IT-Sicherheit (und Datenschutz) im Internet der Dinge

Dr. Sebastian Pape, Institute of Business Informatics, Goethe-Universität Frankfurt

Frank Wagner, Senior Experte Datenschutz, Deutsche Telekom, Darmstadt

Dr. Sebastian Pape, Aktuelles

Sichere Informationsinfrastrukturen für kleine und mittlere Energieversorger

Julian Dax[1], Daniel Hamburg[3], Michael Kreusch[5], Benedikt Ley[1], Sebastian Pape[2], Volkmar Pipek[1], Kai Rannenberg[2], Christopher Schmitz[2] und Frank Terhaag[4]

1.) Universität Siegen, 2.) Goethe Universität Frankfurt a.M., 3.) TÜV Rheinland i-sec GmbH, 4.) regio iT GmbH, 5.) Arbeitsgemeinschaft für sparsame Energie- und Wasserverwendung (ASEW)

Motivation

Kritische Infrastrukturen spielen eine wichtige Rolle für das Funktionieren heutiger Informationsgesellschaften. Der **Schutz dieser Infrastrukturen** liegt dementsprechend im Interesse der Allgemeinheit. Durch den zunehmenden und sich verändernden Einsatz von Informations- und Kommunikationstechnik (IKT) im Energiesektor zur Steigerung von Effektivität und Effizienz aber auch zur Realisierung einer nachhaltigen und sicheren Energieversorgung im Rahmen der Energiewende, ist die **Abwehr IKT-basierter Angriffe** auf die kritische Infrastruktur eine ständig wachsende Herausforderung. Die meist privatwirtschaftlichen Betreiber im Energiesektor stehen dabei vor der Aufgabe, sowohl den **Schutz als auch die Wirtschaftlichkeit** ihrer Infrastrukturen sicherzustellen. Das Ziel des Forschungsprojekts ist es, hier praxisnahe Lösungsansätze aufzuzeigen.

Innovation

Im Forschungsprojekt SIDATE werden Werkzeuge und Konzepte entwickelt, die eine bessere **Einschätzung des vorhandenen Sicherheitsniveaus** ermöglichen und dabei helfen, die Sicherheit der Infrastrukturen kleiner und mittlerer Betreiberfirmen selbst zu verbessern. Dabei liegt ein besonderes Augenmerk auf der **Praxistauglichkeit** der Werkzeuge und Konzepte, die unabhängig von wirtschaftlichen, organisatorischen und personellen Besonderheiten anwendbar sein sollen.

Neu an diesem Ansatz ist, neben der **Fokussierung auf kleine und mittlere Unternehmen**, dass **Selbsteinschätzung** eine entscheidende Rolle spielt. Mit dem Werkzeugkasten sollen Betreiber schnell und zuverlässig feststellen können, ob alle gesetzlichen Auflagen und Richtlinien zur Absicherung der kritischen Versorgungsinfrastrukturen erfüllt sind und ob die **Umsetzung möglicher Sicherheitsmaßnahmen effektiv und wirtschaftlich** erfolgt.

Ziele

Das Projekt setzt sich zum Ziel, kleine und mittlere Energieversorger bei der Einschätzung und Verbesserung des vorhandenen Sicherheitsniveaus angemessen zu unterstützen. Angestrebt sind unter anderem die **Entwicklung von Metriken** zur Erfassung des Sicherheitsniveaus, sowie einer **Wissensdatenbank und Kooperationsplattform** zur Unterstützung organisationsinterner sowie überorganisationaler Kollaborations- und Austauschprozesse. Um eine möglichst große Anwenderfreundlichkeit zu erreichen, werden dabei **kleine und mittlere Betreiber in den Prozess mit eingebunden.**

Verbundkoordinator:
Prof. Dr. Volkmar Pipek
Computerunterstützte Gruppenarbeit und Soziale Medien
Fakultät III, Universität Siegen
Tel: +49 271 740 4068 • info@sidate.org • www.sidate.org

Verbundpartner:

UNIVERSITÄT SIEGEN · GOETHE UNIVERSITÄT FRANKFURT AM MAIN · TÜVRheinland® Genau. Richtig. · regio iT · ASEW

gefördert vom Bundesministerium für Bildung und Forschung

Industrie 4.0

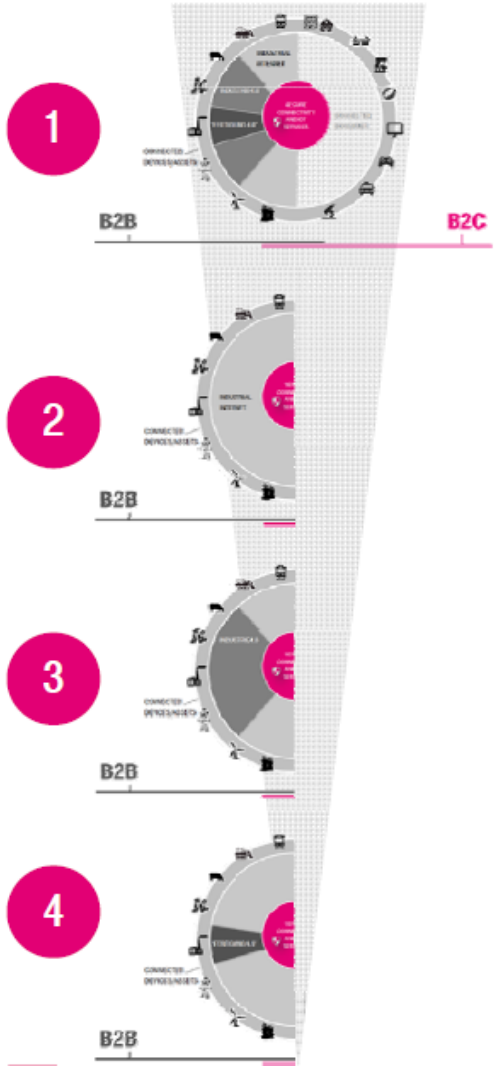
Industrie 4.0 — Vernetzung Cyber Physischer Systeme

Industrie 3.0 — Einsatz von Elektronik und IT

Industrie 2.0 — Arbeitsteilige Massenproduktion (Fließbänder)

Industrie 1.0 — Mechanische Produktionsanlagen (Dampf- u. Wasserkraft)

IOT Taxonomie



INTERNET OF THINGS & SERVICES

- Digitalization and virtualization of business processes (B2B) and customer experience (B2C) by connected devices/assets (e.g. sensor equipped machinery, robots, wearable)
- IoT & Services enabled by NG connectivity (secure QoS differentiated/software compatible con.), platforms and data analytics (large amounts & real-time) – provided x-industry i.e. B2B and B2C
- Concrete use cases turn IoT into IoServices. Services characterized by increasing convergence of industries (e.g. automotive & energy) and domains (B2B & B2C)

