Das Internet der Dinge: Evolution oder Revolution?

Teil 1 einer Serie

Vorwort:

Shawn DuBravac, Ph.D.

Chief Economist bei der Consumer Electronics Association (CEA) (Wirtschaftsverband für Unterhaltungs- und Haushaltselektronik) und Autor des New York Times-Bestsellers "Digital Destiny: How the New Age of Data Will Transform the Way We Work, Live, and Communicate"

Carlo Ratti, Ph.D.

Director, MIT SENSEable City Lab ,und Designer des Future Food District auf der Weltausstellung Expo 2015 in Mailand

AIG®

CEA® Consumer Electronics Association

Danksagung

Die folgende Veröffentlichung wurde ermöglicht durch die Mitarbeit der Consumer Electronics Association (CEA)® und deren Chefökonom, Dr. Shawn DuBravac, Autor des New York Times-Bestsellers “Digital Destiny: How the New Age of Data Will Transform the Way We Work, Live, and Communicate.”

Außerdem danken wir folgenden AIG Mitarbeitern für ihre wertvollen Beiträge zu diesem Whitepaper:

David Bassi
Lex Baugh
Nicolas Berg
Julien Combeau
Jason Kelly
Erik Nikodem
Garin Pace
Matthew Power
Joe Trotti

Inhaltsverzeichnis

Vorworte

Dr. Shawn DuBravac
ist Chief Economist bei der Consumer Electronics Association (Wirtschaftsverband für Unterhaltungs- und Haushaltselektronik) und Autor des New York Times Bestsellers "Digital Destiny: How the New Age of Data Will Transform the Way We Work, Live, and Communicate."

Wir stehen am Beginn der nächsten industriellen Revolution. Das können wir mit Sicherheit sagen. Doch das sogenannte Internet der Dinge (IoT, Internet of Things) mit seinen vernetzten Maschinen und Geräten wird bisherige technische Errungenschaften wie die Druckerpresse, die Dampfmaschine oder die Erzeugung von Elektrizität noch übertrumpfen. Rund um die Welt, von den Industrie- bis hin zu den Entwicklungsländern, wird es hierdurch erneut zu einem starken wirtschaftlichen Anstieg kommen. Beachtlich ist ebenfalls die Geschwindigkeit, mit der diese Veränderungen voranschreiten. Vor einem Jahrzehnt waren etwa 500 Millionen Geräte mit dem Internet verbunden. Heute gehen wir von 10 bis 20 Milliarden Geräten aus. In fünf Jahren könnten es bereits 40 bis 50 Milliarden sein.

Doch im Gegensatz zu früheren industriellen Revolutionen sind wir uns dieser heute schon bewusst. Das Internet der Dinge ist keine isolierte weltverändernde Erfindung wie die Baumwollentkörnungsmaschine, die seinerzeit die Herstellung von Baumwolle revolutionierte. Heute werden Branchen nicht von einer Innovation überrascht, die ihre Herstellungsverfahren überholt und ihre Produkte überflüssig macht. Stattdessen können alle Branchen und Unternehmen davon profitieren, indem sie IoT-Objekte in ihre jeweiligen Geschäftsmodelle integrieren, um neue, bessere Wege für ihre Geschäftsabläufe zu finden. Das heißt natürlich nicht, dass mit IoT nicht auch Risiken oder Herausforderungen verbunden sind. Neue Branchen werden entstehen, während alte Geschäftsmodelle in Vergessenheit geraten. Unternehmen werden sich auf ein völlig neues Wirtschafts- und Risikoumfeld einstellen müssen. Das IoT-Phänomen ist insofern einzigartig, als vorausdenkende Unternehmen sich jetzt schon darauf vorbereiten und daran anpassen können, um die potenziellen Risiken des neuen Wirtschaftszeitalters zu minimieren.

Der Boom des Internets der Dinge geht mit einem neuen Datenzeitalter Hand in Hand. Zu den wichtigsten Eigenschaften eines „IoT-Gerätes" gehört seine Fähigkeit, Daten über smarte Sensoren zu erfassen und über das Internet zu übermitteln. Wie aus diesem Whitepaper hervorgeht, war der sinkende Preis für Sensoren seit dem Start des neuen Jahrtausends maßgeblich für den Vormarsch des IoT verantwortlich. Kurz gesagt: Sensoren sind heutzutage spottbillig. Dadurch können wir heute riesige Datenmengen erfassen, was früher nicht möglich war.

Laut der norwegischen Forschungsorganisation SINTEF wurden 90 % der weltweiten Daten allein in den vergangenen zwei Jahren generiert. Jede Sekunde werden 205.000 neue Gigabytes generiert, was in etwa 150 Millionen Büchern entspricht. Diese Datenmengen entstehen in einer Welt mit 10 bis 20 Milliarden verbundenen und mit smarten Sensoren ausgestatteten Geräten. Auf der ganzen Welt werden mehr Daten generiert als je zuvor und - was noch wichtiger ist - wir übertragen und verwenden diese Daten immer häufiger. Stellen Sie sich nun eine Zukunft mit 40 bis 50 Milliarden IoT-Objekten vor.

Wettbewerbsvorteile und zukünftige Erfolge werden davon bestimmt werden, wie Branchen oder Unternehmen mit diesem riesigen Datenaufkommen von IoT-Objekten umgehen. Jedes Unternehmen wird in irgendeiner Form seine Strategie, Entscheidungen und Prognosen auf Daten stützen. Daten werden die Verantwortlichen für Versorgungsketten über Sicherheitslücken oder ineffiziente Prozesse in der Versorgungskette informieren. Marketingfirmen lesen in den Daten, ob ihre Kunden auf die aktuelle Kampagne ansprechen. Dank detaillierter Daten können Unternehmen mehr Einblick in ihre Prozesse und Produkte erhalten als je zuvor. Im Herzen dieser neuen industriellen und Datenrevolution liegt die Versicherungsbranche. Schon seit Jahrzehnten verwenden internationale Versicherungsunternehmen große Datenmengen, um Risiken zu verstehen und zu reduzieren. Nun, da immer mehr IoT-Objekte auf allen Ebenen der Weltwirtschaft zu finden sind, können Versicherungsgesellschaften diese Daten optimal analysieren und wichtige Erkenntnisse für zukünftige Entscheidungen gewinnen. Diese Erkenntnisse könnten dazu beitragen, die Welt zu einem noch sichereren und produktiveren Ort zu machen, als wir es uns je erträumt haben.

Dr. Carlo Ratti,
Director, MIT SENSEable City Lab, und Designer des Future Food District auf der Weltausstellung Expo 2015 in Mailand.

Seit Jahrzehnten werden wir von immer neuen und besseren Gadgets geblendet. Leistungsfähigere Computer; bessere Musik-Player; hochauflösendere Fernsehgeräte und noch smartere Telefone. Dieser Trend lässt Technologie wie eine lange Reihe von wunderbaren Spielereien erscheinen, die es in unserem Leben noch nie vorher gegeben hat. Man könnte annehmen, dass das so weitergeht; dass die nächste revolutionäre Innovation in einem weiteren Plastik- oder Metallbehälter daherkommt. Doch vielleicht kommt es auch ganz anders.

In der Tat steht eine weitere technologische Revolution bevor, aber sie ist viel einfacher und zur gleichen Zeit vermutlich bahnbrechender als ein neues innovatives Einzelgerät. Wir steuern auf eine datengetriebene Revolution zu. Diese könnte viele Ineffizienzen, Hindernisse, Gefahren und unsichere Arbeitsweisen des modernen Lebens beseitigen. Und die weltweite Versicherungsindustrie verspricht, im Zentrum dieser technologischen Revolution eine maßgebliche Rolle zu spielen.

Ob Sie es das „Internet der Dinge" (Internet of Things – IoT) oder das „Internet aller Dinge" nennen: Es geht bei diesem Veränderungsprozess um den stetigen, aber unaufhaltsamen Vormarsch von vernetzten und mit Sensoren ausgestatteten Objekten – kurzum die Online-Digitalisierung unserer physischen Welt. Eigenständige Objekte können kontinuierlich große Mengen an Daten aufnehmen, analysieren und übermitteln, die sie in ihrer Umgebung erfasst haben. Im Gegenzug reagieren Volkswirtschaften, Städte, Unternehmen und Menschen auf diesen Informationsfluss – wodurch sich eine noch nie dagewesene Fülle an Möglichkeiten ergibt.

Das Internet der Dinge führt zu umfassenden digitalen Netzwerken innerhalb des physischen Raums – dem vernetzten Lebensnerv der „Smart City". Das umfasst nicht nur Netzwerke kommunaler Dienstleistungen, wie etwa Strom und Wasser. Wirklich „smarte" Städte kombinieren Elemente aller kommunalen Zielgruppen, darunter Bürger, die Regierung und Unternehmen. Und einmal mehr entsteht in verschiedenen Teilen der Welt ein breites Spektrum von Implementierungsmodellen.

In den Vereinigten Staaten war der grundlegende Gedanke smarter Stadträume von zentraler Bedeutung für die derzeitige Generation erfolgreicher Unternehmensgründungen. Die Stadtplanung selbst hat positive Auswirkungen auf die grundlegende Umgestaltung der meisten Aspekte des städtischen Lebens – von der Mobilität über die Optimierung des Energieverbrauchs bis zur persönlichen Gesundheit. Diese neuen Initiativen erhalten große Unterstützung von Risikokapitalfonds.

In Südamerika, Asien und Europa ist man dabei, den möglichen Nutzen von „smarten" Städten zu ermitteln und arbeitet daran, erhebliche Investitionen in diesem Bereich zu erschließen. Rio de Janeiro baut in seinem „Smart Operations"-Center Kapazitäten auf. Singapur ist gerade dabei, ein ehrgeiziges „Smart Nation"-Projekt zu starten.
Das Programm Horizont 2020 der Europäischen Union hat für die Jahre 2014 - 2016 15 Mrd. Euro bereitgestellt - beträchtliche Ressourcen für die Idee von vernetzten, intelligenten Städten - besonders in einer Zeit fiskalischer Einschränkungen.

