BARBARA WIMMER

HILFE ICH HABE MEINE PRIVATSPHÄRE AUFGEGEBEN!

WIE UNS SPIELZEUG, APPS, SPRACHASSISTENTEN UND SMART HOMES ÜBERWACHEN UND UNSERE SICHERHEIT GEFÄHRDEN

Hilfe, ich habe meine Privatsphäre aufgegeben!

Barbara Wimmer

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-7475-0165-8
1. Auflage 2021

www.mitp.de
E-Mail: mitp-verlag@sigloch.de
Telefon: +49 7953 / 7189 - 079
Telefax: +49 7953 / 7189 - 082

Lektorat: Janina Bahlmann
Sprachkorrektorat: Petra Heubach-Erdmann
Covergestaltung: Sandrina Dralle, Christian Kalkert
Satz: III-satz, www.drei-satz.de

INHALT

VORWORT

Begonnen hat alles mit einem Kühlschrank, der die Milch nachbestellen sollte, wenn sie aus ist. Das war eine ganze Zeit lang die erste Version eines vernetzten Geräts, das die Masse erreicht hat. Auf Technik-Messen geisterte bereits vor Jahrzehnten ein Prototyp eines solchen Geräts herum. Jedes Jahr kamen weitere Geräte von anderen Herstellern hinzu und plötzlich gab es den ersten vernetzten Kühlschrank tatsächlich.

Im Jahr 2015 traf ich das lokale CERT.at-Team, das Computer Emergency Response Team Austria, zum Pressegespräch und sie erzählten mir von dem ersten vernetzten Kühlschrank, der Spam-E-Mail-Nachrichten verschickte, anstatt Milch zu bestellen. Die Internet-Verbindung des Kühlschranks war so unsicher, dass er Teil eines sogenannten Botnets geworden war. Sein Besitzer wusste freilich nichts davon, hat er doch den Kühlschrank nur genau einmal mit dem Heim-WLAN verbunden und sich danach nie wieder darum gekümmert. Während sein Kühlschank also Spam-E-Mails verschickte, wunderte ich mich darüber, was wohl mit all den anderen vernetzten Dingen passieren würde, die es auf dieser Welt geben würde. Denn zu dem Zeitpunkt war mir als Technologie-Journalistin bereits klar, dass es nicht bei einem vernetzten Kühlschrank bleiben würde.

Tatsächlich folgten bald jede Menge anderer Gegenstände – und überholten die Vision des Kühlschranks, der zwar nach wie vor ein beliebtes Gadget auf Messen blieb, aber kaum Einzug in Privathaushalte hielt. Im Juli 2020 fragte ich meine Twitter-Follower, wer von ihnen einen vernetzten Kühl-

schrank hat oder jemanden kennt, der einen besitzt. Von 180 Teilnehmern an der Umfrage meldeten sich fünf Prozent mit: »Hier! Ich!« Es waren IT-Nerds oder Sicherheitsforscher, die damit im Labor verschiedene Dinge untersuchten. 17,8 Prozent meiner Follower hatten noch nie von einem Kühlschrank gehört, der die Milch nachbestellen konnte, und 77,2 Prozent hatten keinen und kannten auch niemanden, der so ein Gerät besaß. Die Begründungen reichten von »Ich dachte, das gibt es bisher nur als Technologie-Demo« bis hin zu »Es gibt keinen Händler, bei dem man diese Dinge im Internet nachbestellen kann«.

Hersteller von smarten Kühlschränken haben sich in der Praxis eher dazu entschieden, diese mit einem Display auszustatten, sodass man auch beim Kühlschrank Live-Übertragungen oder Serien gucken kann oder einfach nur Rezepte aus dem Internet anzeigen sowie Musik und Videos streamen. Man kann sich mit dem smarten Kühlschrank aufgrund einer eingebauten Kamera auch Bilder vom Inhalt schicken lassen, während man gerade selbst Lebensmittel einkaufen ist, damit man keine wichtige Zutat vergisst. Ein Kühlschrank, der selbstständig Milch bestellt, blieb aber in großen Teilen eine Vision.

Dem Kühlschrank folgten schon bald Backöfen, Geschirrspüler und E-Herde – und zumindest dank einer Verknüpfung mit Amazon konnte die Bestell-Idee Wirklichkeit werden. Denn der Geschirrspüler kann beim »Amazon Dash Replenishment Service« mitzählen, wie viele Waschgänge getätigt wurden, und dann selbstständig neue Tabs bei Amazon nachbestellen. Alles wurde weitergedacht, doch die Idee kam durch den smarten Kühlschrank ins Rollen.