INDUSTRIAL INTERNET/ INDUSTRIAL INTERNET OF THINGS

- International definition w/ focus on whole B2B side of IoT&S – broad scope incl. all relevant industries (e.g. manufacturing, utilities) and service sectors (e.g. public sector, health, transportation)
- IIoT: integration of complex physical machinery with networked sensors and software
- Definition shaped by IIC Industrial Internet Consortium – initiated by GE)
- Key ingredients: **NG connectivity (secure QoS differentiated/software compatible con.), platforms and data analytics (large amounts & real-time) – x-industry i.e. B2B and B2C not in focus**

INDUSTRIE 4.0

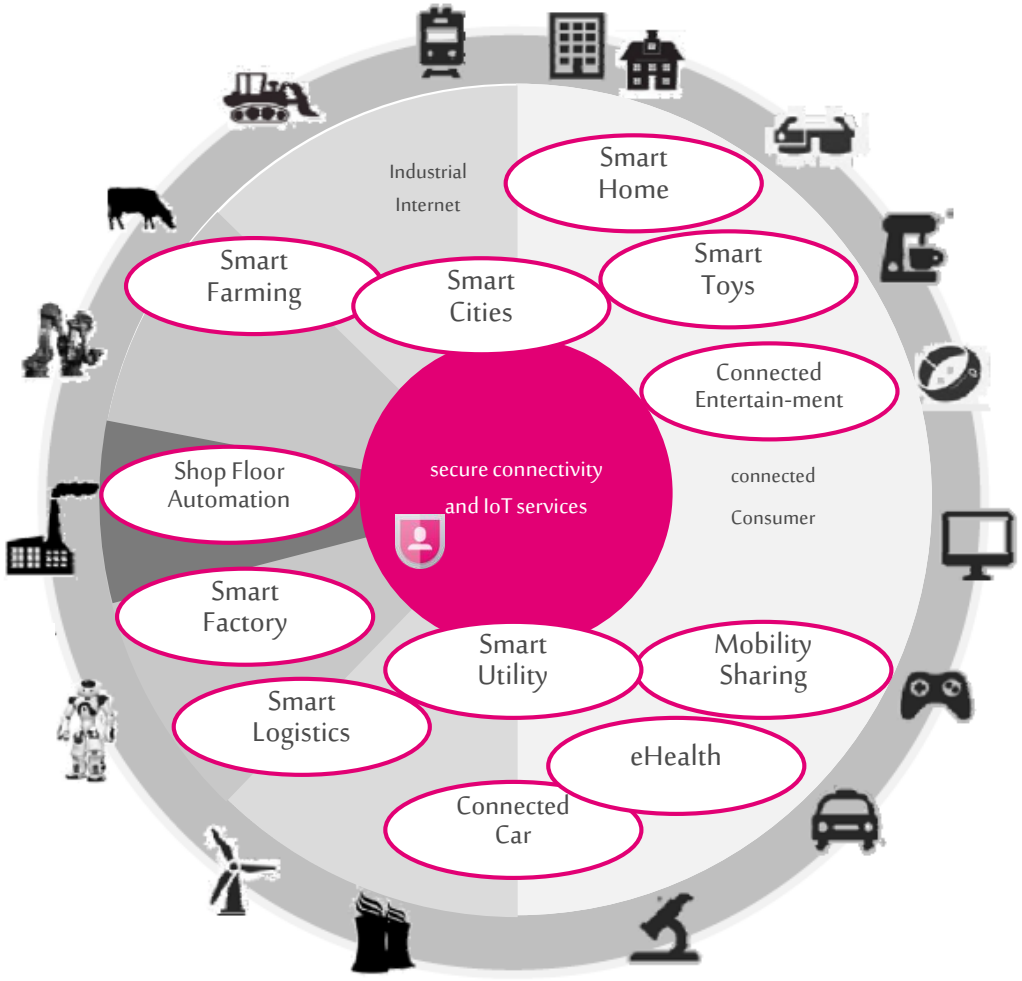
- German definition for digitalization and **NG connectivity (secure QoS differentiated/software compatible con.)**, of industrial production incl. product development and services processes
- 4th wave of industrial revolution in classical manufacturing industry and logistics
- Key ingredients same as for Industrial Internet

FERTIGUNG 4.0

- Part of Industry 4.0 but with focus on 'Smart Factory' only (= use case level)
- Intelligent, **NG connectivity (secure QoS differentiated/software compatible con.),** allows for agile, personalized production and efficiency gains

IOT Framework

B2B



B2C

IOT Framework

IOT LAYERS

End to End Security

Customer Applications


B2B LE


B2B SME

...


B2C

Vertical Solutions


Automotive


Smart Factory

...


Smart Home

Horizontal Services


Cloud


Int. Platform


Data Analytics

Horizontal Connectivity


Access


OSS


BSS

Devices


Sensors


Robots

...


Machines

CHARACTERISTICS

Customer-specific applications
- Tailoring to individual customer needs

Industry-specific solutions
- Native vertical solutions tailored for an industry (e.g. HMI)
- Integration with 3rd Party apps and data via open APIs

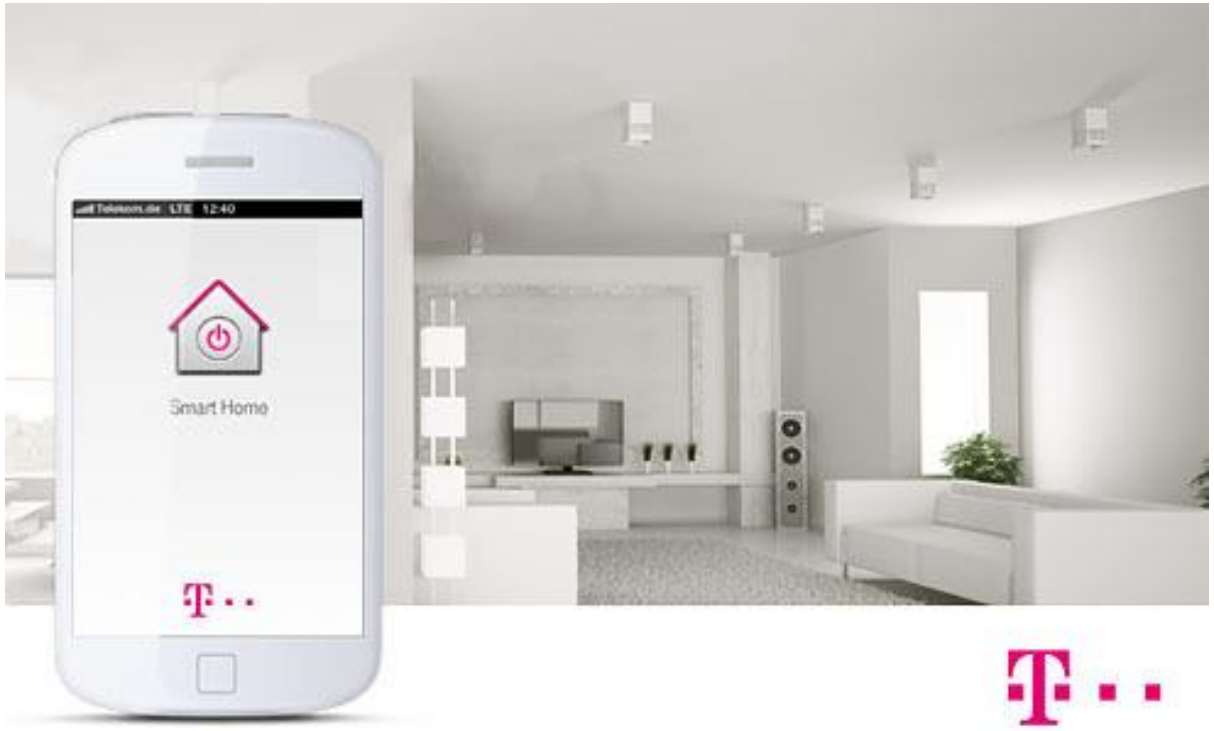
Real-time service enabling
- **Data Analytics:** Big Data engine and intelligence
- **Integration Platform**: Horizontal services (e.g. Device mgmt)
- **Cloud:** Global and local infrastructure