Die Zukunft wird zeigen, wie sich diese verschiedenen Modelle entwickeln werden. Dabei besteht kein Zweifel, dass die weltweite Versicherungsindustrie das Potenzial hat, hierbei eine wesentliche Rolle zu spielen. Wie schätzen wir Risiken ein, die mit dem zum Großteil unerforschten Gebiet des Internets der Dinge einhergehen? Wie können wir Herausforderungen verstehen, die grundlegende Veränderungen bei der Verantwortung für und dem Management von Risiken auslösen könnten, die wir bereits heute kennen?
Das ist das Gebiet, auf dem Versicherer eine Vorreiterrolle spielen können – nicht allein um ihrer Branche willen, sondern um anderen Branchen, Regierungen und insbesondere den Bürgern beratend zur Seite zu stehen.

Summary

Laut Branchenanalysten sind heute zwischen 10 und 20 Milliarden Objekte mit dem Internet vernetzt. Dieses Ökosystem vernetzter Objekte bildet die Grundlage für das Internet der Dinge (Englisch: „Internet of Things", IoT). Obwohl die Technologie für das IoT schon seit Jahren besteht, befinden wir uns noch in einer sehr frühen Phase. Die Anzahl der heute vernetzten Objekte verblasst im Vergleich zu der Anzahl der Objekte, die in nur fünf Jahren mit dem IoT vernetzt sein werden. Je nach Schätzung werden bis zum Jahr 2020 40 bis 50 Milliarden Dinge mit dem IoT verbunden sein; und zwar alles, von Tassen und Kugelschreibern bis hin zu Häusern, Autos und Industriemaschinen.

Das IoT bietet aufregende neue Möglichkeiten für Unternehmen. Viele davon aber bleiben für den Laien unverständlich. Die Medien konzentrieren sich vorzugsweise auf die Verbraucherseite des IoT, wie z. B. auf den Markt für „Wearables", für tragbare Computersysteme. Selbstverständlich sind diese Produkte wichtige Bestandteile des IoT-Universums, aber sie bleiben dennoch eine Nische. Unternehmen, die nicht an Endverbraucher verkaufen, glauben fälschlicherweise, das IoT habe ihnen nichts zu bieten. Allerdings wird das IoT die Geschäftsebenen aller Branchen verändern, von alltäglichen bis zu tiefgreifenden Dingen. Probleme, mit denen Unternehmen seit Jahrhunderten ringen, werden dramatisch entschärft und in vielen Fällen oft vollständig verschwinden. Gemeinsam mit anderen technischen Entwicklungen, wie Cloud Computing, Smart Grids, Nanotechnologie und Robotertechnik ist das IoT ein gewaltiger Schritt. Es wird unsere Wirtschaftssysteme effizienter, produktiver, sicherer und profitabler machen.

Laut einer Studie von RAND Europe liegen die oberen Schätzwerte für das wirtschaftliche Potenzial des IoT bis 2020 über alle Branchen hinweg zwischen 1,09 Billionen EUR (ca. 1,4 Billionen USD) und 11,2 Billionen EUR (ca. 14,4 Billionen USD) – also in etwa das aktuelle Bruttosozialprodukt der Europäischen Union. Bis dahin wird das IoT nicht bloß ein isolierter Bereich der IT-Branche sein, sondern DER Antrieb für den Großteil der Weltwirtschaft. In fünf Jahren wird kaum ein Wirtschaftszweig nicht durch das IoT verändert worden sein. Selbst heute gibt es kaum Branchen, die durch die Integration des IoT gar nichts zu gewinnen hätten. Es gibt natürlich auch einige wegweisende Branchen, in denen das IoT schon heute unerlässlich für deren Arbeitsabläufe geworden ist. Wie wir sehen werden, helfen uns diese Vorreiter-Branchen, die Möglichkeiten des IoT in den kommenden Jahren auszuloten.

Natürlich beinhalten Chancen immer auch Risiken; beim IoT sind diese Risiken mindestens so wichtig wie die Gewinne. Von Cyberangriffen bis hin zu Eigentumsfragen und der Produkthaftung. Unternehmen können es sich nicht leisten, unvorbereitet in diese neue technologische Welt einzutreten. Beispielsweise ist jedes Gerät mit Internetzugang eine mögliche Einstiegsstelle für Cyber-Kriminelle in das firmeninterne System. Ähnlich gefährlich: In einer Welt, in der Maschinen Menschen Entscheidungen abnehmen und Sensoren kontinuierlich Daten erfassen, werden Haftung, psychische Schäden und Datenschutz zu ernsten Themen.

Diese Whitepaper Serie soll sowohl über die Chancen als auch über die potenziellen Risiken des IoT informieren. Selbst wenn wir nicht mit Sicherheit sagen können, was in fünf Jahren auf die Geschäftswelt zukommt – wir können die Themen antizipieren, die bestimmend sein werden. Die IoT-Welt wird ökonomisch komplexer und die Rahmenbedingungen, die Unternehmen und Regierungen zur Stärkung von Wachstum und Wettbewerb festgelegt haben, werden langfristig nicht mehr anwendbar sein. Das IoT wird in allen Ländern und Wirtschaftsbereichen der Welt wesentliche Auswirkungen haben, selbst für Entwicklungsländer, die historisch meistens vom technischen Fortschritt ausgeschlossen blieben. Dr. Shawn DuBravac, Chefökonom der Consumer Electronics Association in Arlington, Va, schreibt in seinem Bestseller „Digital Destiny: How the New Age of Data Will Transform the Way We Work, Live, and Communicate" (Deutsch: „Digitale Bestimmung: Wie die neue Ära der Daten unsere Art zu arbeiten, zu leben und zu kommunizieren transformieren wird"):

> „Es wird nicht nur *vielleicht* passieren, je nachdem für welchen Weg wir uns entscheiden. Es *wird* passieren, egal welchen Weg wir wählen."

Damit Unternehmen das enorme Potenzial des IoT voll ausschöpfen können, sollten sie sich auf die kommenden Risiken vorbereiten. Die Versicherungsbranche ist besonders gut aufgestellt, um Unternehmen bei der Navigation durch diese neue Techniklandschaft zu unterstützen. Viele Elemente des IoT werden schon lange von Versicherern verwendet, um durch bessere Einschätzung von Risiken die Sicherheit zu verbessern. Und so wie Versicherungen Unternehmen helfen sich an die ändernden Gegebenheiten anzupassen, so werden auch sie selbst sich anpassen, um ihre Kernprozesse und -funktionen zu verbessern.

Was ist das Internet der Dinge?

Der Begriff „Internet of Things" ist nicht neu. Schon 1999 prägte ihn der britische Technikpionier Kevin Ashton, der damals als Assistant Brand Manager bei Procter & Gamble arbeitete. 2007 erläuterte Ashton seinen Begriff in einem Artikel:

> „Hätten wir Computer, die alles über Dinge wüssten, die es zu wissen gibt – unter Verwendung von Daten, die sie ohne jegliche Hilfe von uns gesammelt haben – könnten wir alles darüber erfahren und so Abfall verringern und Verluste und Kosten massiv reduzieren. Dann wüssten wir, welche Dinge ersetzt, repariert, zurückgerufen werden müssten und, ob sie neu sind oder ihre besten Zeiten schon hinter sich haben.
>
> Wir müssen Computer dazu befähigen, selbst Informationen zu sammeln, damit sie unsere wunderbar unvorhersehbare Welt eigenständig sehen, hören und riechen können. RFID und Sensortechnik lassen unsere Computer die Welt observieren, identifizieren und verstehen – ohne die Unzulänglichkeiten menschlicher Dateneingabe." [i]

Später, 2012, versuchte RAND Europe in einem Forschungsbericht an die Europäische Kommission, das IoT weiter zu definieren. Der Bericht erläuterte:

> „Das Internet der Dinge baut das heutige Internet zu einem allgegenwärtigen, selbst-organisierenden Netzwerk verbundener, identifizierbarer und ansprechbarer physischer Objekte aus. Es erlaubt die Anwendungsentwicklung quer durch alle wichtigen vertikalen Branchensegmente unter Verwendung eingebauter Chips, Sensoren, Ansteuerungen und Low-Cost-Miniaturisierung ."[ii]

