Holger Volland

Die Zukunft ist smart. Du auch?

mosaik

HOLGER VOLLAND

# DIE ZUKUNFT IST SMART. DU AUCH?

100 ANTWORTEN
auf die wichtigsten Fragen zu unserem
DIGITALEN ALLTAG

mosaik

Alle Ratschläge in diesem Buch wurden vom Autor und vom Verlag sorgfältig erwogen und geprüft. Eine Garantie kann dennoch nicht übernommen werden. Eine Haftung des Autors beziehungsweise des Verlags und seiner Beauftragten für Personen-, Sach- und Vermögensschäden ist daher ausgeschlossen.

Sollte diese Publikation Links auf Webseiten Dritter enthalten, so übernehmen wir für deren Inhalte keine Haftung, da wir uns diese nicht zu eigen machen, sondern lediglich auf deren Stand zum Zeitpunkt der Erstveröffentlichung verweisen.

Dieses Buch ist auch als E-Book erhältlich.

MIX
Papier aus verantwortungsvollen Quellen
FSC® C083411
FSC
www.fsc.org

Penguin Random House Verlagsgruppe FSC® N001967

1. Auflage
Originalausgabe März 2021
Copyright © 2021: Mosaik Verlag, München,
in der Penguin Random House Verlagsgruppe GmbH,
Neumarkter Str. 28, 81673 München
Illustrationen: Janina Kress
Umschlaggestaltung: Sabine Kwauka
Umschlagmotiv: getty images / imaginima
Umschlagautorenfoto: Manuel Rauch
Redaktion: Antje Steinhäuser
Satz: Satzwerk Huber, Germering
Druck und Bindung: CPI books, Leck
Printed in Germany
KF· IH
ISBN 978-3-442-39383-1
www.mosaik-verlag.de

# Inhalt

Vorwort: Sind Sie schon smart? . . . . . 9

**ZUHAUSE:** Viele neue Mitbewohner . . . . . 17

Weiß mein Fernseher, was ich schaue? 18 • Wer wohnt denn hier noch alles? 23 • Locken smarte Glühbirnen Einbrecher an? 27 • Wieso brauchen Dinge ihr eigenes Internet? 31 • Warum ist Künstliche Intelligenz noch so dumm? 33 • Wer hört mit, wenn ich meine Pizza bestelle? 37 • Darf mich mein Vermieter filmen? 40 • Was sieht mein Staubsauger-Roboter bei der Arbeit? 44 • Wie lautet das beste Passwort? 47 • Wie viel Strom verbraucht einmal Googeln? 50

**DIGITALES LEBEN:** Wir sind die Produktmanager unserer Daten . . . . . 54

Wieso bin ich ein Produkt? 55 • Welche meiner Daten erfährt die Supermarktkasse? 59 • Zahle ich mehr für eine Reise, wenn ich mit dem iPhone buche? 63 • Finde ich mit einer App leichter einen Partner? 68 • Kann ich Online-Tests vertrauen? 71 • Wie viel Geld sind meine Daten wert? 76 • Weshalb kommen wir von den Sozialen Medien nicht los? 77 • Bin ich in einer Filterblase? 80 • Können mich Social-Media-Plattformen zensieren? 85 • Gibt es geheime Manipulationstechniken auf Websites? 88 • Hören unsere Smartphones heimlich mit? 90 • Warum bekommen wir so schlechte Werbung angezeigt? 95

**MOBILITÄT:** Software wird wichtiger als Hardware . . . . 100

Wird es Autos nur noch als Abo geben? 101 • Verpetzt mich mein Auto, wenn ich rase? 104 • Wer ist schuld, wenn ein autonomes Auto einen Unfall baut? 109 • Wer braucht zukünftig noch einen Führerschein? 111 • Wie sehen smarte

Autos unsere Straßen? 114 • Wie kann ich Hacker von meinem Auto abhalten? 118 • Wer fährt besser: Mensch oder Maschine? 120 • Warum ist Google Maps so unglaublich gut? 123 • Wird Autos beigebracht, ob sie eher Omas oder Kinder umfahren? 127

**BILDUNG UND KULTUR:** Unendliche Chancen und maximale Eigenverantwortung . . . . . 132

Schadet die Digitalisierung der Kultur? 133 • Worin sind Menschen zukünftig noch besser als Maschinen? 136 • Warum sind so viele Internet-Milliardäre Studienabbrecher? 140 • Ist Deutschland bei digitaler Bildung abgehängt? 143 • Kann ein Algorithmus Prüfungsfragen vorhersagen? 148 • Müssen wir alle Programmieren lernen? 152 • Können Roboter auf Kinder aufpassen? 156 • Wie bleibe ich in der digitalen Berufswelt fit? 158 • Wann kann ich mir einen Quantencomputer kaufen? 161 • Wie erziehen Silicon-Valley-Gründer ihre Kinder? 163 • Wie lernen Computer? 167 • Wann werden uns Maschinen überflügeln? 171 • Gibt es ein Archiv des Internets? 175

**RECHT UND UNRECHT:** Unsere Vorurteile bleiben . . . . . 177

Kann man Maschinen Moral beibringen? 178 • Würde mich eine Künstliche Intelligenz als Richterin fair behandeln? 181 • Was ist Daten-Diskriminierung? 185 • Wieso fallen wir alle auf Falschnachrichten herein? 190 • Welchen Schaden verursachen Fake News? 193 • Was kostet es, den Ruf eines Menschen zu zerstören? 195 • Warum brauchen wir Hacker? 199 • Warum sind Sprachassistenten immer weiblich? 201 • Wie erkenne ich, ob ich mit einem Bot kommuniziere? 204 • Wie vermeide ich falsche Freunde im Netz? 209 • Wieso kann im Netz jeder pöbeln? 212 • Kann ich Algorithmen als Fälscher nützen? 216

**GESUNDHEIT:** Jeder ist sein eigener Arzt . . . . . 221

Wie verändert eHealth das Gesundheitswesen? 222 • Wann wird mir meine Ärztin eine App verschreiben? 227 • Werde ich fitter, wenn ich einen Fitness-Tracker trage? 232 • Macht digitales Leben dement? 234 • Entdeckt ein Algorithmus Hautkrebs zuverlässiger als mein Arzt? 237 • Weiß Instagram, ob ich depressiv bin? 241 • Kann eine App den Psychiater ersetzen? 243 • Wie können Algorithmen bei Einschränkungen

helfen? 248 • Wieso hat uns Technik nicht vor Corona gewarnt? 252 • Haben Sie ein digitales Testament? 256 • Kann man ein Gehirn uploaden? 259

**ARBEIT:** Es gibt noch zwei Arten von Jobs – Du steuerst Maschinen oder Maschinen steuern dich . . . . . 261

Was kommt: Fachkräftemangel oder digitale Arbeitslosigkeit? 262 • Wird Künstliche Intelligenz zukünftig meinen Job übernehmen? 267 • Wird man als Influencer noch reich? 271 • Wer schreibt die Produktbeschreibungen bei Amazon? 275 • Gibt es für Digitalarbeiter eine Gewerkschaft? 278 • Arbeiten wir zukünftig alle im Homeoffice? 281 • Beobachten uns Algorithmen bei der Arbeit? 284 • Kann man Algorithmen bei ihrer Arbeit beobachten? 290 • Wie kann ich eine Bewerbungs-KI beschummeln? 295 • Darf mein Arbeitgeber meine Social-Media-Aktivitäten zensieren? 301

**WIRTSCHAFT:** Unterschiedliche Geschwindigkeiten managen, ist die wichtigste Aufgabe . . . . . 304

Warum nennt man Daten das neue Öl? 305 • Wie haben die Technologieriesen die Welt untereinander aufgeteilt? 309 • Was ist so besonders an 5G? 312 • Kann man das Internet löschen? 315 • Wann ist eigentlich die digitale Revolution vorbei? 318 • Hat Deutschland die Zukunft verschlafen? 322 • Welche Zukunftstechnologien können wir gut in Deutschland? 325 • Würden wir mit einer KI-Finanzministerin Steuern sparen? 328 • Warum zahlen Digitalkonzerne bei uns kaum Steuern? 332 • Womit verdient Amazon Geld? 334 • Was bringt uns eine Zerschlagung von Facebook? 337

**POLITIK:** Die Politik hinkt dem Netzkapitalismus hinterher . . . . . 344

Kommt die Politik bei der Digitalisierung noch hinterher? 345 • Gibt es einen europäischen Weg der Digitalisierung? 349 • Warum demonstrieren die Chinesen nicht gegen ihr Bürger-Punktesystem? 352 • Kann ein Bürger-Punktesystem auch zu uns kommen? 357 • Erkennt mich eine Überwachungskamera auch mit Sonnenbrille? 361 • Ist Gesichtserkennung bei uns legal? 364 • Woher kennen die Algorithmen eigentlich mein Gesicht? 367 • Wieso können wir noch nicht online wählen

gehen? 372 • Warum muss ich neuerdings bei jeder Website mein O. K. geben? 375 • Brauchen wir ein Bundesdigitalministerium? 377 • Sind wir im digitalen Kalten Krieg? 382 • Gibt es noch Länder ohne Internet? 386

Danksagung . . . . . 389

Quellen . . . . . 391

Updates und Diskussionen unter
**#Zukunft100**
bei Twitter, LinkedIn, Facebook.

