

BARBARA WIMMER

HILFE **ICH HABE MEINE** **PRIVAT** **SPHÄRE** **AUFGEgeben!**



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



INHALT

Vorwort	7
Kapitel 1: Was ist das Internet der Dinge?	13
Kapitel 2: Digitale Unmündigkeit durch Vernetzung	27
Kapitel 3: Warum wir auf eine Totalüberwachung zusteuern	51
Kapitel 4: Hey, Einhorn: Wie uns Spielzeug ausspioniert	69
Kapitel 5: Warum das Internet der Dinge so unsicher ist	93
Kapitel 6: Hey Auto: Wir sind die Testpiloten	111
Kapitel 7: Hey Alexa: Digitale Assistentenzwanzen	129
Kapitel 8: Privatsphäre bei Siri & Co? Fehlanzeige!	149
Kapitel 9: Hey App: Was weißt du alles über mich?	169
Kapitel 10: Corona: Apps zur Rückverfolgung von Infektionsketten	191
Kapitel 11: Hey, Smart City: Machst du wirklich alles besser?	211
Kapitel 12: Technologie gestalten und regulieren	229
Kapitel 13: Zusammenfassung und wie Sie sich wehren können	247
Stichwortverzeichnis	263

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 Kühlschrank 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-

schränk 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 größeren 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 Assistentenzwanzen 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.

HEY, EINHORN: WIE UNS SPIELZEUG AUSSPIONIERT

Es ist weiß und kuschelig, hat rosa Pfoten, einen pfiifigen, rosaroten Irokesen-Haarschnitt und einen süßen, runden Bauch: das Einhorn-Spielzeug »CloudPets« der Firma Spiral Toy. Das Medienportal des Mitteldeutschen Rundfunks bezeichnete es in einer Twitter-Nachricht als »das gefährlichste Einhorn der Welt«¹. Denn wenn man auf die linke Pfote drückt, bekommt man nicht etwa ein »Hallo, Juliana!« mit der Stimme der Mutter zu hören, sondern eine Botschaft eines Daleks aus der beliebten Science-Fiction-BBC-Serie »Dr. Who«. Dieses will die gesamte Welt auslöschen und zerstören. Mit böser, finsterner Stimme dröhnt es aus dem Einhorn: »Auslöschen, Zerstören!« Das sind Dinge, von denen man nicht will, dass es Kinder in jungem Alter zu hören bekommen. Sie können beängstigend sein und Kinder regelrecht verstören.

1 vgl. <https://twitter.com/MEDIEN360G/status/946421154369232896>

Und jetzt stellen Sie sich vor, dass Sie gar nichts davon wissen. Wenn Ihr Kind jetzt nicht gerade weinend zu Ihnen läuft und sich von Ihnen in die Arme nehmen lässt, bekommen Sie möglicherweise gar nichts davon mit. Nun möchte ich Ihnen in aller Ruhe erklären, was es mit diesem Einhorn auf sich hat.

Das Spielzeug-Einhorn ist vernetzt und verfügt über eine Internet-Verbindung. Das erkennt man im Falle von »Cloud-Pets« unter anderem an dem WLAN-Wolken-Symbol, das auf einer der beiden Pfoten des Einhorns abgebildet ist. Bei dem Einhorn-Plüschtier, das es auch in der Variante Hund oder Katze gibt, können Sie und andere Familienmitglieder über eine App Nachrichten aufnehmen und via Plüschtier an Ihr Kind schicken. Sobald die Nachricht angekommen ist, blinkt das rote Herz des Plüschtiers. Durch das Drücken der rechten Pfote kann Ihr Kind die von Ihnen aufgenommene Nachricht dann abhören. Mit dem Drücken der linken Pfote kann Ihr Kind dank eines eingebauten Mikrofons auch selbst Nachrichten aufnehmen und an Sie zurücksenden. Diese erscheinen bei Ihnen dann in der dazugehörigen App. Auf diesem Weg ist es zum Beispiel möglich, Ihrem Kind auf kreative und lustige Weise mitzuteilen, dass das Mittagessen fertig ist, und es zum Essen in die Küche kommen soll. Oder aber Ihr Bub liegt im Krankenhaus und Sie wollen ihm außerhalb der Besuchszeiten sagen, dass Sie an ihn denken. Oder die Oma Frida, die in Australien lebt, will ihrem Enkel eine Grußbotschaft zukommen lassen. Die Aufmerksamkeit des Kindes ist Ihnen mit dieser Methode gewiss. Denn wenn das Kind das Einhorn (oder die Katze oder den Hund) liebt, wird es jede Botschaft über diesen Kanal mit besonderer Wertschätzung entgegennehmen.

