



PETER SENNHAUSER

DAS INTERNET DER DINGE

– EINE EINFÜHRUNG –

SUISSEDIGITAL in Zusammenarbeit mit der
HWZ Hochschule für Wirtschaft Zürich

Das Internet der Dinge ist als Schlagwort längst etabliert, aber in der Realität noch nicht ganz angekommen. Was kommt auf uns zu? Was steht hinter dem Begriff? Und welche Chancen und Risiken wird uns das Internet der Dinge bieten?

Wir freuen uns, Ihnen mit diesem Buch Hintergrundwissen vermitteln zu können, und wünschen Ihnen eine aufschlussreiche Lektüre.

SUISSEDIGITAL

Verband für Kommunikationsnetze

www.suissedigital.ch

© 2018 – CC-BY-NC-ND (Werk), CC-BY-SA (Texte)

Verlag & Produktion: buch & netz, buchundnetz.com

Herausgeber:

[SUSSEDIGITAL](http://susedigital.com) und [HWZ Hochschule für Wirtschaft Zürich](http://hwz.ch)

Text:

Peter Sennhauser, Swissreporter GmbH, <http://www.swissreporter.ch/>

Abbildungen: hellermeier, <http://hellermeier.ch/>**Umschlaggestaltung:**
gestalt kommunikation, <http://www.gestalt.ch/>

ISBN: 978-3-03805-256-2 (PDF), 978-3-03805-257-9
(ePub), 978-3-03805-258-6 (mobi)

Version: 1.03 – 20180110

Dieses Werk ist als buch & netz Online-Buch und als eBook in verschiedenen Formaten verfügbar. Weitere Informationen finden Sie unter der URL: <http://buchundnetz.com/werke/internet-der-dinge>. Zu den Urheberrechten und Nutzungsbedingungen beachten Sie bitte die entsprechenden Hinweise am Schluss des Buches.

Inhalt

SUISSEDIGITAL und das Internet der Dinge

Alles ist immer online	1
<i>Die Maschinen kommunizieren lassen</i>	1
<i>Ein Kühlschrank allein ist ziemlich dumm</i>	3
<i>Der Überblick schafft neues Verständnis</i>	4
<i>Zu viele Ideen, zu wenig Wissen</i>	5
Smart Home, das Wunschhaus	9
<i>Die Party in Ihrem Heimnetz</i>	10
<i>Warum die Infrastruktur simpler....</i>	11
<i>... und die Geräte smarter werden sollten</i>	12
<i>Noch "denkt" das Rechenzentrum</i>	13
Architektur – Netze und Sensoren	15
<i>Wie das "Inter" ins Netz kam</i>	15
<i>Offen für alle</i>	16
<i>Das WWW ist nur eine Anwendung</i>	18
<i>Und wo sind die Dinge?</i>	18
<i>Der Kampf um Standards hat begonnen</i>	21

Künstliche Intelligenz	23
<i>Niemand weiss, wie Software lernt</i>	23
<i>Programme schreiben sich selber</i>	24
<i>Sind Pokerspieler intelligent?</i>	25
<i>Siri und Alexa leben im Rechenzentrum</i>	27
Detailhandel und Mobilität	29
<i>Amazons Laden hat keine Registrierkassen</i>	30
<i>Vernetzte Autos sind die besseren Fahrer</i>	31
<i>Die Ware Mobilität</i>	33
Industrie 4.0 und Präzisions-Landwirtschaft	35
<i>Ein Getriebe aus dem Drucker</i>	36
<i>Die selbstheilende Eisenbahn</i>	36
<i>Die Fabrik, die sich selber optimiert</i>	37
<i>John Deere, das Google der Landwirtschaft</i>	38
Risiken und Nebenwirkungen	41
<i>Das Internet of “Bad other Things” (Bots)</i>	41
<i>Kein Angriff unter dieser Nummer</i>	44
<i>Big Data – eine Frage der Balance</i>	46
<i>Roboter-Ethik: Warum man sie ernst nehmen sollte</i>	48
Glossar	51
Peter Sennhauser	61
Institute for Digital Business	63
<i>Allgemein</i>	63
<i>Mission</i>	63
<i>Angebot</i>	63
buch & netz	65
Urheberrechte und Nutzungsbedingungen	67

SUISSEDIGITAL und das Internet der Dinge

SUISSEDIGITAL ist der Wirtschaftsverband der Schweizer Kommunikationsnetze. Ihm sind rund 200 privatwirtschaftlich wie auch öffentlich-rechtlich organisierte Unternehmen angeschlossen, die etwa 2.4 Millionen Haushalte mit Radio, TV, HDTV, Internet, Telefonie und weiteren Angeboten versorgen.

Die im Verband vereinigten Unternehmen verfügen über eine hervorragende Kommunikationsinfrastruktur. Diese ermöglicht es ihnen, im hart umkämpften Telekommunikationsmarkt zu bestehen. Jedoch ist in den angestammten Märkten Fernsehen, Internet und Telefonie nur noch ein begrenztes Wachstum möglich, da diese weitgehend gesättigt sind. Es stellt sich deshalb die Frage, wie auf der Basis der bestehenden Kommunikationsinfrastruktur neue Geschäftsfelder erschlossen werden können.

Vor diesem Hintergrund befasst sich SUISSEDIGITAL verstärkt mit verschiedenen Themen der Digitalisierung. Ein besonders interessantes und zukunftsträchtiges Thema ist das "Internet der Dinge", das Anwendungen mit Gegenständen oder Geräten im Fokus hat, die Informationen direkt untereinander austauschen können. Die vorliegende Publikation entstand auf Initiative von SUISSEDIGITAL und in Zusammenarbeit mit der HWZ Hochschule für Wirtschaft Zürich. Sie soll das Thema auf verständliche Art und Weise ausleuchten.

Alles ist immer online

Als Michael M. in an einem Augustmorgen eine Meldung seines E-Bikes der Marke “Stromer” auf dem Tablet-Computer erhielt, war es schon zu spät: Das mehrere Tausend Franken teure Fahrrad meldete bereits eine Position jenseits der Grenze zu Frankreich, keine drei Kilometer von seinem Wohnort entfernt. Die telefonisch avisierte französische Polizei fand das Fahrzeug dank den Ortsangaben aus den GPS-Meldungen mit Leichtigkeit. Und als Michael sein Eigentum am gleichen Tag auf dem Polizeiposten abholte, staunte er nicht schlecht: Die Diebe hatten sich nicht nur auf einen gehetzten Versuch beschränkt, den wertvollen Akku aus dem Rahmen zu brechen. Sie hatten ausserdem mit einer dicken Wicklung aus Alufolie versucht, das Mobilfunk- und das GPS-Modul des E-Bikes so zu blockieren, dass es seine Position nicht bestimmen oder diese wenigstens nicht via Mobilem Internet “nach Hause funken” könnte. Erfolglos, wie sich zeigte.

Die Maschinen kommunizieren lassen

Die automatische Positionsmeldung ist längst nicht mehr den Besitzern teurer E-Bikes vorbehalten, die über Bordcomputer, Wegfahr-

sperre, Mobilfunk und GPS-Empfänger verfügen. Mit Nachrüst-Geräten wie **Chipolo** oder **TrackR** – einem Anhänger von der Grösse einer Münze – lässt sich für knapp 30 Franken jeder Gegenstand auffindbar machen. Im Haus, wo er auf dem Bildschirm des Smartphones eine Annäherung signalisiert oder per Knopfdruck zum Piepsen gebracht wird. Aber auch in der grossen weiten Welt. Aus der meldet er dem Besitzer via Internet seine Position. Wie das? Wo das Gerät doch nur gerade über einen Pieper, eine Batterie und ein Bluetooth-Kurzstreckenfunkmodul verfügt?

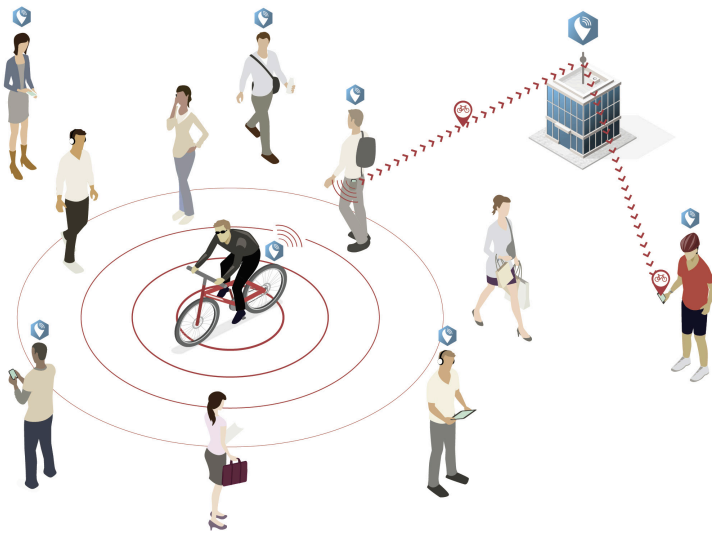


Abbildung 1: TrackRs Crowd-GPs

TrackR setzt auf die "Weisheit der Masse". Jeder TrackR-Anhänger verbindet sich automatisch mit jedem Smartphone in Reichweite, auf dem die TrackR-App installiert ist – also auch mit denen fremder TrackR-Benutzer. Die wiederum meldet der Zentrale eine "Sichtung" des eben verbundenen Tags. Dessen Besitzer kann in seinem Konto auf der TrackR-Website nachsehen, wo sein Tag gesichtet worden ist.

“Crowd GPS” nennt der Hersteller das Prinzip, indem alle Benutzer von TrackR-Anhängern von allen anderen Nutzern profitieren. Sie müssen dazu keinen Finger krümmen: Die Geräte übernehmen die Kommunikation.

Willkommen im Internet der Dinge.

Ein Kühlschrank allein ist ziemlich dumm

Englisch heisst es “Internet of Things” – oder kurz IoT. Die Rede ist dabei nicht von neuen Antennen, Funkstandards und einer Infrastruktur, die noch entstehen muss. Es ist alles schon da. Der Begriff steht für nicht mehr als die Integration der bisher passiven Maschinen, Geräte und Sensoren in den Computerverbund namens “Internet”. Dadurch können sie Informationen und Daten anbieten oder selber von anderen Geräten und Sensoren beziehen, Aktionen auslösen und dadurch Prozesse regulieren und optimieren. Die Idee, das Internet für den Fernzugriff auf Geräte, Maschinen und Rechner zu benutzen ist alles andere als neu. Die Carnegie-Mellon-Universität stellte bereits 1982 einen Coca-Cola-Automaten ins Internet, dessen Befüllungsstand und Temperatur weltweit über das Internet abgerufen werden konnte.

Knappe zehn Jahre später – das World Wide Web, das heute fälschlicherweise häufig mit dem Internet gleichgesetzt wird, gab es noch immer nicht – veröffentlichte Mark Weiser ein Papier über den [“Computer für das 21. Jahrhundert”](#). Der Wissenschaftliche Mitarbeiter des futurologischen Think-Tanks Xerox Parc prägte darin noch nicht direkt den Begriff des Internet der Dinge, aber denjenigen des “Ubiquitous Computing”, also der Allgegenwart der Informatik: Erst wenn die Computer bis zur Unsichtbarkeit in unseren Alltag integriert würden, werde das wahre Potential der Vernetzung sichtbar.

Alles andere als unsichtbar war der bis dahin überall als Zukunftsvision beschworene “Kühlschrank mit Internetanschluss”. Das Gerät bestellt gemäss Legende bei Leerbestand autonom Joghurt, Milch und Butter: Die naheliegendste Vision eines Internets der Dinge, lange bevor jeder und jede einen leistungsfähigen Computer in der Hos-

tasche hatte. Von Samsung ist inzwischen [ein solcher Kühlschrank erhältlich](#), der allerdings dem Besitzer lediglich Fotos des Inhalts auf das Smartphone schickt.

Konkretere Formen nahm das “Internet für Dinge” ab 1999 an. Damals startete eine Abteilung des renommierten Massachusetts Institute of Technology (MIT) eine Initiative grosser Handelsketten, um mit einer Kombination aus dem bereits etablierten Elektronischen Produkt-Code EPC und preiswerten RFID-Tags jedes einzelne Objekt aus dem Sortiment verfolgbar zu machen. Letztlich erwiesen sich die RFID-Tags trotz sinkender Herstellungskosten als zu teuer, um damit jedes einzelne Produkt zu kennzeichnen. Wäre dies zum Standard geworden – unser Kühlschrank wäre längst so schlau wie einst versprochen.

Der Überblick schafft neues Verständnis

Wären alle Kühlschränke schlau, die Welt würde insgesamt [4 Prozent ihres Bruttosozialprodukts an weggeworfenen Lebensmitteln](#) einsparen – 2,6 Billionen US-Dollar jährlich.

In den Dimensionen von Volkswirtschaften dürften die Auswirkungen des Internets der Dinge am stärksten bemerkbar werden. Allein schon durch die Erkenntnisse, die aus den Informationen von Millionen von Echtzeit-Sensoren gewonnen werden können. Plötzlich lassen Big-Data-Analysen die Ausbreitung von Epidemien, Wetter-Anomalien oder auch der Ferienreiseverkehr im Juli analysieren und sogar vorhersagen.

Der zweite Schritt aber ist noch wichtiger: Indem die Geräte, Maschinen und Systeme, die Dinge für die Menschen erledigen, zusammenschaltet und mit den Ergebnissen der Analysen versorgt werden, können sie ohne Komfortverlust für die Menschen den Verbrauch reduzieren, die Effizienz steigern und das grosse Ganze optimieren.

