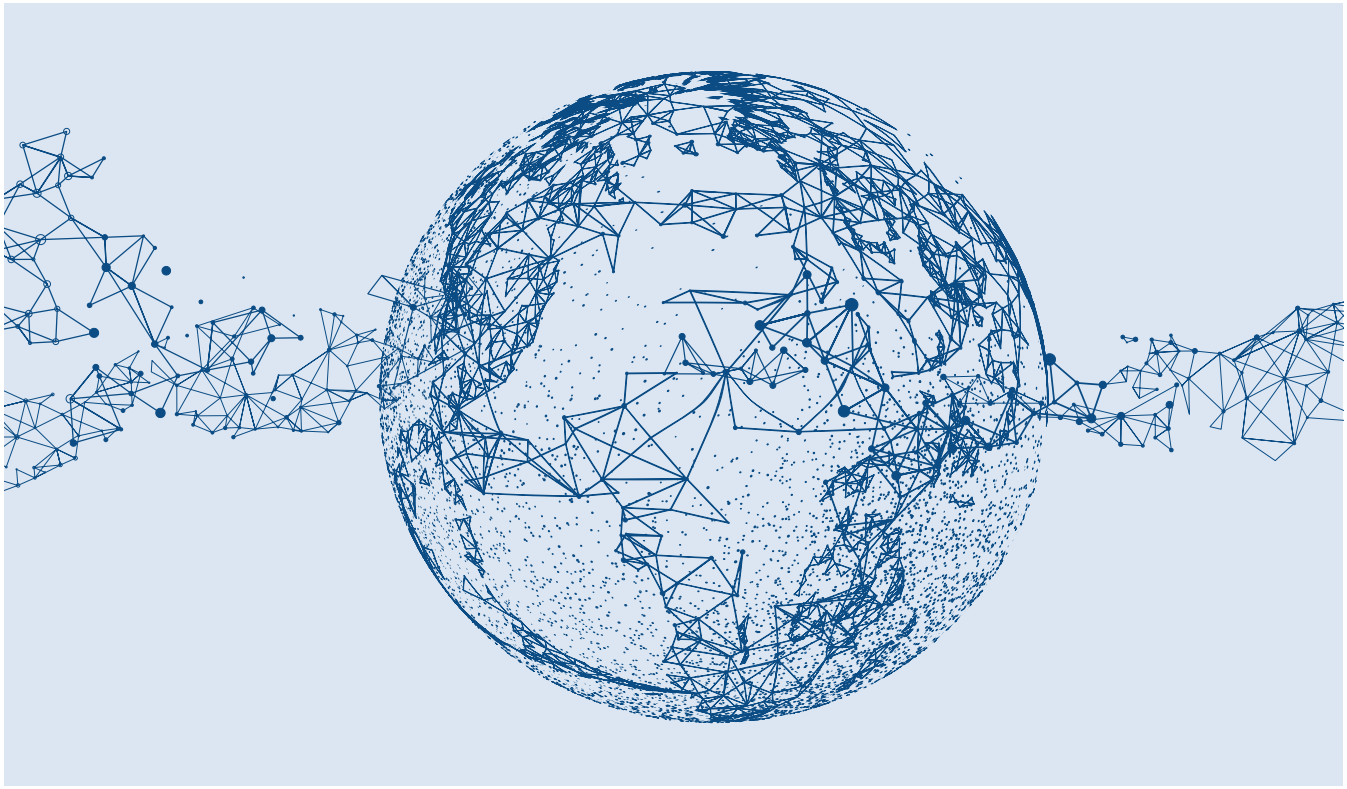
Analysen & Argumente

Konrad Adenauer Stiftung

DIGITALE GESELLSCHAFT

JULI 2018
AUSGABE 308



Internet of Things

Richard Lackes

Zum Mitnehmen

- Als „Internet der Dinge" (IoT) wird ein System intelligenter, über ein Kommunikationsmedium verbundener Produkte bezeichnet. Smart Home, Smart Cities, E-Health, autonomes Fahren, intelligente Fertigungs- und Logistiksysteme sind bekannte Anwendungsbeispiele. IoT ist ein wichtiger Innovationstreiber der Digitalisierung.

- Das IoT ist mit Risiken verbunden, die besonders Fragen des Datenschutzes und des Dateneigentums betreffen. Objektdaten und (besonders geschützte) Personendaten können nicht scharf voneinander abgegrenzt werden. Gute Regelungen zu schaffen, ist eine Gratwanderung: Zu restriktiver Datenschutz legt IoT lahm.

- In Deutschland gibt es Nachholbedarf in Bezug auf leistungsfähige und sichere Kommunikationsnetze sowie einheitliche Standards. Vor allem diese Defizite wirken sich hemmend auf den weiteren Ausbau von IoT aus.

INHALT

Begriff und Zielsetzung

Kaum ein Begriff steht mehr für den technologischen Fortschritt und für die zu erwartenden gravierenden Umwälzungen von Wirtschaft und Gesellschaft durch die Digitalisierungsbewegung wie der Begriff des Internet of Things (IoT, Internet der Dinge). Erstmals verwendet wurde er von Kevin Ashton, der ihn allerdings sehr stark auf die automatische Identifizierbarkeit von Objekten reduzierte (Ashton, 2009). Inzwischen hat sich diese Perspektive erweitert, so dass man heute zu Recht sagen kann, dass das IoT in den kommenden Jahren wesentlicher Treiber und integraler Bestandteil der digitalen Transformation sein wird. Manche vergleichen seine Bedeutung sogar mit der des World Wide Web in den späten 90er Jahren (Saarikko et al., 2017, S. 667). Die mit „intelligenten, vernetzten Objekten" assoziierten Hoffnungen, Potentiale und Chancen mischen sich mit Befürchtungen und Ängsten hinsichtlich ihrer Beherrschbarkeit und ihrer Risiken (Miorandi et al., 2012).

