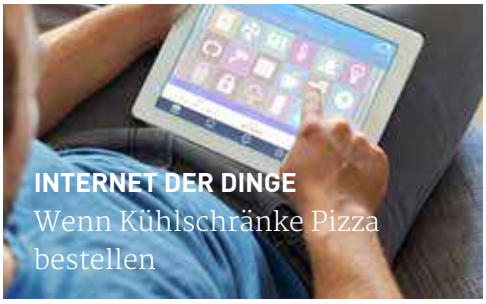
PHOENIX
Pharmahandel GmbH & Co KG
a PHOENIX company

TEAM NEWS

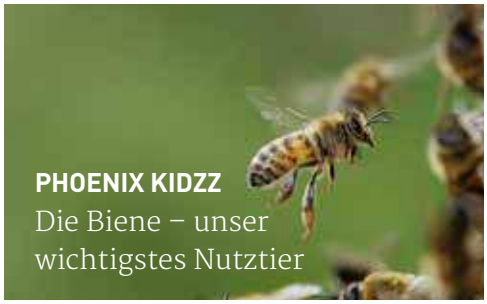
01/2016

TEAMFORUM
Mehr.Wert.Erleben.

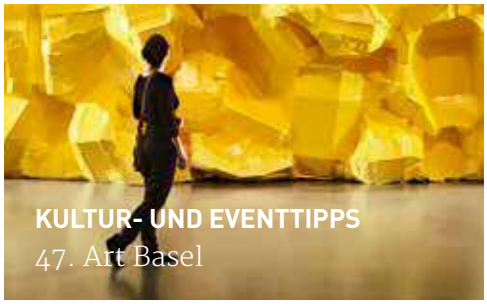
FASZIENTRAINING
Fitnesshype oder hoffnungsvolle Schmerztherapie?