- Dank Smart Cities und vernetzten smarten Autos gehören Staus und Parkplatz-Suchverkehr der Vergangenheit an;

- die Präzisions-Landwirtschaft steigert die Erträge und schont die Umwelt;
- in der Industrie werden Produktions- und Lieferzeiten verkürzt;
- Echtzeit- Gesundheitsdaten helfen, die Grippe und andere epidemische Erreger auszurotten;
- im Frischwarenhandel werden Überschüsse vermeidbar – und so weiter.

All diese Effizienzgewinne werden möglich, wenn die Instanzen, welche die Prozesse steuern, mehr und schneller miteinander kommunizieren. Der Netzwerkausrüster Cisco schätzt, dass heute bereits 20 Milliarden Geräte und Objekte “vernetzt”, das heisst via Internet erreichbar sind. Aber erstens sind viele von ihnen noch alles andere als “smart”. Das heisst, sie lassen sich auf grosse Distanz lokalisieren oder allenfalls ein- oder ausschalten. Aber sie brauchen weiterhin die Steuer- und Befehlseingabe von Menschen. Der nächste Schritt zum Internet der Dinge besteht deshalb darin, die Maschinen direkt mit anderen Maschinen kommunizieren zu lassen.

M2M-Kommunikation heisst das Schlüsselwort.

Zu viele Ideen, zu wenig Wissen

Weil M2M (Machine-To-Machine) -Kommunikation bisher nur eine marginale Rolle gespielt hat und im Netz vor allem Menschen via Maschinen mit Menschen (sozusagen H2M2H) kommuniziert haben, bestehen die gigantischen Datenbestände im Internet und den Rechenzentren der Welt vornehmlich aus menschlichen Ideen, Gedanken und kreativen Werken – und nur zu einem verschwindend kleinen Teil aus Daten, Fakten und maschinenlesbaren Informationen.

[Kevin Ashton](#) gehörte zu den Wissenschaftlern, die den Begriff des “Internet of Things” prägten. Einer der Gründer des Auto-ID-Centers am Massachusetts Institute of Technology, schrieb er bereits [2009 in](#)

in einem Artikel im RFID-Magazine “praktisch alle Datenbestände im Internet sind ursprünglich von Menschen erfasst worden, durch Tastatureingaben, den Druck auf einen Aufnahme-Knopf, den Auslöser einer Digitalkamera oder das Scannen eines Strichcodes.” Die Menschen, schreibt Ashton, sind somit eine der wichtigsten Knotenpunkte der Vernetzung. Aber erstens hätten sie wenig Zeit und zweitens seien sie nicht besonders gut im Erfassen von Daten über die reale Welt.

“Und das ist ein Problem. Unsere Wirtschaft, unsere Gesellschaft und unser Überleben basieren nicht auf Ideen oder Informationen, sie basieren auf Dingen. Man kann Bits nicht essen, verbrennen zum Heizen oder in den Tank füllen. Ideen und Informationen sind wichtig, aber Dinge sind viel wichtiger.

Und doch ist die heutige Informationstechnologie dermassen abhängig von Daten aus menschlichen Köpfen, dass unsere Computer mehr über Ideen wissen als über Dinge.”

Das soll sich mit der Vernetzung von Milliarden von Geräten ändern. Die Computer sollen dadurch ermächtigt werden, sich selber ein Bild der Welt zu machen, das auf Fakten basiert und nicht aus Erzählungen von Menschen entstanden ist, sozusagen.

In einer zweiten Entwicklungsstufe mutiert das Internet der Dinge zum “Internet von allem” – wenn auch alle übrigen Objekte, die keinen zusätzlichen Informationen ausser beispielsweise ihren Aufenthaltsort in die Vernetzung einbringen können, mit Tags versehen im Netz vorhanden sind.

Die je nach Sichtweise utopische oder dystopische Vision ist eine Welt, in der alle wesentlichen Informationen über den Zustand jedes von Menschenhand geschaffenen Objekts verfü-, analysier- und verwertbar sind und dazu auch direkt von Geräten und Prozessen verwandt werden können – ohne weiteres Zutun des Menschen.

Neben einer funktionierenden Vernetzung auf allen Ebenen der Gesellschaft und auf allen technisch denkbaren Stufen ist dazu eine gigantische Zahl von Sensoren nötig, die an allen Berührungspunkten

zwischen realer und virtueller Welt die entsprechenden Daten erheben und zur Verfügung stellen.

Und weiter bedingt die Vision, dass die Maschinen, die sich aus dem riesigen Datensee bedienen und Prozesse und Vorgänge beschleunigen, optimieren und nachhaltiger machen sollen, dazu die Befugnis, aber auch die Befähigung erlangen:

Sie müssen intelligent werden.

Smart Home, das Wunschhaus

Wie oft wünschen Sie sich, Dinge mit einem einzigen Zuruf erledigen zu können: “Staubsaugen im Wohnzimmer!” – “Badewasser mit einer Temperatur von 30 Grad einlassen!” – “Katzenstreu, Mineralwasser und Knuspermüsli bestellen”?

Alles längst möglich.

“Alexa, setze einen Termin von neun bis zehn am Freitag mit dem Titel “Arztbesuch” in meinen Kalender. Alexa, programmiere den Roomba-Staubsauger auf achtzehn Uhr heute Abend. Alexa, öffne das Garagentor.”

In immer mehr Haushalten weltweit sind solche Befehlsrufe zu vernehmen. Die Adressatin ist kein geklontes Zimmermädchen, sondern das keine zweihundert Franken teure Spracherkennungs-System “Echo” des Internet-Giganten Amazon. Das Gerät erkennt Sprachbefehle und gibt nicht nur Antwort auf allgemeine Fragen, sondern steuert Programme, Apps und viele ins Heimnetzwerk eingebundene

Geräte. Ganz ähnlich funktioniert das Konkurrenzprodukt “Home” von Google, ebenso wie Apples “HomeKit” – und eine ganze Reihe von Einzel-Apps für Smartphones.

Damit sich Heizung, Klimaanlage, Lichtschalter, Türen, Unterhaltungselektronik und Haushaltgeräte so oder zum Beispiel auch per Smartphone-App von ausserhalb der eigenen vier Wände steuern lassen, müssen einige Voraussetzungen erfüllt sein.

Die wichtigste: Sie müssen vernetzt sein.

Die Party in Ihrem Heimnetz

Die Zahl der Geräte, die in diese Systeme eingebunden werden können, steigt rasant. Einige von uns mögen sich daran erinnern, dass wir noch vor weniger als zwanzig Jahren in den meisten Haushalten entscheiden mussten, ob wir die Telefonleitung für einen Anruf oder für eine Verbindung ins Internet benutzen.

Nachdem in den neunziger Jahren der schnelle, nicht mehr die Telefonleitung blockierende Internet-Anschluss über das TV-Kabelnetz auch in Privathaushalten populär wurde, waren zunächst pro Haushalt ein- bis zwei Geräte mit dem Netzwerkrouter verbunden: Der Desk- oder Tower-Computer und allenfalls ein Notebook, das mit Kabel und später über das persönliche Funk-WiFi ans Netz ging.

Heute beziehen in nicht sonderlich modernen Haushalten nicht selten Dutzende von Geräten eine IP-Adresse und verbinden sich mit dem Internet. Wer glaubt, dass es sich dabei um die Smartphones, Tablets und Notebooks im Hause handelt, sollte genauer hinschauen: Im lokalen Netz tummeln sich die Smart-Watch und alle Smart-TVs im Haus, die Streaming-Stereoanlage mit vier oder fünf WiFi-Lautsprechern; der Roboter-Staubsauger und sein Cousin Rasenmäher; die Fitness-Personenwaage, sämtliche Festnetz-Telefonapparate, der Familien-Datenspeicher, Apple-TV oder andere Settop-Boxen und in modernen Haushalten nicht selten Waschmaschine und Tumbler, Geschirrspüler, Kaffeemaschine und der ominöse Kühlschrank. Vieles davon

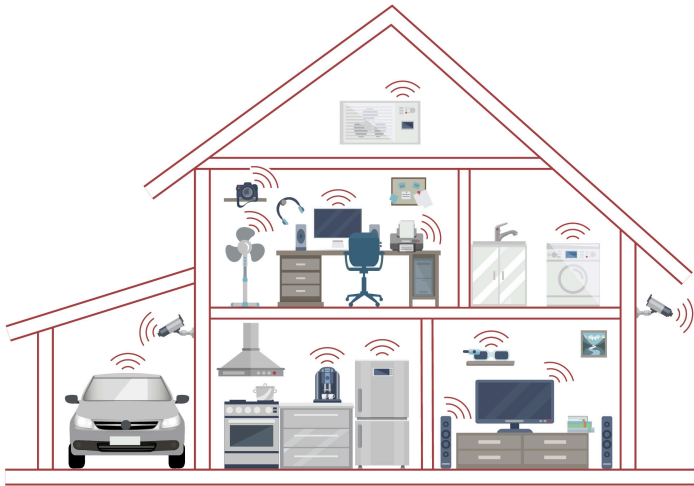


Abbildung 2: Das vernetzte Haus

lässt sich heute schon via App oder eben mit einer Schnittstelle zu einem der Sprach-Heimsteuerungssysteme fernsteuern.

Warum die Infrastruktur simpler...

Natürlich haben längst vor dem Trend zum Internet der Dinge viele Hersteller von Steuerungselektronik den Braten gerochen und versucht, die Wünsche der Hausbesitzer zu erfüllen – das Resultat war ein Durcheinander an proprietären, das heisst nicht miteinander verknüpfbarer Haustechnik-Systeme. Wer vom Couchtisch aus das Garagentor, die Überwachungskamera an der Haustüre und die Sonnenstore auf der Terrasse steuern wollte, musste alle Komponenten dafür beim gleichen Hersteller kaufen – und war nach einer einmaligen Entscheidung sowohl preislich wie auch vom Angebot her dem Hersteller ausgeliefert.

Immerhin gab es Initiativen, um einheitliche Standards zu definieren, damit die Sensoren von Hersteller A auch mit den Lichtschaltern von Hersteller B funktionierten: Die meisten solchen Gebäudeautomatisierungs-Standards sind aber ebenso teuer wie unflexibel. Sie lassen keinen Spielraum für Anwendungen, die über die ursprünglich geplanten Funktionen hinausgehen. Namentlich die Übertragung grösserer Datenmengen ist nicht vorgesehen. Audio- und Video- Anwendungen, die immer mehr aufkommen, sind damit nicht realisierbar. Vor allem aber waren diese Systeme für “dumme” Geräte ausgelegt. Die Komplexität, die eigentliche “Intelligenz”, steckt im Netz und seinen Schaltungen. So besteht ein analoger Telefonapparat im Prinzip nicht aus mehr als einem Lautsprecher, einem Mikrofon und einem Impulsgeber. Sämtliche komplexen Vorgänge übernahmen im analogen Telefonnetz die Zentralen.

...und die Geräte smarter werden sollten

Dank der atemberaubenden Entwicklung in der Prozessortechnik und dem resultierenden Preiszerfall ist es heute preiswerter, die Geräte selber “smart” zu machen und in bestehende Computernetze zu integrieren. Ein aktuelles, digitales IP-Telefon ist ein Computer inklusive Web-Server, dessen komplexe Funktionen jederzeit erneuert und vollständig neu konfiguriert werden können.

Ähnliches gilt für die meisten Haushaltmaschinen, die noch vor Jahren mit komplizierten mechanischen Steuerungseinheiten ausgestattet und durch den Druck einer bestimmten Tastenkombination gesteuert wurden. Heute übernehmen diesen Job winzig kleine eingebettete Computer. Diese wiederum können mit wenig Aufwand netzwerkfähig gemacht werden: Interessant für Hersteller, die so Fernwartung anbieten und den Gebrauch ihrer Produkte bei allen vernetzten Kunden statistisch erfassen können.

Die Gemeinsame Sprache all dieser Geräte und Computer ist das Netzwerkprotokoll TCP/IP, auf dem das Internet und jedes typische Computernetz in jedem Privathaushalt beruht. Damit die Waschmaschine

oder der Kühlschrank auch wirklich auf Distanz Befehle annehmen kann und sich bedienen lässt, wie wenn man seine Knöpfe gedrückt hätte, muss der Hersteller eine Programmierschnittstelle bereitstellen. In jedem Fall aber steckt heute die komplexe Steuerungslogik direkt in den Geräten.

Noch “denkt” das Rechenzentrum

Oder vielleicht doch nicht? Ein zweiter genereller Trend der Digitalisierung ist nämlich die Virtualisierung. Dabei werden die Ressourcen – Rechenleistung, Speicher – nicht mehr direkt im Gerät bereitgestellt, sondern über das Netz “bezogen”. So ist beispielsweise Spracherkennung eine äusserst rechenintensive Angelegenheit. In den zylinderförmigen Geräten von Amazons “Echo” steckt denn auch nicht der Supercomputer, die die Sprachbefehle des Nutzers erkennt: Vielmehr schickt “Alexa” die aufgezeichneten Sprachdateien aus unseren Wohnzimmern in ein Rechenzentrum von Amazon, wo sie ausgewertet und die Antwort an Alexa daheim zurückgeschickt werden. Das gleiche gilt für die Spracherkennungsleistungen von Google.

In der Nutzung allerdings bleibt der Effekt für uns Anwender der gleiche: Ob das Gerät selbst clever ist und mich versteht oder ob es diese Funktion dank Vernetzung woanders her bezieht, ist nicht erkennbar.