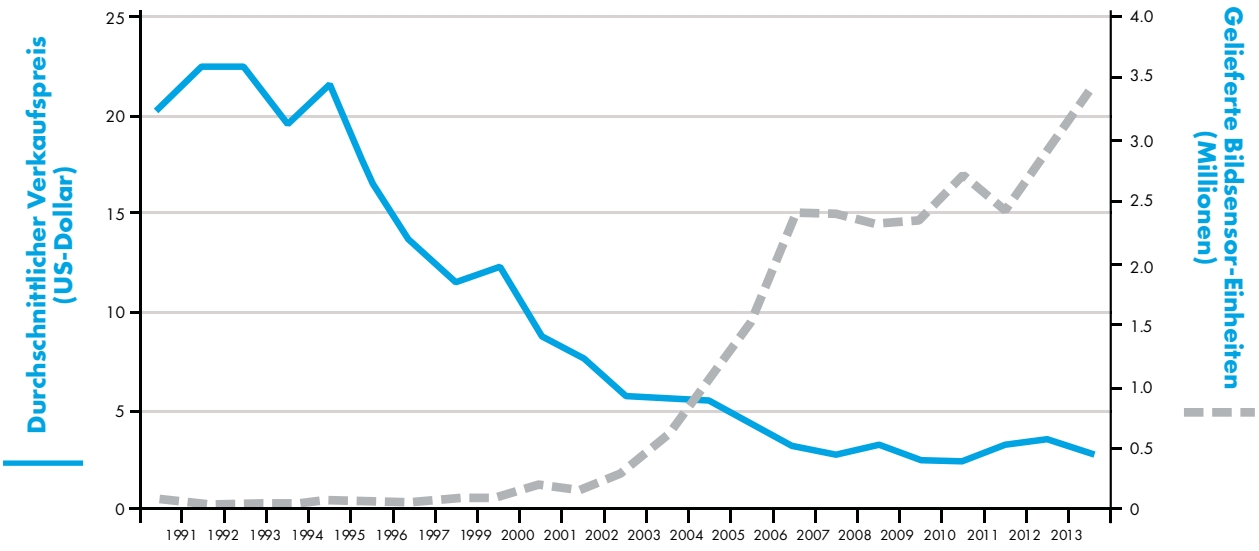
Die Definitionen von Ashton und RAND sind gleichermaßen korrekt. Allerdings dehnt RAND Ashtons ursprüngliches Konzept von „befähigten Computern" auch auf „physische Objekte" aus. Mit anderen Worten, das Internet der Dinge basiert nicht nur auf Computern. Stattdessen kann jeder Gegenstand, selbst der menschliche Körper, Teil des IoT werden, wenn er mit den richtigen elektronischen Teilen ausgestattet wird. Diese Teile können variieren, je nach Funktion, die sie ausführen sollen. Aber sie fallen in zwei große Kategorien:
1.) Das Objekt muss fähig sein, Daten zu erfassen, in der Regel durch Sensoren; und
2.) muss es fähig sein, Daten über das Internet an welchen Ort auch immer zu übertragen.
Ein Sensor und eine Verbindung sind also die zwei wichtigsten elektronischen „Teile" eines IoT-Objekts.

Obwohl diese Technologie seit mehr als einem Jahrzehnt existiert, waren zwei Entwicklungen in den letzten zwanzig Jahren die wichtigsten Antriebe für das IoT als Paradigmen veränderndes Phänomen. Zum einen das explosive Wachstum mobiler Geräte und Applikationen und zum anderen die breite Verfügbarkeit von drahtlosem Internetzugang.

In einem Bericht von Cisco aus dem Jahr 2011 steht, dass im Jahr 2003 ca. 500 Millionen Geräte mit dem Internet verbunden waren, beinahe ausschließlich PCs. Teilte man die Zahl der vernetzten Geräte durch die Weltbevölkerung (damals 6,3 Milliarden), gab es weniger als ein Gerät (0,08) pro Person auf der Erde.[iii] Bis 2010 explodierte der Markt für Tablets und Smartphones. Die Zahl vernetzter Geräte erhöhte sich auf 12,5 Milliarden, obwohl die Weltbevölkerung nur auf 6,8 Milliarden anstieg. In nur sieben Jahren hatte sich die Anzahl vernetzter Geräte pro Person auf der Welt um 2.250 % erhöht, von 0,08 auf 1,8.
In Europa, mit der höchsten weltweiten Durchdringung des Marktes mit Handys, gibt es 1,1 Milliarden Mobilfunkverträge für eine Bevölkerung von knapp 800 Millionen Menschen.[iv] Das sind ca. 1,3 Mobilfunkverträge pro Kopf. Deutlicher: In Europa gibt es mehr Mobilfunkverträge als Menschen.

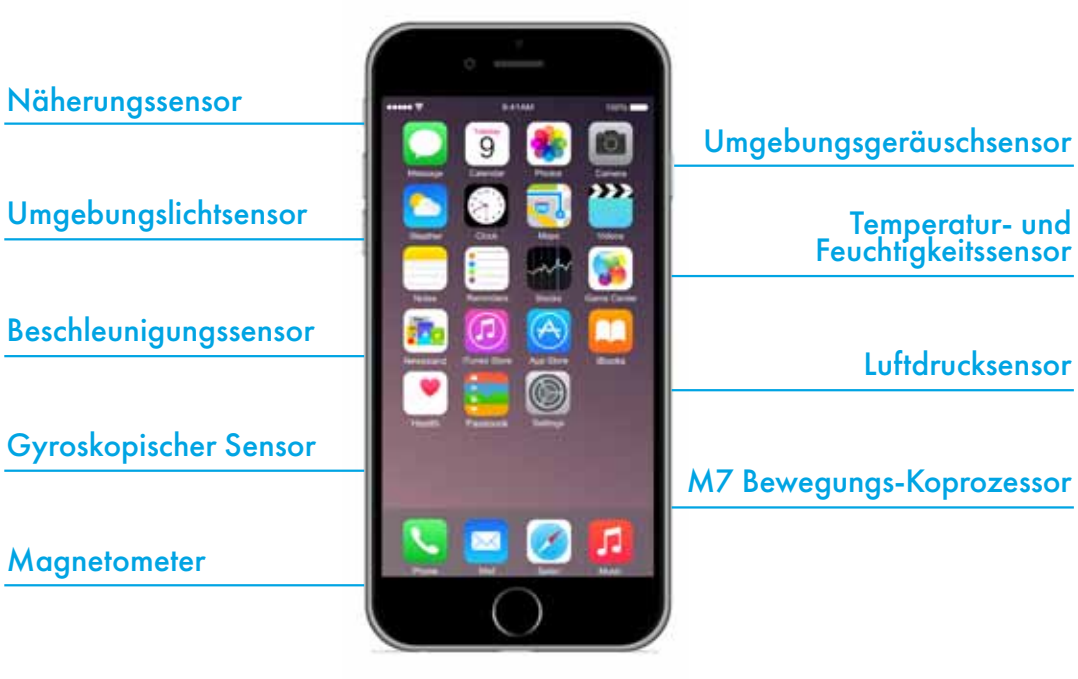
Die andere Entwicklung reicht noch weiter zurück als die Mobilfunktechnologie: Sensoren. Allerdings waren Sensoren während des 20. Jahrhunderts meist so teuer, dass sie nur in High-End-Geräten eingesetzt wurden. Anfang der 1990er Jahre kosteten Solid-State-Bildsensoren zwischen 20 und 25 USD. Zum Ende des Jahrzehnts kosteten sie nur noch 5 USD. Der Markt für Digitalkameras wuchs infolgedessen enorm. Andere Sensoren, wie die in Ihrem Smartphone, erlebten eine ähnliche Entwicklung des Kosten-Leistungs-Verhältnisses. 2007 kosteten Beschleunigungssensoren für eine einzige Bewegungsachse ca. 7 USD. Heutige Beschleunigungssensoren messen sechs Bewegungsachsen und kosten weniger als 50 US-Cent

SINKENDE PREISE ENTFACHEN DEN ABSATZ



Quelle: DuBravac, Shawn. “Digital Destiny.” S. 78

Natürlich wären heutige Smartphones ohne die vielen Sensoren in jedem Gerät alles andere als „smart". Aktuelle Smartphones beinhalten zwischen fünf und neun Sensoren, je nach Modell. Dazu gehören:



Vor fünfzehn Jahren hätte der Einbau nur eines einzigen dieser Sensoren (geschweige denn neun davon) die Produkte für Durchschnittskunden unerschwinglich gemacht. Heute kosten all diese Sensoren insgesamt weniger als 5 USD; der billigste fängt bei 7 US-Cent an.[v]

Allerdings können Sensoren weit mehr, als nur unseren Handys nette Funktionen zu verleihen. Tatsächlich sind sie ein kritischer Bestandteil, der das IoT „aktiviert". Durch kontinuierliche Erfassung von Umgebungsdaten ersetzt der Sensor den Menschen als Haupteingabequelle für Daten in den Computer. Weil Sensoren Daten in für Menschen unerreichbarer Geschwindigkeit und Menge erfassen können, führten sie zu dem Phänomen „Big Data", also der Ansammlung und Auswertung extrem großer Datensätze.

Was ist „Big Data"? Es ist alles und jedes, was uns umgibt. Konkret: Die Daten, die heutige Sensoren erfassen können (und Menschen nicht), revolutionieren die Wirtschaft und Geschäftsprozesse. Autohersteller weltweit nutzen Sensoren nicht nur in eigenen Autos, sondern auch in ihren Produktionsstätten, wo sie autonome Maschinen unterstützen und die Sicherheit der Werksmitarbeiter verbessern.

Andere Faktoren, die das IoT besonders in Handel und Industrie unterstützen, sind kostensparende Cloud-Speicher sowie die an Bedeutung gewinnende Datenanalyse, die es ermöglichen, dass Organisationen Informationen aus enorm großen Datenmengen beziehen und verwalten können.[vi] Und wir sind nicht weit von den wichtigsten Playern entfernt – den Sensoren. Sensoren erfassen Daten, und mobile Internetverbindungen übertragen die Daten an andere Geräte oder in die Cloud.

Wir müssen anerkennen, das IoT ist nicht nur ein einziges, leicht zu erklärendes Phänomen. Das IoT umfasst verschiedenste Segmente und Märkte. Für den Verbraucher bedeutet das IoT tragbare Computertechnologie und „smarte" Applikationen, wie Temperaturregler und Fernseher. In der Industrie ermöglicht das IoT autonome Maschinen und sensorische Anlagen. Im Handel bedeutet IoT Big Data und Marktanalytik. In Kürze: Von der Herstellung bis zum Endprodukt, das IoT ist so vielfältig wie die globale Wirtschaft selbst.

Nun müssen wir uns fragen: Wie können Unternehmen diese vernetzten Objekte verwenden, um ihre Prozesse zu verbessern, die Produktivität zu erhöhen, Kosten zu reduzieren und Risiken zu vermeiden?

