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 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-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, 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 eingesetzten mechanischen Ferraris-Zähler besitzt der neue, elektronische Stromzähler keine mechanisch bewegten Teile und hat eine weitaus kürzere Lebensdauer.

Diese Smart Meter sind nichts anderes als vernetzte Geräte, die miteinander kommunizieren und dem Netzbetreiber Rückmeldung geben. Doch diese Geräte können auch aus der Ferne an- und abgedreht werden – und bieten damit ein Einfallstor für Kriminelle. In Deutschland sind sie für Haushalte mit einem Jahresstromverbrauch von über 6000 kWh verpflichtend sowie bei Haushalten, die Solaranlagen betreiben, die über eine Leistung von bis zu 100 Kilowatt Strom erzeugen. Auch wer für sein E-Auto

eine Ladestelle errichtet hat, ist davon betroffen. Doch prinzipiell kann der neue Stromzähler auch in Ihrem Haushalt landen, wenn Sie das nicht wollen: Das letzte Wort hat dabei nämlich der Netzstellenbetreiber oder Vermieter.

Auch in Österreich werden die Stromzähler intelligent. Dort gibt es eine Verpflichtung, die vorsieht, dass alle Haushalte mit dem Gerät ausgestattet werden. Konkret bekommen dort bis Ende 2022 sogar 95 Prozent der Haushalte smarte Stromzähler. Die gesammelten Daten können detaillierte Auskünfte über den Stromverbrauch eines Haushalts geben und die Gefahren eines Cyberangriffs dadurch steigern. Aber auch die Gefahren eines Systemfehlers in der IT steigen dank der zunehmenden Komplexität.

Weitere Entwicklung

Sie sehen also, wie weit das Internet der Dinge reicht und was alles unter diesem Begriff zusammengefasst werden kann. Bei den vernetzten Haushaltsgeräten hört die Entwicklung nicht auf und deshalb sollten Sie genau darüber Bescheid wissen, denn auch Ihr Leben ist auf jeden Fall davon betroffen. Im vergangenen Jahrzehnt – von 2010 bis 2020 – sind technologische Entwicklungen insgesamt ganz massiv vorangeschritten. Von künstlicher Intelligenz bis zum Überwachungskapitalismus durch die großen Internet-Konzerne Amazon, Facebook und Google haben vor allem Telekom-Konzerne die Vernetzung von Maschinen und Dingen massiv vorangetrieben.

Das Internet der Dinge wird sich auch in den nächsten zehn Jahren zunehmend ausbreiten und wächst zudem, wie bereits zu Beginn aufgezeigt, exponentiell weiter. Im Jahr 2020 stehen wir damit noch relativ am Anfang. Bisher haben wir all diese Entwicklungen zu wenig kontrolliert und reguliert. Das soll sich in der nächsten Dekade ändern, wie Zukunftsexperten erläutern. Es soll ein Jahrzehnt folgen, in dem wir als Gesellschaft Technologie nicht nur verwalten und dabei zusehen, wie sie uns überrollt. Stattdessen werden wir diese als Gesellschaft aktiv gestalten.

Der berühmte NSA-Whistleblower Edward Snowden, der 2013 die Überwachungsmaschinerie der NSA aufgedeckt hatte, sprach am Chaos Communication Congress in Leipzig via Videoschaltung ebenfalls von dieser Aufbruchsstimmung. »Derzeit erleben wir ein überwachtes Internet. Aber der Wechsel kommt. Und er wird durch Leute erreicht, die aufmerksam sind, sich um Dinge zu kümmern«, sagte Snowden und forderte die Hacker-Community, die am Congress mit knapp 17.000 Menschen vertreten war, dazu auf, sich aktiv an diesem Prozess zu beteiligen.[10] Statt immer nur die negativen Dinge zu sehen oder gar den Kopf in den Sand zu stecken und sich zu denken, dass man »als Einzelner nichts ausrichten kann« oder »es noch schlimmer sein