Mitfühlende Kühlschränke, hellsichtige Glühbirnen

Das Internet weitet sich rasch aus und umfasst zunehmend auch Alltagsgegenstände. Doch die «Internetifizierung» von allem birgt grosse Sicherheitsrisiken. VON STEFAN BETSCHON

Das Internet der Dinge sei eine «Revolution, die darauf wartet, stattfinden zu können», schrieb die amerikanische Marktforschungsfirma Gartner vor einem Jahr. Das Internet der Dinge ist das Internet der Zukunft, ein Internet, das neuartige Geräte miteinander verbindet und dem Menschen vielfältige neue Möglichkeiten erschliesst.

Es gibt heute noch eine klar erkennbare Grenze zwischen online und offline, zwischen der Bildschirmwelt und der richtigen Welt. Das Internet der Dinge (Internet of Things, IoT) soll diese Grenze verschwinden lassen. Der Mensch, wo immer er geht und steht, wäre umgeben von internetfähigen Geräten, er hätte Zugriff auf Sensoren oder Aktoren rund um die Welt, alles und jedes wäre parat zur Eingabe oder Ausgabe von Daten.

Eine Schar ummauerter Gärten

Ein schöner Traum. Er weckt Hoffnungen auch auf gute Geschäfte. Beim McKinsey Global Institute bewertet man die wirtschaftliche Bedeutung, die das Internet der Dinge in zehn Jahren haben wird, mit vier bis elf Billionen Dollar. Es gibt bereits viele interessante IoT-Anwendungen – die Glühbirne als Alarmanlage, die internettaugliche Bewässerung für Topfpflanzen –, sie sind aber proprietär, unkommunikativ. Bis jetzt präsentiert sich das Internet der Dinge als eine Ansammlung von ummauerten, abgeschlossenen Gärten.

Wer «Internet» sagt, meint allgemein akzeptierte Kommunikationsstandards, die den Aufbau eines grossflächigen, einheitlich strukturierten Netzwerks der Netze erlauben. Dass sich für den Aufbau eines weltumspannenden Internets der Dinge einheitliche Standards herausbilden, ist aber nicht zu beobachten. Es gebe, so berichtet das amerikanische Institute of Electrical and Electronics Engineers, mehr als 100 Industriekonsortien, die sich für die Erarbeitung von IoT-Standards zuständig fühlten.

Vielleicht wäre es besser, nicht Internet zu sagen, wenn man sich zum Internet der Dinge äussern möchte? Viele Forscher tun das. Sie reden lieber von Machine to Machine Communication, Smart Objects Networking, Ubiquitous Computing, Pervasive Computing, cyberphysischen Systemen.

Berge versetzen

Laut der kalifornischen Internetfirma Cisco gab es 2010 12,5 Milliarden Internetknoten, 2020 sollen es 50 Milliarden sein. Morgan Stanley prognostiziert 75 Milliarden, Huawei gar 100 Milliarden Geräte. Doch mit Internetknoten kann sehr Verschiedenes gemeint sein, ein Türschloss, ein Auto oder eine ganze Stadt, eine Smart City.

Die Dinge, die das Internet der Dinge ausmachen werden, unterscheiden sich von den Dingen des herkömmlichen Internets dadurch, dass sie nicht universal programmierbare Computer sind, sondern für einen Anwendungszweck spezialisierte Geräte. Sie unterscheiden sich von den Dingen, die nicht dem Internet der Dinge zugerechnet werden, dadurch, dass sie auf elektrischen Strom angewiesen sind, dass sie elektronische Komponenten umfassen und dass sie mit ähnlichen Komponenten über standardisierte Verfahren der Datenfernübertragung in Verbindung treten können. Das setzt voraus, dass sie eindeutig identifizierbar sind.

Ein IoT-Ding kann – etwa im Rahmen des Zürcher Permasense-Projekts, das auf über 3000 Meter Höhe in den Walliser Alpen Verformungen von Felsen beobachtet – ein kleines Kästchen sein mit Batterie, Prozessor, Speicherkärtchen, Sensor und Antenne. Ein IoT-Ding kann zusätzlich zum Sensor auch noch Antriebselemente, Aktoren, umfassen, die Steuersignale mechanisch umsetzen. Beim «smarten» Briefkasten der Swissprime Technologies AG sorgt ein Aktor dafür, dass der Briefkasten mit dem Smartphone auch aus grosser Entfernung für Lieferanten geöffnet und wieder verschlossen werden kann.

Als Vorzeigeprodukt für das Internet der Dinge dient seit Mitte der 1990er Jahre der internetfähige Kühlschrank. Für den britischen «Guardian» ist der Internetkühlschrank ein «Technik-Zombie», nutzlos, aber nicht totzukriegen. In jüngster Zeit kamen Internetkühlschränke von Samsung ins Gerede – nicht wegen ihrer «Smartness», sondern weil sie Hackern Tür und Tor öffneten.

