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-