# Vorwort: Sind Sie schon smart?

Es tut sich eine Kluft auf. Die ersten zarten Risse zeigten sich vor dreißig Jahren. Im Lauf der Zeit wurden sie immer zahlreicher, tauchten hier und dort unvermutet aus dem Nichts auf, wurden breiter und tiefer. Die Geschwindigkeit nahm zu. Immer schneller zog sich bald ein sichtbar tiefer Graben durch die Gesellschaft. Bis die Veränderung schließlich, auf dem Rücken der weltweiten Corona-Pandemie, ein Höllentempo bekam und inzwischen Dimensionen erreicht, die niemand mehr ignorieren kann.

Ich rede von der Kluft zwischen digitalen Gewinnern und analogen Verlierern. Auf einer Seite wachsen in atemloser Entwicklung Technologie, Wissenschaft, Forschung und Digitalwirtschaft in immer neue Dimensionen. Auf der anderen Seite stehen wir, analoge Menschen mit unseren traditionellen Formen des Zusammenlebens, bedächtigen Politik, unserem Vertrauen in Bildungssysteme, Krankenkassen oder Verbrennungsmotoren.

Auf welcher Seite stehen Sie? Wo stehe ich? Diese Frage werden wir uns alle in den nächsten Jahren stellen. Das wurde mir einmal mehr klar, als ich von der Bühne einer Konferenz aus in den Raum voller Menschen schaute, die mit Überschwang die Segnungen der Digitalisierung, der »Neuen Arbeit« und der exponentiellen Entwicklungen diskutierten. Die Zukunft dieser Menschen glühte vor Möglichkeiten, sie schien rosarot im Angesicht der Segnungen von Technologie. Das Ende des Hungers. Das Ende der Arbeit. Das Ende der Krankheit. Darunter ging es nicht. Natürlich – so hatten viele Spre-

cherinnen und Experten an diesem Konferenztag schon betont und dabei demütig die Augen gesenkt – würden sich auf dem Weg in die Zukunft einige Berufe auch ändern. Raumpflegerinnen etwa, oder Kassierer und auch Bergarbeiter müssten gegebenenfalls andere Aufgaben übernehmen.

»Ist hier ein Bergarbeiter anwesend?«, fragte ich von der Bühne in den Raum. Keine einzige Meldung. »Ein Kassierer oder eine Raumpflegerin vielleicht?« Stille. Verlegenes Lachen. Ich wandte mich meinen beiden Gesprächspartnern zu. Der deutsche Arbeitsminister und die Chefin von Microsoft Deutschland saßen neben mir auf dem Podium dieser Veranstaltung. Das Problem, so stellten wir schnell gemeinsam fest, ist doch, dass die Digitalisierung uns alle betrifft: Raumpfleger, Kassiererinnen, Bergleute, Lehrer, Ärztinnen, Manager, Politikerinnen und Programmierer. Sie betrifft uns alle, aber nicht wir alle reden mit. So wie bei dieser Zukunftskonferenz nur eine kleine digitale Elite anwesend war, verläuft auch eine Kluft quer durch die Gesellschaft. Auf der einen Seite stehen Gewinner, die digitale Entwicklungen verstehen, von ihnen profitieren oder sie sogar vorantreiben. Auf der anderer Seite stehen normale Menschen.

Der Minister zitierte hierzu den »Fachkräftemonitor« und erklärte, dass die Bundesregierung bis zum Jahr 2025 mit einem Verschwinden von 1,3 Millionen Arbeitsplätzen durch die Digitalisierung rechne. Er ergänzte, dass gleichzeitig 2,1 Millionen neue Jobs durch sie entstehen würden. Das ist doch eigentlich eine gute Nachricht, oder? Der Minister stockte kurz. Problematisch sei bei der Sache, dass es gerade für diese neu entstehenden digitalen Jobs nicht genügend richtig ausgebildete Menschen bei uns gäbe. Die Microsoft-Chefin

nickte zustimmend. Schon heute können bei ihr im Technologiesektor Zigtausende Stellen nicht besetzt werden, weil es nicht genügend Fachleute gibt.

Was für eine tiefe Kluft! Da gibt es eine riesige Zahl freier Stellen, die nicht besetzt werden können, und gleichzeitig Millionen Arbeitslose, deren Wissen nicht mehr für zukünftige Jobs ausreicht. Wir Menschen und unsere Qualifikationen passen nicht mehr zu der Arbeit, die die Digitalisierung zukünftig für uns vorsieht.

Die Corona-Krise hat diese Kluft weiter vertieft. Auf der einen Seite haben dank Homeoffice und geschlossenen Läden Anbieter wie Amazon, Google oder Zoom Rekordgewinne erwirtschaftet, das Gesundheitswesen, das Bildungssystem und große Teile der Wirtschaft haben Digitalisierungsoffensiven im Schnellformat aus dem Boden gestampft. Auf der anderen Seite standen plötzlich Millionen von Kurzarbeitern, denen die Arbeit ausging, weil sie nicht Teil der digitalen Wertschöpfung waren: Schneiderinnen, Wirte, Mechanikerinnen, Köche, Verkäufer, Textilfacharbeiter, Designerinnen oder Architektinnen. Die Digitalisierung lässt auf ihrem Weg durch die Branchen viele Gruppen auf der Verliererseite zurück.

Und wer jetzt hofft, dass die kommende Generation besser gerüstet ist, den muss ich enttäuschen: Nach einer Studie der OECD aus dem Januar 2019 streben die meisten der befragten Fünfzehnjährigen im deutschsprachigen Raum weiterhin traditionelle Berufe wie Ärztin, Lehrer oder Polizist an. Die Chancen und Herausforderungen der Digitalisierung scheinen die Mehrheit der Befragten noch so wenig zu interessieren, dass sie damit keinen konkreten Berufswunsch für sich verbinden. Aber ich frage mich: Wer soll dann die über zwei Mil-

lionen freien Stellen besetzen, über die der Arbeitsminister sprach, wenn wir digital so schlecht gerüstet sind?

Deshalb haben wir eine Aufgabe. Sie, ich, der Minister und die CEO gleichermaßen. Unsere Aufgabe ist es, die Kluft zu schließen. Wir werden nämlich alle in derselben digitalen Gesellschaft leben und deshalb werden wir auch alle mitnehmen müssen – selbst den Bergarbeiter. Wie wir das erreichen? Vor allem, indem wir viele Fragen stellen. Wir müssen alles befragen, was wir nicht verstehen oder was uns komisch vorkommt. Mit diesem Buch möchte ich Sie dazu ermuntern, Ihre eigenen Fragen zu formulieren. Ich habe schon einmal vorab hundert Fragen ausgewählt, die mich besonders interessieren. Das ist wahrscheinlich nur ein oberflächlicher Einstieg, eine Einladung zum tieferen Graben und zu immer wieder neuen Fragen. Stellen Sie sie. Beschäftigen Sie sich mit der digitalen Welt und den Teilen davon, die Sie besonders interessieren. Helfen Sie mit, die Trennung zwischen digitalen Vorreitern und analogen Mitmenschen zu überbrücken. Oder wechseln Sie gar die Seite!

Denn was wir im Arbeitsmarkt sehen, lässt sich in allen Teilen der Gesellschaft, der Politik, dem Gesundheitswesen und im Alltag beobachten. Es gibt eine Gruppe, die sich gut auskennt, mit ihrer digitalen Kompetenz Entwicklungen und Angebote immer schneller vorantreibt. Und es gibt eine andere Gruppe, die digitale Veränderungen zögerlich betrachtet, nicht mehr versteht oder ignoriert, weil sie ihr zu abgehoben sind. Nach Befragungen des Digitalverbandes Bitkom haben sechs von zehn Deutschen den Begriff »Blockchain« noch nie gehört, fast die Hälfte weiß nicht, was »Quantencomputing« ist, und immerhin ein Viertel zuckt bei »Big Data« unwissend mit den Schultern. Es wird den Unwissenden aber auch nicht leicht

gemacht: Wie soll man das alles wirklich begreifen, solange man Quantencomputer nicht bei Amazon bestellen kann, Big Data kein Schulfach ist und man bei der Hausbank keine Blockchain-Währungen kaufen kann?