Von da an wurde »einfach gemacht, was geht«, wie es der Datenschützer Max Schrems einmal im Zusammenhang mit dem Internet der Dinge ausgedrückt hat. Es wurde vernetzt, was möglich ist, und nicht drüber nachgedacht, ob das auch sinnvoll ist. So präsentierten die Tech-Firmen Jahr für Jahr

auf ihren Messen immer mehr vernetzte Gegenstände – bis sich auch die Vorfälle häuften, bei denen es um die Sicherheit ging, und es plötzlich im Jahr 2016 ein so großes Botnet aus verwaisten vernetzten Geräten gab, dass infolge einer Überlastung ein wichtiger Service-Provider ausfiel und dadurch Dienste wie Twitter oder Netflix lahmgelegt wurden.

Die Sicherheitsforscher von CERT.at hatten mich bei unserem Gespräch ein Jahr zuvor bereits davor gewarnt, dass solche Dinge passieren werden. Mich hat das zum Nachdenken gebracht. Seither beschäftige ich mich intensiv mit dem Internet der Dinge und den Auswirkungen der zunehmenden Vernetzung auf die Gesellschaft. Was wird passieren, wenn das so weitergeht, fragte ich mich.

Ich habe bereits damals bei meiner redaktionellen Arbeit bemerkt, dass wenige der Hersteller auch nur im Ansatz darüber nachgedacht haben, wie sie ihre Geräte absichern können. Dabei sind vernetzte Kühlschränke nichts anderes als Computer – und wir wissen, dass ein Anti-Virus-Programm das Mindeste ist, was nötig ist, um uns vor gröberen Problemen zu bewahren. Der Ausfall des Internet-Service-Providers durch den Zusammenschluss unzähliger vernetzter Geräte zu einem Botnet hat gezeigt, dass wir durch die zunehmende Vernetzung als Gesellschaft vulnerabler und anfälliger werden und wir – bzw. die Hersteller von Geräten – nicht so lax mit Sicherheitsthemen umgehen sollten wie bisher.

Ein andermal, es war ungefähr zur selben Zeit, stand ich auf einem Flughafen in der Warteschlange zum Schalter, um mein Gepäck aufzugeben. Ich war rechtzeitig zwei Stunden vor dem Abflug da, doch es gab einen »Computerfehler« im System. Die Passagiere konnten nicht abgefertigt werden, weil das Flughafenpersonal keinen Notfallplan hatte für einen Check-In ohne Internet-Verbindung. Zahlreiche Maschinen sind daher an dem Tag halb leer abgeflogen, da sie nicht auf die Passagiere warten konnten, die in der Halle standen und stundenlang vergeblich darauf warteten, einzuchecken.

Durch die zunehmende Vernetzung werden wir als Gesellschaft immer abhängiger vom »Always On«. Und manchmal trifft uns das viel härter als eine Spam-Mail, die automatisiert von einem Kühlschrank verschickt wurde. Experten warnen seit Jahren davor, dass wir auf die Folgen, die die zunehmende Vernetzung haben könnte, nicht ausreichend vorbereitet sind. Dem stimme ich zu. Ihnen, liebe Leserinnen und Leser, möchte ich mit dem Buch einen Überblick über die wichtigsten Entwicklungen in diesem Bereich geben – und über die lauernden Gefahren.

Eine dieser Gefahren ist, dass wir als Gesellschaft auf eine Totalüberwachung zusteuern – denn unsere Daten werden nicht nur von kommerziellen Firmen gesammelt, auch Cyberkriminelle und der Staat wollen gleichermaßen darauf zugreifen können.

Cyberangriffe sind nicht nur für große, kritische Anlagen ein Problem, sondern auch, wenn sie in unseren Wohn- und Kinderzimmern stattfinden, etwa wenn unbekannte Angreifer eine Baby-Cam übernehmen und die Mutter beim Stillen beobachten oder wenn sie über vernetztes Spielzeug direkt mit dem Kind in Kontakt treten und ihm den Befehl erteilen, die Haustür zu öffnen. Auch Connected Cars sind nicht sicher und auf den »Autopiloten« sollten Sie sich besser nicht allzu sehr verlassen.