Eine neues Wirtschaftszeitalter

Um die Chancen des IoT für Unternehmen zu erkennen, müssen wir erst seine makroökonomischen Auswirkungen verstehen. Laut einer Studie von RAND Europe für die Europäische Kommission liegen die oberen Schätzwerte für das wirtschaftliche Potenzial des IoT über alle Branchen hinweg zwischen 1,09 Billionen EUR (ca. 1,4 Billionen USD) und 11,2 Billionen EUR (ca. 14,4 Billionen USD) weltweit.[vii] Weiterhin wird der Umsatz mit vernetzten Geräten und Dienstleistungen bis 2020 ca. 2,5 Milliarden USD erreichen, während die geschätzten Gesamtinvestitionen anhand der Zahl vernetzter Geräte – zu heutigen Preisen – mindestens 2 Billionen EUR erreichen wird. Beispielsweise weist die RAND-Studie darauf hin, dass China bereits 625 Mio. EUR (775 Mio. USD) für IoT-Investitionen vorgesehen hat.[viii]

Eins ist sicher: In fünf Jahren wird es keine Branche geben, auf die das IoT keinen direkten Einfluss hat. Die Einführungsgeschwindigkeit – gepaart mit Kundenerwartungen – wird schnell jede Branche ohne IoT (geschweige denn einzelne Firmen) in ein Relikt aus der Vergangenheit verwandeln. Allerdings haben viele Branchen Zeit, das IoT zu verstehen und zu erkennen, wie es ihren langfristigen strategischen Zielen dienlich sein kann.
Mit dem ersten Teil dieser Whitepaper Serie wollen wir den Lesern aktuelle Beispiele aufzeigen, wie bestimmte Branchen das IoT bereits nutzen. Unsere Hoffnung ist, dass die Leser basierend auf den unten genannten Beispielen eine Strategie für ihr eigenes Unternehmen implementieren können.

Weil das IoT für alle Geschäftsbereiche von Nutzen ist, haben wir die Anwendungen des IoT in vier Kategorien eingeteilt:

- Sicherheit
- Effizienz
- Datengestützte Entscheidungsfindung
- Infrastruktur

AUTOMOBILINDUSTRIE

Sicherheit: 2010 berichtete die Weltgesundheitsorganisation, dass 1,24 Millionen Menschen weltweit bei Kfz-Unfällen starben.[ix] Jedes Jahr sterben in Europa 30.000 Menschen bei Kfz-Unfällen[x].
In den USA ist die Zahl ähnlich. In Asien ist das Problem weitaus schlimmer. Allein in China und Indien sterben jährlich mehr als 400.000 Menschen durch Kfz-Unfälle[xi].
Die IoT-Technologie, besonders Sicherheitssensoren an Autos, könnten die weltweiten durch Kfz-Unfälle verursachten Todesfälle drastisch reduzieren.
Weil die große Mehrheit an Kfz-Unfällen aus menschlichem Versagen resultiert, ist das Ziel autonomer Fahrzeuge, menschliche Entscheidungen beim Fahren zu ersetzen.

Im Mai 2015 erklärte die in den USA ansässige deutsche Firma Daimler Trucks North America, dass sie bereit sei, ihren fahrerlosen Freightliner Inspiration Truck auf den Fernstraßen Nevadas zu testen.[xii] Fahrerlose Autos, die von den Firmen Google[xiii] und Tesla[xiv] entwickelt werden, gehen langsam online. Beispielsweise beinhalten sie Sicherheitssensoren, die dem Fahrer einen Rundumblick des Autos geben. Andere arbeiten autonom und schützen das Auto ohne direkte Eingriffe des Fahrers. Autofirmen nutzen die erfassten Daten auch, um sicherere, effizientere Autos zu entwickeln. Während diese Datenerfassung Datenschutzbedenken weckt, sind sie der nächste Schritt in der Entwicklung der Automobile.

FINANZSEKTOR

Effizienz: Pionier beim Einsatz von Mobiltechnologie war der Finanzsektor, um dem Durchschnittskunden das Banking zu vereinfachen. Ein deutliches Beispiel für die Überschneidung zwischen Bankensektor und IoT sind Geldautomaten, die zum Teil mit Sensorik ausgestattet sind. Zukünftig können Nutzer vielleicht mit ihren biometrischen Merkmalen Geld von sensorischen Geldautomaten abheben, ohne jemals die Geldkarte zu zücken. Das IoT verspricht, die Finanztransaktionen eines Kunden mit anderen Aspekten seines Lebens zu verknüpfen. Ein Beispiel ist der Abgleich zwischen Daten aus der Gesundheitsüberwachung und dem Finanzportfolio. Wie Deloitte bemerkte, könnte eine sensorisch erfasste Gesundheitskrise des Nutzers der Bank signalisieren, automatisch das Portfolio zu reorganisieren, um seine finanzielle Risikobelastung zu verringern.[xv]

In einem Bericht aus dem Jahr 2014 über die „Bank of Things" bemerkte Accenture: „Die Bank der Dinge wird die Bedürfnisse des Kunden voraussehen, auf sich ändernde Bedingungen reagieren und schnell passende Lösungen bieten, die dem Kunden helfen, seine Ziele zu erreichen. Sie bleibt vertrauensvoller Berater, Unterstützer und Wertaggregator für die Kunden, handelt aber nun mit einem intimen Verständnis der Bedürfnisse und Vorlieben jedes einzelnen Kunden."[xvi]

TRANSPORT

Sicherheit: Wie der Rest der Transportbranche, statten auch Schifffahrtsunternehmen seit Jahrzehnten ihre Flotten mit verschiedensten Sensoren aus, um kritische Bordsysteme, Wetter- und Seebedingungen sowie die Ladung zu beobachten. Das IoT erlaubt es diesen Sensoren nun, Daten zu sammeln, deren Analyse der Fahrtoptimierung und der Verbesserung von Sicherheit und Ladeprozessen dient.

In einem Beispiel nutzt eine Open-Source-Software die Sensoren eines Schiffs, um Echtzeitpositionsdaten an andere Schiffe und Seeverkehrskoordinierungsstellen an Land zu senden. Die IoT-Software „unterstützt kollaborative Entscheidungen unter den wichtigsten Beteiligten, um die Seefahrt sicherer, effizienter und umweltfreundlicher zu machen", erklärt ein Experte.[xvii]

Datengestützte Entscheidungsfindung: Bei der Fachmesse International Consumer Electronics Show (CES) 2015 enthüllte die schwedische Firma Ericsson eine erweiterte IoT-Lösung für die Seeschifffahrt. Die cloudbasierte Plattform kann Schiffe auf See mit „Landstationen, Wartungsdienstleistern, Kundendienstzentren, Flotten-/Transportpartnern, Häfen und Behörden" verbinden. Die IoT-Lösung kann es Betreibern an Land und auf See ermöglichen, den Kraftstoffverbrauch, die Motorleistung, das Wetter sowie den Verkehr und die Navigation für eine verbesserte Fahrtoptimierung zu überwachen.
Weiterhin kann sie Ort und Zustand bestimmter Ladungen verfolgen. Und durch verbesserte Kommunikation können Unterhaltungsoptionen und Telemedizin sogar das Wohlergehen der Schiffsbesatzung verbessern.[xviii]

PROPERTY (REAL ESTATE)

Effizienz: Für Immobilien gibt es bereits „smarte" Objekte, wie Temperaturregler und andere Geräte, die Hausbesitzern helfen, die Energieeffizienz zu steigern und Nebenkosten zu senken. Je mehr Häuser „connected" werden, umso mehr können wir davon ausgehen, dass sich diese Produkte verbreiten werden. Aber der echte Mehrwert von IoT in Häusern entsteht, wenn verbundene Geräte und andere Haushaltsgegenstände miteinander kommunizieren. Beispielsweise könnte ein „smarter" Temperaturregler die Außentemperatur an das Schranksystem weiterleiten, welches dann zweckmäßge Kleidung für den Tag empfiehlt. Ein weiteres Beispiel ist, wenn ein Heimsystem, nehmen wir wieder den Schrank, sich mit dem Kalender des Nutzers synchronisiert. Der Schrank weiß, ob der Nutzer an diesem Tag ein Meeting hat und wählt die passende Kleidung.

Datengestützte Entscheidungsfindung: In der Immobilienwirtschaft kann ein Haus mit IoT den menschlichen Makler beinahe ersetzen. Es kann sich selbst auf den richtigen Immobilienportalen eintragen und Objektpräsentationen planen, weil es „weiß", wann die Bewohner außer Haus sein werden.[xix] Einige Makler experimentieren bereits mit der iBeacon-Technologie[xx] von Apple und mit „For Sale" Verkaufsschildern. Das Konzept: Ein potenzieller Hauskäufer, der sich in der Nähe eines zu verkaufenden Hauses befindet, erhält sofort eine Nachricht auf sein Smartphone von iBeacon mit Detailinformationen zum Haus. Im Haus kann die iBeacon-Technologie verwendet werden, um potenziellen Kunden Grundrisse, Videoreferenzen der Vorbesitzer und erforderliche Renovierungen anzuzeigen – möglicherweise in Zusammenarbeit mit einem Baumarkt.[xxi]

Infrastruktur: Überflutung, Brand, Verfall der Bausubstanz: Diese Risiken muss jedes Unternehmen akzeptieren. Allerdings kann die IoT-Technologie helfen, besonders durch Sensoren in Risikobereichen, diese beständigen Probleme zu verringern oder in einigen Fällen ganz auszuschalten. Beispielsweise können elektrische Systeme mit Sensoren ausgestattet werden, die den Stromfluss durch ein Gebäude kontrollieren. Wenn ein Kabel oder eine Verbindung ausfällt oder kurz vor dem Ausfall ist und dadurch das Brandrisiko steigt, können die Sensoren automatisch Techniker alarmieren. Immobilienfirmen können IoT-Sensoren in ihren Gebäuden nutzen, um eine Vielzahl von Risiken zu überwachen, beispielsweise gefährliche Gase, Ungezieferbefall, Fehlfunktionen der Lüftungs- und Klimaanlage sowie den allgemeinen Verschleiß. Selbst wenn ein bestimmtes Gebäude im Topzustand zu sein scheint, können Analysten die enormen Datenmengen der eingebauten Sensoren durchforsten, um Hinweise auf zukünftige Probleme frühzeitig zu erkennen.