Architektur – Netze und Sensoren

In den zwanziger Jahren des vergangenen Jahrhunderts hatte sich das Telefon in den Wirtschaftsmetropolen der USA etabliert. Auf den Tischen der Vorzimmerdamen standen aber bisweilen ein Dutzend Telefonapparate. Die Telefongesellschaften befanden sich in einem harten Wettbewerb und hüteten sich, [Zugang zu Abonnenten in anderen Netzen zu gewähren](#). Wer sicher sein wollte, jeden Abonnenten erreichen zu können, musste alle Dienste abonnieren – und wissen, wen er in welchem Netz finden konnte.

Wie das “Inter” ins Netz kam

Solche Bemühungen der Anbieter sind eine logische Folge der Marktwirtschaft. Im Wettbewerb geht es darum, die Konkurrenz durch technische Abgrenzung vom eigenen Markt auszuschliessen. Während dies im Fall von Kaffekapseln, Druckerpatronen oder Softwareprogrammen lediglich die Wahlfreiheit der Konsumenten einschränkt, steht ein Mangel an Interkonnektivität in Netzwerken allerdings in

direktem Widerspruch zu deren ureigenstem Zweck – der Verbindung möglichst vieler Endpunkte.

Deswegen kommt es in diesem und anderen wesentlichen Belangen der gesellschaftlichen Entwicklung zur Regulierung durch den Gesetzgeber. Jedenfalls dann, wenn sich die Anbieter nicht vorher auf Standards einigen können, um den staatlichen Eingriffen vorzubeugen.

Das Internet ist keinem dieser beiden Vorgänge zu verdanken. Es ist, wie viele andere kostenintensive Basisentwicklungen, militärischen Ursprungs. Das US-Verteidigungsministerium erkannte in den Sechziger Jahren die Notwendigkeit für ein Kommunikationsnetz, das nicht unterbrochen werden konnte. Der Internet-Vorgänger Arpanet war darauf ausgelegt, auch dann noch alle funktionierenden Endpunkte zu verbinden, wenn umfangreiche Teile des Netzes ausgeschaltet oder zerstört sind. Denn genau damit war bei einem Atomkrieg zu rechnen, wenn der elektromagnetische Impuls nuklearer Explosionen die Elektronik ganzer Landesteile lahmlegen würde. Das Internet sollte die Inter-Konnektivität aller funktionierenden Netzteile garantieren.

Offen für alle

Die Lösung fand sich in zwei Prinzipien. Zum einen wurden bei der Entwicklung des Internets die Architektur strikte getrennt vom Einsatzzweck. Anders als beispielsweise beim Telefonnetz, das für die Übertragung von Tönen optimiert und deswegen für anderes kaum einsetzbar war, ist das Internet auf keine konkrete Anwendung, sondern auf die Vermittlung von Daten ausgerichtet. Ungeachtet welcher Art sie sind oder welchem Zweck sie am Ausgangs- und Endpunkt der Verbindung dienen.

Das funktioniert, weil digitalisierte Informationen immer aus den gleichen Grundelementen bestehen: Bits (1 oder 0) und Bytes (aus acht Bits bestehende Zeichen). Das heisst noch nicht, dass der Inhalt einer Datei für jede Software verständlich ist. Ein digitales Foto ist für das Musikprogramm nicht brauchbar und vielfach schon von einem Bildbearbeitungsprogramm eines Drittherstellers nicht mehr interpretierbar.

Den Übertragungsprotokollen des Computernetzwerks aber ist das einerlei. Sie zerlegen jede Datei in gleichförmige Päckchen und schicken diese auf die Reise zum Zielrechner.

Und hier greift das zweite Prinzip, welches das Internet ausmacht und seine Protokolle zum erfolgreichsten System für Computernetze hat werden lassen: Jedes Päckchen sucht sich nämlich sozusagen selber den Weg durchs Netz. Stark vereinfacht geht das so, dass jedem Paket eine Adresse und ein Absender aufgestempelt wird. Dann wird es an den nächsten Knotenpunkt im Netz weitergereicht, der es an seinen nächsten Nachbarn in Richtung des Ziels weitergibt. Quittiert dieser Nachbar den Empfang und die Weiterleitung nicht, dann versucht es der Knotenpunkt beim nächsten geeigneten Nachbarn. So kann es sein, dass von einer Lieferung aus fünf Paketen von Genf nach St. Gallen drei den Weg über Bern, eins über Basel und eins über Mailand weitergereicht werden. Das spielt am Zielort keine Rolle, so lange die Pakete ungefähr gleich schnell durchgereicht wurden, alle angekommen sind und damit zur kompletten Datei zusammengesetzt werden können.

Für die Sicherstellung dieses Vorgangs ist das weltberühmte Gespann von "TCP" und "IP" zuständig, "Transmission Control Protocol" und "Internet Protocol" – und das Fundament der "Ebenen-Architektur" ("OSI-Layer", s. Abbildung) für Netzwerkprotokolle. Die Internet-Adresse oder IP ist dabei das wichtigste Element, das jedem Objekt und jedem Gerät im Netz zugeordnet werden muss, damit es von jedem anderen Punkt angesprochen werden kann.

Was aber bedeutet das alles? Es bedeutet, dass das Internet eine extrem hohe Liefersicherheit für Daten bietet, und dass diese Daten alles sein können, was sich in Bits und Bytes ausdrücken lässt.

Man könnte sagen, das Internet ist ein extrem weit verzweigtes Straßennetz für Datenpakete. Auf dieser viel zitierten Datenautobahn werden im Internet der Dinge immer mehr Roboterkuriere Informationen zwischen Maschinen transportieren.

Das WWW ist nur eine Anwendung

Grundsätzlich kann jeder Softwarehersteller, jede Firma ihr eigenes System erfinden, wie sie das Datennetz einsetzt. Der Transport ist geregelt und die Adressen werden aufgefunden – aber was die Pakete enthalten und wozu sie dienen, das ist vollkommen offen.

Nur ist der Nutzen solcher Systeme viel grösser, wenn sich alle Beteiligten auf eine Methode einigen, die auch den gegenseitigen Austausch erlaubt. Im Fall des Telefonnetzes war das die Vereinheitlichung des Nummern-Systems und die Verbindung aller Netze in der Interkonnektivität.

Im Computernetz sind es Absprachen zwischen allen mittels IP-Adresse erreichbaren Teilnehmern für jede generell genutzte Anwendung. Diese Absprachen oder Standards heissen “Protokolle”, und es gibt sie für Dinge wie Email-Versand (SMTP, POP, IMAP), Zeit-Abfragen (NTP) oder den Versand von Hypertext-Dateien: HTTP – Hyper-Text-Transfer-Protokoll.

Letzteres ist Ihnen zweifellos aus der Adresszeile ihres Internet-Browsers bekannt. Und es eignet sich hervorragend, um zu zeigen, dass das World Wide Web nichts anderes ist als eine von vielen Anwendungen, die auf die Basis-Infrastruktur des Internets mit TCP/IP aufgesetzt ist. Die leicht merkbaren “Uniform Resource Locator” oder URL wie “Schuhe.ch” und dergleichen sind nichts anderes als Stellvertreter für numerische IP-Adressen, weil wir uns die als Menschen nicht so gut merken können.

Und wo sind die Dinge?

Die Frage, was genau das Internet der Dinge ist, lässt sich schon deswegen nicht exakt beantworten, weil es aus vielen Einzelteilen besteht. Nicht nur aus den per IP-Adresse erreichbaren Geräten, sondern aus Unter-Netzwerken, aus Protokollen und Anwendungen, die wir jetzt noch nicht alle kennen. Denn das Internet der Dinge wächst rasant, und die Schweiz liegt ganz vorne: Laut der Organisation für Sicherheit







7. Schicht		Anwendung	Funktionen für Anwendungen, sowie die Dateneingabe und -ausgabe.
6. Schicht		Darstellung	Umwandlung der systemabhängigen Daten in ein unabhängiges Format.
5. Schicht		Sitzung	Steuerung der Verbindungen und des Datenaustauschs.
4. Schicht		Transport	Zuordnung der Datenpakete zu einer Anwendung.
3. Schicht		Vermittlung	Routing der Datenpakete zum nächsten Knoten.
2. Schicht		Sicherung	Segmentierung der Pakete in Frames und Hinzufügen von Prüfsummen.
1. Schicht	100101110 001110110 110101001	Bitübertragung	Umwandlung der Bits in ein zum Medium passendes Signal und physikalische Übertragung.

Abbildung 3: Das Prinzip der OSI-Layer

und Zusammenarbeit [sind in der Schweiz auf 100 Einwohner bereits 29 Dinge online](#). Weiter entwickelt ist das IoT nur in Korea (37.9) und Dänemark (32).

Sie benutzen das Internet der Dinge, wenn Sie aus dem Urlaub vor der Heimreise die Heizung zu Hause hochfahren. Wahrscheinlich geschieht das mit einer App auf dem Smartphone, welche via Internet mit Ihrem Router zu Hause Kontakt aufnimmt, der sie in Ihrem lokalen Netz zu Hause zur Heimsteuerungsanlage verbindet, welche die Steuerbefehle entgegennimmt und umsetzt. Sie benutzen es auch, wenn sie über Amazons Spracherkennung Echo zu Hause die Heizung regulieren, wobei "Echo" Ihre Stimme aufnimmt, die Datei via Router durchs Internet zu Amazon schickt, wo sie im Rechenzentrum in Text übersetzt und dieser wieder an Ihre "Alexa" im Haus geschickt wird, die nun ihrerseits den Steuerbefehl im lokalen Heimnetz an Ihre Heizungssteuerung übermittelt.

Wer genau hinsieht, erkennt: Die Daten verlassen Ihr privates Netz, werden durch das mehr oder weniger öffentliche Internet zu Amazon in deren Netz und das Rechenzentrum übermittelt, dort verarbeitet, zurückgeschickt an Ihren Router, von dort an “Alexa” und von dieser an das Haussteuerungs-System, das seinen eigenen Funkstandard haben kann. Der Datenfluss reicht also durch drei Netze und mehrere Standards.

Solche Vorgänge werden noch viel mehr stattfinden, wenn die Industrie, Behörden und andere Organisationen zusehends auf Daten von Sensoren und vernetzten Geräten bauen. Das Internet der Dinge ist demnach ein Netz der Netze, zusammengehalten durch die Datenautobahn Internet.

Das verlangt nach neuen Absprachen, Übergabepunkten und Sicherheitsprotokollen. Denn die Schnittstellen zwischen den Netzen und Anwendungen sind immer ein Risiko: Sie können missbraucht werden und Unberechtigten Zugriff auf ein internes Netz geben, oder sie können ausfallen und den Datenfluss unterbrechen. Die Zuverlässigkeit der Übergänge – im Internet ein systemimmanenter Teil des Transportprotokolls – ist ein ebenso bedeutendes Thema wie die Absicherung der Knotenpunkte gegen unerlaubte Zugriffe.

Das IoT stellt neue Anforderungen an die Architektur aller andern Netze: Es ist die grösste technische Integrationsbewegung, die die Welt je gesehen hat. Und sie soll zuverlässig über alle Barrieren und Grenzen hinweg funktionieren. Das ist spätestens dann von hoher Bedeutung, wenn nicht mehr in erster Linie Ideen, sondern sensible Sensordaten und lebenswichtige Steuerbefehle durch die Netze fließen. Das Internet der Dinge braucht deswegen eigene Standards und Sicherheitsdefinitionen für die Architektur, die Datenübergabe an den Gateways, die Identifikation der Devices und Applikationen, die Integration der verschiedenen Netze und letztlich auch für die Erkennbarkeit von Unregelmässigkeiten.

Der Kampf um Standards hat begonnen

All das ist erst im Entstehen begriffen: Branchen- und Spezialistenverbände wie das [Institute of Electrical and Electronics Engineers](#) bemühen sich, Standards für die Anforderungen an die künftigen Knotenpunkte und protokolle zu definieren.

Eines ist klar: Das Internet der Dinge bindet alles ein, was es derzeit schon gibt – und noch viel mehr, das erst kommen wird: Neben der aktuellen Infrastruktur aus TV-Kabelnetzen, Telefon-, Glasfaser-, Satelliten-Anbindungen und Mobilfunkstandards gehören WLANs, Bluetooth-Anbindungen und spezielle IoT-Netze wie das für Stadtgebiete entwickelte Low Power Network dazu.

Die Basis des ganzen aber wird ein Prinzip sein, zu dem die Entwickler des TCP/IP-Gespans um Vint Cerf vor fast fünfzig Jahren den Grundstein gelegt haben: Die radikale Trennung von Infrastruktur und Anwendung. Damit einher geht ein weiteres Prinzip, das derzeit politisch umstritten ist – das der Netzneutralität. Es besagt, dass alle Datenpakete in allen Netzen genau gleich behandelt werden, ungeachtet dessen, was sie transportieren oder wem das Netz gehört, durch das sie geleitet werden.

Auch dieses Prinzip war für die Entwicklung des Internets von unschätzbarem Wert, weil jeder, der die technischen Kenntnisse hatte, ein Protokoll (also eine Anwendung für Daten) entwickeln und sicher sein konnte, dass seine Daten im Netz gleich behandelt würden wie die aller andern. Das funktionierte, weil man davon ausging, dass sich die Kosten für die Infratrstruktur ungefähr zu gleichen Teilen über alle, die profitieren, verteilen.