Unter IoT versteht man ein System intelligenter, über ein Kommunikationsmedium vernetzter Produkte (Porter/Heppelmann, 2014, S.66 f.). Beliebige Alltagsgegenstände (physische Objekte, things), wie Haushaltsgeräte, Fahrzeuge, Container, Pumpen, Kleidung etc. werden mit Intelligenz (smart objects) ausgestattet und mit einem Kommunikationsnetz verbunden. Sie erweitern somit das traditionelle Internet of People.

Internet of Things zielt darauf ab,

- die Verwendungsmöglichkeiten und das Nutzungsspektrum von sonst nicht oder weniger intelligenten Objekten zu erweitern,
- innovative Anwendungen und digitale Services für Anwender und Nutzer (sowohl Konsumenten als auch Produzenten) zu ermöglichen,
- Ressourcen durch effizienteren Einsatz zu schonen,
- existierende Geschäftsmodelle effizienter zu gestalten bzw. neue Geschäftsmodelle zu generieren,
- die Produktivität von Wirtschaftsbereichen zu steigern und
- die Zufriedenheit der Anwender zu erhöhen.

Anwendungs- und Einsatzmöglichkeiten von IoT finden sich in privaten, aber auch öffentlichen und industriell-gewerblichen Bereichen (Lee/Lee, 2015), wie

- Smart Home und Smart Meter für das Energiemanagement (Stojkoska/Trivodaliev, 2017),
- Smart-City-Konzepte,
- E-Health und E-Care im Medizin und Gesundheitsbereich,
- Smart Security zur Verbesserung der Sicherheit im privaten und öffentlichen Umfeld,
- Intelligente Mobilitätssysteme und autonomes Fahren,

- Intelligente Supply Chains etc.,
- Intelligente Fertigungs- und Logistiksysteme (Industrie 4.0) und
- Intelligente Wartungssysteme.

Was ist neu an IoT? Architektur des Datenhandlings

Einzelne Aspekte sind keineswegs neu: Alltagsgegenstände, wie Fahrzeuge oder moderne Waschmaschinen, sind heute schon mit einer gewissen Intelligenz ausgestattet. Auch globale Kommunikationsnetze wie das Internet existieren bereits seit längerem.

Offene, globale Systeme

Neu ist neben der grundsätzlichen Intelligenzerweiterung bisher nichtintelligenter Objekte (z.B. Schuhe, Uhren, Container) durch eingebettete Prozessoren vor allem die synergetische Kombination der Technologien zur Datenerfassung (Sensortechnologie) und Datenverarbeitung auf der einen Seite sowie der Kommunikations- und Speichertechnologie (Cloud-Speicher) auf der anderen Seite (s. Abb.1 links). IoT-Objekte erfassen also nicht nur isoliert und lokal ihre eigenen Zustandsdaten und steuern sich dann gemäß eines starren Algorithmus selbst (wie moderne Waschmaschinen), sondern sie öffnen sich über die Kommunikationsschnittstelle anderen Objekten, Speichermedien oder Anwendungen (s. Abb. 1 rechts). Dadurch können sie ortsungebunden überwacht und gesteuert werden. Aus einem geschlossenen, singulären, lokalen System (wie das einer modernen Waschmaschine) wird ein offenes, globales, mit vielen unterschiedlichen Komponenten bestücktes IoT-System (z.B. Smart Home). Diese Systemöffnung ermöglicht aber zugleich schädliche und missbräuchliche Einwirkungen, etwa den unbefugten Abruf von Daten einer Überwachungskamera, das Ausschalten der Kamera oder Abbremsen eines Fahrzeuges.

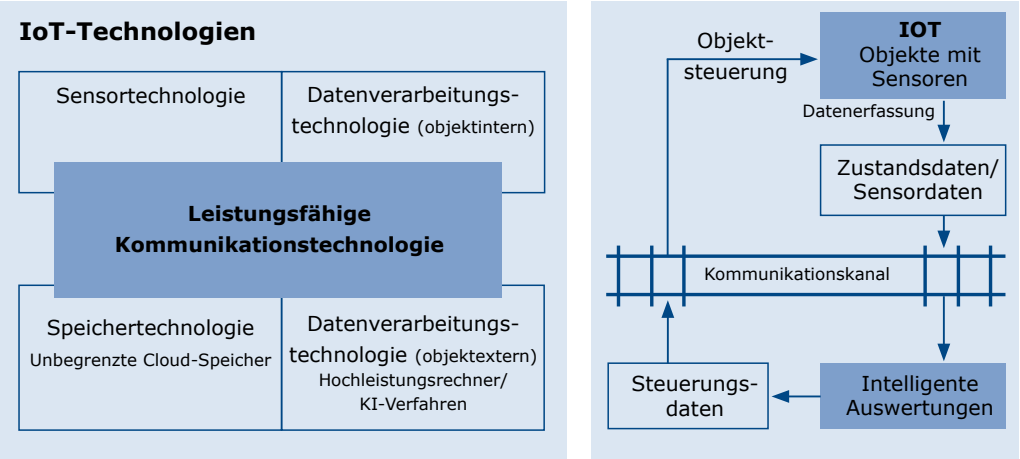


Abbildung 1: Technologiekomponenten und Architektur des Internet of Things

Objekte im Verbund

Durch die Kombination solch innovativer Technologien entstehen neue Applikationen: Mehrere IoT-Objekte gleicher oder unterschiedlicher Art können im Verbund, sogar mit wechselnden Rollen, zusammenarbeiten (autonom gesteuerte Fahrzeuge kommunizieren untereinander und mit den Ampeln der Umgebung zum besseren Management des Verkehrsflusses). Um ein physisches Objekt auch in einem Informations- und Kommunikationssystem als virtuelles (elektronisches) Objekt verwalten und administrieren zu können, muss es zwingend eine Identität erhalten. Nur wenn es eindeutig individuell angesteuert werden kann, lässt es sich gezielt adres-