ENERGIESEKTOR

Effizienz: Der Energiesektor profitiert bereits enorm vom IoT. Auf Verbraucherebene sind Nutzer in der Lage, durch fortschrittliche Anwendungen und „smarte" Geräte Energieverbrauch und -kosten zu verringern. Natürlich können Unternehmen diese Technologien ebenfalls nutzen, wenngleich auf einem viel höheren Niveau. Ein Bürogebäude mit mehreren Mietern kann beispielsweise den Energieverbrauch für jedes Stockwerk erfassen und überwachen. Nach Analyse der Daten kann das Gebäude feststellen, wo Energie verschwendet wird und dadurch gezielt Kosten reduzieren.

Die Energiebranche ist schon lange ein Vorreiter des IoT. Besonders Versorgungsunternehmen entwickeln innovative Wege, den Energieverbrauch gewerblicher, industrieller und privater Kunden aus der Ferne zu messen. Laut Ericsson wird erwartet, dass die Zahl vernetzter Geräte bei Versorgungsunternehmen weltweit von 485 Millionen im Jahr 2013 auf 1,53 Milliarden in 2020 wächst. Tatsächlich ist die Versorgungsbranche die zweitgrößte Quelle für Einkünfte von „Machine-to-Machine"-Dienstleistungen, gleich nach der Auto- und Transportindustrie. „Diese Geräte reichen von Messgeräten, Netzsensoren und Antriebssystemen bis zu Minikraftwerken und elektrischen Apparaten. Sie werden zur Netzüberwachung und -kontrolle, für Messungen, zur Bestandsverwaltung und -verfolgung sowie zur Außendienstkommunikation verwendet.[xxii]

RAUMFAHRT

Sicherheit: „Fly-by-Wire"-Systeme sind seit Jahrzehnten Bestandteil der Luft- und Raumfahrtindustrie. Einfach ausgedrückt, erlaubt „Fly-by-Wire" dem Piloten, sich auf das Monitoring des Flugzeugs zu konzentrieren, während Sensoren und automatisierte Systeme sich um den Rest kümmern. „Fly-by-Wire" schreitet so schnell voran, dass Flugzeuge in vielerlei Hinsicht bereits autonome Maschinen sind. Beispielsweise flog Kapitän Chesley B. Sullenberger („Sully"), der Pilot, der kurz nach Abflug vom Flughafen New York LaGuardia eine Notlandung auf dem Hudson River vollführte, einen Airbus A320. Bereits dessen Vorgängermodelle waren Wegbereiter für digitale „Fly-by-Wire"-Systeme gewesen. Es tut der Leistung von Kapitän Sullenberger keinen Abstrich, wenn wir sagen, dass das „Wunder vom Hudson" zur Tragödie hätte werden können, hätten die hochentwickelten Sensoren des Flugzeugs es ihm nicht erlaubt, sich voll auf die sichere Wasserlandung des Flugzeugs zu konzentrieren.[xxiii]

Effizienz: Auf dem Boden verwenden Luft- und Raumfahrtunternehmen das IoT, um die Wartung zu optimieren und Sicherheitsmaßnahmen zu verbessern. Beispielsweise verwendet die Wartungssparte für Flugzeugmotoren von General Electric Bordsensoren in Düsenflugzeugen, um Echtzeitdaten über die Motorleistung zu erfassen. Die Menge der erzeugten Daten erlaubt es GE die Motoreneffizienz voranzutreiben, Kraftstoffkosten zu sparen und Reisezeiten zu verringern.[xxiv]

GESUNDHEITSWESEN

Datengestützte Entscheidungsfindung: Es gibt eigentlich keinen Bereich im Gesundheitswesen, der das IoT nicht nutzt oder nutzen wird. IoT-fähige tragbare Geräte erlauben es Ärzten, Gesundheitsdaten ihrer Patienten zu erfassen, die andernfalls unerkannt blieben. Jährliche Vorsorgeuntersuchungen könnten obsolet werden, weil Ärzte bereits über ausreichend Patientendaten verfügen, wodurch sie wissen, ob eine persönliche Untersuchung notwendig ist. Gleichfalls kann der Arzt frühzeitig bei Patienten mit besorgniserregenden Gesundheitsanzeichen ohne erkennbare Krankheitssysteme gegensteuern, bevor sie schwerwiegendere Probleme verursachen. Klinikärzte können anhand dieser Daten nicht nur die Gesundheit einzelner Patienten besser verstehen, sondern auch detaillierte Datensätze von Patientengruppen erstellen, um die ältesten Krankheiten der Menschheit zu behandeln und zu verhindern.

Derweil können Krankenhäuser, die schon immer enorme Mengen Daten erzeugt und gespeichert haben, das IoT nutzen, um handlungsfähige Erkenntnisse aus den gesammelten Daten zu gewinnen. Beispielsweise lagern viele Krankenhäuser vorsorglich mehr ein als sie benötigen, um Engpässe gerade bei kritischen Vorräten zu vermeiden. IoT-fähige Scanner geben Krankenhausverwaltungen Einsicht in ihre Bestände. So wissen diese, wann Engpässe auftreten können. Außerdem können IoT-Geräte Behandlungszeiten in Krankenhäusern drastisch reduzieren, besonders in Notfallsituationen. Sanitäter können IoT-Geräte nutzen, um Vitalzeichen und andere Daten eines Patienten zu ermitteln, welche dann sofort an die Notaufnahme weitergeleitet werden. Die Ärzte kennen somit den Zustand eines Patienten, schon bevor dieser bei ihnen eintrifft und verlieren keine wertvolle Zeit mehr damit, den Zustand des Patienten einzuschätzen.

PRODUKTION

Sicherheit: Weiterhin verspricht das IoT, die Zahl von arbeitsbedingten Verletzungen und Todesfällen drastisch zu reduzieren. Laut der Internationalen Arbeitsorganisation (ILO) sterben jährlich 2,3 Millionen Menschen durch Arbeitsunfälle und Berufskrankheiten.[xxv] Laut der Europäischen Kommission erleiden jährlich mehr als drei Millionen Arbeiter ernsthafte Arbeitsunfälle und 4.000 sterben bei Unfällen während des Arbeitseinsatzes.[xxvi] Das IoT kann die Arbeitssicherheit verbessern, besonders für diejenigen, die alleine in gefährlichen Bereichen arbeiten, wie z. B. auf Baustellen. So kann beispielsweise tragbare Computertechnologie mit eingebauten Sensoren ausgestattet werden, um zu erkennen, ob sich ein Arbeiter vielleicht über das gesunde Maß hinaus anstrengt oder ein unsicheres Manöver durchführt. Die Sensoren können auch gefährliche Umweltbedingungen überwachen, wie z. B. extreme Temperaturen und Giftstoffe in der Umgebung. Die aus diesen tragbaren Sensoren gewonnenen Verhaltensdaten können Sicherheitsbeauftragten bei der Vorhersage helfen, wann ein Arbeiter möglicherweise einen Unfall haben wird. Dieses voraussagende Element des IoT, obwohl in vieler Hinsicht noch theoretisch, ist eine der aufregendsten Fähigkeiten, wenngleich aber auch sehr anfällig gegenüber Missbrauch.

Datengestützte Entscheidungsfindung: Unternehmen können ebenfalls IoT-Produkte nutzen, um Integrität, Qualität und Sicherheit von Komponenten in ihren komplexen Lieferketten sicherzustellen. Gartner Inc., eine IT-Forschungs- und Beratungsfirma, schätzt, dass eine „30-fache Zunahme internetfähiger physischer Geräte bis 2020 den Informationszugang für Supply Chain Marktführer sowie die Gefährdung durch Cyber-Risiken erheblich verändern wird".[xxvii] IoT-Geräte entlang der Lieferkette geben Managern tiefere Einblicke in ihre Prozesse als je zuvor. Von Transportsichtbarkeit zu Depotsicherheit, IoT-Objekte versprechen eine Revolution der Entwicklung, Absicherung und Aufrechterhaltung von Lieferketten.

LEBENSMITTEL

Effizienz: Lieferfirmen bieten Privatkunden bereits heute die Möglichkeit, ihre Waren an jeder Bearbeitungsstation nachzuverfolgen. Jedoch ist diese Technologie für Unternehmen noch wesentlich nützlicher. Richtig platzierte IoT-Sensoren können Unternehmen helfen, ihre Anlagen in Echtzeit zu verfolgen. Durch die gesammelten Daten können Unternehmen Effizienzlücken und Engpässe in ihren Lieferketten erkennen. Ebenso wichtig sind Sensoren in Lagereinrichtungen, wie z. B. auf Gefrier-LKWs, die warnen können, wenn Kühlgeräte ausfallen oder ein Ausfall kurz bevorsteht. Dies nimmt die Verpflichtung zur Überwachung vom Fahrer, da er vermutlich die Waren erst mehrere Stunden nach Ausfall der Kühleinheit prüft. So kann wertvolle Fracht gerettet werden, bevor sie verdirbt. Landwirte können in ihre Felder eingebaute IoT-Technologie nutzen, um kritische Informationen, wie z. B. den Wasserverbrauch, zu überwachen. Beispielsweise kann ein Sensor einem Landwirt Lücken in einem Sprinklersystem aufzeigen oder signalisieren, wo er zuviel Wasser auf einer bestimmten Anbaufläche verbraucht. Besonders in den Entwicklungsländern verspricht das IoT, bahnbrechende Auswirkungen auf die Produktion und Verteilung von Lebensmitteln zu haben.