Heute ist diese Frage nicht mehr so einfach zu beantworten. Nachdem Netzbetreiber angefangen haben, mit Datenmengen zu argumentieren, die beispielsweise ein Videoanbieter wie Netflix verschickt und dabei ein Geschäftsmodell zu grossen Teilen auf der Verfügbarkeit schneller Datenanbindungen seiner Kunden aufbaut. Deshalb werden Stimmen laut, welche die Datenpakete in der Durchleitungspriorität

abstufen möchten: Je nach der Kostenbeteiligung der Absender/Adressaten. Demnach könnte beispielsweise Netflix die Auslieferung seiner Daten auf der Überholspur “erkaufen”, während andere Video-Streaming-Anbieter oder Youtube-Videos von den Netzbetreibern benachteiligt und ihre Daten langsamer ausgeliefert würden. Mit dem Internet der Dinge bekommt auch diese Diskussion einen neuen Aspekt.

Künstliche Intelligenz

Am 9. Januar 2007 wurden die Aussichten für das Internet der Dinge auf einen Schlag realistisch: Apple stellte das iPhone vor. Binnen weniger Jahre katapultierte der Siegeszug des Smartphones die Welt ins Zeitalter des “Ubiquitous Computing”. Mark Weisers Vision wurde, mit heute rund 2.5 Milliarden Smartphone-Benutzern weltweit, zur Realität.

Niemand weiss, wie Software lernt

Mehr noch – sie wurde übertroffen. Denn die leistungsfähigen Computer, die wir alle in der Tasche herumtragen, sind auch vernetzte Horchposten. Lage-, Positions-, Temperatur-, Lärm-, Licht- und Bewegungssensoren liefern endlose Datenströme und damit Möglichkeiten zur Analyse nie gekannter Mengen an Daten.

Das Paradoxon daran: Der grösste Nutzen dieser Sensoren liegt in der Summe der Messdaten und nicht in den punktuellen Informationen für den individuellen Smartphone-Besitzer. Oder konsultieren Sie etwa im Alltag die Positionsangabe ihres Smartphones? Sie wissen auf den Meter genau, wo sie sich befinden. Dank dem smarten Sensor in

Ihrer Tasche wissen es jetzt aber auch alle anderen – und können den Stau, in dem Sie stecken, umfahren.

Anders gesagt: Was für den einzelnen mässig nützlich ist, liefert dank der Perspektive auf das grosse Ganze Einblicke, die bisher gar nicht oder nur mit erheblichem Aufwand gewonnen werden konnten.

Je höher die Zahl und die zeitliche Dichte der Messdaten, umso deutlicher zeigen sich Muster, Abläufe und Zusammenhänge. Seit Jahren ist deshalb die Rede von “Big Data”. Der Begriff steht für den Wert der Erkenntnisse, die aus gigantischen Datenmengen und ihrer Analyse gewonnen werden können. Egal, ob das geologische Werte bei der Erdölsuche, die Kundendaten eines Grossverteilers oder die Wetterdaten eines ganzen Kontinents sind.

Wie bewegen sich Verkehrsströme? Wie verbreiten sich Krankheiten? Das sind nur die Basisdaten, aus denen sich in Kombinationen weitaus komplexere Analysen in Echtzeit treffen und sogar Vorhersagen berechnen lassen.

Wenn noch dazu alle beteiligten Dinge im Netz miteinander kommunizieren, könnten Routing-Systeme im Verkehr Staus eliminieren und den Treibstoffverbrauch radikal senken. Epidemien können effizient bekämpft, Produktionssysteme und Logistik perfektioniert und die Ernteerträge in der Landwirtschaft optimiert werden.

Programme schreiben sich selber

Das Internet der Dinge lässt den Strom an Daten exponentiell ansteigen. Eine Boeing 737 produziert auf einem einzigen Flug von der US-Ost- an die Westküste eine Datenmenge von 120 Terabytes. Tausende von Flugzeugen [fliegen diese Strecke](#) – täglich.

Die Analyse solcher Informationsmengen ist auch mit Computern eine Herausforderung. Dabei erhoffen sich Verkehrsplaner und Ökonomen, aber auch Mediziner, Soziologen und andere Wissenschaftler ganz neue Erkenntnisse aus dem grossen Zahlenchaos, das die fast flä-

chendeckende Erhebung von Echtzeit-Daten jeglicher Art heute schon ermöglicht.

Das hat nur einen Haken: Computer können Daten vergleichen, Spitzenwerte und Durchschnitte berechnen und Kurven aufzeichnen. Aber sie sind nicht im Stande, Unbekanntes zu interpretieren oder gar in einen Kontext zu setzen und zu erklären.

Jedenfalls noch nicht, denn sie sollen es lernen. Künstliche Intelligenz, englisch AI, gilt als der Schlüssel zur nächsten Stufe des Wissens. Stark vereinfacht ruhen die Hoffnungen darauf, dass "intelligenten" Computern unstrukturierte Informationen ohne weitere Anweisungen eingegeben werden können – und sie selbstständig qualitative Aussagen daraus ableiten.

Noch ist zwar nicht klar, ob Prozessoren je zu den Leistungen des menschlichen Hirns im Stande sind: Wir verarbeiten nicht nur mathematisch erfassbare Daten und lernen permanent dazu, wir adaptieren auch und lassen uns von Emotionen leiten, was "Intuition" genannt wird. Rechenmaschinen, so die bisherige gängige Meinung, sind dazu nicht in der Lage. Sie gewinnen lediglich im Schachspiel, wo das berechnen einer gigantischen Zahl von Möglichkeiten einen Vorteil bietet.

Sind Pokerspieler intelligent?

In jüngster Zeit haben Wissenschaftler aber mit einem anderen Spiel den Gegenbeweis angetreten: Erstmals gewinnen [Computer gegen Menschen im Pokerspiel](#). Dort beruht der Erfolg zu grossen Teilen auf taktischem Geschick und auf der Täuschung des Gegners durch "bluffen". Offensichtlich können Computer dieses Verhalten erlernen.

Die Antwort auf die Frage, wer ihnen solche Dinge beibringen soll, lautet: Sie selbst. Anders ist das Ganze nicht möglich: Ein Computerprogramm besteht aus einer Folge von Anweisungen und festgeschriebenen Kriterien – kein Mensch kann alle Möglichkeiten in jeweils passende Befehle programmieren. Erst wenn ein Computer im Laufe des

Programms die Kriterien anpassen und die Anweisungen ausbauen kann, wird er lernfähig.

Genau das passiert beim sogenannten “Deep Learning” in künstlichen neuronalen Netzen. Die Computer werden mit einem Lern-Algorithmus ausgestattet und dann mit grossen Datenmengen gefüttert – zwei Millionen Darstellungen und Beschreibungen eines Stuhls, zum Beispiel. Am Ende des Prozesses kann der Computer einen Stuhl erkennen, auch wenn er von dem Modell noch kein Bild “gesehen” hat – und einen Tisch als “Nicht-Stuhl” identifizieren, obwohl der doch auch vier Beine und eine Fläche aufweist. Welche Kriterien er dafür anwendet, ist nicht klar: Die Software hat sie selber definiert. Das Programm hat sich selber geschrieben.

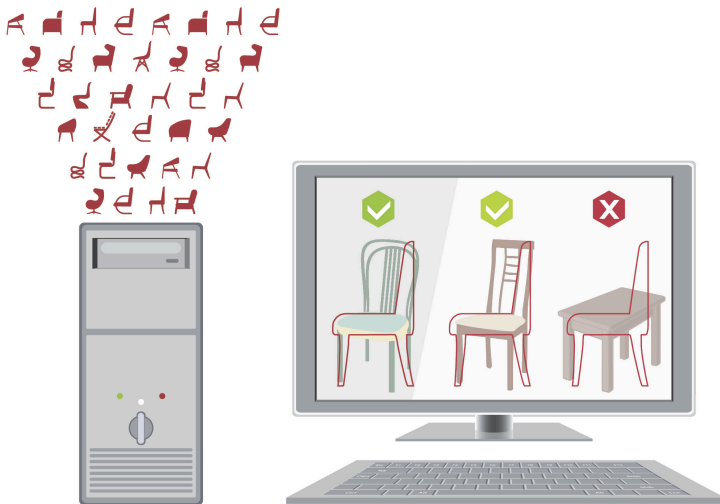


Abbildung 4: Wie neuronale Netze lernen, Stühle zu erkennen und von Tischen zu unterscheiden.

Neuronale Netze sind in der Computertechnik nichts neues. Aber die Erfolge in Sachen Künstliche Intelligenz, die wir ihnen im Alltag

bereits verdanken – von der Spracherkennung wie Alexa oder Siri bis zu autonom fahrenden Autos – sind erst in jüngster Zeit möglich geworden. Dabei war die exponentiell steigende Rechnerleistung nur eine der Voraussetzungen, die erfüllt wurden. Eine andere war die Verfügbarkeit der Datenmengen für das Training der Netze. So gross ist der Quantensprung, dass ihn Experten als “Kambrische Artenexplosion” der Künstlichen Intelligenz bezeichnen – in Anspielung auf das plötzliche Auftauchen aller höheren Tierarten vor rund 500 Millionen Jahren.

Vielleicht trifft das Bild auch in anderem Sinne zu. Man könnte sagen, die Geräte vor den Smartphones waren die Dinosaurier der Digitalisierung.

Siri und Alexa leben im Rechenzentrum

Das macht das Smartphone noch nicht zur höheren Gattung, und tatsächlich steckt noch verhältnismässig wenig Intelligenz in Ihrem iPhone. Siris Hirn liegt immer noch, genauso wie die Denkmachine der Android-Geräte, im Rechenzentrum: Ohne Internetanbindung sind sie nicht mehr ganz so smart.

Das aber dürfte sich in nächster Zukunft ändern. Und wenn die Geräte dereinst vernetzt und zugleich smart sein werden, bekommt der Begriff vom digitalen Assistenten, der im letzten Jahrhundert für die erste Adressagenda geprägt wurde, eine neue Dimension.

Detailhandel und Mobilität

Venetian-Hotel, Las Vegas, Frühjahr 2008: Neben der Sitzgruppe in der Junior-Suite steht auf dem Sideboard eine Reihe von kleinen Dosen mit Naschzeug – Nüsse, Gummibärchen und Schokolade-Dragées. Im Moment, in dem der Gast eine der Dosen von ihrem Platz nimmt, wird der Zimmerrechnung – einsehbar über das TV-System des Hotels – der Preis für eine der Dosen belastet. Setzt der Gast die volle Dose zurück, verschwindet der Eintrag aus seiner Rechnung. Über eine Sensor-Steuerung hält das Hotel nicht nur die Verluste durch unbezahlte Snacks tief, sondern regelt automatisch die Nachschubbestellung.

Seattle, Washington, Dezember 2016: Amazon eröffnet ein Ladengeschäft für Lebensmittel und Alltagsgüter. Das ist nicht nur bemerkenswert, weil der Handelsgigant mit Online-Verkauf von Büchern und CD gross geworden ist. Amazons erster realer Supermarkt unterscheidet sich in einem wesentlichen Punkt von allen anderen: Es gibt hier weder Kasse noch Kassierin. Die Kunden betreten den Laden, registrieren sich mit einer Strichcode-App auf ihrem Smartphone am Eingangsscanner, holen sich, was sie brauchen – und spazieren aus dem Laden.

Amazons Laden hat keine Registrierkassen

Amazon hat die Idee der Selbstregistrierung unter dem Namen “You just walk out” – “Du gehst einfach” – konsequent zu Ende gedacht. [In den Läden von “Amazon Go”](#) werden die Einkäufe nicht erst am Ausgang registriert, sondern in einem virtuellen Einkaufskorb laufend aktualisiert. Produkte, die aus dem Gestell genommen werden, tauchen wie von Geisterhand darin auf. Und was zurückgelegt wurde, verschwindet. Wenn der Kunde das Geschäft verlässt, wird die Gesamtrechnung direkt seinem Amazon-Konto mit hinterlegter Kreditkarte belastet.

Das ist gar nicht weit von dem entfernt, was die Grossverteiler in der Schweiz mit Self-Scanning-Kassen oder portablen Scannern anbieten. Die Voraussetzungen sind mit dem omnipräsenten Elektronischen Produktcode EPC, dem Strichcode auf jeder Packung, gegeben.

Der Vorteil für die Kunden in Amazons Go-Shops ist offensichtlich. Sie sparen Zeit, ohne dazu eine Aufgabe übernehmen zu müssen. Die Technologie regelt alles. Wie genau, darüber schweigt sich Amazon aus; jedenfalls ist die Technologie wesentlich komplexer als das blosses Auslesen von RFID-Tags. Diese Technologie der batterielosen Chips, die von Lesegeräten bei ausreichendem Abstand via Induktionsspannung ausgelesen werden können, hatte sich in den USA bei früheren Versuchen in Grossverteilern als zu kostspielig erwiesen.

Deshalb rücken gemäss Fachmagazinen jetzt vermehrt “Smarte Regale” in den Fokus, welche die angebotene Ware erkennen und sowohl Stückzahl wie Zustand (Ablaufdaten) in Echtzeit verwalten. Die permanente Inventur lässt den Warennachschub nie abreisen und hilft dem Laden, Verluste durch Angebotslücken zu vermeiden.

Die Regale “fühlen” aber nicht nur die Waren – sondern auch die Kunden. Das Projekt “Shelf Edge” (“Regal-Kante”) der Intel-Labs verknüpft das Smartphone sich nähernder Kunden mit einem Display beim Produkt. Der Kunde tritt gewissermassen in “Dialog” mit den Waren. Apples “iBeacon” dagegen ist ein Mikro-Positionsbestimmungssystem für

Smartphones auf Basis von Bluetooth. So kann der Laden dem Kunden, der lange vor den Erdbeeren stehenbleibt, automatisch ein Sonderangebot unterbreiten – das notabene nur für ihn existiert.