INTERNET DER DINGE
Wenn Kühlschränke Pizza bestellen



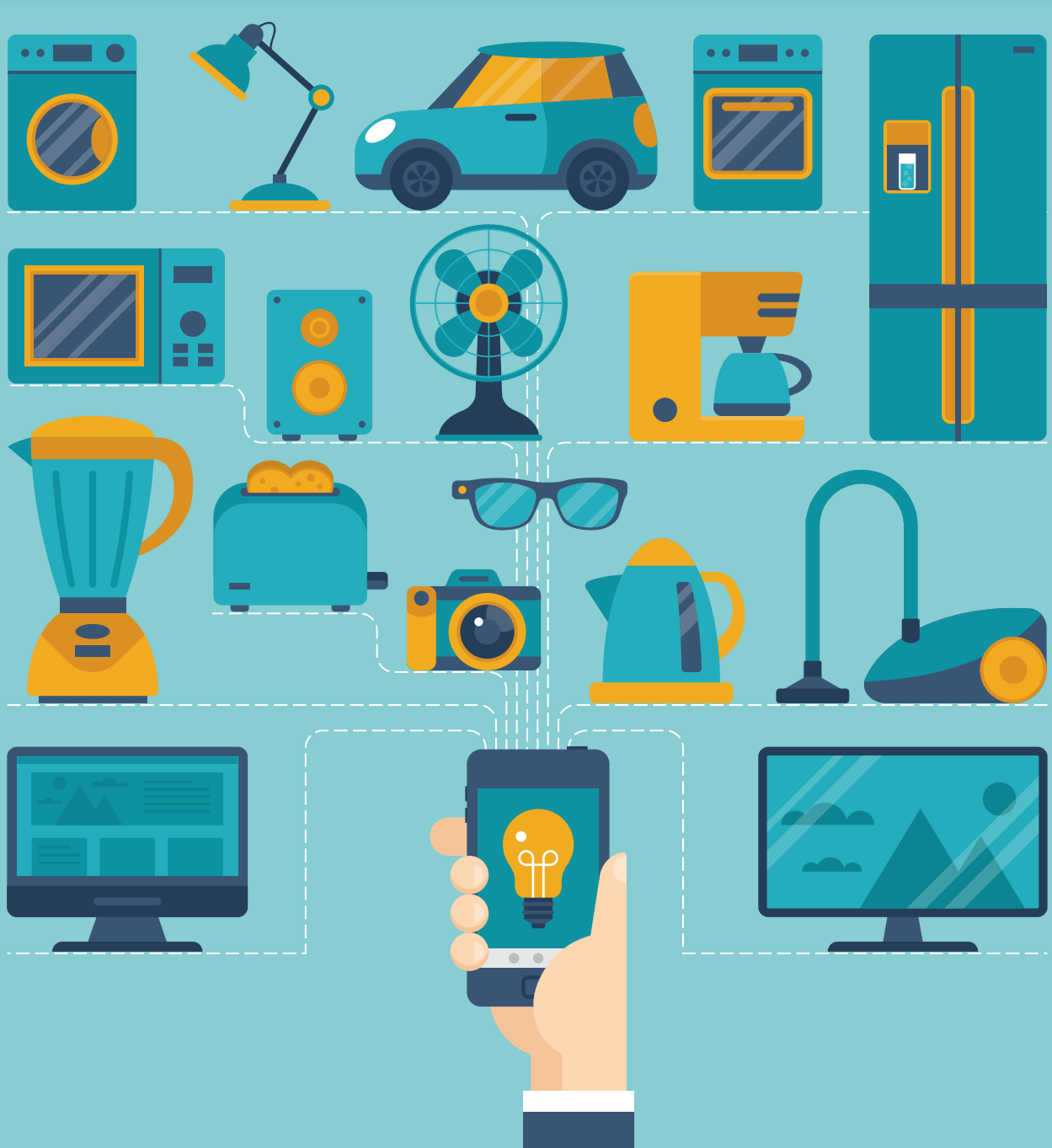
PHOENIX KIDZZ
Die Biene – unser wichtigstes Nutztier



KULTUR- UND EVENTTIPPS
47. Art Basel

WENN KÜHL-SCHRÄNKE PIZZA BESTELLEN

INTERNET DER DINGE



Alles soll „smart“ werden: Stromzähler, Kühlschränke oder Autos. Denn: Milliarden Geräte gehen in den nächsten Jahren online, gesteuert übers Internet. Vernetzung und Kommunikation, so lauten die Verheißungen der IT-Industrie, die auch Logistik und Industrie revolutionieren will. Doch um welchen Preis? Werden uns Algorithmen in Zukunft das Denken abnehmen?

Stellen Sie sich Ihren Alltag 2025 vor: Sphärenklänge wecken Sie sanft, weil Ihr Nachtsensor am Handgelenk merkt, dass Sie genug geschlafen haben. Ein kurzes Funksignal — und schon ist Ihre Stereoanlage im Schlafzimmer angesprungen. Zugleich schaltet sich die Kaffeemaschine ein, und Ihr intelligenter Thermostat weiß, dass Sie aufstehen. Daher steigt jetzt die Raumtemperatur. Und: Ihre Mobil-App wertet bereits aktuelle Verkehrsdaten aus. So ist der Bordcomputer in der Lage, in Ihrem “Google Driverless Car“ die optimale Route zur Arbeit festzulegen … „Zufällig“ mit einem kleinen Umweg — zu einem Kaffee-Stopp in der Bäckerei, die eine Anzeige bei Google laufen hat.