Risiken des IoT

Tatsächlich sind die Chancen und Potenziale des neuen IoT-Zeitalters riesig. In vielerlei Hinsicht bestimmt nur unsere Fantasie die Grenzen des IoT. Besonders wenn wir all die unerfassten Daten sehen, all die Informationsbruchstücke, die uns durch die Finger rieseln, und wie es das IoT uns ermöglichen wird, diese Daten endlich zu erfassen und so zu nutzen, wie es der Menschheit noch nie möglich war. Dann ist es leicht, die dunkle Seite des IoT zu ignorieren. Aber Unternehmen können es sich nicht leisten, in IoT-Systeme zu investieren, ohne erst einmal die Hauptrisiken zu verstehen, die jedem mit dem Internet verbundenen System innewohnen. Seit wir unseren ersten Computer anschalteten wussten wir, dass unsere Abhängigkeit von der Technik zu kleineren oder größeren Störungen führen kann. Dies soll Unternehmen nicht abschrecken, das IoT einzubinden; die Chancen überwiegen die Risiken bei weitem. Aber dennoch muss jede Firma verstehen, dass das IoT für jedes Problem, das es löst, ein neues schafft. Unsere vier größten Risiken des IoT:

DATENSCHUTZ

Die Milliarden von Sensoren auf der Welt erfassen ständig all ihre Umgebungsdaten. Dazu gehören auch Menschen. Also ist es wichtig, Datenschutzbedenken in der Welt des IoT sehr ernst zu nehmen. Ein Großteil der Industrieländer hat versucht, Verbraucher vor illegaler Nutzung vertraulicher Informationen zu schützen, aber in vielen Fällen reichen die Gesetze nicht, um den vielen neuen Erfassungs- und Nutzungsmöglichkeiten für personenbezogene Daten nachzukommen. Der kürzliche Versuch der EU, das Urheberrecht zu aktualisieren (siehe unten) ist ein Symptom dafür, wie veraltet viele Gesetze der Industrieländer sind.

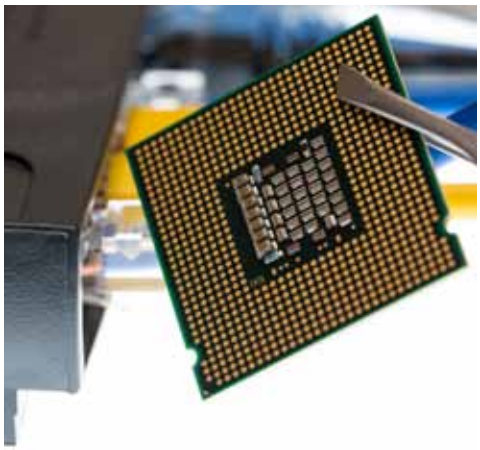
Als das Internet sich noch in einem früheren Stadium befand, gewöhnten sich Kunden an Tracking-Software, auch bekannt als Cookies. Weil es keine speziellen Gesetze gegen die Verwendung von Cookies auf Webseiten zur Analyse von Nutzerverhalten gab, nahmen viele Firmen die Praxis einfach an, ohne viel über Nutzerrechte nachzudenken. Tatsächlich waren es Browser, die auf die Ängste der Verbraucher reagierten und Tools anboten, um Cookies einzuschränken und sie nach einer Browser-Sitzung zu löschen. Gesetze regeln heute in der EU, wie Cookies verwendet werden und welche Daten sie über Nutzer sammeln dürfen[xxviii]. Aber mit dem Aufkommen von Mobiltechnologie, die keine Cookies benötigt, um Nutzerverhalten nachzuverfolgen, sind viele dieser Gesetze schnell veraltet und greifen nicht mehr in der Welt des IoT.

Gleichsam verlassen sich die USA auch für neue IoT-Geräte und Systeme auf ältere Regulierungsmodelle. Aber es gibt kein einheitliches Bundesgesetz über die Sammlung und Nutzung personenbezogener Daten. Stattdessen verlassen sich die USA auf einen Flickenteppich aus bestehenden Bundes- und Einzelstaatenrechten, um die Privatsphäre der Verbraucher zu schützen. Die öffentliche Empörung über die US-Bundesregierung, besonders über die NSA wegen „Data-Minings" zwecks Strafverfolgung und Terrorabwehr, zeichnet die kommenden Debatten aus.

Die US-Handelskommission, die Federal Trade Commission (FTC), veröffentlichte im Januar 2015 einen Bericht, der den Status des IoT in den USA untersuchte und „Best Practices" für Unternehmen für den Schutz von Kundendaten vorschlug. Der Bericht der FTC fährt allerdings mit den lockeren Regeln der US-Regierung zum Internet, und damit zum IoT, fort. Beispielsweise resümiert der Bericht, dass „jegliche Gesetzgebung zum Internet der Dinge zu diesem Zeitpunkt voreilig wäre in Anbetracht der schnell fortschreitenden Technologie." Der Bericht wiederholt gleichwohl den häufigen Aufruf der Kommission, die Gesetze zur Datensicherheit sowie zur Anzeigepflicht zu stärken.[xxix]

Datenschutzbedenken gelten auch für den Arbeitsplatz. Auf dem Markt gibt es viele Programme, mit denen Arbeitgeber das Verhalten der Mitarbeiter verfolgen können, im Regelfall über den PC des Mitarbeiters. Das IoT erlaubt es Arbeitgebern, Sensoren in allen Ecken des Büros einzubauen, um die Gewohnheiten der Mitarbeiter zu überwachen. Beispielsweise klagte eine ehemalige Vertriebsleiterin in Kalifornien gegen ihren Arbeitgeber. Sie erhob den Vorwurf, der Arbeitgeber habe sie gezwungen, eine Überwachungs-App auf ihr Smartphone zu laden, wodurch der Arbeitgeber ihren Aufenthalt sowohl während als auch außerhalb der Arbeitszeit überwachte.[xxx] Da das IoT menschliche Handlungen nachverfolgen und aufzeichnen kann, entstehen zahlreiche ethische Fragen, die noch nicht vollständig beantwortet sind, wie z. B.:

- Kann ein Arbeitnehmer aufgrund Daten aus einem IoT-Objekt bestraft werden?
- Muss ein Arbeitgeber seine Angestellten über Sensoren informieren, die ihr Verhalten überwachen?



CYBER-SICHERHEIT

Cyber-Attacken sind heute eine der Hauptgefahrenquellen für Unternehmen. Laut einer Schätzung kostet Cyber-Kriminalität Unternehmen jährlich 400 Milliarden USD.[xxxi] Aus Sicht des IoT ist es am bedenklichsten, dass die Cyber-Kriminellen scheinbar sichere Systeme mit mehreren Schutzstufen knacken. Der komplexe Bereich Sicherheit für IoT-Geräte ist für Unternehmen ein wichtiger Verbesserungsaspekt, besonders im Hinblick auf die Vorbereitung für den Tag, an dem das „IoT-Ökosystem" zum Leben erwacht, wenn Milliarden Objekte mit dem Internet und miteinander verbunden sein werden.

Wir müssen uns vor Augen halten, dass jedes Gerät mit Internetverbindung eine mögliche Eintrittsquelle für Hacker ist. Beispielsweise gelang es 2014 einem Hacker, sich in einen Baby-Monitor einzuhacken und ein zweijähriges Mädchen zu belästigen.
Die nachfolgenden Recherchen zu dem Produkt der chinesischen Firma Focsam ergaben, dass 40.000 der 46.000 Geräte nicht über das nötige Sicherheitsupdate verfügten, welches die Lücke verhindert hätte.[xxxii]

Wir müssen auch bedenken, dass je mehr Systeme automatisiert und miteinander vernetzt werden, diese für Hacker, besonders in der Industrie, im steigenden Maße angreifbar werden. Eine Stadt, die ein intelligentes Stromnetz baut, erkennt vielleicht große Kosteneinsparpotenziale bei der vereinfachten Fehlerbehebung, die das System bietet. Gleichzeitig gibt genau dieses System einem potenziellen Hacker einfachen Zugriff, um von seinem Computer aus die gesamte Stromzufuhr der Stadt lahmzulegen.

In einem weiteren Beispiel veröffentlichte der US-Rechnungshof, das Government Accountability Office (GAO), im April 2015 einen Bericht, der die Gefahren der zunehmenden Vernetzung zwischen Flugzeugen und Bodensystemen erörtert. „Diese Vernetzung kann möglicherweise Unbefugten Zugriff auf die Bordelektronik geben", warnte der Bericht.[xxxiii] In anderen Worten, ein Hacker-Terrorist könnte das System nutzen, um die Kontrolle über das Flugzeug zu erlangen.

Die vernetzte Natur des IoT, d. h. jedes verbundene Objekt nutzt Daten anderer vernetzter Objekte, birgt auch das Risiko, dass ein kleiner Fehler zu katastrophalen Systemstillständen führen kann. Ein fehlerhaftes Objekt könnte fehlerhafte Daten an ein normal funktionierendes Gerät übertragen. Während die fehlerhaften Daten durch das System aufsteigen, beginnen sie immer mehr Systeme zu infizieren. Im Falle einer Umweltkatastrophe wie Überflutung könnten fehlerhafte Sensoren in Dämmen und Deichen zu enormen Sachschäden oder sogar zu Todesfällen führen.

Derartige Beispiele unterstreichen die neuen Risiken, denen viele Unternehmen ausgesetzt sein werden, wenn es um Cyber-Sicherheit im IoT geht. Wir erwarten zwar, dass die Hersteller dieser Geräte im Laufe der Zeit ihre Sicherheitsmaßnahmen verbessern, die reine Anzahl vernetzter Geräte wächst jedoch exponentiell.