Neben den Gefahren, die im Bereich der IT-Sicherheit lauern, machen sich große Konzerne wie Amazon oder Google mit digitalen Assistenzwanzen in unseren Wohnzimmern breit – und nutzen die Datensammlung auch noch dazu, ihre Produkte zu verbessern. Auch App-Hersteller sind nicht viel besser, wenn es um das Sammeln und Speichern unserer Daten geht. Von diesen Herstellern werden unsere intimsten Details oftmals an Werbetreibende weiterverkauft und landen damit auch bei Firmen, mit denen wir niemals persönlich in Kontakt waren. Immer mehr Daten werden gesammelt, auch in vernetzten Städten.

Ich möchte Ihnen aber nicht nur die Gefahren aufzeigen, sondern auch, was Sie tun können, um dieser Entwicklung nicht hilflos ausgeliefert zu sein. Wir befinden uns mitten drin in einer Entwicklung, die Teil eines »immer schneller, höher, weiter!« ist, ohne an die Konsequenzen zu denken. Das müssen wir wieder ändern. Gemeinsam.

1

WAS IST DAS INTERNET DER DINGE?

Neue Technologien beeinflussen Ihr Leben und zwar vielleicht sogar, ohne dass Sie davon etwas wissen. Dieser Satz soll Ihnen jetzt keine Angst einjagen. Stattdessen will ich Sie auf den Inhalt dieses Buches sanft vorbereiten, denn von dem ein oder anderen werden Sie überrascht sein.

Zum Beispiel: Wussten Sie, dass es im Jahr 2017 in Österreich bereits mehr Geräte, die miteinander vernetzt waren, als Menschen gab? Diese Zahl stammt von einem, der es wissen muss: T-Mobile-Chef Marcus Grausam, er lancierte sie in einem Interview.[1] 2020 soll die Zahl der vernetzten Dinge in Österreich bereits auf 20 Millionen Dinge gestiegen sein.

Auch für Deutschland ist die Prognose beeindruckend. Auf rund 82 Millionen Einwohner kommen im Jahr 2020 bereits rund 767,5 Millionen vernetzte Geräte. Diese Zahl stammt von Cisco, einem weltweit tätigen Telekommunikations-

1 vgl. *https://futurezone.at/b2b/a1-chef-schon-mehr-vernetzte-geraete-als-menschen/400672259*

unternehmen, das von einem stark exponentiellen Wachstum ausgeht. Laut dem Deutschlandchef von Cisco sollen in vier Jahren bereits auf jeden Deutschen rund zehn vernetzte Geräte kommen – vom Baby bis zum Greis.[2]

Weltweit soll laut der Vorhersage von Cisco die Zahl der vernetzten Geräte in den kommenden fünf Jahren deutlich stärker steigen als die Zahl der Internetnutzer und der Weltbevölkerung.

Sie können sich unter diesen sogenannten »vernetzten Geräten« nichts vorstellen? Das liegt daran, dass diese Dinge auf den ersten Blick schwer greifbar sind und es so wirkt, als würde es Sie nichts angehen. Unter dem Sammelbegriff »Internet der Dinge« (im Englischen: »Internet of Things«, abgekürzt: IoT) fasst man alle jene Technologien und Geräte zusammen, die selbstständig über das Internet miteinander kommunizieren können.

IoT-Geräte und ihre Macht über uns

Um etwas konkreter zu werden: Ein vernetztes Gerät kann eine Kaffeemaschine sein, die sich per App einschalten lässt. Oder ein Spielzeug-Teddy, der mit der Stimme der Mutter zum Kind spricht. Oder eine Lampe, die mit dem Lichtschalter kommuniziert und sich automatisch ein- und ausschaltet. Oder ein smarter Lautsprecher, der Ihre Lieblingsmusik spielt. Oder der Pflanzensensor, der Ihren Garten automatisch bewässert, wenn Sie im Urlaub sind. Oder die Fußgängerampel, die automatisch auf Grün umschaltet, wenn Sie sich ihr nähern. Oder der Getränkeautomat am Bahnsteig, der automatisch eine Meldung an seinen Eigentümer abschickt, wenn jemand versucht, ihn aufzubrechen, oder wenn er kaputt ist.