sieren und können seine Daten korrekt zugeordnet werden. In den ersten Entwicklungsstufen wurde hierfür die RFID-Technologie (Radio Frequency Identification) verwendet (Atzori et al., 2017). Die auf dem RFID-Chip abgelegte Objektidentifizierungsnummer adressiert eindeutig ein individuelles Objekt. Hierfür wurde mit dem Electronic Product Code (EPC) von der Organisation EPCglobal ein Standard geschaffen, der – analog zu einer Ausweisnummer des Menschen – beliebige Objekte weltweit über einen 96-Bit-Code eindeutig identifiziert (Bassie et al., 2013, S. 222) und ihnen eine „Identität" verschafft. Dieses elementare, in seiner Bedeutung aber nicht zu unterschätzende Feature erlaubt nicht nur ein dezidiertes Tracking und Tracing mobiler Objekte (ihre permanente Echtzeit-Lokalisation und Nachverfolgung), sondern schafft erst die Basis für eine leistungsfähige Kommunikation in einem Kommunikationsnetzwerk, wie es für IoT benötigt wird.

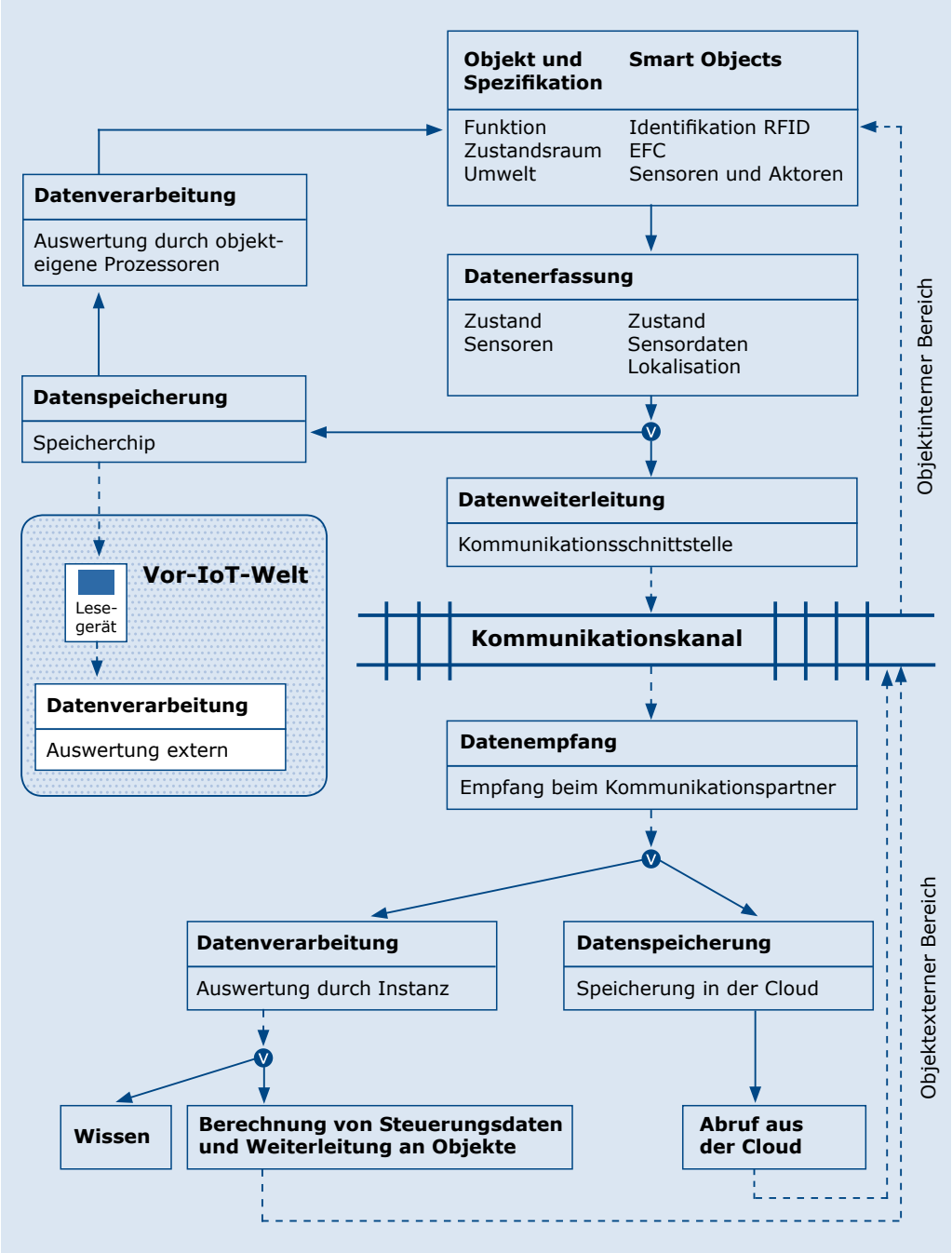


Abbildung 2: Architekturüberblick des Datenhandlings in IoT-Systemen

Grundlegend für die Transformation von Alltagsgegenständen zu IoT-Objekten ist die Ergänzung dieser Objekte um smarte Komponenten (Prozessoren, Sensoren, Kommunikationstechnik). Objektbezogene Daten lassen sich auf einem Mikrochip speichern und/oder über eine Kommunikationsschnittstelle weiterleiten (vgl. Abb. 2). Nachdem die Daten über den Kommunikationskanal (WLAN, Internet etc.) an andere Kommunikationspartner (andere Objekte, Instanzen, Cloud-Speicher etc.) im Kommunikationssystem weitergeleitet wurden, können sie dort ausgewertet werden. Unter einer Instanz in einem Kommunikationssystem wird hierbei ein anderer Kommunikationspartner (Mensch, Maschine, anderes Objekt, Software bzw. App, Organisation) verstanden, der „übergeordnet" ist und Auswertungsaufgaben übernimmt. Ein bisher lokal begrenzter Handlungs- und Wirkungsbereich wird durch die Integration der Kommunikationskomponente aufgebrochen, und es erschließen sich neue, höherwertige, ortsunabhängige Nutzungsmöglichkeiten. Je nach Funktionalität einer Instanz werden aus den empfangenen oder abgerufenen Objektdaten Steuerungsdaten berechnet und über den Kommunikationskanal an das Objekt (oder andere Objekte des Verbunds) zurückgesendet. Hierdurch werden Objektzustandsänderungen beliebig weit entfernter Objekte ausgelöst (z.B. Einschalten der Klimaanlage, Zoomen der Kamera). Mit der Integration von Cloud-Speichern im