Secure managed access
- **BSS:** Customer and contract management
- **OSS:** Real time connectivity management
- **Access:** Secure and reliable connectivity

"Connected Things"
- Intelligent devices, sensors communication modules
- Device gateways to exchange information

Datenschutz in Smart-Home Umgebungen

- Smart Home Devices
  - Ein Morgen im Smart Home
  - Weitere Geräte
- IT-Sicherheit
- Datenschutz
  - Probleme
  - Gegenmaßnahmen
- Verlässlichkeit von Daten



7:40 Uhr – Kaffee kochen

Informationen:

- Tagesrhythmus
- Kaffeekonsum

[Quelle: Philipps / Saeco]

Datenschutzbestimmungen I

Was bringt die Zweckerfüllung mit sich?

Wenn Sie die App verwenden, zeichnen wir die **Art der Verwendung** Ihrer Saeco GranBaristo Avanti auf, um Ihnen hilfreiche Tipps, Tricks und Wartungsinformationen für Ihre Maschine bieten zu können. Wir erfassen diese Daten **zu Marktforschungszwecken** und/oder, um Ihnen hilfreiche Tipps zur Verbesserung der Leistung sowie zur Wartung Ihres Saeco Kaffeevollautomaten zu bieten.

Welche persönlichen Daten werden zu diesem Zweck verarbeitet?

Wenn Sie die App verwenden, erfasst Philips Daten zu Ihrer Verwendung der Saeco Avanti sowie **historische Daten zum Kaffeeverbrauch**. Außerdem ermittelt Philips, auf welche Art die App genutzt wird.

Die App funktioniert nicht ohne die Erfassung dieser Daten. Wenn Sie diese Daten nicht weitergeben möchten, können Sie die App nicht verwenden.

[Quelle: Philipps / Saeco]

Datenschutzbestimmungen II

Greifen wir für den genannten Zweck auf andere Parteien zurück?

Beim Speichern der Daten sowie bei der Erfassung und Analyse statistischer Daten greifen wir auf einen **Drittanbieter** zurück.

[...]

Welche **persönlichen Daten** werden zu diesem Zweck verarbeitet?

Wir können bestimmte Registrierungsinformationen nutzen, z. B. Benutzername, Vorname, Nachname, E-Mail-Adresse, Land, Sprache, Passwort, Anrede, Alter.

Greifen wir für den genannten Zweck auf andere Parteien zurück?

Philips greift auf einen **Drittanbieter** für die Erfassung und Einbehaltung unserer Registrierungsaufzeichnungen, einschließlich der von Ihnen bereitgestellten persönlichen Daten, zurück.

[Quelle: Philipps / Saeco]

Datenschutzbestimmungen III

Was bringt die Zweckerfüllung mit sich?

Wir erfassen und sammeln diese persönlichen Daten und **entfernen die individuelle Kennzeichnung**, um Nutzungsstatistiken zu erstellen, anhand derer wir Inhalt, Funktionen und Benutzerfreundlichkeit der App verbessern können.

Welche persönlichen Daten werden zu diesem Zweck verarbeitet?

Zu diesem Zweck verarbeiten wir Ihre **eindeutige Benutzergerätenummer**, die **IP-Adresse** Ihres Geräts, den **Typ des Internetbrowsers** für Mobilgeräte oder das **verwendete Betriebssystem** sowie **Zeiten und Daten**, zu denen die App verwendet wurde. Zudem erfassen wir **Sitzungs- und Nutzungsdaten**, also Informationen zu Ihrer Verwendung der App, z. B. Informationen zu Verbindungsanforderung, Serverkommunikation und **Datenweitergabe**, **Netzwerk-Statistiken**, Servicequalität sowie **Datum und Zeit** des Zugriffs.

[Quelle: Philipps / Saeco]

Datenschutzbestimmungen IV

So leiten wir Ihre Informationen an Dritte weiter

Wenn Philips einem Drittanbieter die Übertragung Ihrer persönlichen Daten **außerhalb Ihrer geografischen Region** erlaubt, werden Schritte zum Schutz Ihrer Privatsphäre durch die Nutzung von vertraglichen Vereinbarungen oder anderen Mittel, die einen vergleichbaren Schutz während der Informationsverarbeitung durch vertrauenswürdige Drittanbieter bieten, eingeleitet.

[...]

Mitunter werden Geschäftsbereiche oder Teile eines Geschäftsbereichs von Philips an andere Unternehmen verkauft. Im Rahmen des zugehörigen Eigentumsübergangs können **die persönlichen Daten**, die in direkter Verbindung zu diesem Geschäftsbereich stehen, **an das erwerbende Unternehmen übergeben werden**.

[Quelle: Philipps / Saeco]

Datenschutzbestimmungen V

Ihre persönlichen Daten können aus dem Land, in dem Sie sich befinden, an andere Unternehmen von Philips an **anderen Orten weltweit** weitergeleitet werden. Diese Länder verfügen möglicherweise nicht über ähnliche Datenschutzbestimmungen. Für den Fall, dass Ihre Daten außerhalb Ihres Landes oder Gerichtsstandes übertragen werden, werden diese möglicherweise **gemäß den Gesetzen in diesen Ländern** gehandhabt. Falls gemäß lokalem Gesetz erforderlich, werden wir Sie vorab um Ihre Zustimmung zur Weitergabe Ihrer persönlichen Daten außerhalb Ihrer geografischen Region bitten.
[...]