2 vgl. *https://www.ip-insider.de/2020-fast-800-mio-vernetzte-geraete-in-deutschland-a-537991/*

Nicht all diese vernetzten Geräte stehen zusätzlich zu unserem WLAN-Router, mit dem wir Menschen eine Internet-Verbindung herstellen, bei uns zu Hause in den Wohnzimmern. Die vernetzten Geräte, die miteinander kommunizieren, sind auch in unseren Städten, der Infrastruktur, Fabriken und Büros zu Hause und sie haben prinzipiell den Sinn und Zweck, unser Leben zu erleichtern. Der Anwendungsbereich ist dabei genauso vielfältig wie die Vielzahl an vernetzten Geräten. Er reicht von der allgemeinen Informationsversorgung über automatische Bestellungen bis hin zu Warnfunktionen. In Betrieben geht es vor allem um Effizienzsteigerung und darum, Produktionsabläufe zu erleichtern.

Die Vision, alles miteinander zu vernetzen, wurde übrigens bereits im Jahr 1991 erstmals aufgeschrieben. Der Computerwissenschaftler Mark Weiser, der als Tüftler bei Xerox in Palo Alto in Kalifornien arbeitete, beschrieb seine Vision in einem Aufsatz namens »Computer for the 21st Century«. Der Begriff »Internet der Dinge« stammt vom MIT-Technikpionier Kevin Ashton.

Doch was hat das jetzt mit mir zu tun, werden Sie sich fragen? Sie machen Ihren Kaffee am liebsten mit einer Espressokanne und gießen Ihre Pflanzen zweimal täglich selbst. Tatsächlich sind Sie mit dieser Ansicht nicht alleine: Vielen Konsumenten ist das Internet der Dinge egal – aber nur, solange es sich nicht plötzlich um Anwendungen handelt, die auch Ihr persönliches Leben verbessern könnten. Könnten, wohlgemerkt. Denn fast jedes IoT-Gerät hat derzeit seinen Preis, wenn es um Datenschutz und Sicherheit geht.

Robert Martin etwa hatte auf Amazon ein Gadget entdeckt, von dem er dachte, dass es gut zu seinen Gewohnheiten passte. Nie mehr aussteigen, um die Garagentür zu öffnen, sondern dies bequem aus der Ferne erledigen. Alexa per App am besten schon ein oder zwei Ecken vor seinem Haus befehlen, das Tor zu öffnen, damit er bequem ohne Wartezeit in seine Garage reinfahren kann. So stellte sich Robert Martin das vor, als er ein entsprechendes Produkt von Garadget erwarb.

Doch Robert Martin staunte nicht schlecht, als er eines Tages seine Garagentür plötzlich nicht mehr bequem per App öffnen konnte. Der smarte Türöffner des Start-ups reagierte nicht mehr auf seinen Knopfdruck am Smartphone. Auch seine Sprachbefehle per Alexa gingen ins Leere. Das Start-up hatte die Verbindung schlichtweg gekappt und die Hardware vom Netzwerk, mit dem die App verbunden war, getrennt. Das geschah in voller Absicht, um dem Mann eins auszuwischen.

Offiziell begründete das Unternehmen seinen Zug damit, dass der Mann »toxisch« sei und das Produkt von Anfang an nicht wirklich wollte.[3] Robert Martin hatte nämlich, nachdem seine ersten Installationsversuche gescheitert waren, eine negative Bewertung auf Amazon über den smarten Türöffner abgegeben, der in den USA zu dem Zeitpunkt, im Jahr 2017, für rund 99 Dollar erhältlich war. In dieser Bewertung bezeichnete Robert Martin den smarten Türöffner als »Scheißteil«, weil es nicht gleich wie gewünscht funktioniert hatte. »Schrott. Gebt nicht euer Geld dafür aus«, lautete sein Ratschlag an andere potenzielle Kunden. Auch im Support-Forum des Start-ups sparte er nicht mit einer ausfallenden Wortwahl, um seine Kritik anzubringen.

Der Hersteller blockierte ihn daraufhin einerseits im Online-Forum, andererseits trennte er die Verbindung des smarten Türöffners zur App. Er »empfahl« Robert Martin, das Gerät an Amazon zurückzuschicken, um sein Geld zurückzubekommen. Eine andere Option wurde dem Mann, der das Gadget eigentlich behalten wollte, nicht zur Verfügung gestellt.

Jeder hat sich schon einmal geärgert, wenn ein neues Gerät nicht das tut, was man will. Und natürlich sollte man nicht fluchen und den Hersteller beschimpfen, wenn etwas nicht

3 vgl. *https://www.theatlantic.com/technology/archive/2017/04/garadget-sabotage/521937/*

gleich wie erwartet funktioniert. Doch das Start-up hat hier eine Grenze überschritten: Es hat lieber sein eigenes vernetztes Gerät sabotiert, als mit dem Kunden zu sprechen. Es hat den Account des Kunden ausfindig gemacht, überwacht, die ID gesperrt und die Verbindung gekappt und ihn damit für sein »toxisches« Verhalten nach eigenem Gutdünken bestraft.

