DGI-Forum Wittenberg 2015

Jan Rähm*

Das Netz der Dinge

Die physische Welt wird smart

DOI 10.1515/iwp-2016-0016

Ist heute die Rede von vernetzten Objekten, denken viele Menschen an zwei, drei Dinge in einem Netzwerk wie iPad, Smartphone oder Laptop. Aber wenn vom Internet der Dinge die Rede ist, geht es um die kommende Ära, in der nicht nur nahezu alle technischen Geräte, sondern auch kleinste Dinge wie einzelne Sensoren intelligent werden und vernetzt sind.

Die Geburtsstunde des Internet der Dinge war, so sagt es die englisch-sprachige Wikipedia, im Jahr 1982. Damals bastelten Studenten und Mitarbeiter der Carnegie Mellon University an einem Cola-Automaten und schlossen ihn ans damalige Netzwerk an. Der Automat sollte erstens mitteilen, wie viele Dosen noch drin und zweitens ob die auch kühl genug sind. Damit war das wahrscheinlich erste Ding am Netz. Wohlgemerkt: 1982. Der Begriff „Internet der Dinge“ tauchte Ende der 1990er Jahren das erste Mal in der Wissenschaft auf. Seitdem hat sich viel getan und jetzt 2015 ist das Internet der Dinge zum Schlagwort geworden. Heute soll alles, egal wie sinnvoll das auch ist, irgendwie smart und vernetzt sein: Vom Würstchengrill bis zur Deckenlampe, von der Waschmaschine bis zum vielgescholtenen Kühlschrank, der selbst im Internet einkauft. Den gibt es bis heute nicht. Die Waschmaschine, die selbst Waschmittel bestellt, die jedoch gibt es seit 2015 sehr wohl. Alles soll vernetzt sein. Alles soll kommunizieren. Warum? Das scheint den Herstellern manches Mal selbst noch nicht ganz klar zu sein. Und auch das „Wie“ ist, gelinde gesagt, noch nicht zu Ende gedacht.

Laut einer Definition – und derer gibt es durchaus einige – beschreibt das Internet der Dinge ein Konzept, das Objekten ermöglicht, über das Internet zu netzwerken. Reale Dinge melden ihren über Sensoren ermittelten Status und Zustand über miniaturisierte elektronische Schaltungen zur weiteren Verarbeitung in einem Netzwerk.

Alles ist mit allem vernetzt im Internet der Dinge (Bild: „wilgengebroed“ via Wikimedia.org, CC BY 2.0).

Stark vereinfacht könnte man sagen: Das Internet der Dinge beschreibt die Vernetzung von so ziemlich allen Dingen, in oder an die man Informationstechnik stecken kann. Diese Dinge sprechen daraufhin im Idealfall miteinander über diverse Netzwerke, tauschen Daten aus. Und aus den getauschten Daten kommen die angeschlossenen kleinen und großen Rechner zu großartigen neuen und eigenen Schlussfolgerungen. Oder sie machen einfach das Leben ein klein bisschen einfacher. So wie in der spanischen Stadt Santander.

Smarte Stadt, smartes Leben

Santander ist seit 2010 eines der größten Testfelder in Sachen Internet der Dinge, Geschmacksrichtung „Smart City“. Die gesamte Stadt wurde mit einem Netzwerk aus rund 12.000 Sensoren überzogen. Damit werden beispiels-

***Kontaktperson:** Jan Rähm, Freier Journalist & Autor, Frankenallee 14,
14052 Berlin. E-Mail: jan@radiofuzzie.com, www.radiofuzzie.com

weise der Verkehr und die Parkplatzsuche optimiert. Andere Sensoren messen den Schadstoffgehalt in der Luft oder ermitteln Temperatur und Luftfeuchtigkeit. Mit Hilfe dieser Informationen wird unter anderem die Bewässerung der Grünflächen gesteuert. Licht- und Bewegungssensoren steuern die Straßenbeleuchtung. Nur wenn nötig strahlen die Lampen mit voller Kraft. Die Müllabfuhr wird ebenso eingebunden und optimiert. Geleert werden die Tonnen, wenn sie voll sind und nicht nach festem Plan. Auch der öffentliche Nahverkehr in Santander ist in die smarte Stadt integriert. Dazu gehören in Santander Busse, ein kommunales Fahrradverleihnetz und der Taxiverkehr. Wann der Bus kommt und ob freie Räder beziehungsweise Taxis in der Nähe sind, erfahren die Bürger per App auf Smartphone und Tablet.

So kann das Internet der Dinge aussehen – hier als intelligente Stadt, als Smart City. 2015 sollte die Zahl der vernetzten Dinge laut Marktforschern 4,9 Milliarden überschreiten. Das Internet der Dinge stapft also unbeirrbar voran. Aber gänzlich unbeirrbar? Nein, nicht ganz. Noch immer behindern grundsätzliche Fragen das Vorankommen.