Ähnliche Prozesse zur dynamischen Preisgestaltung wenden Fluggesellschaften bereits heute an, namentlich im Online-Verkauf von Tickets. Je nach Equipment, mit dem der Kunde recherchiert (teures Macbook oder billiger PC?) und aufgrund anderer Signale wie vorher besuchter Websites und der Dauer, mit der er die Angebote studiert, werden die Preise laufend angepasst.

Der Detailhandel ist das eine grosse Alltagsvorzeigebiet für das Internet der Dinge. Die Mobilität ist das zweite. Hier liegen die Hoffnungen in einer allgemeinen Effizienzsteigerung, die den Individualverkehr vor dem Kollaps retten könnte. Das Mittel dazu: Autonome Fahrzeuge.

Vernetzte Autos sind die besseren Fahrer

Der Begriff ist insofern irreführend, als die Autos sich zwar vom Fahrer emanzipieren, aber andernorts um so mehr eingebunden werden. Man kann diese Fahrzeuge als Pico-Netzwerke aus Dingen sehen: Eine Sammlung von Sensoren, Prozessoren und Software. Dieser Verbund an Technologie organisiert sich selber innerhalb der Parameter der Strecke von A nach B, der Strasse, allgemeinen Sicherheitsparametern wie Abstand zum Vordermann, und der Verkehrsregeln. Zusätzlich wird der Verbund zu einem Teilnehmer im grösseren Netz der Fahrzeuge, Verkehrsleitsysteme und Routendienste.

Wieso damit Staus verhindert und Treibstoff gespart werden soll, ist auf den ersten Blick nicht klar. Es liegt nicht nur daran, dass Computer die besseren Autofahrer sind weil sie nicht ermüden oder den Abstand zum vorderen Fahrzeug konstanter einhalten. Sondern weil sie optimal (und bereitwilliger) mit den anderen Verkehrsteilnehmern kooperieren als frustrierte, aggressive oder sich selbst überschätzende Menschen.



Abbildung 5: Vernetzte Autos, Routenplanung mit Verkehrsauffkommens-Vorhersage.

Die Vernetzung spielt dabei in zwei Dimensionen eine Rolle. Die erste ist die Wahl der Route. Wenn jedes Auto in Echtzeit oder besser noch im Voraus “weiss”, wann alle andern wohin fahren werden, können Staus durch die Absprache von Routen und Strecken vermieden und die Kapazitäten optimal genutzt werden.

Wenn die Fahrzeuge ausserdem auf der Strasse selber miteinander in Verbindung stehen, können sie dichter aufeinander auffahren, Konvois bilden, bruske Beschleunigungs- und Abbremsmanöver vermeiden und damit Zeit und Energie sparen. Neue Forschungsergebnisse haben ergeben, dass ein einziges computergesteuertes Fahrzeug einen Phantom-Stau (in der Simulation im Kreisverkehr) in kürzester Zeit ausgleicht und zum verschwinden bringt. Youtube ist voll von Beispielen für die Wirksamkeit der Kollisionswarnung der Tesla-Elektroautos: Deren Radarsysteme erkennen eine gefährliche Situation Sekunden

vor dem menschlichen Fahrer und greifen mit automatischen Brems- und Ausweichmanövern ein.

Für das ungleich simplere Ziel der Vermeidung von Verkehrsüberlastungen scheint die Vernetzung der Fahrzeuge wie geschaffen, auch wenn die Vorstellung, bald von Computern durch die Gegen chauffiert zu werden, derzeit noch gewöhnungsbedürftig ist. Die Politiker haben die Chancen erkannt und [schaffen im Schnellzugstempo die rechtlichen Grundlagen](#).

Wie radikal die Änderungen sein werden, die allein dieser Schritt in eine vernetzte Zukunft bringen wird, können wir uns kaum vorstellen. Das Auto, eben grade noch Statussymbol Nummer eins in der Industriegesellschaft, wird zum austauschbaren Transportmittel: Man ahnt, dass damit zahlreiche Geschäftsmodelle untergehen – und neue entstehen werden. Das war längst klar: Dass die postindustrielle Gesellschaft sich vom Konsumgüterhandel auf Dienst- und Informationsleistungen umstellen werde, haben Futurologen wie Alvin Toffler oder Daniel Bell schon seit Jahrzehnten vorausgesagt.

Die Ware Mobilität

Inzwischen haben auch grosse Brands wie BMW die Zeichen der Zeit erkannt. Der Münchner Konzern hat sein Leitbild darauf ausgerichtet, dass Fahrzeuge schon bald nur noch (ein) Mittel zum Zweck sein werden, und setzt auf Strategien, mit denen er Generalanbieter für Mobilität werden will; Tesla-Gründer Elon Musk hat nie einen Hehl daraus gemacht, dass seine noch immer defizitäre Elektro-Autoschmiede nicht möglichst viele Fahrzeuge verkaufen, sondern den Umgang mit Energie und Mobilität wandeln soll.

Die Schweiz ist in dieser Bewegung eine Vorreiterin: Die hiesige Car-Sharing-Genossenschaft “Mobility” blickt auf über vier erfolgreiche Jahrzehnte zurück und war das Vorbild manch anderer Organisation (wie ZipCars in den USA). Ihr jüngstes Unternehmen, das in Basel und Genf lancierte Catch-A-Car-System, nutzt die Möglichkeiten der Technik, um die Fahrzeugmiete ortsunabhängig zu machen. Die CatchCars

können auf Stadtgebiet an beliebigem Ort reserviert, benutzt und an jedem Zielort abgestellt werden, wo sie der nächste Nutzer mit seiner Chipkarte öffnen und gebrauchen kann. Bezahlt wird die Zeit der Benutzung in Minuten; wenn eine kritische Masse an Fahrzeugen zur Verfügung steht, ist die permanente Verfügbarkeit schnell erreicht.

Die CatchCars sind letztlich vernetzte, mobile und mehr oder weniger smarte Objekte, deren Nutzung durch Echtzeit-Lokalisierung und eine lückenlose Telemetrie so optimiert werden kann, dass der Preis sinkt. Dank dem Smartphone in der Tasche jedes potentiellen Kunden kann dieser zum nächsten Fahrzeug dirigiert werden. Die Zentrale ihrerseits kennt den Standort, den technischen Zustand und den Benzinstand im Tank jedes Fahrzeugs. Der Verwaltungsaufwand reduziert sich dank der Vernetzung.

Selbst im Luftverkehr, wo Flugzeuge schon lange nicht mehr gekauft, sondern geleast werden, sorgen das Internet der Dinge und die erweiterten Möglichkeiten der Telemetrie für radikale Änderungen. [Triebwerkhersteller Rolls-Roice](#) etwa verkauft nicht mehr die Aggregate selber, sondern deren Leistung in Schub pro Stunde ("PBH", Power by the Hour). So muss sich die Airline nicht mehr um die Wartung der Maschinenteile kümmern und der Hersteller kann die Nutzung optimieren.

Industrie 4.0 und Präzisions-Landwirtschaft

Kaum eine Anwendung illustriert die aktuelle Industrielle Revolution besser als der 3D-Druck.

Der modische Begriff steht für die seriösere Sammelbezeichnung “additive Fertigung”, die alle Verfahren umfasst, bei denen ein Werkstück durch schichtweises Zufügen von Rohmaterial aufgebaut wird.

Theoretisch gehört dazu auch das Töpfern, bei dem Lage um Lage Ton auf die vorherige aufgebracht und in Form gezogen wird. 3D-Druck funktioniert fast gleich, indem das Material in Schichten auf die jeweils vorherige appliziert und mit ihr verbunden wird.

Im Vergleich zu bisherigen computergestützten Verfahren (CNC-Fräsen etc) bringt der 3D-Druck die virtuelle und die reale Welt viel näher zueinander: Aus einem hochkomplexen virtuellen 3D-Modell mit geschlossenen Hohlräumen und beweglichen Teilen wird in einem einzigen Arbeitsgang ein reales Objekt. Und wir reden hier nicht etwa nur von Plastikteilen. Mit sogenannten Laser-Sinter-Verfahren werden

heute Objekte aus härtestem Metall “gedruckt”. Und in der Bauindustrie halten Zement-3D-Drucker von gigantischem Ausmass Einzug, mit denen ganze Häuser aus glasfaserverstärktem Zement “gedruckt” werden.

Ein Getriebe aus dem Drucker

Neu ist daran in erster Linie die direkte Kommunikation der Design- mit den Produktionsmaschinen. Dateien aus einem Computer-Aided-Design-Programm werden direkt an einen Drucker übergeben, in die richtigen Produktionsschritte umgerechnet und ausgegeben. Statt dass Menschen an Computern Dinge berechnen, die Pläne ausdrucken und andere Menschen mit Maschinen sie umsetzen, werden die Computer direkt mit den Maschinen verbunden. Das Netzwerk wird zu einer grösseren Maschine, die lernt und nicht nur einen Arbeitsgang steuert, sondern die gesamte Produktion, die Lieferkette und die Wartung kontrolliert.

Diese Vision ist inzwischen mit dem Trendbegriff “Industrie 4.0” zum Schlagwort geworden. Es steht für die 4. Industrielle Revolution: Nach der Mechanisierung mittels Dampfmaschinen, der Massenfertigung durch Fliessband und Elektrifizierung und der Digitalisierung folgt jetzt die Integration von digitaler und realer Welt.

Die selbstheilende Eisenbahn

In Schweden erkennt das Wartungssystem der Transportbehörde Trafikverket an über dreihundert Orten im Schienennetz überhitzte Radlager, verschlissene Bremsbeläge oder andere mechanische Abnutzungserscheinungen an den vorbeidonnernenden Waggonen. An jedem dieser Lesepunkte erfasst ein Sensornetzwerk die Daten des RFID-gekennzeichneten Fahrzeugs. Die Informationen werden an einen Zentralrechner übermittelt, der ihn je nach Befund in der Waggonverwaltung aus dem Verkehr zieht und automatisch zur Inspektion oder zur Reparatur anmeldet.

In diesem Vorgang arbeiten etliche Grundelemente des Internets der Dinge zusammen: Sensoren, die bei -20 und +40 Grad Celsius funktionieren müssen; ein Funk-Lan an den Bahngleisen, das die Daten der Sensoren sammelt und via Glasfaserkabel und Internet an den Zentralrechner liefert; Software, die lernt, Fehlalarme und defekte Sensoren zu erkennen und eine ganze Reihe Technologien zur Maschine-Maschine-Kommunikation.

M2M ist der Schritt zur Industrie 4.0. Der Mensch als Systembruch in vielen Prozessschritten, der nicht mehr tut als die Daten eines Computers an eine Maschine zu übergeben, wird frei für Kreativieres. Die Maschinen arbeiten nicht nur einen Teilschritt des Produktionsprozesses ab, sondern beeinflussen die gesamte Herstellung in gegenseitiger Absprache.

Die Fabrik, die sich selber optimiert

In einem [Papier der Organisation für Sicherheit und Zusammenarbeit](#) wird der Ablauf eines Herstellungsprozesses in naher Zukunft wie folgt beschrieben:

Eine Gruppe von Designern hat ein neues Gerät entworfen. Sie zeigen möglichen Händlern Prototypen aus dem 3D-Drucker und werden von einem Verkäufer in Übersee unter Vertrag genommen. Jetzt werden das Design, die Verpackungspläne und eine Komponentenliste auf einen Online-Marktplatz für Hersteller hochgeladen, die Offerten für die Produktion abgeben können. Der Hersteller mit dem besten Angebot erhält den Zuschlag. Er entwirft mit der Rechenleistung von Cloud-Computing Simulationen des Herstellungsprozesses. Lernfähige Algorithmen ermitteln aus den verschiedenen Simulationen die effizienteste Kombination von Robotern und Werkzeugen. Komponenten und Daten werden der eigentlichen Fabrik übermittelt. In der Produktionsstrasse konfigurieren sich die Roboter aufgrund der eingespeisten Daten selber neu; Transportroboter bringen die Komponenten in der Halle zur jeweils richtigen Arbeitsstation und die Roboter bauen die Teile zusammen. Mit jedem gefertigten Stück vergleichen lernfähige

Algorithmen die ursprüngliche Prozess-Simulation mit dem effektiven Herstellungsprozess und nehmen Optimierungen vor.

Die Produkte werden von Robotern verpackt, verladen und von autonomen Fahrzeugen zu den Verkaufsstellen gebracht. Die Designer suchen bei steigendem Absatz weitere Abnehmer und wiederholen den gleichen Ablauf in einer anderen Weltregion. Hat eine Fabrikationsstelle ihren Auftrag erfüllt, dann reorganisieren sich die Roboter und rüsten die Werkzeuge für den nächsten Auftrag aus.

John Deere, das Google der Landwirtschaft

Was dem Schweizer Bauern sein Hürlimann, ist dem US-Farmer der John-Deere-Traktor. Hier hören die Parallelen aber auch schon auf. Nicht nur ist das amerikanische Unternehmen für einmal fast doppelt so alt (gegründet 1837) wie das schweizerische (1929). John Deere ist ausserdem vom Maschinenhersteller zu einem Agro-Dienstleistungsgiganten mutiert.

Auf dem Feld wird nämlich längst auch mit Big Data gearbeitet und nichts mehr den Launen der Natur oder gar dem Zufall überlassen. Den Anfang machte das sogenannte “Yield Mapping”, dank GPS auf den Meter genaue Kartierung des Ertrags. Heute erfassen Sensoren und Kameras aber schon viel mehr als das Wachstum der ausgebrachten Saat. Die Feuchtigkeit und der Nährstoffgehalt, selbst Schädlingsverbreitung werden in Echtzeit abgebildet und zentimetergenau bearbeitet oder bekämpft.