VOM „SMART HOME“ BIS ZUR „SMART FACTORY“

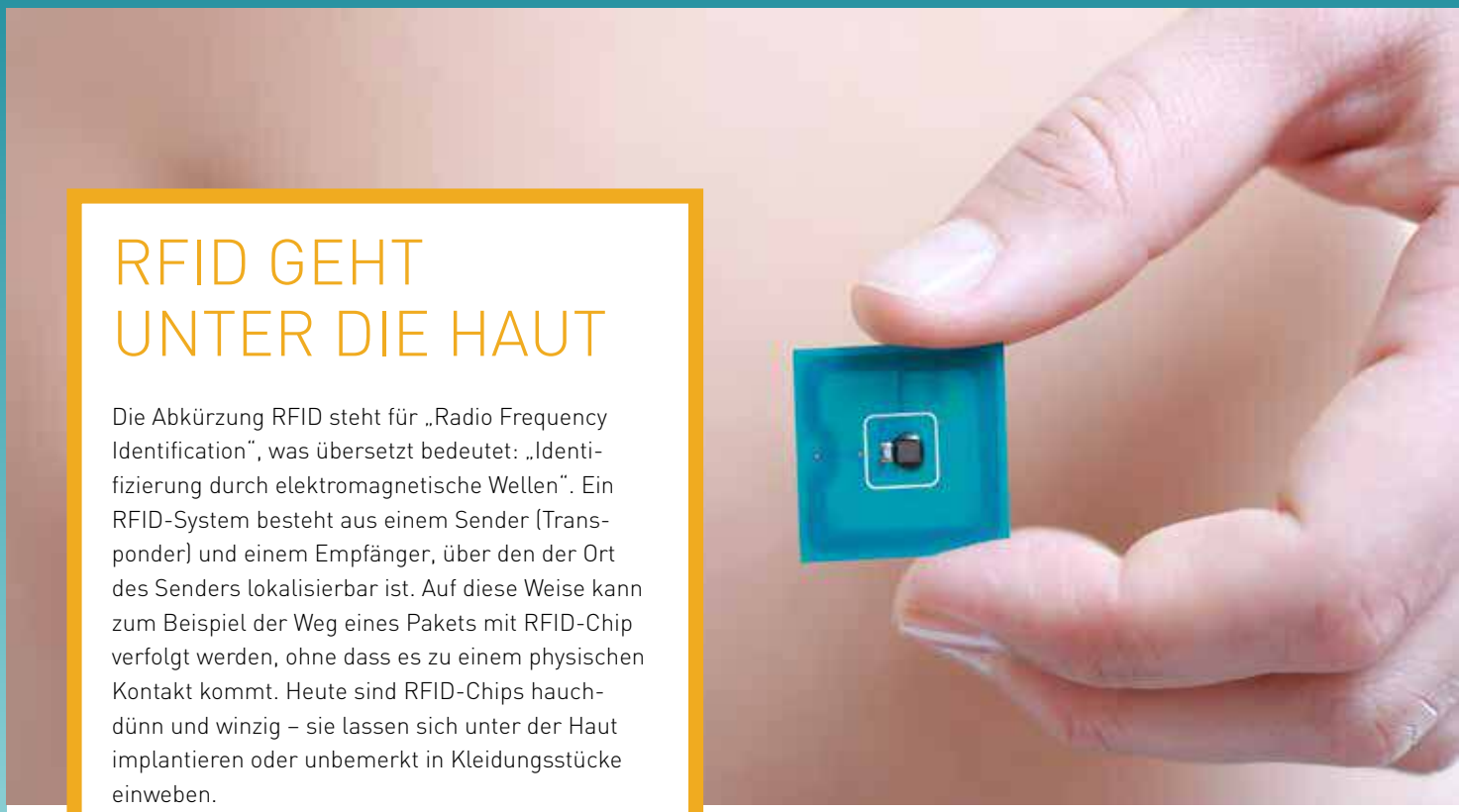
Diese Wunderwelt soll auf uns warten, der englische Begriff lautet „Internet of Things“ (IoT), das „Internet der Dinge“. Mark Schulte definiert es auf Silicon.de in dieser Weise: „Lösungen, die auf dem Internet der Dinge basieren, verbinden üblicherweise Dinge (Autos, Geräte, Gebäude, etc.). Sie ermöglichen somit den Austausch und die Analyse von Daten mit dem Ziel, Maßnahmen abzuleiten und einen Mehrwert zu generieren.“ Die Absicht: Ein „Smart Home“ soll entstehen, genauso wie „Smart Factories“ oder „Smart Mobility“. Die Intelligenz hält Einzug in die Welt der Maschinen, so das globale Marketing-Versprechen.