Kommunikationssystem lassen sich, unabhängig von den begrenzten Speicherkapazitäten in den Objekten selbst, beliebig große Datenmengen erfassen und speichern. Komplette Historien von mannigfaltigen, in kurzen Zeitabständen erfassten Zustands- und Umweltdaten (Bilder, Videos etc.), Big Data also, sind so auswertbar (McAfee/Brynjolfsson, 2012). Man erkennt in Abbildung 2 auch, dass der Kommunikationskanal bzw. das Kommunikationsnetz die kritische, für alle relevanten Aktivitäten zuständige Ressource darstellt. Seine Leistungsfähigkeit ist in besonderem Maße entscheidend für die Leistungsfähigkeit des Gesamtsystems.

Neue, höherwertige Nutzungsmöglichkeiten

Im Schaubild der Abbildung 2 ist im linken Bereich das klassische Vorgehen – vor IoT – bezüglich des Datenhandlings moderner Produkte, etwa moderner Kraftfahrzeuge, skizziert. So werden bei einem Werkstattbesuch durch den lokalen Anschluss eines speziellen Lesegerätes die im Bordcomputer des Fahrzeugs gespeicherten Zustandsdaten mit ihren Änderungen ausgelesen. Allerdings erfolgt dies nur fallweise, wenn Störungen auftreten oder Wartungsarbeiten anstehen, und nur in einer entsprechend ausgestattete Fachwerkstatt („Instanz"). Charakteristisch sind der starke Lokalitätsbezug zum Objekt, die Datenerfassung und -speicherung durch das Objekt selbst, der nur temporäre, von außen angestoßene Datenzugriff und die sehr spezielle, zweckgebundene Auswertung. Genau diese Restriktionen werden durch IoT aufgehoben. Das heißt, der nächste Schritt und damit der Übergang in die IoT-Welt bestünde am Beispiel des Fahrzeugs darin, dass die Fahrzeugdaten nicht nur bei einem Werkstattbesuch, der unregelmäßig, unkontrolliert und oft erst nach Auftritt einer Problemsituation stattfindet, ausgelesen würden, sondern permanent – auch während des Fahrzeugbetriebs – über ein entsprechendes Kommunikationsnetzwerk weitergeleitet und zentral ausgewertet würden (z.B. Komponentenverschleiß, vorbeugende Wartungsmaßnahmen oder Empfehlungen zur Fahrweise).

IoT-Welt und Vor-IoT-Welt im Vergleich

Die IoT-Welt unterscheidet sich von der Vor-IoT-Welt durch folgende Möglichkeiten:

- umfassende Datengewinnung und Datensammlung zu vielen Objekten,
- Globalität (Standortunabhängigkeit von Gerät und Instanz),
- permanente Verbindungsmöglichkeit,

- tiefgehende, nicht nur auf Einzelobjekte bezogen Datenanalyse und Datenverwertung und
- Steuerbarkeit und Kontrolle der Objekte durch beliebig weit entfernte Instanzen.