De facto konnte Robert Martin nicht mehr mit seinem Auto aus der Garage fahren. Er konnte in seinem eigenen Heim nicht mehr das tun, was er wollte, weil er von einem Hersteller abhängig war, der Macht über ihn hatte. Und wer rechnet schon damit, dass dieser ihn nicht als Kunden haben will?

Der Fall hätte in Europa für beide negative rechtliche Konsequenzen haben können. Robert Martin hätte in Europa von Garadget wegen »übler Nachrede« verklagt werden können, und zwar dann, wenn seine Online-Bewertung »unsachlich« gewesen ist und wenn sich davon jemand »persönlich angegriffen« fühlen könnte. Ob eine Bewertung beschimpfend oder verspottend ist, hat allerdings im Einzelfall untersucht zu werden. Garadget ist nach wie vor am Markt und mittlerweile auch zu einem beliebten Hersteller von smarten Garagentoröffnern geworden. Das Beispiel zeigt, wie viel Kontrolle Hersteller von vernetzten Geräten über ihre Dinge haben – und wie sie im schlimmsten Fall ihre Macht missbrauchen können.

Überwachung mal andersrum

Nicht nur Hersteller können Gadgets aus der Ferne steuern, wie die Niederländerin Rilana Hamer am eigenen Leib erfahren musste. Sie hatte sich eine billige Überwachungskamera angeschafft, mit der sie ihr Haustier überwachen wollte. Sie hatte einen jungen Welpen, auf den sie mit der Kamera ein Auge werfen wollte, auch wenn sie selbst nicht zu Hause war. Sie hatte dazu die Kamera mit ihrem Heim-WLAN-Netzwerk verbunden. Doch statt Rilana Hamers Welpen fing die Über-

wachungskamera unterdessen an, seine Besitzerin in ihrem eigenen Zuhause zu beobachten – und ungefragt mit ihr zu kommunizieren. Als dies das erste Mal passierte, schrieb Rilana Hamer auf Facebook: »Für einen Moment dachte ich, ich bin verrückt geworden. Ich bin heimgekommen und habe meine täglichen Dinge erledigt. Aufräumen und im Haus singen ... bis ich im Wohnzimmer etwas gehört habe. Ich bin eingetreten und habe gesehen, wie sich die Kamera bewegt hat«, heißt es in dem Posting. Danach habe sie das Wohnzimmer wieder verlassen. Als sie es das nächste Mal betrat, bewegte sich die Kamera von ihr weg und sagte auf Französisch: »Guten Tag. Wie geht es Ihnen?«[4]

Rilana Hamers zog sofort den Stromstecker und trennte die Kamera vom Internet, doch der Vorfall ließ ihr keine Ruhe: »Ich war voller Sorge und dachte ernsthaft, ich werde verrückt. Ich bin beobachtet worden. Aber wie lange schon? Was hat die Person gesehen? Mein Haus, meine persönlichen Befindlichkeiten ...« Und so kam es, dass Rilana Hamers die Kamera noch einmal auspackte und einsteckte. Wieder begann die Kamera, sich ungefragt zu bewegen. Dieses Mal filmte sie den Vorfall und die Person am anderen Ende begrüßte sie auf Spanisch. »Verlassen Sie sofort mein Haus!«, sagte die Niederländerin. Und zurück kam stattdessen die Aufforderung eines Unbekannten zum Oralverkehr.

Am nächsten Tag brachte die Frau die Überwachungskamera zu dem niederländischen Discount-Supermarkt zurück, in dem sie das vernetzte Gerät billig gekauft hatte. Doch was war passiert? Die Überwachungskamera wies praktisch keinen Schutz gegen unbefugtes Eindringen auf und konnte aus der Ferne bequem und einfach von Unbekannten gesteuert werden. Diese hatten vollen Zugriff auf die Bilder der Überwachungskamera sowie auf das eingebaute Mikrofon, weil der Hersteller eingebaute Sicherheitsmaßnahmen komplett »vergessen« hatte.