Der Kühlschrank ist nicht die einzige Schwachstelle des Smart Home. Ende vergangenen Jahres sorgten Barbiepuppen für Angst und Schrecken: Dieses Spielzeug gibt es in einer künstlich-intelligenten Ausführung mit Mikrofon, das stets eingeschaltet ist. Um gesprochene Sprache verarbeiten zu können, ist die Puppe auf eine Verbindung mit dem Internet und mit einem Server der amerikanischen Firma Toytalk angewiesen. Dieser Dienst, der auch von anderen Spielzeugherstellern genutzt wird, konnte gehackt werden.

Auch internetfähige Babyphones lassen sich mit bescheidenem Aufwand abhören. Betroffen sind die Produkte mehrerer Hersteller, unter anderem solche von Philips. Internetfähige Türschlösser von Yale, Überwachungskameras von Foscam, Heizungssteuerungen von Nest, Musikanlagen von Bose, Drohnen von Parrot oder ein Jeep von Fiat-Chrysler – sie alle sorgten in den vergangenen zwölf Monaten für Schlagzeilen, weil sie von Unbefugten über Internet- oder Mobilfunkverbindungen kontrolliert, zu Spionagezwecken missbraucht oder gar zerstört werden konnten. Sicherheitsexperten von Hewlett-Packard haben 10 populäre IoT-Produkte untersucht und fanden im Schnitt pro Gerät 25 Sicherheitslücken. Laut dem Bericht, der keine Produktnamen nennt, sammeln 9 von 10 Produkten unnötigerweise persönliche Informationen; 70 Prozent der Produkte verzichten bei der Datenübertragung auf Verschlüsselung.

«Die Sicherheitslücken verweisen auf grundlegendere Probleme.»

Leuchtenschlacht

Als IoT-Vorzeigeprodukt sieht sich der Kühlschrank neuerdings von der smarten Glühbirne in den Schatten gestellt. Das Angebot an Lampen mit IoT-Funktionen weitet sich rasch aus; ein Journalist des amerikanischen Nachrichtenmagazins «Time» schrieb bereits von der «Battle of the Bulbs» (Leuchtenschlacht). Philips offeriert für E27-Fassungen LED-Glühbirnen – Hue genannt –, die sich per iPhone, iPad oder Android-Handy steuern lassen. Dieses Produkt erregte jüngst mediale Aufmerksamkeit, weil Philips mit einem Firmware-Upgrade zu verhindern versuchte, dass auch Lampen anderer Hersteller in das System eingebunden werden können. Grosse Erwartungen weckte hierzulande ein Produkt der Startup-Firma Comfylight AG. Die LED-Lampe mit E27-Gewinde kann sich merken, wann sie eingeschaltet und ausgeschaltet wird, und dieses Benutzungsmuster zur Abschreckung von Einbrechern reproduzieren, wenn niemand zu Hause ist. Die Lampe, die demnächst in den Verkauf kommen soll, verfügt über einen Bewegungsmelder und kann die Abwesenden mittels Smartphone über Eindringlinge informieren.

Das Comfylight-Produkt benutzt zur Kommunikation mit der Umgebung WLAN-Verbindungen, Philips Hue setzt auf Zigbee. Das sind – neben WLAN und Bluetooth – nur zwei von vielen Kommunikationsprotokollen, die für Smart-Home-Anwendungen wichtig werden könnten.

Bei der mobilen Datenfernübertragung dürfte für IoT-Anwendungen die Mobilfunktechnik der fünften Generation (5G) Bedeutung erlangen. Für IoT-Geräte mit beschränktem Energiebudget werden Verfahren für den Aufbau von sogenannten Low Power Wide Area Network von vielen Anbietern offeriert. Die Swisscom hat sich für eine LoraWAN genannte Technik der kalifornischen Halbleiterfirma Semtech entschieden.

Mischmasch

Bereits 1966 hat der deutsche Informatiker Karl Steinbuch vorausgesagt, dass es «in wenigen Jahrzehnten» keine Industrieprodukte mehr geben werde, in die nicht ein Computer «hineingewoben» sei. Die Wortkombination «Internet of Things» soll 1999 durch Kevin Ashton geprägt worden sein. Ashton gehörte zu den Gründern der Auto-ID Center, die am Massachusetts Institute of Technology (MIT) aber etwa auch an der ETH Zürich die Möglichkeiten von Radio Frequency Identification (RFID) erforschten. RFID-Funketiketten empfahlen sich damals als einfache Möglichkeit, Gegenstände «smart» zu machen.