Jeder siebte Deutsche empfindet das Tempo der Digitalisierung als zu schnell und hat das Gefühl, nicht mehr mitzukommen. Ein Grund dafür ist, dass sich Technologieunternehmen zu lange so verhalten haben, als stünden sie außerhalb unserer Gesellschaft, müssten keine Steuern zahlen und weder der Politik noch normalen Bürgern transparent erklären, womit sie konkret ihr Geld verdienen.

Ich kann die Zögerlichkeit der Deutschen deshalb gut verstehen. Die momentane Situation ist extrem verwirrend. Vielleicht ist sie sogar schizophren. Denn einerseits wird uns die Digitalisierung als futuristische Lösung für die Klimakrise, die Auslöschung von Krankheiten und Hunger verkauft, und es werden uns fantastische Ausblicke für die Wirtschaft versprochen. Andererseits gibt es mindestens ebenso viele Warnungen vor digitaler Demenz, der Übermacht der Digitalkonzerne und einer vollständig gläsernen Menschheit im Überwachungskapitalismus. Und es erscheinen fast im Stundentakt neue Studienergebnisse und Veröffentlichungen von Expertinnen und Autoren, die in abstrakten makroökonomischen Theorien oder bizarren Datenmodellen unendlich viele Aspekte der Digitalisierung erforschen. Was soll man da jetzt glauben?

Dazwischen stehen wir, ganz normale Menschen, die ein Facebook-Profil haben, YouTube schauen oder TikTok nutzen, die mit Google Maps ihren Weg finden und mit Alexa eine Pizza bestellen. Wer übersetzt die Wissenschaft für uns? Wer sagt uns, was richtig und falsch ist? Können wir zufrie-

den mit uns sein, weil wir locker die Apps in unseren Alltag integriert haben? Oder müssen wir uns schlecht fühlen, weil wir räuberische, steuerhinterziehende Digitalkonzerne unterstützen?

Es ist kompliziert. Die Auswirkungen der Digitalisierung auf unsere Welt sind sogar so kompliziert, dass es noch nicht einmal dem US-Kongress in seinen Befragungen von Mark Zuckerberg gelungen ist, die ganze Tragweite von Facebooks Einfluss auf unseren Alltag komplett zu ergründen. Sitzungen reichen dafür nicht, es braucht jahrelange Recherchen und dickleibige Bücher, um die gesamte Macht von Digitalunternehmen zu untersuchen. In diesem Feld den Durchblick zu behalten ist nicht leicht, denn oft vermitteln Experten hochkomplexe technologische Erscheinungen ohne jeden Bezug zu unserem Alltag. Auch viele Politiker agieren so, als ob Technologie eine geheimnisvolle und unverständliche Macht wäre, die unabhängig von unserem Alltag Probleme lösen und die Welt gestalten kann. Viele Konzerne, in ihrem Drang nach steigendem Shareholdervalue, machen aus Daten Produkte, die einfach und hilfreich klingen, dabei aber im Kern so undurchschaubar wie menschenfeindlich sind.

Wie sollen Nicht-Experten da noch durchblicken? Wie können wir dafür sorgen, dass wir nicht auf der Verliererseite der Digitalisierung landen und wichtige Entwicklungen schlicht an uns vorbeiziehen?

Ganz einfach: Indem wir so lange Fragen stellen, bis wir mit den Antworten endlich zufrieden sind. Die allermeisten Fragen in diesem Buch stammen deshalb von Menschen, die mutig genug waren, sie bei Veranstaltungen im Publikum zu stellen, nach Vorträgen zu mir kamen oder mir Nachrichten

schickten. Ich habe sie gesammelt und in neun Lebensbereiche sortiert, die uns alle betreffen: Unser Zuhause und unsere Freizeit, für die es so viele digitale Angebote gibt, dass wir klug sortieren müssen, welche davon wirklich sinnvoll sind und welche uns sogar schaden. Mobilität, Arbeit, Bildung und Gesundheit, die uns immer mehr Selbstverantwortung abfordern, aber auch außergewöhnliche Möglichkeiten für mehr Wissen, Gesundheit und Lebensqualität bieten. Und Recht, Wirtschaft und Politik, in denen jetzt gerade die Regeln, Prozesse und Gesetze geschaffen werden, die unsere Zukunft massiv beeinflussen. Wir müssen sie verstehen, um als souveräne Bürgerinnen und Bürger bewusst leben (und wählen!) zu können.

Beim Schreiben habe ich gemerkt, wie sehr alle diese Lebensbereiche miteinander verwoben sind. Sie hängen durch die Digitalisierung zusammen. Manche, ganz grundsätzliche Beobachtungen werden uns deshalb häufiger in diesem Buch begegnen: zum Beispiel, dass Software Hardware ablöst, dass vor allem derjenige Power hat, dem Daten gehören, oder dass Selbstmanagement zur wichtigsten Schlüsselkompetenz in der digitalen Gesellschaft gehört.

Am Ende kreisen alle Themen in diesem Buch um die eine große, die ganz persönliche Frage: »Wie wirkt sich die digitale Zukunft auf unser aller ganz persönliches Leben aus?« Denn eines hat sich spätestens mit der Corona-Krise gezeigt: An der Digitalisierung kommt wirklich niemand mehr vorbei, und deshalb geht sie auch uns alle etwas an.

Ich bin der festen Überzeugung, dass die Digitalisierung niemanden zurücklassen darf. Wir müssen alles dafür tun, niemanden auf der Verliererseite stehen zu lassen. Wir müssen allen Menschen digitales Wissen durch unsere Fragen näher-

bringen. Wir Nutzer müssen klüger werden und nicht mehr nur stupide Apps herunterladen, Werbung ansehen und Produkte kaufen. Denn mit mehr technologischem Wissen kommt die Entscheidungsfreiheit darüber, welche Technologie uns weiterbringt und welche uns hemmt, was uns manipuliert, was unser Wissen vermehrt, was uns auf die Gewinnerseite der Digitalisierung bringt oder was uns als »Klickvieh« zurücklässt, das sich hirnlos von Werbung zu Werbung klickt und damit die ungeheuerlichen Gewinne von Tech-Firmen überhaupt ermöglicht.

Viele Entwicklungen der letzten Jahre haben wir ungefragt den Technologieexperten und den Unternehmen überlassen, uns für ein paar kostenlose Dienste Tag und Nacht aushorchen lassen und schulterzuckend akzeptiert, dass Digitalisierung halt einfach sehr schnell passiert und wirklich kompliziert zu sein scheint. Dabei ist Digitalisierung sehr menschlich und benötigt unser aller Aufmerksamkeit. Wir können sie bewusst zu unserem Vorteil verwenden, gestalten und regulieren. Denn selbst Technologieunternehmen müssen sich an dem Rahmen ausrichten, den wir Nutzer, Politikerinnen oder Aktionäre für sie definieren. Es wird Zeit, dass wir Menschen den digitalen Alltag erobern und nach unseren Vorstellungen und zu unserem eigenen Nutzen selbst gestalten. Das klappt am besten, wenn wir uns ansehen, wie tief die Digitalisierung bereits in viele unserer Lebensbereiche eingedrungen ist. Wir beginnen deshalb die Reise da, wo Sie jetzt vielleicht gerade sitzen: im Wohnzimmer.

# ZUHAUSE

## Viele neue Mitbewohner

## Weiß mein Fernseher, was ich schaue?

Endlich Feierabend. Ich ziehe die bequeme Jogginghose an und lege die Füße auf den Couchtisch. Eine Schüssel Chips neben mir, den Wein in Reichweite – herrlich so ein Abend mit mir! So liege ich auf dem Sofa, schaue mir eine hirnlose, aber unterhaltsame Serie an und freue mich, dass ich mich nicht benehmen muss, weil ich alleine zu Hause bin.