4 vgl. *https://www.grahamcluley.com/hacked-smart-camera-hola/*

Rilana Hamers wird nie erfahren, wer da versucht hat, mit ihr zu sprechen, sie und ihre Gewohnheiten auszuspionieren, und wer sie da womöglich auch einmal nackt durchs Wohnzimmer tanzend und singend aus der Ferne beobachtet hat. Sie hatte befürchtet, verrückt geworden zu sein. Was sie in dieser Situation aber definitiv war: komplett machtlos. Ihr einziger Ausweg war, die Überwachungskamera, mit der am Ende sie selbst überwacht worden war, nicht mehr zu verwenden und zurückzubringen.

Datenlecks

Schlechte Security und potenzielle Gefahren wie die unkontrollierte Fernsteuerung durch Fremde ist bei billigen Produkten von weniger namhaften Herstellern an der Tagesordnung. Ein anderes Problem, das relativ häufig auftritt, ist der Datenverlust durch Datenlecks.

So hat etwa ein Hersteller von smarten Glühbirnen, Steckdosen und Überwachungskameras zu Weihnachten 2019 Daten von rund 2,4 Millionen Nutzern und ihren vernetzten Geräten unabsichtlich frei im Internet zugänglich gemacht. Die Sicherheitsforscher von IPVM fanden insgesamt 40 Millionen Datensätze zu dem Vorfall. Dazu gekommen war es, weil der Hersteller, die US-amerikanische Firma Wyze, eine Kundendatenbank überspielt hatte, um das Durchsuchen von Informationen für die Mitarbeiter zu erleichtern. Bei der Überspielung der Daten wurde aus Versehen das Sicherheitsprotokoll gelöscht und – schwups – waren die Daten frei im Netz verfügbar.[5]

Darunter waren neben der E-Mail-Adresse aller Nutzer, die das Gerät benutzten, etwa Daten wie die Spitznamen, die die Besitzer ihren smarten Geräten verpasst hatten, sowie die genaue Typenbezeichnung und Firmware des Geräts. Auch das WLAN-Netzwerk, mit dem sie verbunden waren, befand

5 vgl. *https://blog.12security.com/wyze/*

sich darunter, sowie der Zeitpunkt, wann das Gerät zum letzten Mal benutzt worden war. Von 24.000 Nutzern waren auch sogenannte »Tokens« betroffen, mit denen die Wyze-Geräte mit Alexa-Geräten verbunden worden waren. Zudem befanden sich unter den frei im Netz verfügbaren Daten Informationen wie die Körpergröße, das Gewicht, das Geschlecht, das Alter, der tägliche Proteinbedarf, die Knochendichte sowie zahlreiche andere Gesundheitsdaten der Nutzer.

Die Firma hat zwar insgesamt rasch reagiert, aber diese Daten waren so lange frei im Netz, dass sie potenziell von Kriminellen runtergeladen werden konnten. Das bedeutet, dass Ihre Daten gegen Sie eingesetzt werden und Ihnen schaden können. Sie können nichts dagegen tun, sind völlig machtlos.

Sie denken vielleicht, dass sich sowieso niemand dafür interessiert, wann Sie Ihre smarte Lampe das letzte Mal ein- und ausgeschaltet haben oder wie viel Sie wiegen. Doch aus dem Verhalten Ihrer Lampe kann man etwa ablesen, ob Sie sich gerade im Urlaub befinden. Ihre Daten zum Übergewicht können an sogenannte »Datenhändler« auf dem Schwarzmarkt verkauft werden, damit Sie etwa gezielt Werbung für Diätprodukte erhalten. Ihre Spitznamen der Geräte können als Passwort-Kombinationen ausprobiert werden, um sich in Ihre Accounts einzuhacken. Sie müssen bedenken, dass es Kriminellen nur um den Profit geht, und deshalb sind sie sehr einfallsreich. Sie leben schließlich davon. Das Gemeine an derartigen Datenlecks ist, dass Sie als betroffener Kunde möglicherweise gar nichts merken. Ihre Daten können missbraucht werden, oder auch nicht.

Der Hersteller Wyze musste in diesem Fall als Sicherheitsmaßnahme ein Update an seine Nutzer senden. Dadurch, dass auch Tokens zu Android- und Alexa-Geräten betroffen und frei im Netz verfügbar waren, wären bestimmte Angriffe von Kriminellen auf diese Accounts nahezu problemlos möglich gewesen. Es bestand also eine akute Gefahr für alle betroffenen Nutzer. Diese wurden durch das Update von Wyze zu ihrer eigenen Sicherheit dazu gezwungen, all ihre smarten,

vernetzten Geräte, die mit anderen Accounts von Drittanbietern wie Amazon Alexa oder Google Assistant verbunden waren, neu zu konfigurieren.