Entwicklungsstand und Anforderungen für die IoT-Umsetzung

Anforderungen an das Kommunikationsnetz und die Datensicherheit

Wegen der fundamentalen Bedeutung der Kommunikationskomponenten in IoT-Systemen braucht es ein sehr leistungsfähiges und sicheres Kommunikationsnetz. Hierzu gehören nicht nur eine hohe Bandbreite des Kommunikationskanals und leistungsfähige, flächendeckende Zugangsmöglichkeiten, sondern auch die Verwendung eines einheitlichen Kommunikationsprotokolls („einheitliche Sprache") und entsprechender Schnittstellenstandards für die einbezogenen Geräte sowie Sicherheitsmaßnahmen gegen unbefugten Zugriff auf die im Netz transportierten Daten (Ziegeldorf et al., 2014). In Deutschland besteht hier noch beträchtlicher Nachholbedarf. Um ein unbedingt erforderliches flächendeckendes und leistungsfähiges Internet mit entsprechenden Zugangsmöglichkeiten bereitstellen zu können (Deutschland liegt bezüglich der Internetgeschwindigkeit laut statista 2017 auf Platz 25, weit hinter den USA, Japan, Skandinavien und Südkorea), sind in den nächsten Jahren erhebliche Investitionen in die Infrastruktur erforderlich. Die physikalischen Netze, die heute in Betrieb sind, werden selbst nach Auslastungsoptimierung durch network slicing (die Aufteilung der Netzkapazität in parallel nutzbare virtuelle Bereiche) nicht flächendeckend in der Lage sein, die Vielzahl geplanter neuer smarter Geräte zu versorgen. Mit der notwendigen Infrastrukturinvestition allein ist es aber nicht getan. Auch fehlende Standards hinsichtlich der Schnittstellen hemmen die Entwicklung im IoT-Umfeld. Standardisierungsbemühungen müssten intensiv unterstützt werden. Dies ist besonders schwierig, weil nicht nur nationale und europäische, sondern Interessenten weltweit betroffen sind. Zumindest eine starke europäische Initiative für einheitliche Standards sollte rasch zu Ergebnissen führen.

Leistungsfähige und sichere Kommunikationsnetze

Um einen nicht manipulierbaren und abhörsicheren Datenaustausch über öffentliche Netze zu schaffen, müssen IoT-Systeme sichere Verbindungen nutzen, entsprechende Übertragungsprotokolle einsetzen und ihre Daten grundsätzlich mit leistungsfähigen Verfahren verschlüsseln. Die smarte Klingel eines Smart Homes darf also nicht ihre Daten (Klingelsignal, Sprache, Video) unverschlüsselt über einen ausländischen Server an das Smartphone des Hausbesitzers weiterleiten, wie es viele Apps in diesem Bereich derzeit tun. Zum Schutz der Anwender sollten Verschlüsselungen zwingend vorgeschrieben werden. Trotz Verschlüsselung kann die Datensicherheit gefährdet sein, wenn der empfangende Server (vor allem wenn er sich im nach anderen Kriterien kontrollierten Ausland befindet) einen „Schlüssel zur Entschlüsselung" besitzt, um anspruchsvollere Auswertungen vornehmen zu können. Es braucht also eigentlich eine Vertrauen garantierende, „zertifizierte" Serverinstanz – eine Art „Notariats-Server".

Sicherer Datenaustausch

Anforderungen an die IoT-Software.
Wie sollen die Programme erstellt werden?

Im Bereich der Software für IoT-Systeme empfiehlt es sich, wie bei anderen Anwendungen auch, dauerhafte flexibel skalierbare, auf die Benutzerbedürfnisse anpassbare Standardsoftwarelösungen, zumindest für die Basisfunktionalitäten, zu etablieren. Darüber hinaus wird sich ein Markt für höherwertige Services im IoT-Bereich entwickeln (Smart Security, Smart Mobility, Smart Healthcare, Global Maintenance-

IoT-Software

Systeme im industriellen Bereich etc.), mit innovativen Geschäftsmodellen wie differenzierte Sharing-Lösungen, Pay-per-Use-Konzepten, agilen Microservices, Nutzungslizenzverkauf mit diversen Services statt Produktkauf und temporär agierenden, virtuellen Mitarbeiterteams ohne feste Strukturen. Hochwertige IoT-Applikationen erfordern komplexe Auswertungs- und Verarbeitungsprogramme. Smarte Objekte erzeugen große Datenmengen, die möglichst in Echtzeit (on the fly) analysiert und genutzt werden sollen. Für derartige Big-Data-Analysen ist eine Vielzahl neuer, komplexer Verfahren und Algorithmen zu implementieren. Doch wer soll sie konzipieren und erstellen, wo bereits heute ein eklatanter Fachkräftemangel im IT-Bereich herrscht?

IoT-Startups

Die Förderung junger technologieorientierter IoT-Startups ist sicher ein wichtiger Ansatz. Allerdings zeigen die bisherigen Erfahrungen, dass neue Wege beschritten werden sollten. Empfehlenswert ist, nicht nach den traditionellen Förderprinzipien mit oftmals sehr risikoscheuen Vergabekriterien immer die gleichen, oft etablierten Gruppen, Personen oder Institutionen zu fördern. Wirklich neue, bahnbrechende Innovationen sind so nicht zu erwarten. Das Silicon Valley verdankt seinen Erfolg auch nicht General Motors, Exxon oder AT&T, sondern kleinen, engagierten und hochqualifizierten Startup-Unternehmen mit unkonventionellen Ideen. Warum sollte nicht versucht werden, eine bewusst risikoorientierte Förderung hochqualifizierter, kleiner, agiler Innovationsteams durchzuführen, die in der Gesamtschau möglicherweise bessere Ergebnisse liefert? Selbstverständlich sollte das Eingehen derartiger Risiken auch mit einer adäquaten Erfolgsbeteiligung verbunden werden. Wenn man zudem diese kleinen Innovationsteams durch eine agile Dachorganisation (keine Behörde!) beratend unterstützen und koordinieren würde, ließen sich weitere Synergieeffekte und eventuell neue Produktideen oder Geschäftsmodelle generieren („Ideenbrüter").