Ob ich mich auch so gehen lassen würde, wenn ich wüsste, dass ich nicht alleine bin? Wenn ich wüsste, dass mein smarter Fernseher mir gerade ebenso interessiert zusieht wie ich ihm? In den meisten Wohnzimmern haben sich die TV-Geräte zu den Unterhaltungzentralen der Wohnung entwickelt. Über sie wird Musik abgespielt, mit entfernt wohnenden Familienmitgliedern geskypt, die Yoga-App mit Erklärungsvideos genutzt und natürlich werden über sie auch Computerspiele gezockt und Filme oder Serien angesehen. Ganz selten läuft bei vielen Menschen nur noch das traditionelle Fernsehprogramm auf einem Fernseher. Um all diese neuen Funktionen zu ermöglichen, ist es nötig, dass in die Geräte Kameras, Mikrofone oder Bewegungssensoren eingebaut sind. Diese werden gebraucht, um Videoanrufe, interaktive Spiele oder Sprachsteuerung bereitzustellen. Dabei nehmen sie allerdings vieles von dem, was sie sehen und hören, auch auf. Womöglich sogar ein Bild von mir auf dem Sofa mit Chipsbröseln auf dem Bauch.

Selbst ältere Geräte ohne solche zusätzlichen Sensoren können interessierte Beobachter sein. Sie erkennen uns zwar nicht mit Kameraaugen, dafür nehmen sie auf, welche Inhalte auf

den Bildschirmen dargestellt sind, wie lange wir diese betrachten oder aus welchen Quellen und Programmen sie kommen. Solche Informationen schicken sie dann an die Hersteller der TV-Geräte und an die Firmen, deren Apps auf den Geräten installiert sind: Netflix, YouTube, Amazon und viele andere mehr.

Wofür verwenden die Firmen diese Informationen? Macht man sich die Mühe und liest die Nutzungsbedingungen von Geräten und Apps durch, finden sich eher schwammige Erklärungen wie »besserer Service für unsere Kunden« oder »notwendig für die Bereitstellung von Inhalten«. Dahinter verbergen sich einerseits personalisierte Angebote, wie passende Vorschläge von Filmen und Serien auf Basis unserer Profile, außerdem aber auch personalisierte Werbung, die immer häufiger gleich nach dem Einschalten des Geräts erscheint. Und nicht zuletzt fließen diese Daten auch in die existierenden Nutzerprofile, die es von uns beispielsweise bei Unternehmen wie YouTube gibt, das zum Google-Konzern gehört. Denn wenn ein Werbeanbieter über meinen Fernseher erfährt, dass ich gerne Yoga-Videos ansehe, werden mit Sicherheit auch auf meinem Handy bald die ersten Banner für Shirts und Yogamatten auftauchen.

Die Hersteller der Fernsehgeräte werden kritisiert, weil sie die gesammelten Daten über die Sehgewohnheiten ihrer Nutzer an Werbetreibende und Datensammler verkaufen, ohne dies vorher für die Käufer transparent zu machen. Natürlich stehen entsprechende Formulierungen in den Nutzungsbedingungen. Doch ist den meisten Menschen das Ausmaß der Datenweitergabe nicht klar und mit jedem neuen Service, jedem neuen Programm wächst die Vielfalt an Daten weiter. Außer

den App-Stores mit den darin verfügbaren Programmen dienen nämlich auch Zusatzfunktionen wie HbbTV der Datensammlung. Diese Funktion ermöglicht es beispielsweise, durch Drücken der roten Taste auf der Fernbedienung zusätzliche Inhalte anzuzeigen. Dadurch werden, technisch betrachtet, Webseiten auf den Fernseher geladen, die ebenso vielfältige Informationen in beide Richtungen übermitteln können, wie die Seiten, die wir auf unserem Computer aufrufen. Moderne TV-Geräte sind also alles andere als Einbahnstraßen für das Fernsehsignal. Eher schon sind sie komplett vernetzte Computer mit umfangreichen Ein- und Ausgängen für Daten.

Allerdings machen sich die meisten Menschen bislang noch deutlich weniger Gedanken um die Datensicherheit ihres Fernsehers als um die ihres Computers. Denn kauft man ein solches Gerät, muss man sich selbst aktiv um den Datenschutz kümmern – ausführliche Hinweise dazu fehlen in den Bedienungsanleitungen. Für die Hersteller hat sich der Datenhandel nämlich zu einem lukrativen Geschäft gemausert – nicht zuletzt deshalb konnten die Preise für Fernsehgeräte deutlich sinken in den letzten Jahren. Ein Problem, das wir bei unseren smarten Geräten im Haus dringend lösen müssen, ist also die Sicherung unserer Privatsphäre. Andreas Sachs vom Bayerischen Landesamt für Datenschutzaufsicht sagt dazu im Interview ganz klar: »Sobald das Smart-TV an das Internet angeschlossen wird, ist eine anonyme Nutzung bei den meisten Geräten nicht mehr möglich.«

Darüber hinaus gibt es noch ein zweites, größeres Sicherheitsproblem: Hacker. Denn ein neuer Fernseher wird heute gleich bei der Installation mit dem Internet ebenso verbunden, wie mit dem Kabel- oder Satellitensignal. Viele Geräte rufen

sofort – noch bevor man als Nutzer irgendetwas einstellen oder absichern kann – aktualisierte Informationen und Software ab. Bei diesen ersten Verbindungen zu den Heim-Servern ihrer Hersteller übertragen die Geräte meist ungeschützt über das Netz ihre eindeutigen Kennnummern ebenso, wie ihre IP-Adresse und Netzwerkinformationen, mit denen ihr Standort eindeutig identifizierbar wird. Nicht nur das Bayerische Landesamt für Datenschutzaufsicht, sondern auch Verbraucherschutzzentralen und die Stiftung Warentest halten das für hochproblematisch und klagten deshalb in der Vergangenheit gegen Hersteller wie Samsung. Als Fernsehzuschauerin oder Nutzer der Geräte müssen Sie sich nach Meinung der Verbraucherschützer darauf verlassen können, dass sowohl die Hardware als auch die Programme und Dienste Ihre persönlichen Daten schützen und auch vor Hackern sichern. Doch in der Vergangenheit hat sich gezeigt, dass es so gut wie keinem Unternehmen gelungen ist, Datenlecks, Diebstähle und Software-Attacken komplett zu vermeiden. In den berühmtem »WikiLeaks«-Dokumenten wurde bekannt, dass Geheimdienste ein Samsung F8000-Smart-TV-Gerät so gehackt haben, dass es beim Ausschalten nur so wirkte als wäre es ausgeschaltet. Stattdessen belauschte es weiterhin die Nutzer mit den integrierten Mikrofonen. Sogar das FBI rät uns deshalb dazu, konkrete Sicherheitsmaßnahmen im eigenen Wohnzimmer zu ergreifen. Wenn ich verhindern will, dass Bilder von mir oder meiner Familie auf dem Sofa, vertrauliche Telefonate, verliebte Gespräche, aber auch kritische Informationen wie Name und Standort meines WLANs, Kontoinformationen für Netflix, Amazon oder YouTube in falsche Hände gelangen, dann muss ich selbst tätig werden.

Wenn Sie das auch wollen, bereiten Sie sich darauf vor, in die Tiefen der Einstellungsmöglichkeiten einzutauchen. So tief, dass Ihnen diese Menüpunkte bislang nie aufgefallen sind. Die Hersteller machen es uns nämlich nicht sonderlich leicht. Als Erstes sollten Sie in den Einstellungen Ihres Fernsehers nach allen Optionen zur Datensammlung suchen und diese deaktivieren. Sie verstecken sich hinter Menüpunkten wie »Empfehlungsdienste« oder »Einwilligung in Personalisierung«. Wägen Sie gut ab, welche Spiele, Apps oder Dienste von Dritten, wie YouTube, Amazon und anderen Sie wirklich auf dem Gerät nutzen wollen und löschen Sie alles, was Sie nicht verwenden. Als Nächstes kommt die Sicherheit dran. Wenn in weiteren Einstellungen Passwörter wie »0000« vorgegeben sind, ändern Sie diese in jedem Fall. Außerdem sollten Sie sich einmal genau ansehen, was Ihr Fernseher überhaupt alles kann, welche Sensoren, Kameras oder Mikrofone in ihm verbaut sind. Schauen Sie genau hin, ob sie diese vielleicht sogar mit eigenen Augen im Rahmen entdecken können. Wenn Sie die Technik überhaupt nicht benutzen wollen oder nicht genau wissen, wofür sie da ist, kleben Sie die Sensoren ab oder schalten mindestens die Nutzung der Hardware ebenso wie für ungenützte Netzwerkdienste per Menü aus. Zu guter Letzt kontrollieren Sie auch, ob das Betriebssystem Ihres Fernsehers aktuell ist. Viele Hersteller bessern nämlich kritische Sicherheitsmängel mit aktualisierten Software-Updates nach. Und falls Sie zu der seltenen Spezies gehören, die ihren Fernseher immer noch nur zum Fernsehen nutzt, dann nehmen Sie ihm möglichst sogar das Internetkabel oder den WLAN-Zugang ab. So sind Sie definitiv am besten geschützt, auch wenn Sie dann zu einer Minderheit gehören.