Das S für Security

Die oben genannten Beispiele sind der Grund, warum es im Internet unter Sicherheitsexperten einen beliebten Scherz gibt. »Das S in IoT steht für Security«. Welches S, fragen Sie sich? Genau. Es gibt keines. Es gibt keine eingebaute Sicherheit beim Internet der Dinge.

Die fehlende Sicherheit ist einer der Hauptgründe, warum viele vernetzte Geräte zur Überwachung regelrecht einladen. »So ein Gerät kommt mir niemals ins Haus«, sagen Sie sich jetzt? Tja, denken Sie daran: Sobald Sie das Gefühl haben, dass ein vernetztes Gerät für Sie bequem erscheint und Ihnen im Alltag Erleichterung bringt, werden Sie Ihre Sorgen und Bedenken wieder vergessen haben.

Sie sind allerdings nicht komplett hilflos ausgeliefert. Ich werde Ihnen in diesem Buch genau erklären, worauf Sie achten müssen, damit Sie zumindest die größtmögliche Sicherheit für sich erreichen können. Datenlecks wie jenes bei Wyze werden sich aber auch bei seriösen Anbietern nicht immer verhindern lassen, denn absolute Sicherheit gibt es freilich nie. Eines kann ich Ihnen zudem bereits an dieser Stelle verraten: Von vernetzten Billig-Produkten wie der beschriebenen Überwachungskamera von Rilana Hamers sollten Sie generell die Finger lassen. Die Chance, dass Ihnen Ähnliches passiert wie der niederländischen Welpen-Besitzerin, ist groß.

Der IT-Sicherheitsexperte Bruce Schneier beispielsweise glaubt nicht, dass derartige Produkte irgendwann von selbst vom Markt verschwinden. Deshalb sind Sie gefragt. Sie müssen sorgfältig wählen und sich vor einem Kauf genau erkundigen. Bruce Schneier ist der Meinung, dass in jedes Produkt IT-Sicherheit eingebaut werden muss. Das ist allerdings nicht so einfach, denn es gibt nicht eine einzige Lösung, die für alle

Geräte gleichermaßen funktioniert. Deswegen ist Sicherheit eine große Herausforderung, selbst für Hersteller, die das Thema ernst nehmen.[6] Und das sind freilich nicht alle. Dem Hersteller der smarten Überwachungskamera, die die Niederländerin im Supermarkt gekauft hatte, war die Sicherheit schlichtweg egal.

Das Internet der Dinge, also die Vernetzung von allen Dingen, die es gibt, mit dem Internet, hat sich daher bisher weder in der Security-Branche noch bei den Datenschützern einen guten Ruf erarbeitet. Bei vielen Geräten sollte man sich als Kunde tatsächlich schon vor dem Kauf fragen: Brauche ich dafür eine Internet-Verbindung oder sollte ich lieber auf ein Offline-Produkt setzen?

Der Cambridge-Professor und IT-Sicherheits-Experte Ross Anderson bezeichnet vernetzte Geräte als »Internet of Targets«, also »Internet der Ziele«, weil man herkömmliche Gegenstände durch eine Verbindung zum Internet plötzlich zur Zielscheibe von Kriminellen macht. Bruce Schneier warnt allerdings davor, ausschließlich »Worst-Case«-Szenarios auszumalen – also all das Negative, das passieren könnte. »Das würde zu Überreaktionen führen anstatt zu Lösungen«, so der Experte.

Ich möchte Ihnen mit den Beispielen auch keine Angst einjagen, sondern Ihnen lediglich aufzeigen, wie vernetzte Produkte missbraucht werden können. Wenn Ihre Lampe mit dem Internet verbunden ist oder Ihre Überwachungskamera oder in weiterer Folge Ihr Auto, Ihre Waschmaschine oder Ihre Zahnbürste, dann sind diese Geräte denselben Gefahren im Netz ausgesetzt wie Sie. Auf genau diese Probleme machen seit jeher Menschen aufmerksam. Neben dem US-Sicherheitsforscher Bruce Schneier, der mit seinem Werk »Click Here To Kill Everybody« (deutsche Ausgabe: mitp-

6 vgl. *https://www.schneier.com/news/archives/2018/10/how_to_keep_the_inte.html*

Verlag, 2019) sämtliche Gefahren aufgezeigt und Lösungswege bereitgestellt hat, gibt es beispielsweise seit Jahren auf Twitter einen eigenen Account namens »Internetofshit«[7]. Dieser sammelt Beispiele und macht vor allem auf oft satirische Art und Weise auf Privatsphäre- und Sicherheitsverletzungen von vernetzten Geräten aufmerksam.