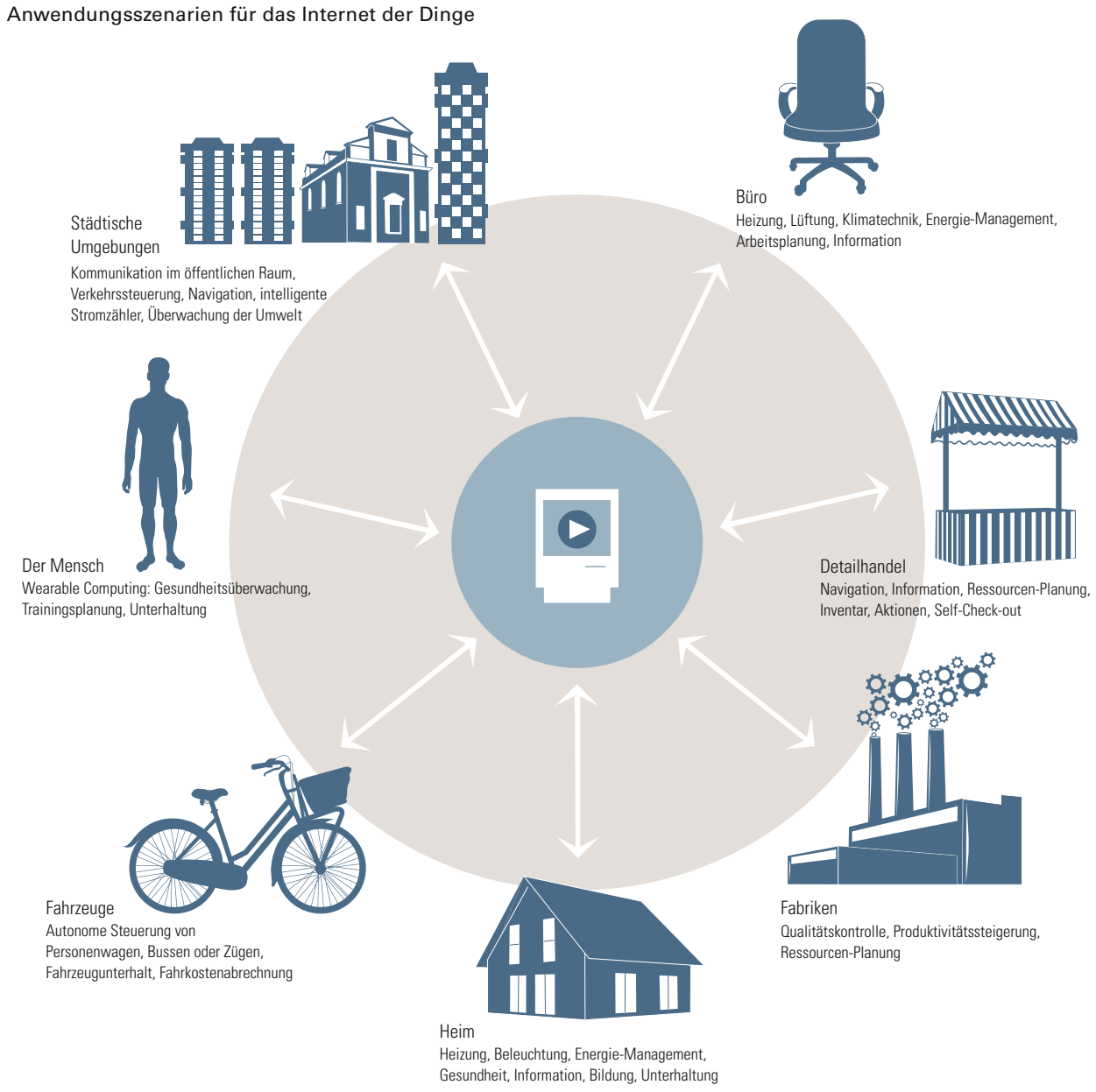
Zu den Mitarbeitern von Ashton gehörte ein gewisser Sanjay Sarma, der inzwischen am MIT als Professor für Maschinenbau tätig ist. In einem Beitrag für das Magazin «Politico» beschrieb Sarna Mitte des vergangenen Jahres, wie er angefangen hatte, sein Haus mit IoT-Geräten vollzustopfen, nur um dann dieses Projekt überstürzt zu «killen». «Ich habe mitgeholfen, das Internet der Dinge zu erfinden, aber ich mache mir Sorgen um die Sicherheit», lautet der Titel seines Beitrags.

Das Problem seien nicht die vielen einzelnen Sicherheitslücken, sondern die unkontrollierbare Komplexität, die sich ergebe, wenn eine grosse Zahl von IoT-Produkten, die unterschiedliche Hersteller übereilt auf den Markt geworfen hätten, kombiniert würden. Die Sicherheitslücken seien nur ein Symptom für grundlegendere Probleme: Es gebe keine Standards und keine verbindliche Architektur für den Aufbau von IoT-Teilsystemen. Sarma wünscht sich, dass wie in den 1970er Jahren, als jene Protokolle standardisiert wurden, die bis heute das Internet definieren, eine staatliche Behörde die Entwicklung eines Internets der Dinge leitet, um einen «hodgepodge» (Mischmasch) von Technologien zu vermeiden.

Eile mit Weile

Der Medienrummel rund um das Internet der Dinge habe 2015 seinen Höhepunkt erreicht, liess Gartner kürzlich verlauten. Nach dem Hype sei es jetzt Zeit für einen «reality check». Noch seien die meisten Geschäftsmodelle «unreif». IoT verheisst eine Revolution – doch die lässt auf sich warten.

Anwendungsszenarien für das Internet der Dinge



QUELLE: MCKINSEY GLOBAL INSTITUTE NZZ-Infografik/lvg.