HAFTPFLICHT

Bei autonomen Fahrzeugen, wie fahrerlosen Autos, stehen wir vor einem offensichtlich ethischen Dilemma: Sollte ein autonomes Fahrzeug in den Sekunden vor einem Unfall alles tun, um seine Fahrgäste zu schützen, selbst wenn es dadurch andere Fahrer oder Fußgänger verletzt? Sind Menschen hinter dem Steuer, stellen Kollateralschäden, so schrecklich sie auch sind, anscheinend kein großes ethisches Problem dar. Ein Mensch in Gefahr kann nicht beschuldigt werden, wenn sein Überlebensinstinkt ihn zwingt, sein Auto auf einen Fußgänger zuzusteuern. Aber sollte ein Fußgänger, der bei einem Unfall zu Schaden kommt, den Autohersteller verklagen können, wenn Maschinen entscheiden? Und kann ein Fahrer, der bei einem Unfall verletzt wurde, einen Autohersteller verklagen? Ein Bericht der Europäischen Kommission zu ethischen Dilemmas des IoT besagte: „Menschen sind es nicht gewohnt, dass Objekte eine Identität haben oder selbstständig handeln, besonders wenn sie unerwartet handeln."[xxxiv]

Andere Fragen der Haftung entstehen, wenn wir die Eigentumsrechte an den Daten betrachten. Milliarden von Geräten sammeln Daten, also ist unklar, wer für welche Daten zuständig ist. IoT-Objekte funktionieren autonom und gemeinsam mit einer Vielzahl

anderer Objekte. Daten werden schnell geteilt, verarbeitet, erneut geteilt und neu verarbeitet, bevor sie für Menschen sichtbar sind. In anderen Worten: Es greift zu einfach, ein einziges Gerät mit einem einzigen Datenstück in Verbindung zu bringen, denn zu viel von dem Potenzial des IoT hängt von der nahtlosen Übertragung von Daten zwischen Objekten ab. Beispielsweise überwacht ein Herzmonitor mit IoT-Zugang nicht einfach das Herz eines Patienten auf Warnzeichen oder drohenden Herzinfarkt. Er kann auch auf Daten von anderen Objekten zugreifen, welche die FitnessGewohnheiten des Patienten überwachen, welches wiederum Daten von einem Gerät bezieht, das die Nahrungsaufnahme überwacht. Wer ist dann verantwortlich, wenn der Patient einen Herzinfarkt hat?

Beunruhigende Fragen treten bei einer Fehlfunktion von IoT-Geräten auf. Zwar können Sensoren in kritische Infrastruktur wie Dämme, Brücken und Straßen eingebaut werden, um die Bausubstanz ebenso wie die Bausubstanz gefährdende Umwelteinflüsse zu überwachen. Auch könnte eine Straße neben einem Flutgebiet mit Sensoren ausgestattet werden, die sobald der Regen einen gewissen Pegel überschreitet, die Techniker vor der Flutgefahr warnen. Der Schutz von Infrastruktur ist einer der interessantesten Aspekte des IoT. Dennoch gilt: Wenn wir mehr und mehr unserer kritischen Infrastruktur- und Sicherheitsdienste an IoT-Objekte übertragen, riskieren wir im Fall einer Fehlfunktion eine Katastrophe.

Das können wir auch auf den Privatsektor übertragen. Ein nicht-tödliches Beispiel:
Im April 2015 haben sich mehrere Flüge von American Airlines verspätet, weil ein Softwarefehler die Tablets der Piloten außer Kraft gesetzt hatte, die sie für die Navigation nutzen.[xxxv] Obwohl dieser Fehler leicht mit einem Softwareupdate zu beheben war, zeigen die Beispiele, wie angreifbar wir bereits sind, weil unsere Geräte vernetzt sind. Sind wir vorbereitet, wenn sie versagen?

Der aktuelle Sachstand des IoT in Europa, den USA und in Asien

EUROPA

Mit seiner hohen Mobilgeräte-Durchdringung ist Europa einzigartig aufgestellt, um von der kommenden IoT-Revolution zu profitieren. Trotz der Unausweichlichkeit des IoT bleiben Hindernisse für einzelne Volkswirtschaften bei der Ausschöpfung des vollen Potenzials. Eines ist schlicht und einfach der Wettbewerb. Beispielsweise trafen sich im März 2015 bei einer Konferenz der Europäischen Kommission in Brüssel Vertreter der europäischen Schwerindustrie, der Autoindustrie, der Haushaltsgeräteindustrie, der Telekommunikationsbranche sowie die Gesetzgeber, um zu besprechen, wie die Wettbewerbsfähigkeit des Kontinents im IoT verbessert werden könnte, besonders da US-Firmen wie Apple und Google den größten Vorsprung zu haben scheinen.

Als Ergebnis der Konferenz entstand eine EU-gestützte Allianz der europäischen Industrie, darunter Top-Firmen wie Bosch, Siemens, Orange, Volvo, Alcatel, Nokia, Philips und Telefonica mit dem Ziel, Innovation im IoT voranzutreiben. Wie Anne Lauvergeon, Vorsitzende des französischen Networking-Startups Sigfox und Vorstandsmitglied der neuen IoT-Allianz sagte: „Um der internationalen Konkurrenz zu begegnen, ist es unumgänglich, ein Ökosystem für IoT-Innovation zu schaffen."[xxxvi]

Gleichzeitig arbeitet die EU auf einen einheitlichen digitalen Markt hin, indem sie bestehende Telekommunikationsgesetze überprüft. Das Ziel der neuen Gesetzgebung ist laut Wall Street Journal, Hindernisse für den Datenverkehr durch „Zerschlagung nationaler Silos in Bereichen wie E-Commerce und Urheberrecht" abzubauen.[xxxvii] Die Notwendigkeit, die Gesetze zu überarbeiten, deutet auf die tiefgreifende Veränderung durch die neue IoT-Wirtschaft hin, in der die Möglichkeit, schnell und einfach massive Datenmengen zu übertragen und auszutauschen, maßgeblich für den Erfolg eines Unternehmens sein wird.

Neben Gesetzesnovellen wird die neue IoT-Wirtschaft auch erhebliche Investitionen für die technische Infrastruktur erfordern. Im März 2015 veranstaltete die Europäische Investitionsbank (EIB) in Berlin eine Konferenz zum Thema „Antrieb für Europa – Innovation und Wettbewerbsfähigkeit".[xxxviii] Während seiner Grundsatzrede sprach Jeremy Rifkin, Vorsitzender der Foundation on Economic Trends und politischer Berater für Frankreich, Deutschland und der EU davon, wie die Hochrüstung und der Ausbau des IoT dem „digitalen Europa" helfen werden, eine „dritte industrielle Revolution" zu erleben.[xxxix]

Allerdings wies Rifkin darauf hin, dass europäische Investitionen in „veraltete" Technologieplattformen im Jahr 2012 insgesamt 741 Milliarden USD betragen haben. Wären nur 25 Prozent dieser Mittel in jeder Region der EU in die IoT-Infrastruktur investiert worden, hätten bis 2040 alle Vorteile des „digitalen Europa" realisiert werden können.[xl]
Also werden laut Expertenmeinung zu viele Euros in die Untermauerung eines alten Wirtschaftsmodells gesteckt – auf Kosten der Zukunft.

USA

2014 investierten Risikokapitalgeber nahezu 11,9 Milliarden USD in Internetfirmen; das ist seit 2000, dem Höhepunkt der Dotcom-Blase, Höchststand.[xli] Zwar wurde nicht all dieses Geld in Geräte für das IoT investiert, aber die Begeisterung um das IoT in den USA ist so groß wie nie. Im März 2015 verkündete IBM beispielsweise, dass es 3 Milliarden USD in eine neue Abteilung für das Internet der Dinge investieren würde.[xlii]

Tatsächlich versucht der Privatsektor, die USA an der Spitze der IoT-Revolution zu halten. 2014 verkündeten Software- und Technologiegiganten wie AT&T, Cisco, General Electric, IBM und Intel die Gründung des „Industrial Internet Consortium", das technische Standards für IoT-Objekte festlegen soll. Auch das Weiße Haus und andere Regierungsorgane sind in das weisungsberechtigte Konsortium involviert.[xliii] Obwohl die FTC vorgeschlagen hat, dass die US-Regierung eine Regulierung des IoT zum jetzigen Zeitpunkt unterlassen soll, haben Regierungsbehörden damit begonnen, gemeinsam mit Privatunternehmen an der Produktion öffentlicher Applikationen für IoT-Technologie zu arbeiten. Beispielsweise trafen sich 2014 Vertreter der Defense Advanced Research Projects Agency (DARPA), des Transportation Department und der Veterans Health Administration in Washington, um über die Möglichkeiten der IoT-Technologie für den öffentlichen Sektor zu beraten.[xliv]

Allerdings hinken die USA anderen Industrieländern, besonders Asien hinterher, wenn es um Breitbandzugang und Geschwindigkeit geht. Laut der Digital-Traffic-Firma Akamai belegen die USA Platz 14 bei der Breitbandgeschwindigkeit.[xlv] Obwohl die allgemeine Vernetzung in den USA zu den höchsten der Welt gehört, beschränken alternde Infrastruktur, lokale Gesetzeshürden und die hohen Kosten von Breitbandverbindungen die Führungsposition der USA bei der Einführung und Innovation des IoT.

ASIEN

Laut RAND Europe investiert China erheblich in das IoT. 2012 sah es 625 Mio. EUR (775 Mio. USD) an Investitionen für das IoT vor, und das chinesische Ministerium für Information und Technologie gründete einen Fonds von 775 Mio. USD, um den Aufbau des IoT über die nächsten fünf Jahre zu fördern. Diese Investitionen gehen bis 2015 landesweit in den Aufbau von zehn IoT-Industrieparks und in mehr als 100 Kernunternehmen. Während der vergangenen Jahre haben die Investitionen Chinas in die IoT-Infrastruktur die Wettbewerber in Europa und den USA überholt.[xlvi]

Während China sicherlich der größte Player auf dem IoT-Markt ist, gewinnt die gesamte Asien-Pazifik-Region sehr viel durch die neueste IoT-Technologie. Die Forschungsfirma IDC schätzt, dass der Markt für das Internet der Dinge in der Asien-Pazifik-Region (ohne Japan) von 250 Milliarden USD in 2013 bis 2020 auf 583 Milliarden USD wachsen wird. Gleichzeitig wird die Zahl der mit dem Internet verbundenen Dinge im Asien-Pazifik-Markt von 2,59 Milliarden in 2013 bis 2020 auf 8,98 Milliarden wachsen.[xlvii]

Obwohl IDC voraussagt, dass bis 2020 eins von fünf mit dem Internet verbundenen Objekten in China sein wird, warnen sie, dass die Größe nicht der Reife des Marktes entspricht. „Während die Möglichkeiten des Marktes in China anderen führenden Ländern wie Südkorea, Indien, Indonesien und Australien in Dollar gemessen weit überlegen sind, bedeutet es nicht, dass China der reifste Markt ist", sagt Charles Reed Anderson, Associate VP, Head of Mobility and Internet of Things bei IDC Asia/Pacific. „Um die Reife eines Marktes einzuschätzen, vergleichen wir die Gesamtzahl der verbundenen Dinge mit der Gesamtbevölkerung, um die Verbindungen pro Kopf zu ermitteln. Basierend auf dieser Berechnung haben wir herausgefunden, dass die drei reifsten Märkte Südkorea, Australien und Neuseeland sind; China belegt Rang sechs unter den 13 Ländern der Asien-Pazifik-Region (ohne Japan)."[xlviii]
Dennoch: Als Werkbank der Welt kann Asien enorme Gewinne aus einer IoT-basierten Wirtschaft ziehen.