Markus Beckedahl, Chefredakteur von netzpolitik.org, bezeichnete beim 36. Chaos Communication Congress in Leipzig smarte Lautsprecher mit Alexa oder Google Home als »nicht vertrauenswürdige Assistenzwanzen«. Auch Datenschützer der britischen Bürgerrechtsorganisation Privacy International warnen seit Jahren vor dem Einsatz und »Alexa« hat nicht umsonst bereits den Datenschutz-Negativpreis »Big Brother Award« erhalten. Zu den immer beliebter werdenden smarten Lautsprechern wird es ein eigenes Kapitel geben, bei dem ich Ihnen die Vorteile und Risiken aufzeigen werde – und Sie dann am Ende selbst entscheiden müssen, ob in Ihrem Fall die Bequemlichkeit oder die Gefahren überwiegen. Letztendlich sollen Sie in der Lage sein, selbst zu entscheiden, welche vernetzten Geräte für Sie infrage kommen, wie Sie damit umgehen oder ob Sie auf manche lieber verzichten.

Und haben Sie sich an dieser Stelle schon gefragt: Was war das erste »Ding«, das Sie vernetzt haben, vielleicht ohne es zu wissen?

Smarte Städte

Vielleicht glauben Sie jetzt, dass Sie das meiste von dem, was Sie bisher gelesen haben, nicht betrifft. Sie könnten am Ende zu der Einsicht gelangen, dass Sie sich »sicher keine Wanze ins Haus stellen«, aber ich habe leider schlechte Neuigkeiten für Sie: Sie sind von der Entwicklung der voranschreitenden Vernetzung von Dingen, die miteinander kommunizieren,

7 vgl. *https://twitter.com/internetofshit*

dennoch betroffen. Es gibt nämlich Dinge, die Sie sich im Gegensatz dazu, ob Sie sich eine »Alexa« ins Haus stellen oder mit einem Smartphone in der Tasche herumlaufen, durch das man permanent weiß, wo Sie sich gerade befinden, nicht aussuchen können. Dinge, die der Staat für Sie anschafft – oder Ihnen per Verordnung in Ihr Haus stellt.

Das betrifft Sie etwa dann, wenn Sie in einer Stadt leben, die Fußgängerampeln vernetzt und mit Kameras ausstattet, damit sie schneller umschalten, wenn Sie über die Straße gehen wollen. Das macht beispielsweise die österreichische Hauptstadt Wien. In Berlin hat am Bahnhof Südkreuz die Deutsche Bahn in einem Pilotprojekt mit der Bundespolizei den Einsatz von vernetzten Überwachungskameras mit Gesichtserkennung getestet. Die BVG (Berliner Verkehrsbetriebe) hat zudem die Kontrolle über mehr als 16.000 Kameras, manche davon sind mit Mikrofonen ausgerüstet.[8] Insgesamt soll es rund 40.000 Überwachungskameras im öffentlichen Raum geben. Berlin schaffte es damit in einem Ranking des britischen Technikportals Comparitech sogar auf Platz 19 der bestüberwachten Städte. Auf rund tausend Menschen in Berlin kommen umgerechnet elf Überwachungskameras. Doch die deutsche Metropole ist damit nicht allein in Europa: Unter den Top 50 der meistüberwachten Städte befinden sich auch London, Warschau, Wien, Madrid und Budapest.[9]

Doch nicht nur im öffentlichen Raum wird viel mehr vernetzt. Wenn Sie in einen Neubau in Deutschland ziehen, werden Sie dort einen sogenannten »Smart Meter« finden. Das ist ein intelligenter Stromzähler, der in ein Kommunikationsnetz eingebunden ist und Ihren Stromverbrauch künftig digital an den Netzbetreiber weitergibt – und zwar in 15-Minuten-Intervallen. Im Gegensatz zum bereits seit Jahrzehnten einge-

8 vgl. *https://netzpolitik.org/2019/berlin-keine-rationalen-argumente-fuer-videoueberwachung-an-s-bahnhof/#spendenleiste*

9 vgl. *https://www.deutschlandfunknova.de/beitrag/ueberwachung-40-000-kameras-fuer-berlin*