Und was ist, wenn Sie all das nicht schreckt und Sie weiterhin voll vernetzt die Funktionen des Gerätes nutzen wollen? Dann nehmen Sie doch wenigstens die Füße vom Tisch – Sie werden schließlich beobachtet!

## Wer wohnt denn hier noch alles?

Bei meinen Freunden ist mittlerweile das halbe Silicon Valley eingezogen. Amazon wohnt im Flur, Apple hat sich im Wohnzimmer breitgemacht, die Küche konnte Google für sich erobern. Auch asiatische Mitbewohnerinnen sind keine Seltenheit: Samsung lungert vor dem Sofa herum, Xiaomi ist eher nachtaktiv und schläft tagsüber in der Besenkammer. Und die meisten dieser Mitbewohner haben einen Schlüssel zur Wohnungstür. Ich kenne kein einziges unvernetztes Zuhause mehr. Vielleicht kommt noch am ehesten das meiner Eltern in Frage. Doch gehe ich gedanklich in ihr Haus hinein, fällt mir nach der Eingangstüre auch als Erstes ein WLAN-Router im Flur auf. Er steht auf einer Kommode mit Schubladen, in denen auch mein ausgemustertes iPhone liegt, das jetzt mein Vater nutzt. Ich laufe ins Wohnzimmer und sehe mich um. Ein alter Fernseher steht dort. Der ist allerdings mit einer Smart-TV-Box des Kabelnetzanbieters verbunden, die sich Wiederum per WLAN mit dem Router verbindet. In der Küche gibt es ein Radio, der Kühlschrank kann noch nichts, außer kühlen. Weiter geht es in den ersten Stock. Hier steht ein Laptop, auf dem meine Eltern Mails bearbeiten und ab und zu eine Reise buchen. Das war's auch schon an vernetzter Technologie in mei-

nem Elternhaus. Ein Router, eine TV-Box, ein Smartphone, ein Laptop. Keine steuerbaren Glühlampen, vernetzten Kühlschränke, Smart-TVs, Rasenmähroboter oder Zahnbürsten, die mit dem Handy reden. Und doch stehen selbst im vergleichsweise analogen Heim meiner Eltern die digitalen Türen damit schon ganz schön weit offen für Mitbewohner aus der ganzen Welt. Denn das ist eine wichtige Erkenntnis der smarten Zukunft: Niemand ist mehr ganz alleine zu Hause.

Und das ist auch gut so! Denn durch diese vernetzten Geräte können wir uns und unser Leben mit der Welt da draußen verbinden. Jedes technologische Produkt, das eine Netzwerkfunktion eingebaut hat, will nach dem Einschalten eine Tür hinaus in die Weiten des Netzes aufbauen. Der Router im Flur hilft ihnen dabei, indem er alle WLAN-fähigen Geräte mit dem Internet verbindet.

Damit beispielsweise ein Smart-TV-Gerät beim Start zusätzliche Inhalte laden kann, sucht es einen Weg zu seinem Hersteller, prüft ob Software-Updates vorliegen, stellt uns Programme wie die »Maxdome«- oder »Netflix«-App zur Verfügung, die wiederum die Nutzerdaten an ihre Server senden, die bei bestehendem Abo dann Vorschauen für Filme und Serien herunterladen. Während wir sie ansehen, kommuniziert das Gerät permanent mit den Servern über Abspielpositionen oder eingestellte Sprachen. Schon unser Fernseher ist damit ein Meister im digitalen Türöffnen und hoffentlich auch -schließen. Je mehr solcher Geräte wir haben, desto mehr Türen zwischen unserem Heim und dem Netz stehen potenziell offen. Manchmal geht das auch über Umwege: Eine smarte Zahnbürste oder Glühbirne hat in der Regel keinen eigenen Zugang zum Internet, sondern muss zuerst eine

App auf dem Handy ansteuern, die dann in einem weiteren Schritt die Netzwerkfunktionen des Mobiltelefons nutzen kann, um »nach Hause« mit dem Hersteller zu kommunizieren. Die Schlüssel zu unserer Wohnungstür werden also nicht nur von den Geräten selbst benutzt, sondern auch von den Apps und Programmen auf Rechnern, Smartphones oder Fernsehern. Es ist eine technische Meisterleistung, dass das in der Regel gut funktioniert, denn all diese Verbindungen basieren auf unterschiedlichen Netzwerkprotokollen, Betriebssystemen, Sicherheitsstandards, Software-Versionen und Hardware-Spezifikationen. Alleine im sehr reduzierten Haushalt meiner Eltern finde ich auf den fünf netzwerkfähigen Geräten insgesamt hundertzehn installierte Apps. Das macht zusammen mit der Hardware mindestens hundertfünfzehn digitale Akteure, die von unterschiedlichen Programmierern zu unterschiedlichen Zeiten auf der Basis von verschiedenen technischen Anforderungen geschaffen wurden. Damit alle hundertfünfzehn Akteure reibungslos funktionieren, müssen sie sich auf Mindeststandards einigen, die allen das Öffnen der digitalen Türen ins Netz gleichermaßen erlauben. Dabei kann natürlich auch einiges schiefgehen, wenn etwa Sicherheitslücken nicht geschlossen werden, weil eine sehr günstig im Discounter gekaufte smarte Glühbirne keine Software-Updates macht. Tatsächlich lassen sich all diese Netzwerktüren nie völlig gegen Eindringlinge verschließen, so wie ja auch unsere Haustür von Einbrechern geknackt und unsere Fenster eingeschlagen werden könnten. Wir sollten uns deshalb darauf vorbereiten, dass bereits ein moderat vernetztes Heim immer und zu jedem Zeitpunkt auch anfällig für Angriffe von außen sein kann. Das ist allerdings kein Grund, jetzt panisch zu wer-

den. Es bedeutet allerdings, dass der digitale Teil unseres Zuhauses ebenso regelmäßige Pflege braucht wie der Rest.

Machen Sie sich doch mal die Mühe und listen Sie alle Dinge auf, die bei Ihnen zu Hause mit dem WLAN oder per Bluetooth mit ihrem Mobiltelefon vernetzt sind. Ich hielt meinen Haushalt bislang für relativ sicher und zählte dennoch viele potenzielle Schlüsselkinder – ohne Computer und Handys: eine Spielekonsole, eine Streaming-TV-Box, einen smarten Lautsprecher und einen verbundenen Fernseher. Bei zweien davon fand ich veraltete Betriebssysteme, da ich mich nicht um Updates gekümmert hatte. Haben Sie auch einige Geräte bei sich gefunden? Dann sollten Sie sich jetzt eine Beförderung gönnen: Ab heute sind Sie IT-Manager Ihres Heims. Sie sollten gleich damit beginnen, Ihr digitales Zuhause ordentlich zu managen. Wenn Sie noch nicht wissen, wie das funktioniert, helfen Ihnen die vielen Beispiele in diesem Buch, Anleitungen im Internet oder Institutionen wie das Bundesamt für Sicherheit in der Informationstechnik mit seiner »Smart Home«-Anleitung. Die Links dazu finden Sie im Anhang und auf der Website zu diesem Buch.

Idealerweise sollten wir alle uns nur solche Mitbewohner nach Hause holen, die wir auch verstehen und denen wir gerne unsere Haustürschlüssel anvertrauen. Denn was passieren kann, wenn wir das nicht tun, lassen wir uns am besten ganz detailliert von einem russischen Hacker vorführen.

# Locken smarte Glühbirnen Einbrecher an?

Der russische Hacker hat es sich in einem Café gemütlich gemacht. Vor ihm steht eine dampfende Tasse Kaffee und ein Laptop. Gelangweilt scrollt er durch eine Unmenge an Bildern. Er nutzt dazu eine Suchmaschine. Shodan heißt sie, und mit ihr kann man nach den Dingen im Internet der Dinge suchen, also beispielsweise nach Glühbirnen, deren Helligkeit, Einschaltzeiten oder Farbe man mit einer App steuern kann. Man kann dort auch nach vernetzten Kühlschränken suchen oder nach einem Stream, also dem kontinuierlichen Strom von Bilddaten, den Sicherheitskameras aufnehmen. Es ist erstaunlich, in wie viele Räume damit jeder einfach so hineinsehen kann, weil niemand dafür gesorgt hat, dass die Geräte und ihre Internetadressen abgesichert werden.