Sie sind jederzeit berechtigt, auf Ihre persönlichen Daten zuzugreifen oder eine Korrektur derselben zu verlangen und **gegen die Verarbeitung Ihrer persönlichen Daten Einspruch einzulegen**. Senden Sie uns hierzu eine E-Mail an privacy@philips.com, oder besuchen Sie unsere Kontaktseite.

[Quelle: Philipps / Saeco]

Datenschutzbestimmungen VI

Änderungen an diesen Datenschutzbestimmungen

Die von Philips bereitgestellten Services entwickeln sich stetig weiter, und die Art und Form dieser Services kann sich gelegentlich ändern, **ohne** dass Sie davon **im Voraus in Kenntnis** gesetzt werden müssen. Aus diesem Grund behalten wir uns das Recht vor, **regelmäßig Änderungen an dieser Datenschutzrichtlinie** vorzunehmen. Wir empfehlen, diese Website regelmäßig zu besuchen, um die aktuellste Version anzusehen.

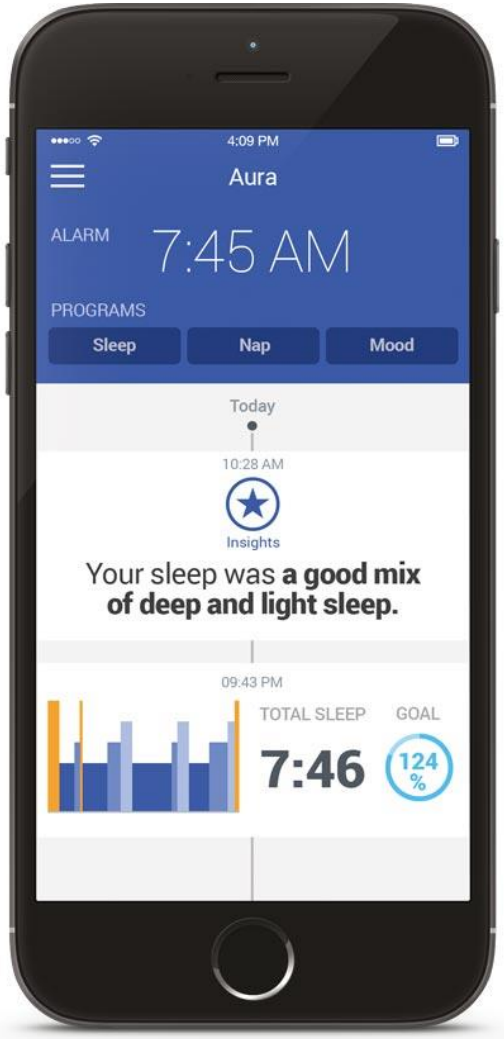
Neue Datenschutzbestimmungen sind mit ihrer Veröffentlichung wirksam. Wenn Sie geänderten Datenschutzbestimmungen nicht zustimmen, sollten Sie Ihre persönlichen Einstellungen ändern oder in Betracht ziehen, die App nicht mehr zu verwenden. Wenn Sie **nach solchen Änderungen** weiterhin auf unsere Dienste zugreifen oder sie nutzen, stellt dies eine **Annahme der geänderten Datenschutzbestimmungen** dar.

[Quelle: Philipps / Saeco]

7:45 – Aufstehen

Informationen:

- Schlafrhythmus
- Schlafgewohnheiten



[Quelle: Withings]

7:50 – Rasieren (Rasierschaum leer)

Informationen:

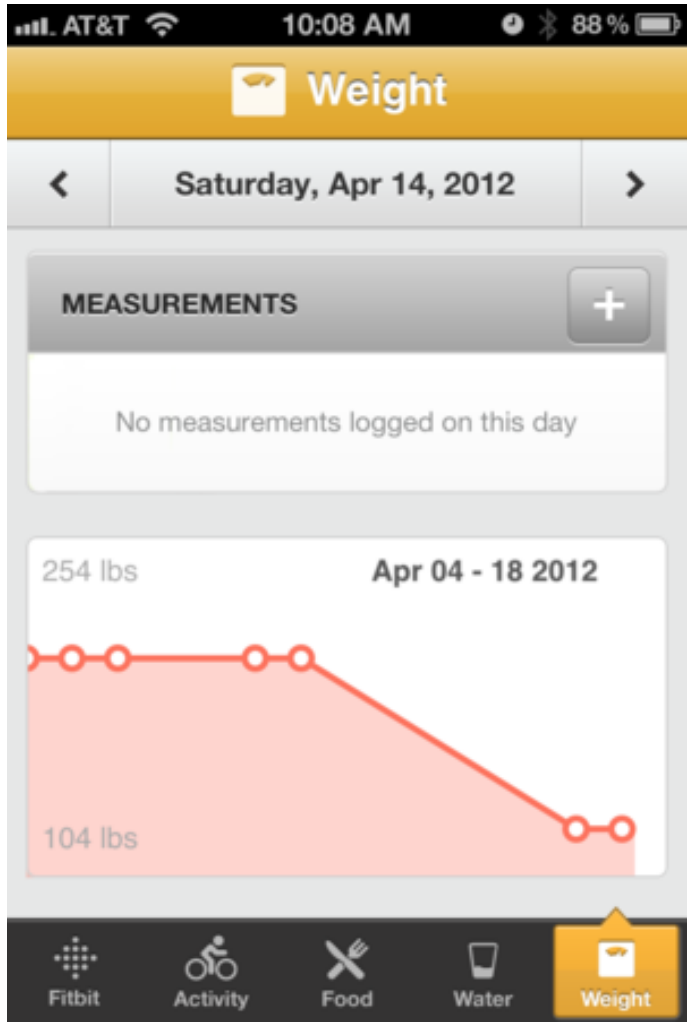
- Tagesablauf
- Bevorzugte Produkte

[Quelle: Amazon]

7:52 – Wiegen

Informationen:

- Tagesrhythmus
- Gewicht



[Quelle: Fitbit]

7:55 – Zähne putzen

Informationen:

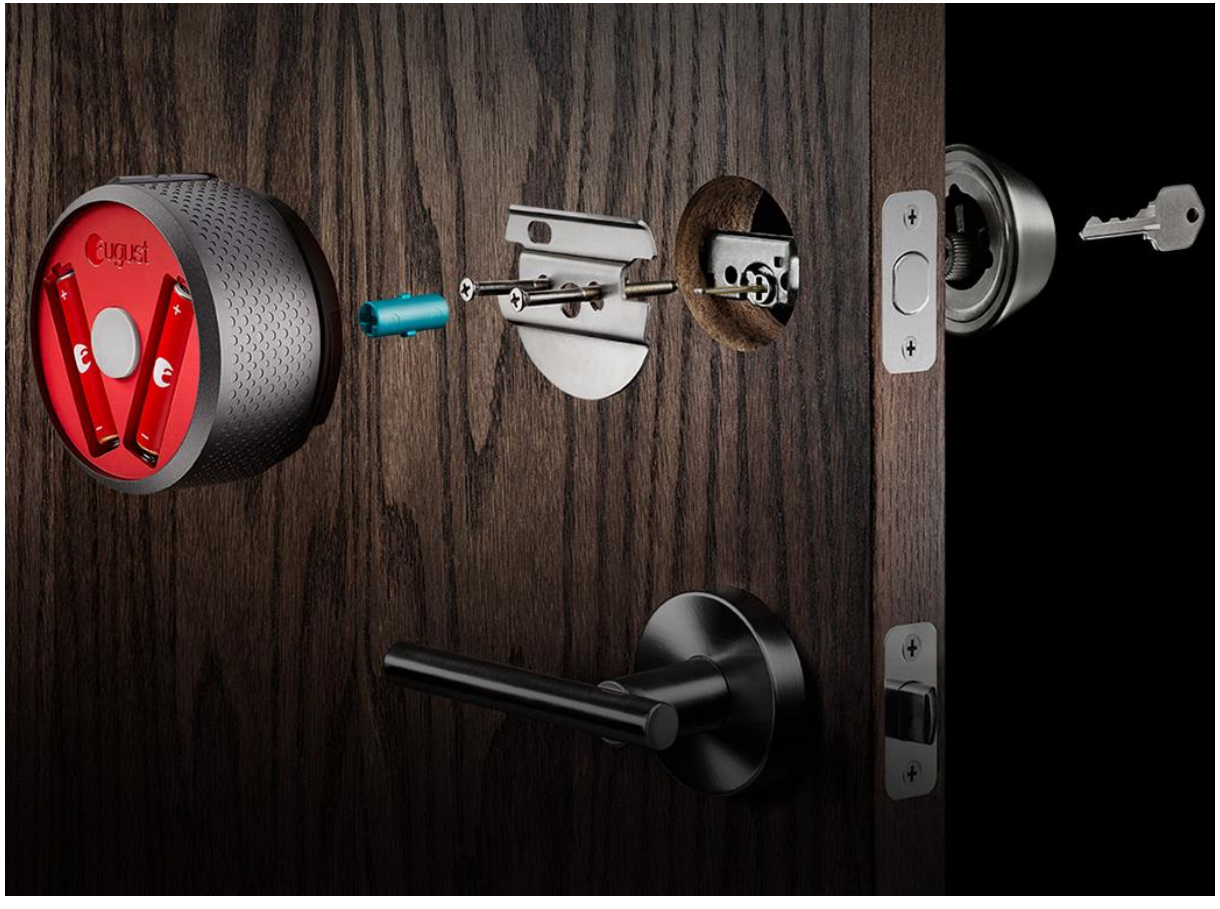
- Tagesrhythmus
- Zahnhygiene

[Quelle: Oral-B]

8:30 Abschliessen

Informationen:

- Tagesrhythmus
- Personen
  im Haushalt

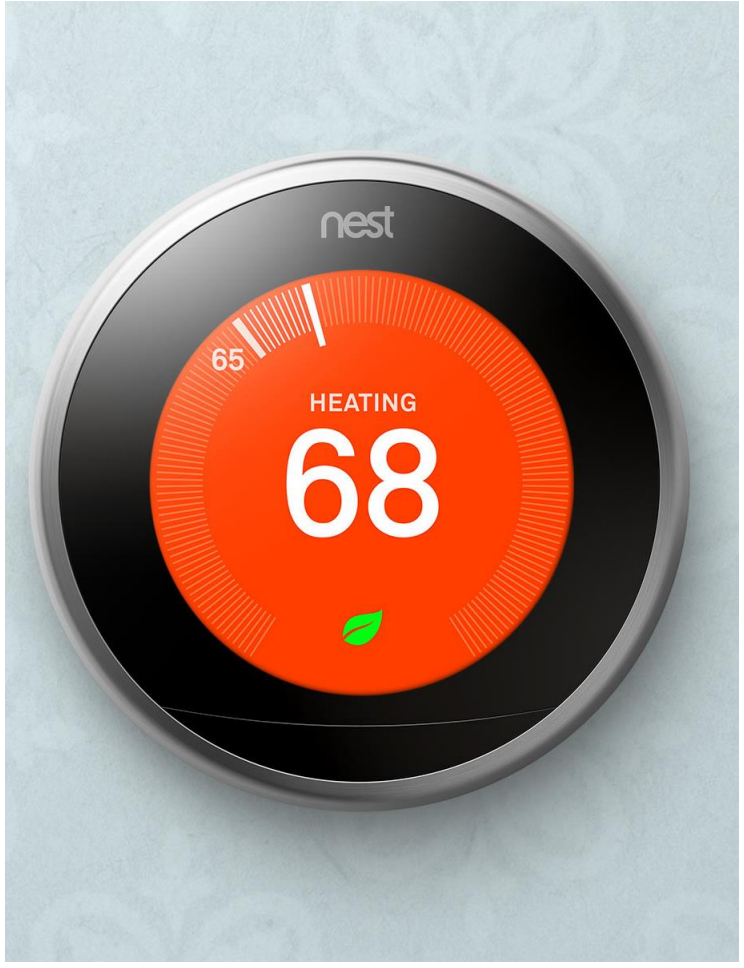


[Quelle: August]

8:35 Heizung drosseln

Informationen:

- Tagesrhythmus
- Personen anwesend



[Quelle: Nest]

8:40 Licht aus?