Fachkräftemangel

Das Problem des Fachkräftemangels im IT-Bereich lässt sich kurzfristig sicher nicht umfassend lösen, sondern erfordert Anstrengungen und Reformen im Bildungs- und Ausbildungsbereich. Dabei reicht es nicht aus, lediglich zusätzliche Studienplätze in Informatik, Wirtschaftsinformatik, Angewandte Informatik etc. einzurichten. Bereits in der Schule müssten die Neigung und das Interesse an solchen Fächern und Inhalten stärker geweckt und Kompetenzen systematisch und gezielt aufgebaut und gefördert werden, insbesondere bei den in mathematisch-technischen Fächern bis heute unterrepräsentierten Frauen. Dafür braucht es wiederum geeignetes Ausbildungs- und Lehrpersonal.

Anforderungen an den Datenschutz. Wem gehören die Daten?

An dem Beispiel der Kraftfahrzeuge ist im Übergang von der Nicht-IoT-Welt in die IoT-Welt ein weiteres Problem zu erkennen, das aus Gründen der Akzeptanz in der Bevölkerung und der Aufrechterhaltung einer demokratischen Wirtschafts- und Gesellschaftsordnung zwingend für alle unterschiedlichen Interessengruppen gelöst werden muss: der Datenschutz.

Datenschutz und Dateneigentum

Am erwähnten Beispiel der durch Fahrzeuge gesammelten Daten und ihrer Verwendung wird die Frage virulent, wer eigentlich auf die Objektdaten zugreifen darf. Wem gehören diese Daten? Wer hat die Kontrolle über die Daten, wenn das Objekt selbst (ein Fahrzeug, ein Container, ein Kühlschrank, ein Sportschuh) kein Träger eines Rechtsguts bzw. Rechtssubjekt sein kann? Gehören die Daten dem Hersteller, der aus ihnen Wissen zur Kundennutzung seiner Produkte, der Produktqualität und

zur Produktverbesserung generieren kann? Oder dem Software-Lizenzgeber, dessen Betriebssystem die Produktnutzung steuert (z.B. Apple für iPhones)? Oder gehören die mit dem Objekt verknüpften Daten dem Eigentümer des Objektes (des Fahrzeugs), der die rechtliche Verfügungsgewalt über das Objekt hat und der das Produkt gekauft hat? Kann er den Zugriff auf die mit dem Objekt verknüpften Daten beliebig öffnen bzw. einschränken? Oder kann eine übergeordnete Instanz, etwa die Verkehrsleitzentrale einer Stadt, ein Versicherungsunternehmen oder staatliche Stellen, wie das Finanzamt, der Zoll oder die Polizei, auf diese Daten zugreifen? Verschärft wird diese Problematik dadurch, dass die Daten eines Objekts (Fahrzeug, Kamera, Fitnesstracker etc.) nicht unbedingt im Objekt selbst (etwa einem Speicherchip) abgelegt sein müssen (und damit physisch mit dem Objekt verbunden sind), sondern nach der Erfassung sofort an eine IoT-Instanz oder in eine Daten-Cloud weitergeleitet werden. Der Cloud-Service-Anbieter verwaltet diese Daten in gesammelter Form und könnte sie, sofern nicht verschlüsselt, auch auswerten. Und dies möglicherweise ohne explizite Autorisierung oder sogar ohne Wissen des Objekteigentümers.

Unautorisierte und unwissentliche Datenweiterleitung

Diese Art der unautorisierten und unwissentlichen Datenweiterleitung von Objektdaten und ihre externe Verwertung mögen als unglaubliches und unverfrorenes, theoretisches Szenario erscheinen. Es ist aber längst Realität. Wenn Google „übliche" Besucherzahlen von Geschäften oder Restaurants bei Suchanfragen automatisch bereitstellt, stammen diese Informationen aus solchen Datenquellen. Objekte, in diesem Fall Smartphones, werden lokalisiert und getrackt, ohne dass dies dem Smartphone-Besitzer bewusst ist. Verknüpft man die erfassten Lokalisationsdaten von Smartphones mit den (festen und bekannten) geographischen Positionsdaten der Beobachtungsobjekte (eines Restaurants, Shops, Zoos etc.) erhält man eine detaillierte Übersicht über die Besuchsintensität der Objekte in den jeweiligen Zeiträumen. Dies erfolgt ohne explizites Einverständnis und oft sogar ohne Wissen des Verantwortlichen für das Beobachtungsobjekt (des Shop-Betreibers, Restaurantbesitzers oder -pächters etc.). Auch wenn der Google-Nutzer lediglich aggregierte Daten zur Besuchsintensität für einzelne Zeiträume erhält, so berechnet Google diese unter Verwendung objektindividueller Identifikationsdaten (z.B. Mobilfunknummer oder Geräte-ID). Das heißt, Google weiß nicht nur, wie viele Besucher derzeit in einem Shop sind, sondern auch welche Objekte – sprich Smartphones – sich derzeit dort befinden. Google weiß auch, wer sich zu welcher Zeit jemals dort befunden hat und wie lange er sich aufgehalten hat!