Kommunikation – nur wie?

Da wäre zu allererst die Frage nach Standards und Schnittstellen. Denn was bringt ein Konzept, in dem alle miteinander reden, aber keiner den anderen versteht. Wir stehen de facto vor einem informationstechnischen Babylon. Die Industrie, die schon länger mit und am Konzept des Internets der Dinge werkelt, kommt langsam aber sicher auf einen Nenner. Man merkt ihr Jahrzehnte Erfahrung in Sachen Maschinensteuerung und Robotik an. Aber auch hier ist noch nicht ausgemacht, welche Lösungen das Rennen machen.

Im Consumer-Markt sieht es dagegen geradezu katastrophal aus. Nahezu jeder Hersteller setzt irgendwie auf eigene Lösungen. Froh kann man schon sein, wenn die Trägertechnologie, also das Kommunikationsmedium an sich, die gleiche ist.

Kompatibilität oder Interoperabilität untereinander? Meist Fehlanzeige. Zudem entstehen in jeder neuen Generation neue „Pseudo-Standards“.

Einen kleinen Erfolg bei der Suche nach Standards und Schnittstellen können Forschung und Industrie verbuchen: Nahezu alle Geräte und Technologien verstehen sich auf das nicht mehr ganz so neue, aber immer noch nicht weit verbreitete Internetprotokoll Version Sechs (IPv6). Nur mit dem ist es überhaupt möglich, Milliarden und Abermilliarden von Geräten ins Internet zu bringen.

Beim noch immer gebräuchlichen Internetprotokoll der vierten Version ist heute schon Schluss, ganz einfach weil es nicht genug IP-Adressen für alle Geräte gibt. Das Problem soll mit IPv6 zumindest vorerst behoben sein.

Security by Obscurity

Noch lange eine Baustelle sein, wird die Sicherheit. Denn wenn Unmengen an neuen Geräten die Netze fluten, gibt es auch Unmengen neuer Schwachstellen und Angriffspunkte. Und so beschäftigt die Sicherheit die gesamte Branche – wieder sowohl Forschung als auch Industrie. Dabei geht es einerseits um die eigentliche IT-Sicherheit. Also die Sicherheit der Systeme und der Schutz vor Angriffen. Aber es geht andererseits auch um die Betriebssicherheit.

Noch immer gilt eher: Security by Obscurity – Sicherheit durch Unklarheit. Die Sicherheit einer Blackbox. Und das obwohl Fälle in der Vergangenheit immer wieder gezeigt haben, dass der Schaden dann in vielen Fällen weit größer und weit schwerer zu beheben war. Das aktuelle IT-Sicherheitsgesetz hat diese Praxis weiter verfestigt. Eine lang geforderte Pflicht zur Veröffentlichung von Sicherheitslücken gibt es weiter nicht. Und das, obwohl es immer mehr Beispiele gibt, in denen die Praxis der „Responsible Disclosure“, also der verantwortungsvollen Aufdeckung, Erfolg hat. Dabei meldet der Finder die Sicherheitslücke dem Betroffenen und gibt ihm Zeit, die Lücke zu stopfen. Anschließend geben beide die Lücke bekannt, wenn diese erfolgreich gestopft wurde. Nur selten gab es in der Vergangenheit Fälle, in denen die Preisgabe erfolgte, bevor die Lücke geschlossen war. Die passierte meist dann, wenn sich das betroffene Unternehmen nicht rührte.

Festzuhalten bleibt: Sicherheitslücken geheim zu halten, nützt nur Geheimdiensten und Kriminellen in der digitalen Welt.

Herausforderung: Gesellschaft

Das Internet der Dinge und Konzepte wie Smart Home, Smart Cars und Industrie 4.0 können nur dann ein Erfolg werden, wenn Anwender aller Art überzeugt sind, dass die Lösungen einem annehmbaren Sicherheitslevel entsprechen. Nur: Mit dem Internet der Dinge ziehen in die Gesellschaft auch neue Probleme ein. Zwei davon: Angst vor Arbeitsplatzabbau und Datensammelwut.

Maschinen, die dem Menschen die Arbeit erleichtern. Das ist gleichermaßen Verheißung wie Drohung. Denn wo Maschinen schwere Jobs übernehmen, verliert der Mensch

natürlich seine Arbeit. Ihm bleibt allenfalls noch, die Maschinen zu überwachen. und dafür werden dann eventuell nicht mehr viele Mitarbeiter gebraucht.

Doch wo Menschen keine Arbeit mehr haben, verdienen sie auf der einen Seite kein Geld und sind auf soziale Absicherung angewiesen. Auf der anderen Seite zahlen sie so auch keine Steuern. Das könnte zu einer doppelten Belastung für Deutschland und Europa werden. So stellt sich die Frage, wie soll mit der Automatisierungsdividende umgegangen werden? Wird es eine Art „Maschinensteuer“ geben? Eine Abgabe speziell für das Internet der Dinge, für die Industrie 4.0?