50 MILLIARDEN GERÄTE SIND BIS 2050 VERNETZT

Dabei findet der Datenaustausch direkt zwischen den „Dingen“ statt, die Schnittstelle „Mensch“ fällt weg. Die erste Stufe war erreicht, als sich Computer vernetzten, daraufhin wurden Smartphones internetfähig, und jetzt folgen intelligente Kühlschränke oder Thermostate sowie smarte Stromzähler — bis hin zu Autos, die eines Tages selbst fahren. Das Unternehmen Ericsson schätzt: 50 Milliarden Geräte werden 2050 online vernetzt sein.

PAKETE ORGANISIEREN SELBST IHREN WEG ZUM ZIEL

Auch das „Fraunhofer-Institut für Materialfluss und Logistik“ hat eine RFID-Vision (s. S. 20): Da der große Aufschwung von E-Commerce gewaltige Waren- und Datenströme ausgelöst hat, ist ein „zukunftsweisendes Logistiksystem“ notwendig. „Intelligente Geräte sollen denken lernen und Waren ihren Weg zum Ziel selbst organisieren“, schreiben die Wissenschaftler auf ihrer Website. Ob Behälter, Palette oder Paket — alle Objekte im Logistikprozess werden mit digitalen Speichern ausgerüstet. Auf diese Weise bekommen sie Informationen zu Zielen und Prioritäten. Das versetzt sie in die Lage, vor Ort einfache Entscheidungen selbst zu treffen.



RFID GEHT UNTER DIE HAUT

Die Abkürzung RFID steht für „Radio Frequency Identification", was übersetzt bedeutet: „Identifizierung durch elektromagnetische Wellen". Ein RFID-System besteht aus einem Sender (Transponder) und einem Empfänger, über den der Ort des Senders lokalisierbar ist. Auf diese Weise kann zum Beispiel der Weg eines Pakets mit RFID-Chip verfolgt werden, ohne dass es zu einem physischen Kontakt kommt. Heute sind RFID-Chips hauchdünn und winzig – sie lassen sich unter der Haut implantieren oder unbemerkt in Kleidungsstücke einweben.

RFID-Chips können so zu „Spychips" werden, wie Katherine Albrecht und Liz McIntyre in ihrem gleichnamigen Buch schreiben: „In einer zukünftigen Welt, die mit RFID-Schnüffelchips durchwoben ist, können Karten in Ihrer Brieftasche Sie ‚verraten', wenn Sie ein Einkaufszentrum, einen Supermarkt oder einen Gemüseladen betreten, und sie teilen dann dem Betrieb nicht nur Ihre Anwesenheit, sondern auch Ihre Kaufkraft mit."

Es könnten überall Lesegeräte versteckt sein, in Wänden, Regalen, Fußböden und Türen. Diese Geräte würden alle RFID-Chips scannen, die wir mit uns tragen, etwa in der Kleidung. So ließe sich unser Alter, Geschlecht und persönliche Vorlieben bestimmen. „Da Schnüffelchip-Informationen auch durch die Kleidung dringen", so Albrecht und McIntyre, „könnte man auch einen Blick auf die Farbe und Größe Ihrer Unterwäsche werfen."

Der Wirtschaft bringt RFID schon große Vorteile: Inventuren werden überflüssig, weil sich im Lager alle Waren genau orten lassen. Transportwege werden in Echtzeit verfolgt, weil die Transponder jederzeit den Standort einer Ware melden. So kann ein Unternehmen bei Verzögerungen schnell reagieren. RFID macht Prozesse in der industriellen Produktion transparenter und effizienter, was die Kosten sinken lässt.