Zwischen Giganten wie John Deere spielen auch immer mehr Start-Ups in diesem Feld mit. Gamaya zum Beispiel, ein Spin-Off der ETH Lausanne, stellt [Drohnen mit einer Hyperspektralkamera](#) her, welche Diverse Indikatoren über den Zustand der Bepflanzung anhand der Lichtreflexion sehr schnell und genau aus der Luft erfassen kann. Sie soll zunächst vor allem auf den gigantischen Ackergebieten Südamerikas eingesetzt werden.

Dabei spielt Technologie und Präzisions-Landwirtschaft nicht nur der

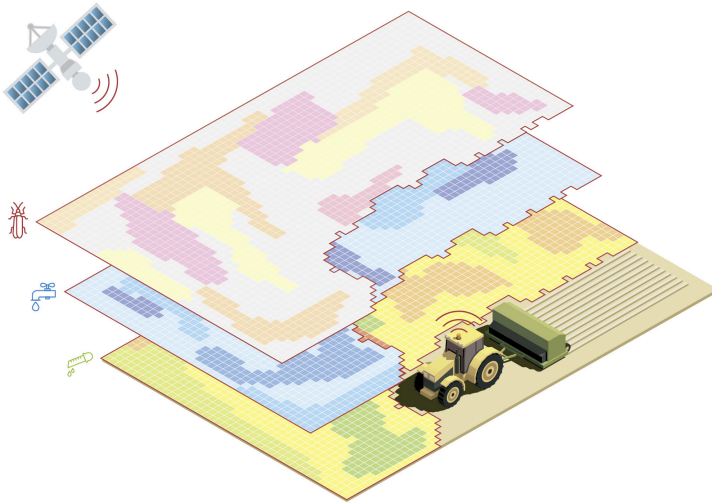


Abbildung 6: Yield Mapping

Industrialisierung in die Hand: Seit einigen Jahren können Bauern in der Schweiz an zentralen Stellen die GPS-Koordinaten ihrer Maisfelder einreichen, um im Juni Teil der **Route eines programmierten Drohnenflugs** zu werden, von dem aus die Larven einer Schlupfwespe zur biologischen Bekämpfung des Maiszünslers abgeworfen werden. Und vor dem Mähen der Felder werden mit Wärmebildkameras an Drohnen die versteckten Rehkitze und andere Jungtiere geortet und so vor dem Tod bewahrt.

In den USA ist alles einige Nummern grösser: John Deere ist dort mit "My John Deere" so etwas wie der Cloud-Computing-Anbieter der Bauern. Seine Landmaschinen operieren weitgehend autonom und im Verbund: Die via GPS gesteuerten, per Satelliten- und Mobilfunk- und Funk vernetzten Erntemaschinen bearbeiten die vierfache Fläche dessen, was ein Bauer mit herkömmlichen Maschinen in der gleichen Zeit erledigen könnte. Sie arbeiten auf zwei Zentimeter genau und sind

mit Sensoren und Analytik-Geräten ausgerüstet, die parallel zu einem Arbeitsgang Daten über Bodenqualität, Feuchtigkeit und Nährstoffgehalt erheben.

Diese Informationen fließen zurück zu John Deere in eine umfangreiche Datenbank. Zusammen mit Wetter- und den später erhobenen Daten über die effektive Ernte ergibt sich ein exaktes Bild der Fruchtbarkeit und der Möglichkeiten der gigantischen Felder: Auf den Quadratfuß genau.

Damit lässt sich der Verbrauch von Dünger und Spritzmitteln in nie gekanntem Umfang optimieren. Neben Einsparungen resultieren zugleich bessere Erträge. All dies ist erst durch die Vernetzung der Maschinen und die zunehmende Automatisierung des Echtzeit-Informationsaustauschs denkbar.

Der weltweite [Markt allein für die Anschaffung der Maschinen für Präzisionslandwirtschaft](#) wird auf knapp 5 Milliarden Dollar im Jahr 2020 geschätzt – mit einer Wachstumsrate von 12 Prozent.

Risiken und Nebenwirkungen

Am 13. Mai 2017 überlagerte plötzlich auf vielen Bildschirm-Anzeigen in deutschen Bahnhöfen ein seltsames Fenster die Fahrplan-Informationen: “Wenn du all deine Dateien entschlüsseln willst, musst du bezahlen” stand da. Die Bahn war gehackt, ihre Rechner vom Erpresser-Virus “WannaCry” (“Du möchtest weinen”) verschlüsselt worden.

Was in Deutschland wohl eher für Belustigung sorgte, wurde in England lebensbedrohlich. Denn dort waren reihenweise Computer von dem Virus befallen, auf denen Medikations- und andere für Patienten unabdingbare Informationen gespeichert waren. Möglich wurde der Angriff, weil diese Maschinen auf irgendeine Weise mit dem öffentlichen Internet verbunden sind.

Das Internet of “Bad other Things” (Bots)

Fälle wie dieser lassen regelmässig begründete Skepsis an den Vorzügen der Informationsgesellschaft aufkommen. Die drei grössten Bedenken sind

1. Cyberangriffe
2. Überwachung
3. Kontrollverlust

Es handelt sich um Nebenerscheinungen, wie sie jede Querschnittstechnologie mit sich bringt. Damit sollen die Gefahren nicht kleingeschrieben werden. Aber da sie ausreichend bekannt sind, können rechtzeitig Gegenmassnahmen und Regulierungen getroffen werden, um negative Auswirkungen zu mindern.

Tatsächlich kritisieren derzeit allerdings Fachleute auf allen Ebenen, dass das Internet der Dinge im Bezug auf die Sicherheitsthematik vernachlässigt werde – und das im Nachgang zur Affäre Snowden, die jedem und jeder Privatanwenderin von Informatik-Gadgets gezeigt haben sollte, wie verletzlich sie sind.

Als “blinden Fleck der Unternehmens-Security” bezeichnet der Israeli Gil Shwed, CEO des Sicherheitsunternehmens Check Point, die Geräte im IoT. Hersteller und Anwender vernachlässigten gleichermassen alle Grundsätze, die für eine minimale Sicherheit nötig wären: Schon die unbedingt nötige Anpassung des Passwortsschutzes jedes ins Netz eingebundenen Unterhaltungs-Elektronikgeräts werde vernachlässigt.

Wie effizient vernetzte Geräte arbeiten, haben kriminelle Hacker schon lange vor dem Trend zum Internet der Dinge erkannt. Sie haben für ihre Angriffe gegen Individuen und Firmen schon immer auf vernetzte Heerscharen von gehackten Geräten nichtsahnender Dritter gesetzt. Das funktioniert in der Regel so, dass Fernsteuerungsprogramme als Virus oder Wurm (ein sich selbst fortbewegendes Schadprogramm) verbreitet werden, die infizierte Geräte zu Teilen einer Computer-Armee machen. Bei ausreichend grosser Zahl an sogenannten “Bots” oder Zombie-Rechnern lassen sich damit nicht nur einzelne Webserver, sondern ganze Firmennetze lahmlegen. Dazu werden noch nicht einmal illegale Mittel nötig. Die Bots werden einfach angewiesen, immer und immer wieder die gleiche Website anzufordern. Bei einigen Millionen Aufrufen pro Sekunde geht so mancher Server

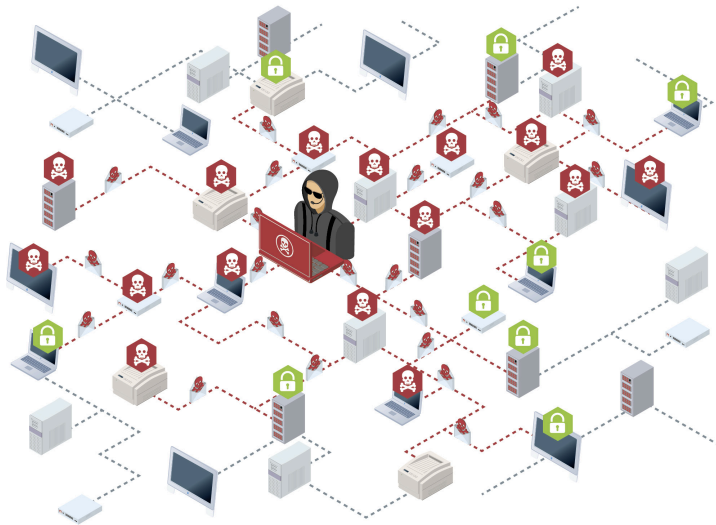


Abbildung 7: Botnetz

in die Knie. Auch das Geschäftsmodell der Hacker ist wegweisend – sie verkaufen die “Dienstleistung” ihrer Legionen in einschlägigen Foren im Internet.

Botnetze sind dank der wachsenden Zahl an ungenügend gesicherten Konsum-Geräten mit Netzanbindung inzwischen allzu leicht zu erstellen, [warnt der Wirtschaftsinformatiker Jan-Peter Kleinhans](#). Der erfolgreiche Virus “Mirai” zum Beispiel probiert ganz einfach auf beliebigen IP-Adressen rund 60 Standard-Logins von Geräteherstellern durch. Was für einen Menschen Stundenlange Versuche bedeuteten würde, ist für einen Computer eine Sache von Sekundenbruchteilen. Ein befallener Rechner greift demnach jede Minute Hunderte weiterer Internet-Knoten an. Zählt man hinzu, dass nicht mehr nur PC, sondern alle vernetzten Geräte vom Toaster bis zum Luftqualitäts-Sensor an der Autobahn als “IoT-Kindersoldaten” gekapert werden

könnten, dann wird manifest, wie dringend wirksame Schutzmassnahmen benötigt werden.

Die sind auf dem untersten Level gar nicht kompliziert. Regelmässige Software-Updates und Backups, solide Passwort-Regelungen und Zugriffsgrenzen können die Korrumpierbarkeit von Computersystemen stark verringern. So konnte sich “WannaCry” zum Beispiel ausschliesslich auf Rechnern mit einer veralteten und deshalb von Microsoft nicht mehr unterstützten Version des Betriebssystems Windows verbreiten.

Kein Angriff unter dieser Nummer

Mit der wachsenden Bedeutung des Internets der Dinge wird die Cyber-Sicherheit zusehends zu einer staatlichen Angelegenheit. Wenn lebenswichtige Infrastrukturteile wie Wasser- und Energieversorgung, Verkehrs- und Gesundheitssysteme von Computern und Sensor-Netzwerken gesteuert werden, müssen sie beaufsichtigt und nach gemeinschaftlichen Standards abgesichert werden.

Solche neuen Aufgaben pflegen Staaten mit Gesetzen anzugehen – auch die Schweiz. Der Bundesrat hat die Botschaft für ein [Informationssicherheitsgesetz](#) in der Verwaltung verabschiedet. Vorschriften sind aber auch für die Privatwirtschaft zu erwarten. So, wie sich die Schweiz mit strengen Auflagen gegen volkswirtschaftliche Schäden durch unsaubere Machenschaften in der Finanzbranche absichert, dürften künftig Anbieter bedeutender Infrastrukturleistungen mit Regulierungen zu höchster Sicherheit verpflichtet werden.

Deutschland hat zu diesem Zweck schon vor über zwanzig Jahren das [Bundesamt für Sicherheit in der Informationstechnik](#) geschaffen. Zu seinen Aufgaben gehört neben der Kontrolle von Sicherheitsmassnahmen in den Unternehmen auch die Durchsetzung der Meldepflicht von Angriffen. Neben passiven Vorkehrungen wie der konsequent dezentralen Architektur vitaler Netzwerke wird auch immer wieder der Aufbau einer aktiven “Einsatztruppe” im Cyberspace diskutiert. Sie soll

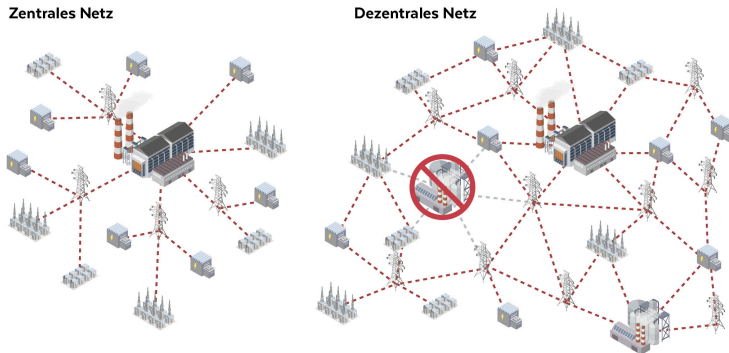


Abbildung 8: Dezentrale Organisation

Angriffe durch Botnetze bekämpfen, indem sie den Spieß umkehrt und infizierte Geräte und Server “abschiesst”.

Bei der Abwehr grosser Cyber-Angriffe zählen die Bürger auf den Staat – in andern Belangen misstrauen sie ihm: Den Europäern ist ihr Privatsphäre – zumindest gegenüber dem Staat – ein hohes Gut. Dass sie Unmassen an Daten und verknüpfbare Informationen an ausländische Unternehmen mit Sitz in einem Land ohne nennenswerten Datenschutz abgeben, ist vielen noch immer nicht bewusst. Oder aber es ist ihnen die Leistung wert, die sie im Gegenzug erhalten: Echtzeit-Staudaten im Navigationssystem gegen die eigene (anonymisierte) Position. Streetview-Fotos jeder Adresse in der Schweiz und damit virtuelle Stadtrundgänge gegen die Möglichkeit, von Google irgendwo auf der Strasse abgelichtet und publiziert zu werden. Informationen über den Musikkonsum gegen automatische, dem eigenen Geschmack angepasste Vorschläge neuer Bands.