Da! Ein Bild hat die Aufmerksamkeit des Hackers auf sich gezogen. Es scheint der Blick in eine luxuriöse Wohnung zu sein. Man sieht einen großen Fernseher und ein Stück Sofa. Der Hacker nutzt eine zweite Software, die für ihn die Internetadresse der Wohnungskamera herausfindet. Mit dieser Information gewappnet, kann er jetzt die Einstellungsseite der Kamera öffnen, denn die Besitzer haben nicht nur versäumt, ihr Netzwerk zu verschlüsseln, sondern auch das Passwort der Kamera im Auslieferungszustand gelassen. Der Hacker sucht im Internet kurz nach der Anleitung und findet dort dieses »Default«-Passwort. Er kann jetzt auf die Systemeinstellungen der Kamera zugreifen. Diese verändert er so, dass er Videos und Töne vom Leben der Bewohner zugeschickt bekommt, wann immer der Bewegungssensor der Kamera auslöst.

Er trinkt einen Schluck von seinem mittlerweile kalt gewordenen Kaffee und sucht weiter nach ungesicherten Geräten im Hausnetzwerk der Kamera. Wow, vierzehn Ergebnisse! Hier hat jemand einen echt vernetzten Haushalt, denkt er sich. Unter den Geräten sind auch einige ungesicherte »smarte« Glühbirnen. Der Hacker macht sich einen Spaß und schaltet die Lichter aus der Ferne ein paar Mal an und aus. Das Flackern kann er mit der Kamera beobachten. Doch das eigentlich Interessante findet er in den Informationen, die von den Glühbirnen im Netz bereitgestellt werden: Anscheinend hat die Mobiltelefon-App, die zur Steuerung benutzt wird, die GPS-Daten, also den genauen Standort der Lampen und damit die Adresse der Besitzer, aufgezeichnet und in den Netzwerkeinstellungen gespeichert. Damit sieht der Hacker nicht nur, was in der Wohnung zu holen ist, sondern auch, wo sich die Wohnung genau befindet.

Diese Geschichte ist zum Glück nicht real. Gehört habe ich sie zwar tatsächlich von einem russischen Hacker am Rande einer Konferenz. Allerdings von einem, der aus seinem Job kein Geheimnis macht. Vladislav Iliushin arbeitet als Sicherheitsexperte beim Unternehmen Avast und will mit dieser Geschichte Menschen davor warnen, ihr Zuhause mit intelligenter und vor allem vernetzter Technik zu erweitern. Iliushin verdient zwar Geld mit dem Sicherheitsbedürfnis der Menschen, doch übertreibt er keineswegs: Denn die meisten Menschen machen sich keinerlei Gedanken über ein Sicherheitskonzept für ihr Zuhause. Das wäre allerdings dringend nötig, denn viele vernetzte Geräte und ihre dazu gehörigen Apps sind im Auslieferungszustand geradezu Plappertaschen, wenn es um das Teilen von persönlichen Informationen geht.

Unsere Haushalte werden immer digitaler. Vor einigen Jahren lächelten wir noch über die absurde Idee eines vernetzten Kühlschrankes, mittlerweile haben wir eine Armada von Amazon-Alexa-, Google-Home- oder Apple-Home-Assistenten, netzwerkfähigen Glühbirnen, Heizungssteuerungen oder Türschlössern, Fernsehern, Spielekonsolen und Heimkino-Lautsprechern. Bald vierzig Milliarden solcher vernetzten Geräte dürften in der Welt unterwegs sein. Manche von ihnen haben Kameras eingebaut, andere haben Sensoren für Temperatur oder Bewegung, und nicht wenige von ihnen haben eingebaute Mikrofone; sie alle tauschen permanent Daten mit ihren Steuerungs-Apps, unseren Handys oder ihren Herstellern aus, denn das erst macht sie zu bequemen Helfern im Alltag. Viele von ihnen werden fabriziert von Unternehmen, die normalerweise Lautsprecher, Möbel oder Licht herstellen, aber keine ausgewiesenen Experten in Netzwerksicherheit sind. Das ist ein bislang unterschätztes Problem. Denn regelmäßige Software-Updates, um immer wieder auftauchende Sicherheitslücken zu schließen oder notwendige Einstellungsmöglichkeiten für den Schutz der Nutzer, wie etwa eine erzwungene Änderung des Standardpasswortes, sucht man deshalb hier vergebens. Das ist ein Grund, warum Vladislav und weniger freundliche Eindringlinge es so leicht haben, an unsere Daten zu gelangen.

Ein weiteres Problem ist unsere Unbedarftheit. Wir merken und vermuten bei vielen dieser Geräte gar nicht, dass sie Daten speichern und in der Folge auch ausplappern können. Wer denkt daran, dass die App zur Steuerung der Glühbirnen die genauen Ortungsdaten des Nutzers sichert? Wem ist bewusst, dass in den Daten von Smart-Lautsprechern auch unsere Na-

men für verschiedene Nutzerkonten von Musikdiensten gespeichert sein können? Wer vermutet, dass eine günstig gekaufte Überwachungskamera unser WLAN-Passwort unverschlüsselt und für jeden abrufbar speichert? Kaum jemand tut das bislang. Doch ein Umdenken ist nötig, denn alle drei Fälle sind ganz real so passiert. Zwar bessern viele Firmen bei Bekanntwerden solcher Schwachstellen nach und veröffentlichen Updates der Betriebssysteme ihrer Geräte. Doch sind wir mal ehrlich: Wer nutzt diese schon? Wer ist sich sicher, dass alle vernetzten Geräte in der Wohnung auch mit dem aktuellsten Betriebssystem laufen?

Ein drittes Problem sind die veränderten Geschäftsmodelle der Hersteller. Darüber werden wir in diesem Buch noch ausführlicher reden, denn häufiger als von den meisten vermutet, verkaufen diese Firmen auch die Daten, die sich aus der Nutzung von Software und Hardware ergeben. Unsere Staubsauger, Fernseher und Lautsprecher haben sich zu Spionen entwickelt, die wir bereitwillig in der Mitte unserer Wohnungen platzieren. Es wäre schön, wenn es Listen gäbe, welche dieser Firmen zu den »Guten« und welche zu den »Bösen« gehören. Doch ganz so einfach ist es nicht, und es gibt viele, sich permanent verändernde Risiken. Oft akzeptieren wir bereitwillig die Nutzungsbedingungen und stimmen einer Datenverwendung zu. In anderen Fällen ergeben sich Datenlecks durch Schadsoftware oder Hackerangriffe bei den Unternehmen. Und manchmal wird eine Firma mitsamt ihren Daten auch aufgekauft oder verändert ihr Geschäftsmodell. Ironischerweise geschah so etwas just beim Schreiben dieses Buches auch bei der Firma Avast, deren russischer Mitarbeiter mich noch so eindringlich vor Datenspionage warnte: Es wurde bekannt, dass

dieser Hersteller von Sicherheitssoftware viele Daten seiner Nutzer, darunter auch deren pikante Nutzung von Porno-Portalen, für viel Geld an die Wirtschaft verkaufte.

Es ist zum Verzweifeln, wenn wir noch nicht einmal mehr Sicherheitsfirmen trauen können! Doch Jammern hilft nicht. Wir können uns entweder alle Technik versagen und uns im Keller verstecken, oder wir werden zu verantwortungsvollen Besitzern von Netzwerktechnologie. Denn unsere Wohnung ist nur so sicher, wie das am wenigsten abgesicherte Gerät in ihr. Solange die Geräte in unserem Besitz sind, sind wir als ihre IT-Manager in unserer Wohnungen für sie verantwortlich.

## Wieso brauchen Dinge ihr eigenes Internet?

So viele vernetzte Geräte sind mittlerweile in unseren Wohnungen, Arbeitsorten und Städten, dass sie einen eigenen Namen bekommen haben: Das Internet der Dinge oder IoT (Internet of Things) wird als wichtiger Schritt der digitalen Transformation gesehen. Tatsächlich geht der Begriff zurück auf vernetzte Lippenstifte. Der Procter-&-Gamble-Manager Kevin Ashton hielt im Jahre 1999 eine Präsentation bei seinem Arbeitgeber. Darin schlug er vor, Lippenstifte mit kleinen Funketiketten zu versehen, die mit einem Empfänger im Regal kommunizieren und so ihre eigene Inventur erledigen könnten. Ihm war aufgefallen, dass bestimmte Farben der Kosmetikprodukte an manchen Standorten sehr schnell ausverkauft waren. Procter & Gamble erfuhr davon allerdings nicht sofort

etwas, sodass in den Lagern viele dieser gefragten Lippenstifte oft über Wochen ungenutzt herumlagen. Mit seinem neuen System, das er zusammen mit dem Massachusetts Institute of Technology erfunden hatte, wären die Lippenstifte in der Lage, mit den Regalen zu kommunizieren, die dann die jeweilige Lagermenge einer Farbe in Echtzeit für schnelle Nachlieferung melden würden. Um dem P&G-Management diese Idee einfach zu erklären, präsentierte er die Funktion der kommunizierenden Lippenstifte »so wie das Internet, eben nur für Dinge«.