Ein Blick auf die künftige Logistik-Lösung: Pakete sammeln mit RFID-Chips Informationen über ihre Umwelt, zum Beispiel zur Luftfeuchtigkeit oder Temperatur. Bei Gefahr schlagen sie selbstständig Alarm, agieren ständig in Netzwerken mit anderen Paketen – und bestellen autonom ihren Transport zu einem bestimmten Ziel. So entstehen logistische Einheiten, die dezentral und autonom „handeln". Der Traum besteht aus Geräten und Paketen, die voll automatisch „wie Zahnräder ineinandergreifen", von der Bestellung bis zur Lieferung, so die Wissenschaftler.

Dieses Konzept trägt in Deutschland den Namen „Industrie 4.0" oder „Smart Factory": „Gemeint ist die zunehmende Vernetzung in der Produktion und den Wertschöpfungsketten", sagt Frederik Armknecht, Professor für Kryptographie an der Universität Mannheim. „In der Produktion wollen Unternehmen, dass einzelne Elemente in größerer Autonomie zusammenarbeiten und kommunizieren."

SPEZIELLE KUNDENWÜNSCHE ERFÜLLEN

Dazu würden Maschinen mit Sensoren ausgestattet, wodurch autonom schnellere Reaktionen möglich wären. Auf zwei Vorteile setzten die Unternehmen: „Sinkende Produktionskosten, weil zum Beispiel eine Maschine merkt, dass ihr ein bestimmtes Material ausgeht und dann selbstständig beim Lager Nachschub bestellt“, so Armknecht. Ein zweiter Pluspunkt könnte sein, individueller zu produzieren. „Immer mehr Kunden äußern spezielle Wünsche, die sich aber in großen Chargen nicht realisieren lassen“, stellt der Mannheimer Professor fest.