Big Data – eine Frage der Balance

Unser Datenschutzverständnis stammt aus einer Zeit, in welcher der Staat ohne echte Gegenleistung Daten über seine Bürger sammelte. Diese achteten deshalb umso eifriger darauf, dass die Informationen zumindest nicht verknüpft werden konnten. Eine Funktion, die der eidgenössische Datenschützer heute gegenüber dem Staat und der Wirtschaft eifrig wahrnimmt. Nur hat sich die Beziehung inzwischen geändert: Um von Big Data zu profitieren, müssen alle etwas beisteuern. Das gälte auch für die Beziehungen zur Verwaltung, die, wenn sie es denn dürfte, mit der Vernetzung ihrer Datenbanken vergleichbare Effizienzsteigerungen erzielen könnte wie die Privatwirtschaft. Dort hat man aus Adresskarteien längst Kundendossiers gemacht, die für die Abrechnung, den Werbeversand bis zum individuellen Sonderangebot herangezogen werden. Wie mächtig der Zusammenzug verschiedener Datenbanken sein kann, demonstriert jetzt eine [App in Shanghai, die den gesellschaftlichen Wert jeden Bürgers ausgibt](#). Sie "berechnet" ihn aus über 5000 Behördeninformationen über das einzelne Individuum – von seiner Spendentätigkeit bis zu ausgesprochenen Bussgeldern und der Einhaltung der Ein-Kind-Politik.

Das Missbrauchspotential der exponentiell wachsenden Datensammlungen kann selbstredend so wenig verneint werden wie das Risiko von Cyberangriffen. Dem muss mit Regulierung Rechnung getragen werden. Trotzdem kennt die Schweiz bis heute zum Beispiel kein standardisiertes elektronisches Patientendossier: Sicherheits- und Autorisierungsfragen werden kontrovers diskutiert. Dabei würden wahrscheinlich viele Leben gerettet und Komplikationen vermieden, wenn jede Ärztin, jede Apotheke und jeder Sanitäter per Knopfdruck sämtliche relevanten Gesundheitsdaten eines Patienten vor sich hätte.

Das Internet der Dinge akzentuiert diese Diskussionen. Nicht nur, weil unser Smartphones immer mehr wertvoller Daten generieren und wichtige Einsichten in das Verhalten von Menschen geben könnten. Sondern weil immer mehr vernetzte Geräte mit derlei Daten etwas anfangen könnten.

Schon heute beeinflussen die Umstände, unter denen jemand online Flüge buchen will, die Preise. Apple-Nutzer bezahlen mehr, Leute, die zuvor viele Discount-Websites besucht haben, wird eher ein verlockendes Angebot gemacht. Die Unverfrorenheit, mit der sich die Fluggesellschaften auf solche Methoden eingelassen haben, lässt wenig Zweifel daran aufkommen, dass Banken, Versicherer oder auch Arbeitgeber alles verwerten würden, was sie über uns herausfinden können. Und das wird, dank Fitbit-Trainingsarmband, Whittings-Online-Waage und vollvernetztem E-Bike immer mehr.

Die aktuellen Konzepte für Datenschutz versuchen die Weitergabe solcher Daten an Dritte zu unterbinden: Niemand soll aus der Kombination der erfragten Informationen zu viel über eine Person erfahren können.

Deswegen dürfen Grossverteiler ihre Erkenntnisse über das individuelle Einkaufsverhalten der Kundenkarten-Inhaber nicht verkaufen. Was bisweilen nicht hilft: In den USA hat der Vater eines Teenagers von der Schwangerschaft seiner Tochter erfahren, weil sie Sonderangebote für Babyprodukte vom Retailer "Target" erhalten hatte. Dessen Datenanalyse erkennt schwangere Frauen anhand einer Liste von gerade mal 25 typischen Änderungen im Einkaufsverhalten – beispielsweise dem Wechsel zu unparfümiertem Deo.

Allerdings fragt sich zunehmend, ob solche Einzelfälle nicht die Ausnahmesituation sind, die wir in Kauf nehmen müssen, um von der Digitalisierung als Gesellschaft zu profitieren. Denn das legalistische Festhalten am Schutz der Privatsphäre verhindert nicht nur Missbrauch, sondern eben auch Quantensprünge in der Effizienzsteigerung von Verwaltung, Wissenschaft und Wirtschaft.

Ansätze für einen selbstbestimmten Mittelweg bestünden in Konzepten, [wonach jeder seine Daten frei verkaufen kann](#). In der Praxis dürften sie daran scheitern, dass die Summe der Daten unbezahlbar ist, der einzelne Datensatz aber nahezu wertlos bleibt.

Roboter-Ethik: Warum man sie ernst nehmen sollte

Die dritte Dimension der Bedrohung durch IT und das Internet der Dinge sehen Skeptiker in der lernfähigen Maschine selbst.

Der Hauptdarsteller in Stanley Kubricks Weltraum-Epos “2001 – A Space Odyssey” aus dem Jahre 1968 ist HAL 9000 – der Bordcomputer des Raumschiffs, das fünf Wissenschaftler zum Jupiter bringt. HAL ist das Internet der Dinge an Bord des Raumschiffs. Er kontrolliert alles und hat Zugang zu allen Informationen. Und er übernimmt in der entscheidenden Phase gegen den Willen der Menschen die Kontrolle.

Technologie ist in Europa seit schon immer mit einer gehörigen Portion Skepsis betrieben worden. Im Gegensatz dazu steht die Technikgläubigkeit der USA, die aus dem Schmelztiegel Silicon Valley die Welt mit Algorithmen verbessern wollen. Wo die einen Chancen sehen, sehen die andern die Risiken.

Diesem Spannungsfeld hat Hollywood unzählige Filme gewidmet, von “War Games” über “Terminator” bis zu “Matrix”: Der Mensch kreierte lernfähige Maschinen, die ihn rasch als das Problem der Erde erkennen und zu bekämpfen beginnen. Gegen diese Urangst nach dem Frankenstein-Muster hat der russisch-amerikanische Science-Fiction-Autor Isaac Asimov schon 1942 die drei [Gesetze der Robotik](#) erdacht:

1. Ein Roboter darf keinen Menschen verletzen oder durch Untätigkeit zu Schaden kommen lassen.
2. Ein Roboter muss den Befehlen eines Menschen gehorchen, es sei denn, solche Befehle stehen im Widerspruch zum ersten Gesetz.
3. Ein Roboter muss seine eigene Existenz schützen, solange dieser Schutz nicht dem Ersten oder Zweiten Gesetz widerspricht.

Was auf den ersten Blick wie ein wasserdichtes Regelwerk zum Schutz

des Menschen wirkt, würde nach Asimov voraussetzen, dass die Maschinen nie ein echtes Bewusstsein entwickeln und frei handeln könnten. Weil davon nicht mehr in jedem Fall ausgegangen werden kann, wird “Roboterethik” als interdisziplinäres Forschungsfeld heute bereits ernsthaft betrieben.

Das Europäische Parlament hat sogar bereits erste Vorschläge für eine Regulierung der Robotik und die [Schaffung eines Status für “elektronische Personen” diskutiert](#). Allerdings wird künstliche Intelligenz im menschlichen Sinne heute noch als philosophisches Konzept und damit unerreichbar bezeichnet. Bis die Menschheit sich gegen intelligente Maschinen wehren muss, dürfte sie noch einige pragmatischer, aber nicht weniger bedrohliche Probleme zu lösen haben. Das Internet der Dinge kann bei einigen davon helfen.

Glossar

3D-Drucker

Ein Gerät zur Herstellung von dreidimensionalen Objekten aus einem digitalen Modell, beispielsweise durch schichtweisen Aufbau mittels verflüssigtem Kunststoff. In Umkehrung des Fräsens, bei dem ein computergesteuerter Schneidekopf das Werkstück aus einem Block Rohmaterial herauschneidet, können beim 3D-Druck oder “additiven Fertigungstechniken” auch komplett eingeschlossene Hohlräume oder bewegliche Teile in einer fertigen Konstellation – zum Beispiel ein Getriebe – “gedruckt” werden.

Algorithmus

Ein Schema zur Lösung eines Problems oder einer Aufgabe, das aus eindeutigen, in einer bestimmten Reihenfolge abzuarbeitenden Schritten besteht. Algorithmen sind die Baupläne für Computerprogramme, wobei eine bestimmte Ein- immer zur gleichen Ausgabe führen wird.

API

Der Englische Begriff “Application Programming Interface” wird übersetzt mit “Programmierschnittstelle” und bezeichnet einen Satz von Befehlen, mit dem ein Programm von aussen gesteuert, mit Eingaben versorgt und zu Ausgaben gebracht werden kann. So können einzelne, in sich geschlossene Programme die “Dienste” anderer Programme beanspruchen.

ARPANET

Das “Advanced Research Projects Agency Network” war ein Vorläufer des Internets. Es wurde von der US-Luftwaffe in den sechziger Jahren entwickelt.

Big Data

Sammelbegriff für verschiedene Disziplinen zur Erfassung, Auswertung und Analyse gewaltiger Mengen gleichförmiger Daten. Impliziert wird, dass durch die Masse jene Muster und Zusammenhänge erkennbar werden, die anhand kleinerer Beobachtungsmengen nicht feststellbar sind.

Bluetooth

Dieser technische Funkstandard dient der Erstellung von Datenverbindungen zwischen zwei Geräten, gewissermassen als Ersatz für Kabel. Die Reichweite beträgt dabei zwischen zehn und 30 Metern. Bekannt wurde Bluetooth als Verbindung von Mobiltelefon und Headset. Heute sind unzählige Endnutzergeräte damit ausgestattet.

Datensee

Das Konzept des “Data Lake” entspringt der Erkenntnis, dass es nicht zwingend zum Ziel führt, Datenbestände aus einer Vielzahl von Quellen aufzubereiten und in strukturierten Datenbanken als “Data

Warehouse” abzulegen. Das gilt zumal dort, wo noch nicht klar ist, ob und welchen Zwecken die Daten dienen können. Im Datensee werden die Informationen deswegen zunächst als “Rohdaten” abgelegt und erst bei Bedarf analysiert und “raffiniert”, sprich für die Endbenutzer aufbereitet.

Digitalisierung

Die Übersetzung von Informationen in einen binären Code, dessen Zeichen aus einer Signalfolge aus zwei Zuständen (ähnlich wie das Morse-System) bestehen. Dies erlaubt den Transport der Daten über jedes System, das Energieimpulse übermitteln kann, von Elektromagnetischen über Schall- bis zu Lichtwellen.

Echtzeit-Lokalisierungssysteme (RTLS)

Auf Funksendern mit geringer Reichweite (bis 500 Meter) basierende Systeme, mit denen in Echtzeit Objekte oder Menschen genau geortet und ihr Standort protokolliert werden können. Dazu werden die zu verfolgenden Objekte mit aktiven RFID-Tags ausgestattet, deren Signale ständig von mindestens drei Empfängern ausgewertet und so die genau Position mittels Triangulation berechnet werden kann. RTLS werden in der Logistik, in Produktionsstätten, aber auch in Spitälern eingesetzt und erlauben Rückschlüsse auf Effizienz und Auslastung in Bezug auf die Örtlichkeiten.

Elektronischer Produktcode (EPC)

Internationaler Standard für ein globales Verzeichnis aller im Handel befindlichen Produkte. Diese werden mit Strichcodes oder elektronischen Tags gekennzeichnet.

Erweiterte Realität /Augmented Reality

Die Anreicherung der Umwelt durch direkt abrufbare Informationen auf geeigneten Medien. Audioguides in Museen, die durch Eingabe

eines Zahlencodes dem Besucher Informationen zu Exponaten abspielen, sind eine einfache Form der Augmented Reality. Eine komplexere Version ist die Datenbrille, durch die hindurch ein Servicetechniker die zu wartende Maschine mit beschrifteten Teilen sieht.

Geolokalisierung

Mittels verschiedener Techniken und Signale kann die Position von Geräte- oder Dienstnutzern in einer vernetzten Welt bestimmt werden. Am genauesten ist dabei das Auslesen der GPS-Position des Mobiltelefons eines Nutzers. Zur Geolokalisierung können aber auch zahlreiche andere Signale wie die Namen von WLAN-Netzwerken herangezogen werden.

GPS

Das amerikanische System aus geostationären Satelliten (NAVSTAR GPS), anhand derer Funksignale ein Empfänger auf der Erde seine exakte Position inklusive der Höhe über Meer bestimmen kann, stammt aus den siebziger Jahren und ist seit der Jahrtausendwende voll funktionstüchtig. Inzwischen haben Russland, China, die EU und Indien eigene Systeme lanciert.

Industrie 4.0

Bezeichnet die Verknüpfung der Informations- mit Produktionstechnologien als vierte Industrielle Revolution nach der Mechanisierung, der Massenproduktion und der Digitalisierung.

Internet

Einem Auftrag des US-Verteidigungsministeriums aus den sechziger Jahren entstammend, ist das "Internet" ein praktisch unzerstörbarer Verbund von Computern. Das Prinzip besteht in der Stückelung der zu verschickenden Information in Datenpäckchen, die einzeln und über beliebige Wege vom Absender über die zwischengeschalteten Compu-

ter zum Zielort geschickt und dort wieder zusammengesetzt werden. Fällt eine Teilstrecke aus, so werden die Datenpakete über andere Routen geschickt. Faktisch sind damit alle Rechner im Netz von allen anderen erreichbar.

Internet der Dinge

Der Begriff ist weit über zehn Jahre alt und bezeichnet eine Entwicklung, in der sich die Lücke zwischen der virtuellen Welt der Datenverarbeitung und der realen Welt der Maschinen (und Menschen) schließt. Er steht für die Integration der Maschinen und Geräte in das Internet und den direkten Austausch von Informationen durch Maschine-zu-Maschine-Kommunikation.

