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.