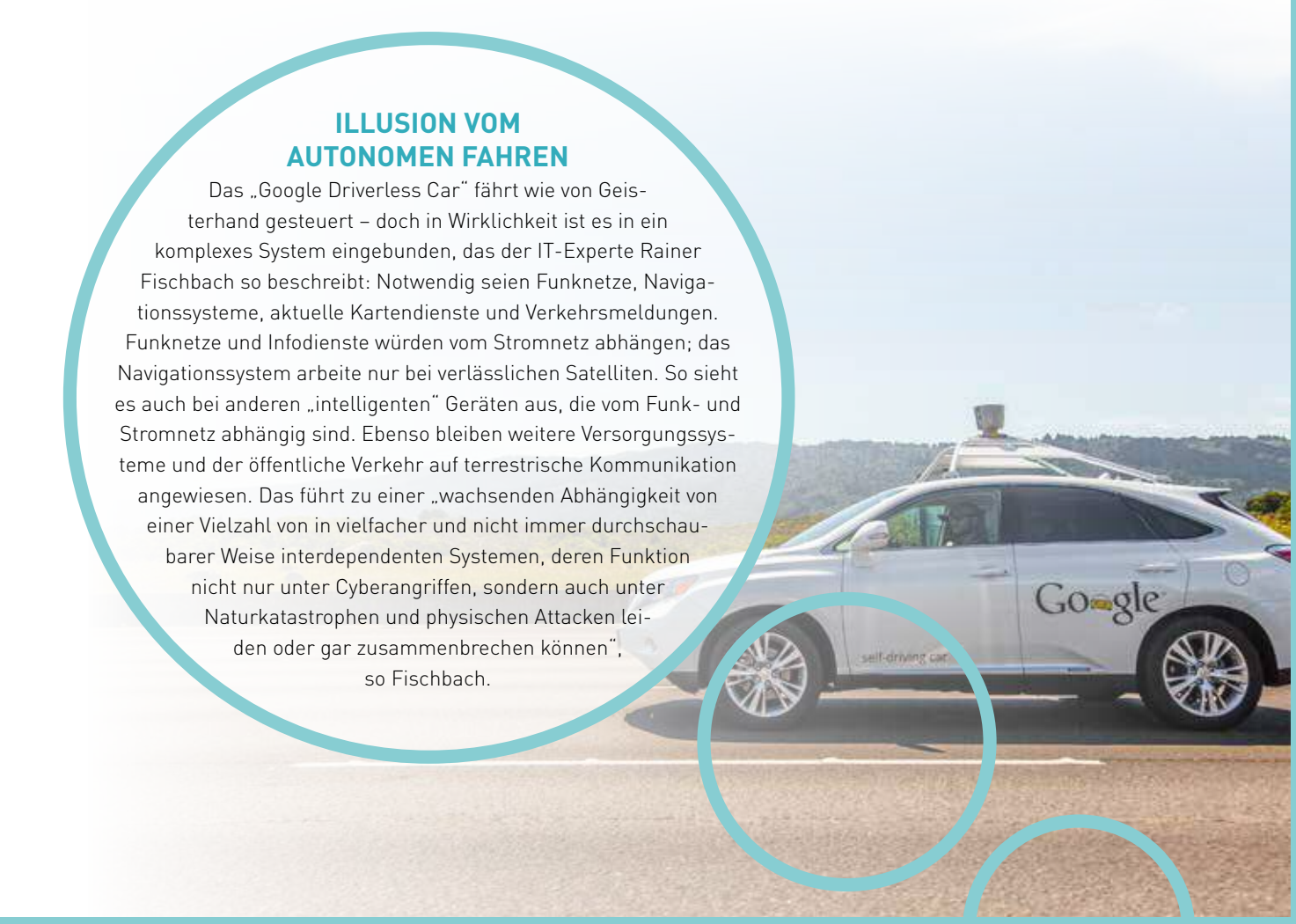
„Die ‚Versmartung der Welt‘ wirft Probleme der Sicherheit und Zuverlässigkeit auf, für die es noch keine Lösung gibt.“ (Fischbach)

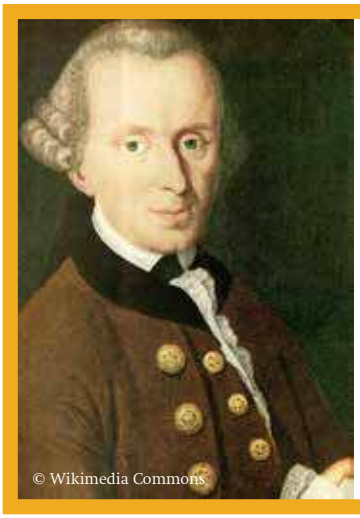
Wenden wir uns wieder Ihrem Alltag im Jahr 2025 zu: Kühlschränke sind intelligent und handeln autonom. Keine Pizza mehr im Kühlfach? Ein Sensor registriert den Mangel und bestellt beim Lieferservice nach. Gleichzeitig geht eine Meldung an die Gesundheitscloud, die Ihr Essverhalten für die Krankenkasse überwacht. Den günstigen Tarif (Piz3) gibt’s nämlich nur bei einer klaren Obergrenze für den Konsum von Pizza …

Kühlschränke geistern aber schon jetzt durch die Medien, weil sie Spam-Mails verschickt haben. Spam-Mails? Tatsächlich: Die US-Sicherheitsfirma „Proofpoint“ berichtet 2014, dass es den „ersten nachweisbaren IoT-basierten Cyberangriff“ gegeben hat. Bei ihm seien handelsübliche „intelligente“ Haushaltsgeräte eingesetzt worden, um weltweit 750.000 Phishing- und Spam-Mails zu verschicken.