Informationen:

- Tagesrhythmus
- Personen anwesend

[Quelle: Philipps]

Weitere Geräte

[Quelle: Mattel]

[Quelle: LG]

[Quelle: Beurer]

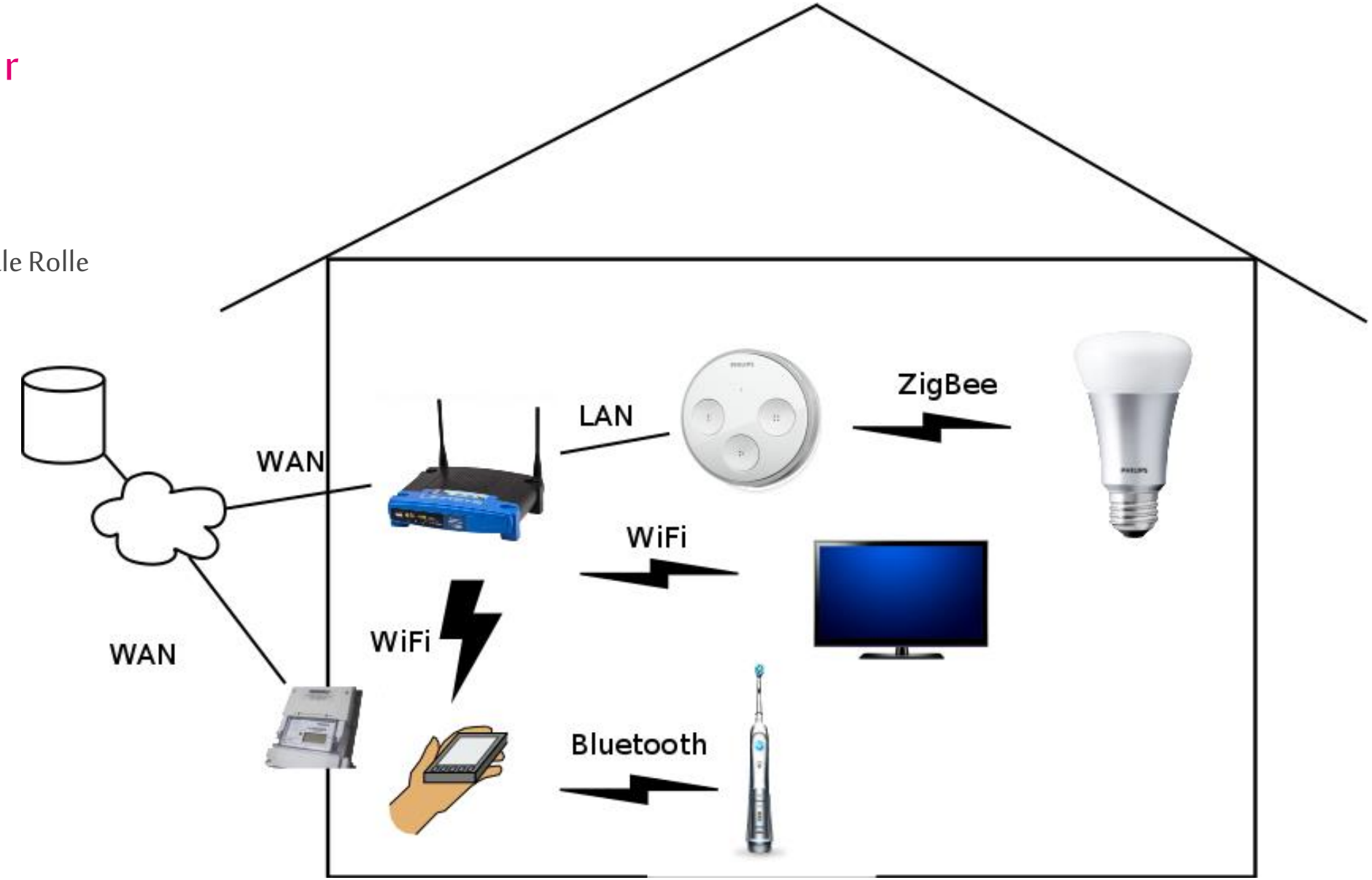
[Quelle: Discovergy]

Zusammenfassung Smart Home Devices

- Starke Vernetzung
- Meist über App bedienbar
- Spezialisiert auf eine Anwendung
- Daten werden oft in der Cloud / bei Drittanbietern gespeichert
    - Zugang über Server des Anbieters
    - Weltweit verteilt
- Meist App und Gerät vom selben Hersteller, aber auch Drittanbieter
- Datenschutzbestimmungen umfangreich / schwer verständlich

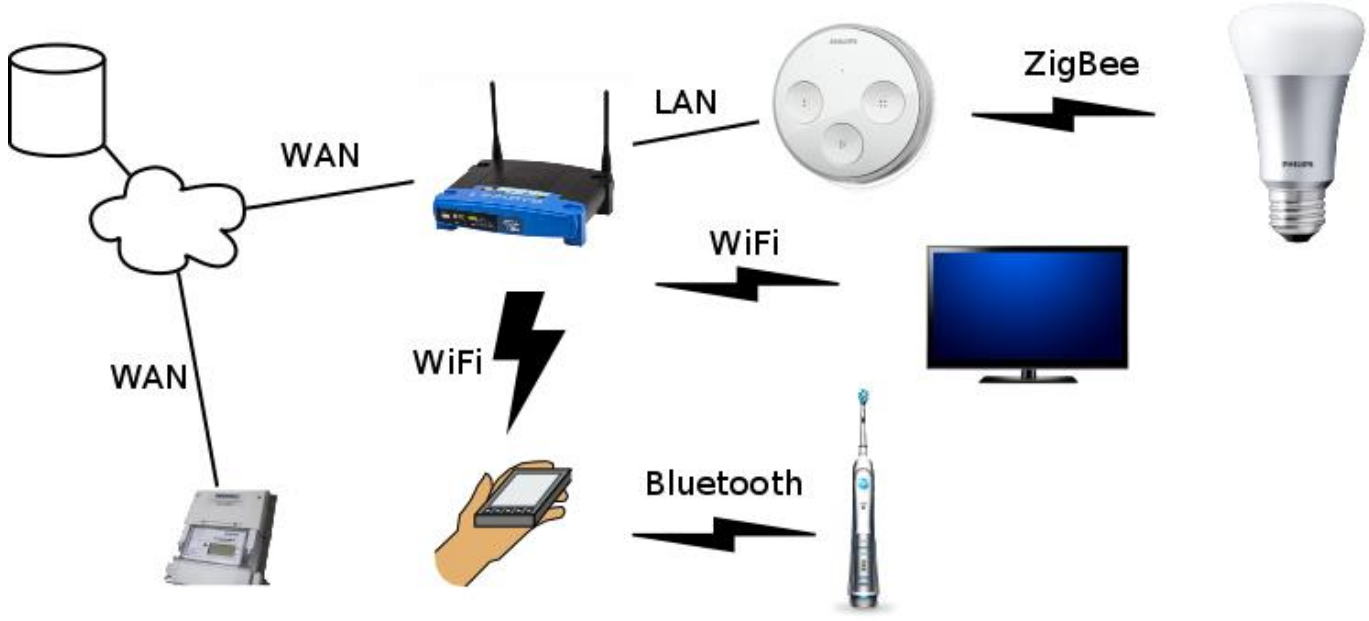
Netzwerkstruktur

- Diverse Protokolle
- Handy / Router zentrale Rolle
- Eingeschränkte Kontrolle



IT-Sicherheit (lokal) in Smart Home Umgebungen

- Probleme:
  - Steigende Komplexität
  - Routersicherheit
  - Handysicherheit
  - Netzwerksicherheit
  - Sicherheitsupdates (kein Display/Tastatur)
  - Kompatibilität vs. Sicherheit



IT-Sicherheit (global) → externe Datenverarbeitung

Probleme:

- Speicherung der Daten auf Servern des Anbieters
  - Welche Daten werden überhaupt übertragen? (Transparenz)
  - Wie lange werden sie gespeichert?
  - Wie sicher werden sie gespeichert?
  - Welche sekundäre Nutzung gibt es?