Schlussfolgerung

Es ist keine Übertreibung zu behaupten, dass das IoT für die gesamte Welt ein neues Wirtschaftszeitalter einläuten wird. Die Verheißungen des IoT sind nicht bloß Verbesserungen existierender Prozesse und Wirtschaftsmodelle, sondern sie bedeuten eine Umwälzung. Die IoT-Wirtschaft wird die Produktion, Funktion und Leistung von Unternehmen revoltionieren. Die Veränderung geschieht schneller als in jeder vorangegangenen industriellen Revolution.

Gleichzeitig bringt das IoT ernorme Herausforderungen für alle Branchen und Industriezweige mit sich. Auf der einen Seite löst es Probleme, die Unternehmen seit Jahrzehnten plagen, wenn nicht seit Jahrhunderten. Auf der anderen Seite schafft es aber auch ganz neue Dilemmas, ethische und praktische. Fragen zu Datenschutz, Cyber-Sicherheit und Haftung für Eigentum und Produkte werden gleichermaßen schnell auftauchen wie die Chancen des IoT wachsen. Während Unternehmen beginnen müssen, die Technologie des IoT zu nutzen, wenn sie langfristig überleben wollen, müssen sie auch Strategien einführen, wie sie den Risiken des IoT begegnen.

In der nächsten Folge dieser Whitepaper Serie untersuchen wir diese Risiken weiter und bieten praktische Tipps, wie Unternehmen diese vermeiden oder minimieren können. Wir stellen auch dar, wie die Versicherungsbranche sich darauf vorbereitet Unternehmen zu helfen, sich in dieser neuen Welt zurechtzufinden. In vielerlei Hinsicht kann die Versicherungsbranche am meisten durch die Sensoren, die enorme Datenmengen erzeugen gewinnen, da sie tiefere Einblicke liefern werden, um die Risiken für Kunden zu minimieren.
Als Vorreiterin bei datengestützter Analytik und Risikoabwehr kann die Versicherungsbranche Unternehmen helfen, ihre Chancen zu maximieren und die Risikobelastung zu minimieren.

Quellenangaben

[i] http://www.rfidjournal.com/articles/view?4986

[ii] RAND: Europe's policy options for a dynamic and trustworthy development of the Internet of Things, 2012

[iii] CISCO: The Internet of Things How the Next Evolution of the Internet Is Changing Everything, 2011

[iv] http://www.ericsson.com/res/docs/2014/emr-june2014-regional-appendices-europe.pdf

[v] Dubravac, Shawn. "Digital Destiny." P. 68

[vi] HBR-Verizon INTERNET OF THINGS:
SCIENCE FICTION OR BUSINESS FACT?, 2014

[vii] RAND: Europe's policy options for a dynamic and trustworthy development of the Internet of Things, 2012 p. 14

[viii] ibid

[ix] http://www.who.int/gho/road_safety/mortality/en/

[x] http://ec.europa.eu/transport/road_safety/specialist/statistics/index_en.htm

[xi] http://morth.nic.in/writereaddata/mainlinkFile/File1465.pdf and
http://www.chinadaily.com.cn/china/2011-01/07/content_11808453.htm

[xii] http://www.forbes.com/sites/dougnewcomb/2015/05/08/daimler-autonomous-truck-has-huge-commercial-implications/

[xiii] © 2012 Google Inc. All rights reserved. Google and the Google Logo are registered trademarks of Google Inc.

[xiv] Copyright 2002-2015 Tesla Motors, Inc. All Rights Reserved.

[xv] http://www2.deloitte.com/us/en/pages/finance/articles/internet-of-things-financial-services-industry.html

[xvi] http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Bank-of-Things.pdf

[xvii] http://osdelivers.blackducksoftware.com/2015/02/11/industrial-internet-of-things-in-the-maritime-industry/

[xviii] http://www.rcrwireless.com/20150106/featured/ericsson-maritime-platform-targets-shipping-connectivity-tag2

[xix] http://www.inman.com/2014/07/08/internet-of-things-could-be-most-disruptive-to-real-estate/

[xx] iBeacon is a trademark of Apple Inc., registered in the U.S. and other countries.

[xxi] http://realtormag.realtor.org/technology/feature/article/2015/03/real-estate-and-internet-things

[xxii] http://www.ericsson.com/res/docs/2014/gtwp-op-transforming-industries-aw-print.pdf p. 4

[xxiii] http://www.cnn.com/2009/OPINION/11/18/langewiesche.miracle.hudson.flight/index.html?iref=24hours

[xxiv] http://www.forbes.com/sites/ptc/2014/06/23/will-the-internet-of-things-revolutionize-the-aircraft-industry/

[xxv] http://www.ilo.org/global/topics/safety-and-health-at-work/lang--en/index.htm

[xxvi] http://www.euractiv.com/sections/social-europe-jobs/commission-publishes-health-and-safety-strategy-eu-workers-302665

[xxvii] http://www.gartner.com/newsroom/id/2688717

[xxviii] http://ec.europa.eu/ipg/basics/legal/data_protection/index_en.htm

[xxix] https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices

[xxx] http://www.techweekeurope.co.uk/mobility/lawsuit-tracking-app-168043

[xxxi] http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/

[xxxii] http://www.forbes.com/sites/kashmirhill/2013/08/27/baby-monitor-hack-could-happen-to-40000-other-foscam-users/

[xxxiii] http://www.gao.gov/products/GAO-15-370

[xxxiv] http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1752

[xxxv] http://www.nytimes.com/2015/04/30/business/several-american-airlines-flights-are-delayed-by-an-app-malfunction.html?_r=0

[xxxvi] http://blogs.wsj.com/digits/2015/03/25/europe-wants-to-bring-its-industry-online-before-google-apple-make-it-obsolete/

[xxxvii] http://www.wsj.com/articles/eu-considers-new-telecom-rules-to-level-the-playing-field-1427295277

[xxxviii] http://www.eib.org/infocentre/events/all/momentum-for-europe.htm

[xxxix] http://www.automatedtrader.net/headlines/153295/digital-europe-the-rise-of-the-internet-of-things-and-the--transition-to-a-third-industrial-revolution

[xl] ibid

[xli] http://nvca.org/pressreleases/annual-venture-capital-investment-tops-48-billion-2014-reaching-highest-level-decade-according-moneytree-report/

[xlii] http://www.theglobeandmail.com/report-on-business/international-business/us-business/ibm-to-invest-3-billion-in-new-internet-of-things-unit/article23722378/

[xliii] http://bits.blogs.nytimes.com/2014/03/27/consortium-wants-standards-for-internet-of-things/?_php=true&_type=blogs&_r=1

[xliv] http://www.washingtonpost.com/business/on-it/dot-va-reps-discuss-how-the-federal-government-could-use-internet-of-things/2014/08/06/d9ac6410-1d84-11e4-ae54-0cfe1f974f8a_story.html

[xlv] http://www.akamai.com/dl/akamai/akamai-soti-q114.pdf?WT.mc_id=soti_Q114

[xlvi] HBR-Verizon INTERNET OF THINGS: SCIENCE FICTION OR BUSINESS FACT?, 2014 p. 7

[xlvii] http://www.idc.com/getdoc.jsp?containerId=prHK25553415

[xlviii] ibid

The Consumer Electronics Association (CEA) is the technology trade association representing the $286 billion U.S. consumer electronics industry. More than 2,000 companies enjoy the benefits of CEA membership, including legislative and regulatory advocacy, market research, technical training and education, industry promotion, standards development and the fostering of business and strategic relationships. CEA also owns and produces CES – The Global Stage for Innovation. All profits from CES are reinvested into CEA's industry services. Find CEA online at CE.org, InnovationMovement.com and through social media at ce.org/social.

American International Group, Inc. (AIG) is a leading global insurance organization serving customers in more than 100 countries and jurisdictions. AIG companies serve commercial, institutional, and individual customers through one of the most extensive worldwide property-casualty networks of any insurer. In addition, AIG companies are leading providers of life insurance and retirement services in the United States. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGinsurance | LinkedIn: www.linkedin.com/company/aig

AIG is the marketing name for the worldwide property-casualty, life and retirement, and general insurance operations of American International Group, Inc. For additional information, please visit our website at www.aig.com. All products and services are written or provided by subsidiaries or affiliates of American International Group, Inc. Products or services may not be available in all countries, and coverage is subject to actual policy language. Non-insurance products and services may be provided by independent third parties. Certain property-casualty coverages may be provided by a surplus lines insurer. Surplus lines insurers do not generally participate in state guaranty funds, and insureds are therefore not protected by such funds. The content contained herein is intended for general informational purposes only, and should not be viewed as a substitute for legal, regulatory, accounting or other advice on any particular issue or for any particular reason.

AIG®

Bring on tomorrow