im Gespräch mit Manfred Kloiber, Deutschlandfunk, 07.07.2018), zu finden unter https://www.deutschlandfunk.de/rechnen-mit-qubits-der-hype-um-die-quantencomputer/, eingesehen am 14.09.2018;
- Forschungsprojekt „Cyberdefence“ (Christian Wurzer, ARD alpha, 28.04.2018), zu finden unter https://www.br.de/fernsehen/ard-alpha/sendungen/alpha-campus/magazin/campus-magazin/, eingesehen am 14.09.2018;
- Einsteins unverhofftes Erbe: Quanteninformationstechnologie, Broschüre des Bundesministeriums für Bildung und Forschung (Dr. Mathias Schulenburg, Bonn/Berlin 2005), zu finden unter www.xplora.org/downloads/Knoppix/BMBF/EInsteins-unverhofftes-Erbe.pdf, eingesehen am 14.09.2018.