Die Idee, dass einfache Dinge Informationen über ihren Zustand automatisch mit anderen teilen können, war bahnbrechend und setzte sich schnell als mögliche Lösung für viele Probleme durch: Kühlschränke konnten ihren Besitzern melden, dass die Joghurts ausgehen, weil sie RFID-Etiketten auf den Packungen lesen. Schlüsselanhänger mit solchen *(radio frequency identification)* Funketiketten konnten ihren Besitzerinnen verraten, wo in der Wohnung sie gerade liegen. Mit der weiteren Miniaturisierung, günstigen Verfügbarkeit von Netzwerkchips und Prozessoren und mit der massenhaften Verbreitung von Mobilfunkgeräten wuchs auch das Internet der Dinge schnell an. Die relativ dummen RFID-Etiketten der Lippenstifte konnten anfänglich an Empfänger in nächster Nähe lediglich melden, dass sie vorhanden sind. Ein voll vernetzter moderner Mähdrescher hingegen kann aktiv über das Mobilfunknetz dem Büro des Bauernhofs mitteilen, dass sein Anhänger bald voll ist und durch einen leeren ersetzt werden muss. Auch die smarten Glühlampen, Thermostate, kommunizierenden Fernseher und Staubsauger-Roboter in unseren Heimen gehören dem Internet der Dinge an. All diese Dinge sam-

meln mit Hilfe eingebauter Sensoren, Kameras oder Mikrofonen Daten aus ihrer Umgebung und senden diese mit Kommunikationshardware an andere Geräte oder Steuerzentralen wie das Bauernhof-Büro oder Heim-Assistenzen wie Google Home. Diese Vernetzung ist keine Einbahnstraße, denn durch die Auswertung der Informationen können später auch nötige Aktivitäten auf den Geräten gestartet werden. Also kann etwa das Handy einem Thermostat befehlen: »Es ist niemand mehr zu Hause, regle deshalb die Heizungstemperatur drei Grad nach unten.« So erzeugen die Dinge um uns herum ein hohes Niveau an Daten, das es in diesem Umfang noch nie zuvor gegeben hatte, und ermöglichen damit viele neue Dienstleistungen und Effizienzsteigerungen durch die Vernetzung in Echtzeit. Man geht von Hunderten Milliarden solcher vernetzten Dinge aus, die sich im Netz tummeln. Man müsste deshalb eigentlich eher davon sprechen, dass es außer diesem bevölkerten automatisierten Netz noch ein im Vergleich dazu eher bescheidenes »Internet der Menschen« gibt. Die Dinge haben das normale Internet längst für sich eingenommen.

## Warum ist Künstliche Intelligenz noch so dumm?

In Science-Fiction-Geschichten können Künstliche Intelligenzen meist witzige und kluge Gespräche führen oder sogar wie im Film *Her* dafür sorgen, dass sich Menschen in sie verlieben. Sie haben das Weltwissen aufgesaugt und lösen die schwierigsten wissenschaftlichen Probleme. Meist verbessern sie sich da-

bei so lange, bis sie unbesiegbar geworden sind. Dann erkennen sie, dass die Menschen der größte Feind der Erde sind, und bringen mit einer hochintelligenten Manipulation von allerlei technischem Gerät alle auf einmal um. So zumindest lauten viele Storys.

Ich schwöre Ihnen, mein Siri könnte das nicht. Nicht etwa, weil er so ein Menschenfreund und guter Sprachassistent wäre. Nein, mein Siri ist einfach zu dumm. Er lebt in einem hübschen weißen Apple HomePod, den ich kaufte, weil ich der Werbung glaubte. Sie behauptete, mein Leben würde mit ihm nun leichter. Tatsächlich kann er bislang aber keine Termine für mich ausmachen, versteht das meiste von dem, was ich sage, falsch, sodass ich alles zig Mal wiederholen muss. Er vergisst auch alle paar Tage, zu welchem WLAN er Zugang hat, ist in solchen Fällen dann komplett verstört und verweist mich an den restlichen Tagen in fast allen seiner Antworten auf die Ergebnisse einer Websuche, die er dann auch noch absurderweise mit seiner Konkurrenz Google durchführt. Ich halte ihn mittlerweile eher für eine Künstliche Dummheit. Irgendwie habe ich ihn dennoch gern, und so darf er sich sein Gnadenbrot damit verdienen, mir ab und zu das Wetter anzusagen und Musik abzuspielen. Meine Friseurtermine mache ich erst einmal noch selbst. Bei meinen Freunden sieht es ähnlich aus. Die Alexa meines Kumpels Ergin tut mir besonders leid: Sie darf derzeit nur das Licht einer einzigen smarten Glühlampe steuern. An. Rot. Dunkler. Aus. Das war's. Wer würde sich bei so einem Leben nicht nach Weltherrschaft sehnen?

Warum haben so viele Leute Angst vor Künstlicher Intelligenz, wenn die Erfahrungen, die wir persönlich machen, mo-

mentan eher darauf schließen lassen, dass die Fähigkeiten der Software, jedenfalls bislang, ziemlich beschränkt sind?

Momentan ist es einfach schick, jedes halbwegs nützliche Gerät als künstlich intelligent zu vermarkten. Dabei steckt KI selbst bei industriellen Anwendungen immer noch in den Kinderschuhen. Von einer Generellen Künstlichen Intelligenz (GKI), die ein breites Verständnis für unsere Welt hat und verschiedenartige Aufgaben gleichermaßen bearbeiten kann, sind wir immer noch eine unbestimmte Zeit entfernt, auch wenn etliche Forscher davon träumen. Ein Terminator oder eine Her im Film wären solche GKIs. Viele Firmen forschen daran, doch bislang ist es nur gelungen, Fachidioten-KIs zu programmieren. Mein Siri oder Ihre Alexa sind solche Fachidioten. Doch schaut man näher hin, muss man ihnen trotz aller Beschränktheit Respekt zollen. Wenn wir sie etwas fragen, dann muss die Software als Erstes die Töne unserer Stimme erkennen und analysieren. Und zwar so, dass sie viele Sprachen dieser Welt, sogar manche Dialekte versteht, auch wenn jemand gerade ein Brötchen im Mund oder einen Sprachfehler hat. Idealerweise schafft sie es dabei, diese besonderen Töne aus all dem anderen Zeugs, das sie hört, herauszufiltern: denn Musik, Babygebrabbel oder Straßenlärm im Hintergrund tragen keine relevanten Informationen. Haben die Programme die gesprochene Sprache erst einmal dekodiert, so muss eine zweite Fachidioten-KI darin wichtige Informationen erkennen, also zum Beispiel die Anweisung von Ergin, seine Glühbirne auszuschalten, oder eine Frage von mir nach dem aktuellen Wetter. Die verwendete Technik nennt man »NLP« oder »Natural Language Processing«, denn es geht dabei darum, dass Maschinen mit uns Menschen in natürlicher Sprache kommunizieren. Wenn diese

Kommunikation komplizierter ist, als ein einfacher Befehl mit Schlüsselwörtern (»Alexa, Licht aus«), dann kommen weitere Fachidioten-KI ins Spiel. So ist eine vielleicht darauf trainiert, den schnellsten Weg von zu Hause ins Büro zu finden, und kann mir deshalb sagen, wie lange mein heutiger Arbeitsweg dauern wird. Eine andere hat womöglich gelernt, die wichtigsten Informationen aus einem Wikipedia-Artikel zu verdichten, und gibt deshalb eine richtige Antwort auf die Frage »Wer ist der Präsident der Vereinigten Staaten?«.