Objekt- und Personendaten

Das Argument, es seien doch „nur" Objektdaten und nicht von Datenschutzvorschriften wie der Europäischen Datenschutzgrundverordnung erfasste Personendaten, ist angesichts der Verknüpfungsmöglichkeiten absurd. Mit einem Smartphone oder einem Fahrzeug ist zumeist nur eine Person, eventuell eine kleine, leicht identifizierbare Personengruppe (z.B. Familie) assoziiert. Auch wenn nur reine Objektdaten (Lokalisierung, Status, Umweltdaten) erfasst werden, mutieren diese über mehr oder weniger komplexe Zuordnungsfunktionen zu personenbezogenen Daten, die eigentlich besonderen datenschutzrechtlichen Bestimmungen unterliegen müssten. Mit leistungsfähigen Mustererkennungsverfahren (z.B. Neuronale Netze und *Deep Learning*) ist es nicht schwierig, aus einer Gruppe die in einem bestimmten Zeitraum relevante Person zu einem Objekt zu identifizieren – durch typische, individuelle Verhaltensmuster bzw. Nutzerprofile, die wie Fingerabdrücke verwendet werden können (bei Fahrzeugen etwa Brems- und Beschleunigungsverhalten, Durchschnittsgeschwindigkeit, typische Fahrdauer etc.). Insofern müssen zumindest „personennahe" Objektdaten wie persönliche Daten behandelt werden.

Gratwanderung: Datenschutz

Allerdings ist zu bedenken, dass ein zu restriktiver Datenschutz IoT-Systeme lahmlegen könnte (Weinberg et al., 2015). Ihr effektives Funktionieren ist auf die Bereitstellung entsprechender Daten zwingend angewiesen und oftmals wesentlicher Teil der Geschäftsmodelle von IoT-Unternehmen. Je stärker assistenzbezogen und je genauer IoT-Services auf die persönlichen Bedürfnisse des Anwenders zugeschnitten sein sollen (bei Smart Healthcare-Systemen zwingend notwendig), umso mehr personenbezogene Daten braucht es. In derartigen Fällen sollte jeder Anwender bewusst und aktiv darüber befinden, wie weit seine Bereitschaft zur Datenüberlassung geht, um diese Dienste nutzen zu können.

Anforderungen an Autonomie und Verantwortlichkeit. Wer kontrolliert die Objekte?

Ein über Datensicherheit und Datenschutz hinausgehender, damit aber eng verknüpfter Aspekt betrifft die Frage, wer eigentlich die Objekte eines IoT-Systems kontrolliert. Wer ist für die Folgen von Objektaktivitäten verantwortlich? Was bei traditionellen, klassischen Produkten mit ihrer lokalen Autonomie selbstverständlich war, nämlich, dass der Besitzer der Produkte sie auch vollständig und eigenständig kontrollieren konnte und damit Folgen verantwortete, ist bei smarten Objekten, insbesondere bei solchen in einem IoT-System, keineswegs klar. Oft funktionieren smarte Produkte nur noch mit einer entsprechenden Software und mit einer zumindest temporären Anbindung an das Kommunikationsnetz. Welchen Einfluss haben dann die Hersteller oder Vertreiber der für die Funktionsfähigkeit elementaren Software? Sie kennen als einzige vollständig ihre Programme und Algorithmen und brauchen für Programm-Updates Zugriffsmöglichkeiten. Wer verantwortet Programmfehler, die zu Schäden durch die von diesen Programmen gesteuerten Objekten führen, wenn durch Softwarefehler in einem Smart Health-System Patienten geschädigt werden oder wenn durch den Ausfall von Ampelsystemen oder autonom fahrenden Fahrzeugen das komplette Verkehrssystem einer Stadt oder Region zusammenbricht? Softwarefehler in einem nicht einsehbaren Programm ist die eine Seite des Problems, bewusste Manipulations- und Eingriffsmöglichkeiten durch die Softwarehersteller oder Hacker die andere. Sie wären in der Lage, aus welchen Motiven auch immer, ein smartes Objekt bewusst außer Funktion zu setzen oder gar unautorisiert fernzusteuern. So könnten sicherheitsrelevante Objekte (z.B. Flugzeuge, Militärfahrzeuge) durch ein Softwareupdate oder eine von Anfang an eingeplante, heimliche Backdoor (Teil einer Software, der einen Zugang zum Programm unter Umgehung der normalen Zugriffssicherung ermöglicht) außer Betrieb gesetzt werden. In einfacherer Form wird dies bereits heute bei einigen Militärflugzeugen praktiziert, wo man für jeden Start einen jeweils neu beim Hersteller anzufordernden Sicherheitscode benötigt.

Verantwortung und Haftung

Auch hier ist dringend Handlungsbedarf vonnöten. Eine systemrelevante Software sollte nicht mehr als Blackbox gekauft bzw. genutzt werden: Die Zuständigen brauchen vollständigen Einblick in die hochkomplexen Programme. Unkontrollierte und unautorisierte Backdoor-Zutritte müssen untersagt werden. Je nach Anwendungsbereich sind zudem Maßnahmen zur Risikobegrenzung (z.B. Notfallpläne, unabhängige, objektautonome Mindestfunktionalitäten) aufzubauen und einzurichten.