- Allgemeine Fragen bezüglich der erhobenen Daten
  - Wie aussagekräftig sind die Daten?
  - Über welchen Zeitraum lassen sie Prognosen zu?
    (Kreditkartendaten vs. Biometrische Daten)

Ergebnisse aus der Wissenschaft: Beispiel Smartmeter

Auswirkung abhängig von der Auflösung

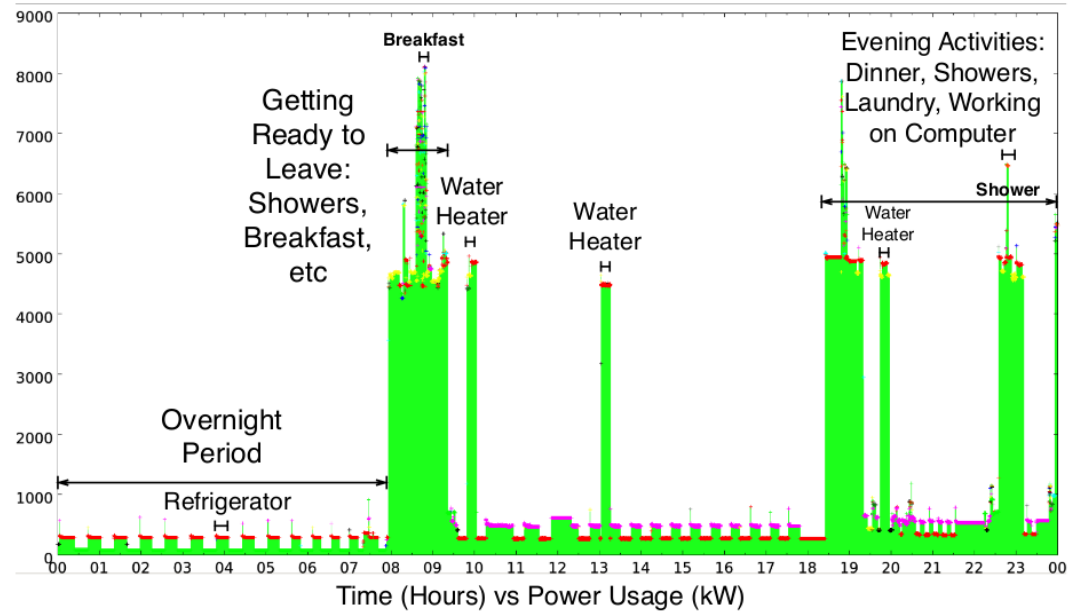
[Molina-Markham et. al. 2010]

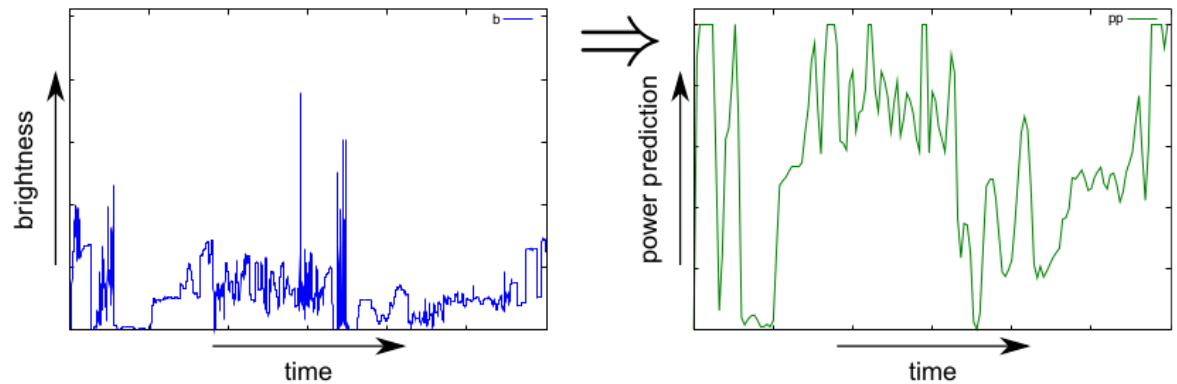
15-minütig : Anwesenheit, Schlafenszeiten, Essenszeiten

Minutenbereich: Frühstück kalt oder warm zubereitet, Fernsehzeiten, Waschmaschine in Betrieb, Kinder alleine zuhause

[Enve et. al. 2011; Greveler et. al. 2012]

0,5-sekündige Erfassung: Identifikation des gesehenen Programms oder Films im TV





Gegenmassnahmen aus der Wissenschaft: Beispiel Smartmeter

[Kalogridis et. al. 2010, 2011]

Reduktion der Lastkurven durch Stromspeicher

Generell:

Aggregation von Daten (je nach Verwendungszweck)

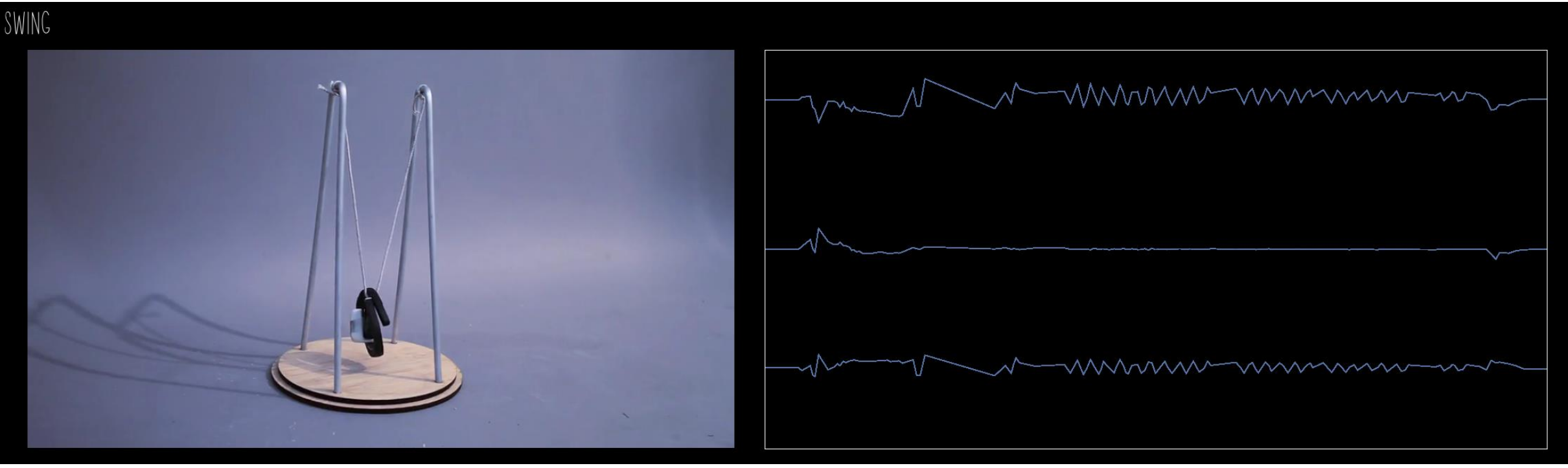
- über mehrere Verbraucher (Lasterfassung zur Netzsteuerung)
- über längere Zeiträume (Abrechnung)