Das deutsche Wirtschaftsministerium zeigt sich zuversichtlich. Man sei optimistisch, dass sich dank der neuen Konzepte in der Digitalisierung auch gänzlich neue Berufe und Berufsbilder entwickeln würden, die sich heute noch niemand vorstellen könne. Entsprechend würden neue Jobs geschaffen. Notwendig sei aber, dass sich die Ausbildung in Schule und Hochschule an die Digitalisierung inhaltlich anpassen würde.

Bleibt zu hoffen, und da sind wir wieder beim Thema Akzeptanz für das Internet der Dinge, dass Wirtschaft und Politik rechtzeitig die richtigen Entscheidungen treffen. Sonst, so steht zu befürchten, könnte es eine „Maschinenstürmerei 2.0“ geben.

Nimmersatte Datenfresser

Daten und Arbeit – Arbeit und Daten. Beides ist im Internet der Dinge eng miteinander verknüpft. Doch während es das eine – die Arbeit – perspektivisch weniger brauchen wird, scheint der Datenhunger der neuen Industrien kaum zu stillen zu sein.

In Deutschland gilt ja: Wer Daten sammeln, Daten auswerten oder Daten gar verwerten will, der muss strengen Auflagen genügen. Nur, schon die reine Datenerhebung durch die Sensoren sehen Rechtswissenschaftler kritisch. Denn die Sensoren sammeln ja permanent und beständig Unmengen an Daten. Die meisten davon sind personenbeziehbar, weil die meisten Sensoren, einer bestimmten Person oder einer Gruppe von Personen zugeordnet werden können. Damit greifen die Sensoren mit ihrer Sammeltätigkeit in das vom Bundesverfassungsgericht entwickelte Grundrecht auf informationelle Selbstbestimmung ein. Der Bürger hat in vielen Fällen weder einen Überblick, welche Daten eigentlich gesammelt werden, noch kann er eine informierte Entscheidung treffen. Beispiel: Auto. Das sammelt schon heute massenhaft Daten.

Erlaubt wäre dies im Rahmen der Rechtsprechung, wenn ich als Betroffener der Datensammlung zustimmen

oder sie ablehnen kann. Dann wäre dem Gesetz genüge getan. Da dies in vielen Fällen unpraktikabel ist, in einigen gar unsinnig, ist es hier am Gesetzgeber, einen sinnvollen Umgang zu finden.

Doch wem gehören die gesammelten Daten im Auto denn eigentlich? Wir sprechen hier ja beispielsweise von Daten wie Fahrgeschwindigkeit, Richtung, Beschleunigung, Standort oder selbst das Setzen der Blinker und so weiter und so fort. Genau an diese Daten wollen ja alle Beteiligten ran: Kfz-Hersteller und Zulieferer für Wartung und Qualitätssicherung. Kranken- und KFZ-Versicherungen geht's ums Risiko. Die Frage, wem die Daten gehören und wer ran darf, ist aktuell völlig offen. Der Fall ist ja schon kompliziert beim Auto, das mir gehört. Er wird nicht einfacher, wenn das Auto geleast ist, dem Arbeitgeber oder gar einem Car-Sharing-Unternehmen gehört.

Und noch ein Datensatz ist heiß begehrt – die Verkehrsunfalldaten. Interesse daran hätten natürlich wieder Autohersteller und Versicherungen, aber auch Polizei und Unfallgegner. Und da kommen wir zum zweiten Grundrechtsproblem. Denn eigentlich habe ich ein Zeugnisverweigerungsrecht. Nur, was, wenn mein Auto gegen mich aussagt? Darf die Polizei vor Ort die Fahrzeugdaten abzapfen? Hier sind wir jetzt im absolut nebulösen Raum der Straf- und der Zivilprozesse.

Klar ist soviel: Das Internet der Dinge stellt große Aufgaben – an Wissenschaft, Politik und Gesellschaft. Doch sicher ist, zurückdrehen lassen wird sich das Rad der Entwicklung nicht mehr. Zu groß sind die Annehmlichkeiten, die wir alle wohl kaum mehr missen wollen.

Deskriptoren: Internet, Datenschutz, Sicherheitsfragen

Jan Rähm
Freier Journalist & Autor
Frankenallee 14
14052 Berlin
jan@radiofuzzie.com
www.radiofuzzie.com

Jan Rähm ist freiberuflicher Wissenschafts- und Technikjournalist. Von Berlin aus beliefert er vor allem öffentlich-rechtliche Hörfunksender in ganz Deutschland und Österreich, aber auch Tageszeitungen und Fachmagazine. 2012 veröffentlichte er zusammen mit Kollegen „Bits und Bomben“ – ein Buch über digitale Kriegsführung.