Fazit

Treiber der Digitalisierung

Internet of Things ist wesentlicher Treiber und Bestandteil der künftigen Digitalisierung von Wirtschaft und Gesellschaft. IoT erweitert das Internet als globales Kommunikationsnetz, indem smarte Produkte und Gegenstände (things) als weitere „Teilnehmer" bzw. „Kommunikationspartner" integriert werden. Sie sind zum einen in der Lage, eine immense Menge zusätzlicher, vielfältiger Daten zu erfassen und im Netz für Auswertungen bereitzustellen. Zum anderen lassen sich die Objekte und ihr Zustand auch von überall her über das Kommunikationsnetz gezielt ansprechen und steuern. Hierdurch eröffnen sich neue, innovative Services und Geschäftsmodelle (Huber/Kaiser, 2015), die die Digitalisierung von Wirtschaft und Gesellschaft vorantreiben werden und zu erheblichen Wohlfahrtsgewinnen, aber auch zu schwierigen Umbrüchen in der Arbeitswelt und der gesellschaftlichen Organisation führen können. Aufgrund der vielfältigen, global ausgerichteten Verflechtungen zwischen den Objekten und Instanzen sowie ihrer Abhängigkeit von koordinierenden Steuerungseinheiten und ihren Softwareprogrammen steigen die Systemrisiken erheblich. Datensicherheit und Datenschutz werden vor neue, hohe Herausforderungen gestellt.

Technologierat

Um diese divergierenden und konfliktären Anforderungen und Interessen systematisch analysieren und ihnen begegnen zu können, wäre die Einrichtung eines alle Stakeholder berücksichtigenden Gremiums, eines „Technologie- und Ethikrates", sinnvoll. Dieser sollte nicht, wie ähnliche bereits existierende Gremien, in erster Linie bremsend wirken, sondern beide Facetten der IoT – die immensen ökonomisch-gesellschaftlichen Potentiale wie auch die Risiken – gleichermaßen in den Fokus nehmen und versuchen, eine Art gesellschaftlichen Konsens für IoT-Applikationen zu erarbeiten. Er sollte gezielt die Chancen der IoT-Technologie verdeutlichen und fördern, positive und negative, wirtschaftliche und gesellschaftliche Folgen analytisch untersuchen und die berechtigten Bedenken und Risiken für Einzelne, die Gesellschaft und die Wirtschaft kritisch diskutieren. Zielsetzung wäre die Erarbeitung entsprechender Rahmenbedingungen (herstellerübergreifende Sicherheitskonzepte, Datenschutzvorgaben etc.) und Handlungsempfehlungen zur IoT-Entwicklung und -Nutzung für die Politik und ihre Gremien.

LITERATUR:

- *Ashton, K. (2009). That "internet of things" thing. In RFID Journal, 22(7), S. 97–114.*
- *Atzori, L., Iera, A., Morabito, G. (2017): Understanding the Internet of Things: definition, potentials, and societal role of a fast evolving paradigm. In: Ad hoc Networks, 56 (2017), S. 122–144.*
- *Bassi, A.; Bauer, M.; Fiedler, M., Kramp, T., van Kranenburg, R., Lange, S., Meissner, S. (Hrsg.) (2013): Enabling Things to Talk - Designing IoT solutions with the IoT Architectural Reference Model. Berlin, Heidelberg: Springer Berlin Heidelberg.*
- *Huber, D., Kaiser, T. (2015). Wie das Internet der Dinge neue Geschäftsmodelle ermöglicht. In HMD - Praxis der Wirtschaftsinformatik, 52(5), S. 681–689.*
- *Lee, I., & Lee, K. (2015). The internet of things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, 58(4), S. 431–440.*
- *McAfee, A., & Brynjolfsson, E. (2012). Big data: The management revolution. Harvard Business Review, 90(10), S. 60–68.*
- *Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012): Internet of things: Vision, applications, and research challenges. In Ad Hoc Networks, 10(2012), S. 1497–1516.*
- *Ng, I.C.L., Wakenshaw, S.Y.L. (2017): The Internet-of-Things: Review and research directions. In: International Journal of Research in Marketing 34 (2017), S. 3–21.*
- *Porter, Michael; Heppelmann, James (2014): How smart, connected products are trans-forming competition. In: Harvard Business Review, Heft 11 (2014), S. 64–88.*
- *Saarikko, Ted, Westergren, Ulrika H., Blomquist, Tomas (2017): The Internet of Things: Are you ready for what's coming? In Business Horizons 60 (2017), S. 667–676.*
- *Stojkoska, B.L.R., Trivodaliev, K.V. (2017): A review of Internet of Things for smart home: Challenges and solutions. In: Journal of Cleaner Production 140 (2017), S. 1454–1464.*
- *Weinberg, B. D., Milne, G. R., Andonova, Y. G., & Hajjat, F. M. (2015). Internet of things: Convenience vs. privacy and secrecy. Business Horizons, 58(6), S. 615–624.*
- *Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: Threats and challenges. In Security and Communication Networks, 7(12), S. 2728–2742.*

Der Autor

Prof. Dr. Richard Lackes, Lehrstuhl für Wirtschaftsinformatik, TU Dortmund

Konrad-Adenauer-Stiftung e.V.

Ansprechpartner:
Dr. Norbert Arnold
Teamleiter Bildungs- und Wissenschaftspolitik
Hauptabteilung Politik und Beratung
Telefon: +49(0)30/26996-3504
E-Mail: norbert.arnold@kas.de

Postanschrift: Konrad-Adenauer-Stiftung, 10907 Berlin

Herausgeberin: Konrad-Adenauer-Stiftung e.V. 2018, Sankt Augustin/Berlin
Lektorat: Jenny Kahlert, PuB, Konrad-Adenauer-Stiftung
Gestaltung: SWITSCH Kommunikationsdesign, Köln
Satz: yellow too Pasiek Horntrich GbR
Druck: copy print Kopie & Druck GmbH, Berlin
Die Printausgabe wurde bei copy print Kopie & Druck GmbH, Berlin klimaneutral produziert und auf FSC-zertifiziertem Papier gedruckt.
Printed in Germany.
Gedruckt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

ISBN 978-3-95721-442-3

www.kas.de