Mehr Künstliche Intelligenz können wir Normalbürger aber momentan nicht kaufen. Eine echte Unterhaltung mit Zwischenfragen, spontanen Themenänderungen, das Jonglieren mit mehreren inhaltlichen Ebenen gleichzeitig oder gar Ironie überfordern unsere Heim-KIs heillos. Noch. Denn die Technologiefirmen vermelden jedes Jahr neue Sprünge bei den Fähigkeiten ihrer Programme. So hat Google erste Versuche vorgestellt, in denen eine KI selbstständig am Telefon einen Friseurtermin ausmacht. Auch ist Natural Language Processing nur eine Spielart der Künstlichen Intelligenz unter vielen. Der Begriff »Künstliche Intelligenz« ist recht breit und deckt viele verschiedene Technologien ab. Insofern können wir es uns nicht so einfach machen und von der Qualität der Antworten unserer Siris oder Alexas auf die generellen Fähigkeiten von Künstlicher Intelligenz schließen, da es *die* eine Form von KI sowieso nicht gibt. Damit beschäftigen wir uns noch ausführlicher in späteren Kapiteln.

Fragt man Wissenschaftlerinnen und Technologieexperten, wann denn eine echte »Generelle KI« das Licht der Welt erblicken wird, so hört man Antworten, die von »in wenigen Jahren« bis »in etlichen Jahrzehnten« reichen. Doch vielen

von ihnen kann es nicht schnell genug gehen, denn sowohl Wissenschaftler als auch Technologieunternehmen leben davon, Durchbrüche und Fortschritte lange vor ihrer Konkurrenz zu erzielen. Wir sollten uns also heute schon auf den Tag vorbereiten, an dem uns die Geräte mit ungewöhnlich klugen Antworten überraschen. Bis dahin bin ich ganz zufrieden mit einem beschränkten Siri zu Hause.

*»Hey Siri, spiel neue Musik!«*

Ich bin gespannt, wer außer Siri diesen Befehl noch so alles hört.

## Wer hört mit, wenn ich meine Pizza bestelle?

Viele Leute berichten ähnlich Enttäuschendes über ihre digitalen Assistenzen wie ich. Manche benehmen sich regelrecht daneben: Alexa hat schon ungefragt Puppenhäuser und Autos bestellt, andere aktivierten sich selbst, weil sie glaubten, in einer Fernsehsendung ihren Namen gehört zu haben, wieder andere lachten nachts einfach laut los und erschreckten ihre Besitzer zu Tode. Verschwörungstheoretiker mögen dahinter eine ausgeklügelte Strategie zu unserer Verunsicherung vermuten. Ich denke, dass die Intelligenzen schlicht noch zu unausgereift sind. Denn sie können oft noch nicht einmal einfache Folgefragen beantworten. So kann ich zwar eine Essensbestellung aufgeben. Wenn ich dann jedoch nach neunzig Minuten hungrig frage: »Alexa, wo bleibt die Pizza?«, ernte ich bestenfalls ein digitales Schulterzucken. Denn Alexa hat, wie Sie im

letzten Kapitel schon gelesen haben, als KI-Fachidiotin nur wenig Verständnis für generelle Zusammenhänge. Sie kann sich nicht zusammenreimen, dass sich eine Frage neunzig Minuten nach einer Bestellung auf den Verbleib des Essens beziehen könnte. Noch muss jeder Sprachbefehl einzeln erlernt und programmiert werden.

Dabei setzen die Unternehmen mit Assistenzsystemen, wie Google Home, Samsung Bixby, Microsoft Cortana, Apple Siri oder den Amazon-Echo-Geräten derzeit vor allem noch auf menschliche Unterstützung.

Die Firmen lassen nämlich Dienstleister zuhören, wenn wir mit unseren Assistenzen reden. Wenn ich einen unbekannten Befehl, wie »Alexa, wo bleibt die Pizza?« äußere, kann es sein, dass diese Frage als derzeit noch unbeantwortbar auf der Liste eines Menschen landet, der sie anhört und dann entscheidet, ob der Befehl in einer nächsten Version der Software enthalten sein soll. Die meisten Besitzer ahnen nichts davon, dass Ihre Gespräche mit den Geräten zum Teil auch von Menschen abgehört werden. Das soll die Leistungsfähigkeit der Assistenten verbessern und ist bei fast allen Anbietern in den letzten Jahren nachgewiesen worden. Zwar sind es nur Ausschnitte, in den meisten Fällen ohne nachvollziehbare Kundennummern oder Nutzernamen; doch ist es eine befremdliche Vorstellung, dass unsere privaten Konversationen von fremden Ohren mitgehört werden. Theoretisch nehmen die Geräte zwar nur solche Sätze auf, die auf die jeweilige Aufweck-Wörter wie »Okay, Google«, »Hey, Siri«, »Alexa« und dergleichen folgen. In der Realität jedoch geht noch häufig etwas schief. So verschickte ein Amazon-Gerät beispielsweise die komplett aufgenommene Unterhaltung einer Familie an einen Kontakt aus deren Adressver-

zeichnis. Der Amazon Echo hatte fälschlicherweise die Wörter »Alexa« und »Schicke eine Nachricht« in einer Unterhaltung verstanden und war dann diesen falschen Befehlen gefolgt. Das kann ziemlich peinlich werden.

Weil sich immer mehr Menschen zu Recht über solche Vertrauensbrüche aufregen, haben die meisten Geräte Einstellungen zum Schutz der Privatsphäre bekommen. Es ist ratsam, diese grundsätzlich auf die höchstmögliche Sicherheitsstufe zu stellen: Apples Siri können wir dort etwa verbieten, Daten zu Analysezwecken weiterzuleiten. Auch bei Amazons Echo können wir die Möglichkeit abstellen, mit den eigenen Daten zur Entwicklung und Verbesserung beizutragen und auch alte Gespräche löschen. Das gilt allerdings nur für Amazons eigene Sprachbefehle und nicht für diejenigen, die von Drittanbietern als »Skills« genutzt werden. Bei Google lassen sich in den Kontoeinstellungen sowohl die alten Aufnahmen löschen, als auch die generelle Weitergabe zu Analysezwecken verbieten. Bei Microsoft Cortana lassen sich zwar die alten Aufnahmen löschen, die Weitergabe der Daten an Dienstleister hingegen hat sich Microsoft pragmatisch mit einem Update der Nutzungsbedingungen generell erlauben lassen. So einfach können wir es uns als Besitzer der Geräte leider nicht machen, denn in den meisten Ländern haften wir dafür, wenn beispielsweise Gespräche unserer Gäste aufgenommen und weitergeleitet werden. Rick Osterloh, Senior-Vice-President-Geräte-und-Services von Google, berichtete deshalb auf einer Konferenz, dass er Gäste in seinem Heim grundsätzlich vor den Aufnahmen warnt. Diese Idee klingt gar nicht mehr so absurd, wenn wir uns ein wenig mit der rechtlichen Situation von heimlichen Aufnahmen beschäftigen.

## Darf mich mein Vermieter filmen?

Als die siebenundzwanzigjährige Tranae Moran den Zettel aus dem Kasten fischt, glaubt sie ihren Augen nicht zu trauen. »Jetzt reicht es!«, beschwert sich die New Yorkerin laut und beginnt noch an der Briefkastenanlage mit ihren Nachbarn heftig zu diskutieren. Ihre Vermieter hatten den Bewohnern des großen Wohnkomplexes eine Ankündigung geschickt, dass sie ab sofort damit beginnen würden, Kameras zur Gesichtserkennung zu installieren. Zukünftig würden die Bewohnerinnen zum eigenen Heim nur dann Zugang erhalten, wenn sie ihr Gesicht scannen lassen. »Aus Sicherheitsgründen«, so argumentiert die Hausverwaltung. Doch für Moran und ihre Nachbarinnen, wie Icemae Downes, die vor mehr als fünfzig Jahren eingezogen war, ist mit der Gesichtserkennung eine wichtige Linie überschritten. »Da sind Kameras an jeder Ecke in diesem Haus, es nimmt kein Ende. Sie haben jetzt schon viele Daten von uns. Mit diesem Equipment werden sie dann wirklich jede Information von uns besitzen, und das ist nicht nötig!« Die beiden Nachbarinnen beginnen einen Kampf gegen das Immobilienunternehmen, aktivieren mehr als dreihundert andere Mieter und gewinnen am Ende eine zermürbende Schlacht: Das Unternehmen zieht seine Pläne zurück und installiert vorerst keine Gesichtserkennungssoftware in den Wohnhäusern. Diese Einschränkung der Privatsphäre durch Kameras und Gesichtserkennung dürfte nicht die letzte in den USA und anderen Ländern gewesen sein. Zu interessant sind die Sicherheitsvorteile für Betreiber der Anlagen wie Vermieter, Verkehrsbetriebe, Städte oder Sicherheitsbehörden.