ILLUSION VOM AUTONOMEN FAHREN

Das „Google Driverless Car“ fährt wie von Geisterhand gesteuert – doch in Wirklichkeit ist es in ein komplexes System eingebunden, das der IT-Experte Rainer Fischbach so beschreibt: Notwendig seien Funknetze, Navigationssysteme, aktuelle Kartendienste und Verkehrsmeldungen. Funknetze und Infodienste würden vom Stromnetz abhängen; das Navigationssystem arbeite nur bei verlässlichen Satelliten. So sieht es auch bei anderen „intelligenten“ Geräten aus, die vom Funk- und Stromnetz abhängig sind. Ebenso bleiben weitere Versorgungssysteme und der öffentliche Verkehr auf terrestrische Kommunikation angewiesen. Das führt zu einer „wachsenden Abhängigkeit von einer Vielzahl von in vielfacher und nicht immer durchschaubarer Weise interdependenten Systemen, deren Funktion nicht nur unter Cyberangriffen, sondern auch unter Naturkatastrophen und physischen Attacken leiden oder gar zusammenbrechen können“, so Fischbach.




© Wikimedia Commons

„Faulheit und Feigheit sind die Ursachen, warum ein so großer Theil der Menschen [...] gerne Zeitlebens unmündig bleiben und warum es Anderen so leicht wird, sich zu deren Vormündern aufzuwerfen". (Kant)

Dazu hatten Kriminelle ein roboterartiges „Botnet" gebildet, und zwar aus mehr als 100.000 Alltagsgegenständen. Darunter: „Heimnetzwerk-Router, vernetzte Multimedia-Center, Fernseher und mindestens ein Kühlschrank", so das Unternehmen. Weiter heißt es in dem Text: „Die bereits erwähnten, mit dem Internet verbundenen Geräte sind in der Regel schlecht geschützt. Sie bieten dadurch eine Umgebung mit zahlreichen leichten, lohnenswerten Zielen, die einfacher zu infizieren und zu steuern sind als PCs, Laptops oder Tablets."

LEICHT ANGREIFBARE INFRASTRUKTUR

Das gilt genauso für die „Industrie 4.0", wie Armknecht betont: „Die vernetzten Geräte sind viel schwächer geschützt. Dadurch ist es nicht möglich, Schutzmaßnahmen für PCs einfach auf die Geräte einer smarten Fabrik zu übertragen." Hinzu kommt: „Es entsteht gerade eine neue Infrastruktur mit Milliarden Geräten, die alle leicht angreifbar sind. Das ist der Preis für eine Technik, die immer kleiner und billiger wird."

Dazu schreibt der IT-Experte Rainer Fischbach („Smarte neue Welt", LuXemburg 3/2015): „Die verfügbaren starken kryptologischen Verfahren (...) für Verschlüsselung und Authentifizierung sind äußerst aufwendig", sobald sie im „Internet der Dinge" zum Einsatz kommen sollen. Sie seien durch die einfachen Geräte „nicht zu bewältigen", zumal oft Aufgaben in Echtzeit zu erledigen sind. Fischbach ist überzeugt: Die beste Verschlüsselung bringe keinen Nutzen, wenn es in Systemen Hintertüren gibt. „Es ist ein Irrglaube zu meinen, so der IT-Experte, „Hintertüren ließen sich für nur einen Akteur reservieren." Seine Schlussfolgerung: „Die ‚Versmartung der Welt' wirft Probleme der Sicherheit und Zuverlässigkeit auf, für die es noch keine Lösung gibt."

ABHÖREN LEICHT GEMACHT

Und Armknecht lenkt den Blick auf ein weiteres Risiko: „In der ‚Industrie 4.0' sollen alle Produkte und Geräte autonom miteinander kommunizieren, was sich natürlich abhören lässt." Selbst das reine „Mithören" sei gefährlich, was der Kryptographie-Experte an einem Beispiel erklärt: „Eine Maschine fordert die Zutaten für Coca Cola an — und schon ist jemand von außen in der Lage, das geheime Rezept für Coca Cola auszuspähen. Überall wo mehr geredet wird, kann auch mehr belauscht werden."