Verlässlichkeit von Daten I

Verlässlichkeit von Daten II

Aber: Kontrolle über Sensor liegt beim Benutzer

→ Daten für Firmen auch nicht immer vertrauenswürdig



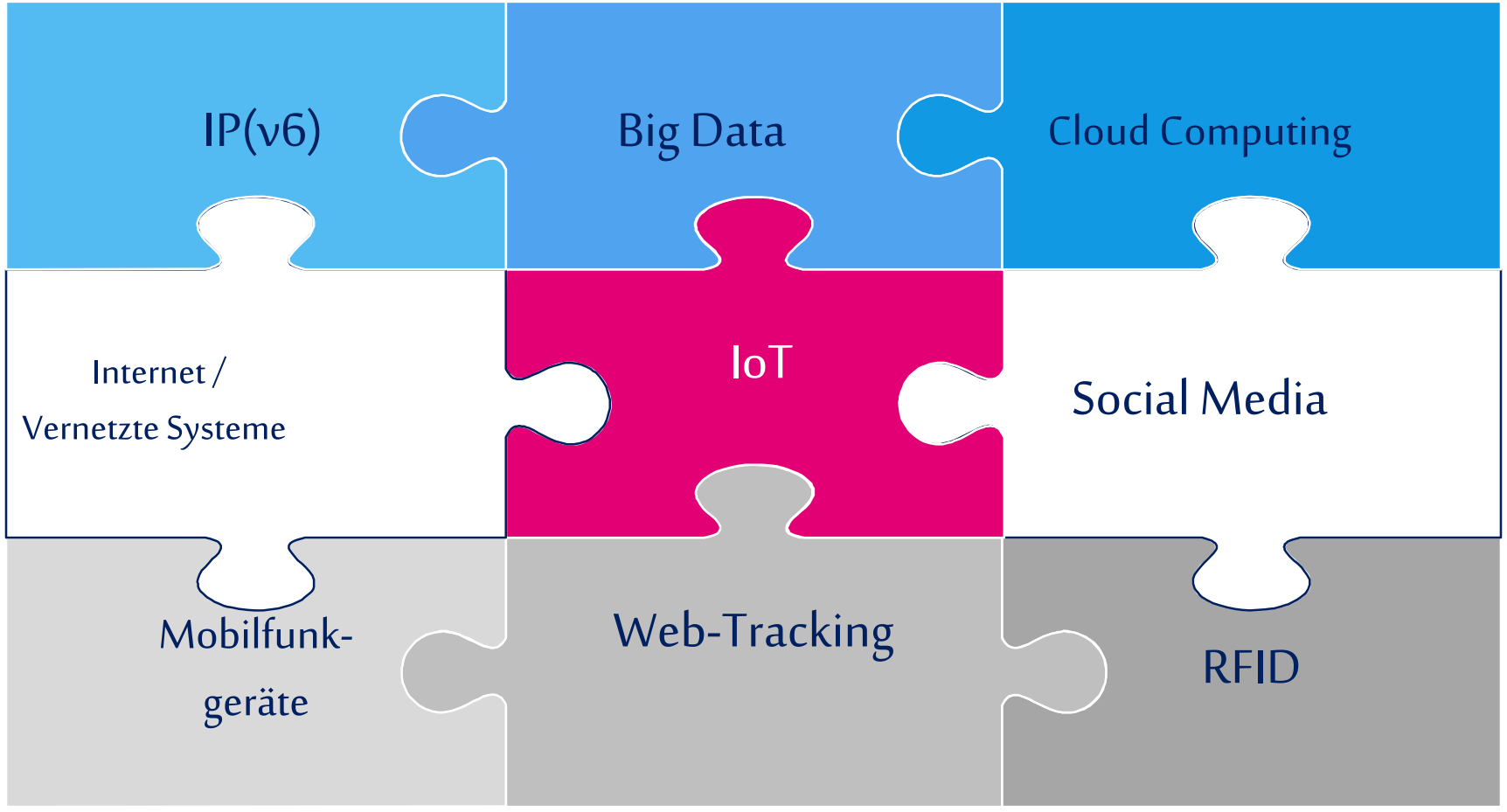
[Quelle: Unfitbits.com]

Gestaltungsoptionen für das Internet of Things

Leitsätze der Deutschen Telekom: Internet of Things

- Verlässliches und transparentes Datenschutzniveau
- Zweckbindung, Datensparsamkeit und Transparenz
- Kultur des Einverständnisses gegenüber Kunden.
- Beschränkung der Weitergabe von personenbezogenen Informationen auf diejenigen, die zur Erbringung der Leistungen unbedingt erforderlich sind
- Veröffentlichung verbindlicher Leitlinien für die datenschutzkonforme Umsetzung von Internet of Things und Industrie 4.0 Geschäftsmodellen
- Transparente Information über etwaige Änderungen dieser Leitlinien und ihrer Umsetzungsanforderungen

Internet of Things – Regelungsframework



Datenschutzanforderungen Internet of Things

- Datenschutz Grundsätze
  - Privacy by Design, Datensparsamkeit, Anonymisierung, frühzeitige Löschung, Transparenz, Einwilligung
- Zukünftiger Datenschutz in Prozessketten
  - Klare Abgrenzung der datenschutzrechtlichen Verantwortung in komplex vernetzten Systemen, höchste Transparenz
- Kundendatenschutz (Kunde-Produkt-Schnittstelle)
  - Bewegungsprofile, Freiwilligkeit bei Einwilligungen, Löschung von Daten
- Arbeitnehmerdatenschutz (Mensch-Maschine-Schnittstelle)

mobile business

Vielen Dank

Dr. Sebastian Pape

sebastian.pape@m-chair.de
http://www.m-chair.de/pape

GOETHE UNIVERSITÄT FRANKFURT AM MAIN