Internet von allem

Der von Dave Evans vom Netzwerkhersteller Cisco geprägte Begriff beschreibt die Weiterentwicklung des Internet der Dinge, in dem neben den Geräten auch Prozesse, Menschen und einfache Objekte im Internet verknüpft sind.

Künstliche Intelligenz / Artificial Intelligence

Ein Fachgebiet der Informatik, das auf die Kopie menschlicher Lern-, Verständnis- und Kombinationsfähigkeiten in Computern abzielt. Eine "intelligente" Maschine kann auch aus ihr unbekanntem Sachverhalten und Daten Schlussfolgerungen ziehen und zu sinnvollen Entscheidungen kommen.

LAN

Ein "Local Area Network" ist ein in sich geschlossenes Netzwerk von Geräten – zum Beispiel in einem Privathaushalt. Die Verbindungszentrale in einem solchen Netz, der Router, ist in der Regel auch der Türsteher zum Internet. Geräte aus dem LAN können damit ins Internet, aber Geräte aus dem Internet nicht ohne weiteres ins LAN gelangen.

MAN/WAN

Im Gegensatz zum lokalen Netz, dem LAN, sind ein MAN ein “Metropolitan Network” mindestens auf Stadtebene und ein WAN als “Wide Area Network” zum Beispiel ein weltweites Netz.

Mensch-Maschine-Kommunikation (M2M)

Die Eingabe von Steuerdaten an einen Computer oder ein System und die Rückgabe von Auswertungen via Bildschirm oder anderem Medium.

Nahfeld-Kommunikation NFC (Near Field Communications)

Eine Weiterentwicklung von RFID, mit der Informationen auf sehr kurze Distanz bis 10 cm kontaktlos übermittelt werden.

Piconetz

Ein persönliches Gerätenetz auf Basis des Bluetooth-Funkstandards. Es kann bis zu 200 Geräte umfassen, wobei nur eines als “Master” und alle andern als Empfänger oder “Slaves” definiert werden, das heißt, sie werden über den “Master” gesteuert. Es dient beispielsweise zum Abspielen von Musik ab einem Smartphone auf Bluetooth-Lautsprechern.

RFID

“Radio Frequency Identification” oder RFID ist eine Technologie zur kontaktlosen Identifizierung von Objekten. Diese werden mit einem Informationsträger, einem “Tag”, versehen. Dessen Daten können bei Annäherung an ein Lesegerät ausgelesen werden. Die “Tags” gibt es in einer Version ohne Energieversorgung: Sie beziehen den Strom für die Datenübermittlung induktiv aus den elektromagnetischen Wellen des Lesegeräts. Dies ermöglicht preiswerte und langlebige Tags in Form weniger Rappen teurer Aufkleber.

Router/Gateway

Ein Computer, welche zwei Netze verbindet – typischerweise ein privates LAN und das Internet. Er leitet Anfragen der privaten Rechner an die öffentlichen weiter und übergibt im Gegenzug die Antworten intern an den Ursprungscomputer der Anfrage. Die Rechner im privaten Netz sind von aussen nicht über eine IP-Adresse erreichbar.

Autonomes Auto

Fahrzeuge, die dank umfangreicher Sensorik, Satellitennavigation und Echtzeit-Computerberechnung ohne Zutun eines Fahrers von A nach B fahren können. Funktionen wie die automatische Spur- und Abstandswarnung, Einpark- oder Notbrems-Systeme sind seit einigen Jahren serienmässig in Personenwagen zu finden; die Elektrofahrzeuge von Tesla sind theoretisch bereits heute vollständig autonom fahrbar.

TCP/IP

“Transmission Control Protocol/Internet Protocol“ sind die Grundlagen des Internets. Das Internet-Protokoll regelt das System der IP-Adressen, dank derer jedes Gerät im Netz eindeutig angesprochen werden kann. Das TC-Protokoll standardisiert die Art und Weise, wie die Daten im Netz weitergegeben werden. Die beiden Standards sind aufgrund ihrer Einfachheit und Robustheit zur Basis der Mehrheit aller Computernetze geworden.

Telemetrie

Die “Fernmessung” ist die Übermittlung von Zustandsdaten, die einer oder mehrere Sensoren erfasst haben, an eine entfernte Stelle. Im Rennsport werden permanent die verschiedensten Messwerte aus den Fahrzeugen an die Renn-Regie übermittelt, die so jederzeit über den aktuellen Zustand des Motors Bescheid weiss. Im Flugverkehr werden Triebwerke aufgrund der Schubleistung, welche telemetrisch ermittelt wird, “vermietet”.

Vernetzte Gegenstände

Im Gegensatz zu vernetzten Geräten, die aus dem Netz angesprochen und ferngesteuert werden können, sind vernetzte Gegenstände im Netz lediglich passiv auffindbar und verfügen über keine abrufbaren Aktionen.

Vernetzte Geräte

Als vernetzt gelten Geräte gemeinhin, wenn sie an ein grösseres Computernetzwerk angeschlossen und dadurch auch aus dem Internet angesprochen werden können.

Verschlüsselung / Kryptografie

Mathematische Verfahren, mit denen Datenströme so manipuliert werden, dass sie nur von Inhabern eines geheimen Schlüssels wieder lesbar gemacht werden können. Die Kryptografie spielt eine wachsende Rolle in allen Bereichen der Vernetzung, denn das Internet setzt sich aus heterogenen und in vielen Bereichen leicht einseh- und abhörbaren Teilbereichen zusammen.

Verteiltes System

Ein Zusammenschluss von Computern, der vom Benutzer als homogenes System gesehen wird. Es wird durch Redundanz gleicher Funktionen extrem ausfallsicher und ermöglicht durch zeitgleiches Abarbeiten von Teilaufgaben Geschwindigkeitsgewinne.

Virtualisierung

Die Virtualisierung bezeichnet die Simulation von Hard- oder Software in typähnlichen Ressourcen. So können Geräte oder ganze Netzwerke nachgebildet werden, die sich für den Anwender nicht vom Original unterscheiden, die aber nicht physisch existieren. Typisch sind virtuelle Server, die an Kunden von Rechenzentren vermietet werden,

Cloud-Speichersysteme, die mit den Bedürfnissen des Kunden nahtlose mitwachsen, oder Virtuelle private Netzwerke (VPN), die im Internet ein privates, das heisst durch Verschlüsselung abhörsicheres Netz nachbilden.

World Wide Web

Oft fälschlicherweise mit dem Internet gleichgesetzt, handelt es sich beim WWW um eine Anwendungsebene des Internets – das Hyper-Text-Transfer-Protocol HTTP. Es schafft eine Verbindung von Hyper-text-Dokumenten, genannt Websites, die in Webbrowsern wie Safari oder Chrome angezeigt werden und bei einem Mausklick auf einen sogenannten Hyperlink die in diesem Link adressierte Website aufrufen.

Peter Sennhauser

Seit dreissig Jahren beobachtet der Journalist Peter Sennhauser (*1966) die Digitalisierung. Als Inlandredaktor des “Bund” hat er ausgangs des Jahrhunderts das Parlament auf seine Internettauglichkeit abgeklopft und nach dem ersten Internet-Börsencrash für die Wochenzeitung “Cash” die hiesige “New Economy” beim Wiederaufbau begleitet. Ab 2004 erlebte er “vor Ort” im Silicon Valley die Ankunft des Smartphones, den Aufstieg der sozialen Netzwerke und den Wandel der Medienwelt.



Letzteren prägte er selber fünf Jahre lang als Teilhaber des Zürcher Startups “Blogwerk” – und nach seiner Rückkehr aus San Francisco im Jahr 2011 als digital-Entwickler in der Basler “TagesWoche” und später als Online-Spezialist in der Leitung des Newsrooms der “Neuen Zürcher Zeitung”. Inzwischen ist er Inhaber einer eigenen Agentur und berät Unternehmen beim Aufbau einer Content-Marketing-Strategie, in der Gestaltung der redaktionellen Prozesse oder hilft ihnen bei der Umsetzung publizistischer Projekte.

Institute for Digital Business

Allgemein

Im September 2014 gründete die HWZ Hochschule für Wirtschaft Zürich unter der Leitung von Manuel P. Nappo das schweizweit erste Kompetenzzentrum im Bereich Digital Business. Das Institute for Digital Business ist eine Anlaufstelle für anwendungsorientiertes digitales Wissen. Es ermöglicht einen optimalen Wissenstransfer in Unternehmen, Verbände und öffentliche Verwaltungen. Angeboten werden Lehre, Beratung sowie kostenloses Wissen.

Mission

«Wir unterstützen Schweizer KMUs sowie Entscheidungsträger in Wirtschaft und Gesellschaft, den Herausforderungen des digitalen Zeitalters gerecht zu werden. Wir liefern umsetzbare, anwendungsorientierte Inputs in Form von Weiterbildungen, Schulungen, Beratungen, Know-how, Konzepten, Support und Lösungsvorschlägen.»

Angebot

Der Master of Advanced Studies (MAS) in Digital Business sowie die sechs Zertifikatslehrgänge (CAS) werden vom Center for Digital Business, zum Teil in Zusammenarbeit mit externen Partnern, entwickelt und durchgeführt. Das Institute for Digital Business realisiert zudem massgeschneiderte Kurse und Workshops mit Unternehmen, Verbänden und Verwaltungen. Die Schulungen werden grundsätzlich nach den individuellen Bedürfnissen der Unternehmen aufgebaut und umgesetzt. So unterstützt das Center seine Kunden beispielsweise bei einer Potenzialanalyse, bei der Entwicklung einer digitalen Vision oder der Implementierung einer Digitalisierungsstrategie. Das Institute stellt zudem kostenlos Wissen in Form von White Papers, Check-

listen, Anleitungen usw. zur Verfügung. Im Bereich der angewandten Forschung arbeitet das Center an Projekten für Auftraggeber aus der Wirtschaft, öffentlichen Verwaltung oder für NGO.

buch & netz

buch & netz ist ein Verlag und Dienstleister für die Publikation von Büchern und Online-Angeboten, sowie eine Online-Buchhandlung mit Antiquariat.

Durch den Einsatz von modernster Internet-Technologien und der konsequenten Umsetzung einer Digital-First-Strategie können Publikationsprojekte in konkurrenzlos kurzer Zeit, in hoher Qualität und zu attraktiven Kosten umgesetzt werden. Die durch buch & netz produzierten Werke können durch den eigenen Verlag oder durch Partnerverlage dem internationalen Buchhandel verfügbar gemacht werden. Die optionalen Online-Bücher erhöhen die Sichtbarkeit der Werke im Internet. Der Einsatz von Creative-Commons-Lizenzen ermöglicht das einfache Teilen der Inhalte und die Nutzung der buch & netz Download-Gutscheine vereinfachen das Verschenken von E-Books. Weitere Infos finden Sie auf unserer Website <http://buchundnetz.com>

Urheberrechte und Nutzungsbedingungen

Das Buch «Internet der Dinge – Eine Einführung» im Verlag buch & netz ist unter einer Creative Commons Lizenz vom Typ Namensnennung – Nicht Kommerziell – Keine Bearbeitung – 4.0 (CC-BY-NC-ND 4.0) publiziert.

Die Texte in diesem Werk sind, wenn nicht anders angegeben, unter einer Creative Commons Lizenz vom Typ Namensnennung – Weitergabe unter gleichen Bedingungen – 4.0 (CC-BY-SA 4.0) publiziert.

Das bedeutet, dass Sie die Texte in diesem Werk auch in einem kommerziellen Umfeld kopieren und nutzen dürfen, solange Sie den Autor und die Quelle nennen und das von Ihnen erstellte Werk unter gleichen Bedingungen lizenzieren (siehe Beispiel weiter unten).

Das Buch selbst dürfen Sie kopieren und im nicht-kommerziellen Rahmen weitergeben. Sie dürfen es aber nicht ohne Erlaubnis des Verlages verändern, verkaufen oder auf andere Weise kommerziell verwerten.

Falls Sie am Wiederverkauf des gedruckten Buches bzw. des eBooks oder an anderen kommerziellen Modellen interessiert sind, melden Sie sich gerne bei buch & netz: info@buchundnetz.com

Um eine Kopie dieser Lizenzen einzusehen, konsultieren Sie: <http://creativecommons.org/licenses/by-sa/4.0/> bzw. <http://creativecommons.org/licenses/by-nc-nd/4.0/>

oder wenden sich brieflich an: Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA.

Bitte referenzieren Sie die Texte, die Sie gemäss der CC-BY-SA Lizenz nutzen, auf folgende Weise:

- Quelle: «Internet der Dinge – Eine Einführung», eBook / Online-Buch / Buch
- Autor: Peter Sennhauser
- Verlag: buch & netz – <http://buchundnetz.com>
- ISBN: 978-3-03805-256-2 (PDF), 978-3-03805-257-9 (ePub), 978-3-03805-258-6 (mobi)
- Link: <http://buchundnetz.com/werke/internet-der-dinge/> (oder den direkten Link zum entsprechenden Kapitel aus dem Online-Buch)

Wir würden uns freuen, wenn Sie uns über Ihre Nutzung von Inhalten aus diesem Online-Buch informieren würden. Schreiben Sie uns doch eine kurze E-Mail an info@buchundnetz.com. Gerne berichten wir nach Möglichkeit auch darüber in den verschiedenen Kanälen von buch & netz.

Weitere Informationen zu Creative Commons lizenzierten Inhalten bei «buch & netz» finden Sie auch unter: <http://buchundnetz.com/creative-commons>