Fazit: „Internet der Dinge" und „Industrie 4.0" — auf den ersten Blick setzt sich ein Trend fort, der mit der Industriellen Revolution begonnen hat: Technik wird immer intelligenter, sie nimmt uns immer mehr Arbeit ab — und befreit uns von stupider Routine sowie von Tätigkeiten, die gesundheitlich bedenklich sind. Wer würde heute schon gerne seine Kinder ins Bergwerk schicken?

2014 verschickte ein Botnet
aus **100.000** elektronischen Geräten
750.000 Phishing- und Spam-Mails

Doch unser digitales Leben der Zukunft hat eine neue Qualität: Komplexe Systeme beherrschen die ebenso komplexen Strukturen des Alltags, weshalb sie ständig automatisiert in unser Leben eingreifen. „Wir treten damit in ein Zeitalter der selbst gewählten Unselbständigkeit ein — gewissermaßen einer das ganze Leben lang dauernden Kindheit", schreibt 2008 der Trendforscher Max Celko („Hyperlocality: Die Neuschöpfung der Wirklichkeit", GDI IMPULS Magazin 2/2008).

„Selbst gewählte Unselbständigkeit" — diese Formulierung erinnert nicht zufällig an Immanuel Kant (1724-1804). Der Philosoph schrieb 1784 in seinem berühmten Essay „Beantwortung der Frage: Was ist Aufklärung?":

„Faulheit und Feigheit sind die Ursachen, warum ein so großer Theil der Menschen […] gerne Zeitlebens unmündig bleiben; und warum es Anderen so leicht wird, sich zu deren Vormündern aufzuwerfen. Es ist so bequem, unmündig zu seyn. Habe ich ein Buch, das für mich Verstand hat, einen Seelsorger, der für mich Gewissen hat, einen Arzt, der für mich die Diät beurteilt, u.s.w., so brauche ich mich ja nicht selbst zu bemühen."

Heute hätte Kant noch Apps hinzugefügt, um seine Aufzählung der Bequemlichkeiten abzurunden …

Wollen wir wirklich, dass Maschinen uns das Denken abnehmen?

BIG BROTHER WIRD ZU BIG MOTHER

Und Max Celko? Er greift zu einer literarischen Figur des 20. Jahrhunderts, um dasselbe Phänomen zu beschreiben: „Big Brother wandelt sich zu Big Mother, die uns umsorgt und für uns komplexe Entscheidungen fällt. […] Wir werden bemuttert von einem Überwachungsapparat." Er verweist auf eine drohende „Apathie", die eine solche Entwicklung mit sich bringen könnte.

Alles nur Kulturpessimismus? Die jüngsten Entwicklungen zur „Versmartung der Welt" (Fischbach) wecken zu Recht Skepsis. Wollen wir wirklich, dass Maschinen uns das Denken abnehmen? Es war ein großer Fortschritt, Maschinen statt Kinder im Bergwerk arbeiten zu lassen. Ist es genauso wertvoll, wenn Kühlschränke automatisch Pizza bestellen und wir die Kontrolle über unser Leben an Computer delegieren? Es wäre spannend, Kant solche Fragen zu stellen. Im bereits erwähnten Essay stellt er fest: „Aufklärung ist der Ausgang des Menschen aus seiner selbst verschuldeten Unmündigkeit." Wem schon das Navi kurz vorm Ziel abgestürzt ist, weiß genau, was Kant gemeint hat: Es geht um unsere „selbstverschuldete Unmündigkeit", weil wir auf immer bequemere IT-Systeme setzen.

So bietet die schöne smarte Welt ungekannten Komfort — aber auch genug Fallen, um vor lauter Sphärenklängen das Denken zu verlernen.