Das klingt jetzt eher nach Werbung für das Produkt als nach dem »gefährlichsten Einhorn der Welt«, werden Sie sich jetzt denken. Die von mir beschriebenen Funktionen des Spielzeugs klingen nicht nur gut, sondern stoßen bei vielen Kindern auch auf ein großes »Will-haben«-Gefühl.

Doch von »CloudPets« für Ihr Kind würde ich Ihnen ganz dezidiert abraten. Die Internet-Verbindung, die bei dem Spielzeug zum Einsatz kommt und ermöglicht, dass Sie mit Ihrem Kind kommunizieren können, ist nicht sicher und wird vom Hersteller auch nicht mehr sicherer gemacht. Das bedeutet in der Praxis, dass nicht nur Sie Ihrem Kind Nachrichten schicken können, sondern praktisch jeder, der ein wenig von Technik versteht.

Gehacktes Einhorn

Besuchern des Chaos Communication Congress ist es bereits im Jahr 2017 binnen einer Minute gelungen, das Einhorn mit der Dalek-Botschaft »Zerstört die Welt!« zu versehen, und zwar ohne dass ich davon etwas von außen gemerkt hätte.² Ich hatte für meinen Vortrag über das »Internet of Fails« eine Botschaft aufgenommen, die lautete: »Hallo, Chaos Communication Congress!« Im Vortrag hatte ich dazu aufgerufen, dass interessierte Hacker gerne im Anschluss mit dem Spielzeug ein wenig spielen dürften. Als ich nach dem Vortrag das nächste Mal auf den Knopf des Einhorns drückte, war die Botschaft des Daleks zu hören. Der Aufruf zum Spielen hatte jemanden angespornt, es gleich auszuprobieren. Auf dem Chaos Communication Congress geschah dies mit meiner Einwilligung und aus »Spaß am Gerät«, wie es in der Hacker-Community so schön heißt. Das hat nichts mit Cybercrime zu tun oder illegalen Aktionen. Bei der jährlichen Veranstaltung des Chaos Communication Club (CCC) geht es darum, derartige Dinge in einer geschützten Umgebung auszuprobieren. Doch Cyberkriminelle haben meist keine so noblen Absichten: Sie wollen das Produkt nicht verbessern, sondern machen sich solche Sicherheitslücken zunutze, um sich damit persönliche Vorteile zu verschaffen.

2 vgl. <https://shroombab.at/2018/01/01/das-gehackte-dalek-einhorn-am-34c3/>

Bei dem Spielzeug von Spiral Toy war der Zugriff auf die Kommunikationszentrale des Einhorns einfach, weil die Bluetooth-Verbindung nicht gesichert ist. Somit kann sich jeder mit dem Einhorn verbinden, wenn er einen simplen Trick anwendet, der sich im Internet mit einer genauen Anleitung findet. Die exakten Details zu dem Angriff sind seit Längerem bekannt. Es reicht, im Chrome-Browser eine bestimmte Seite zu besuchen, und schon ist man im »CloudPets«-Einhorn drin und kann selbst Sprachnachrichten an Ihr Kind schicken. Dafür muss man sich aber im selben Raum befinden – was die Gefahren dieses Angriffs zumindest etwas reduziert.

Es wäre schon schlimm genug, dass Ihr Kind auf diese Weise Dinge zu hören bekommen kann, die nicht für Kinderohren bestimmt sind. Doch es könnte auch jemand versuchen, sich das Vertrauen Ihres Kindes zu erschleichen, indem er immer wieder und wieder mit ihm spricht. Stellen Sie sich vor, aus dem Einhorn spricht eine Stimme mit Ihrem Kind, die darum bittet, doch rasch zur Wohnungstür zu gehen und diese zu öffnen. Dieses Szenario hat etwa der norwegische Verbraucherschutzverein Forbrukerrådet in einem Video verwendet, um vor vernetztem Spielzeug zu warnen.³ Beim Einhorn wäre dies aufgrund der fehlenden Bluetooth-Reichweite zwar nicht möglich, aber dieses Beispiel ist bei Weitem nicht das einzige. Im Video der Verbraucherschützer wird etwa eine vernetzte Puppe aus der Ferne gesteuert. Wie genau man das macht, wurde – aus Sicherheitsgründen – freilich nicht erläutert.

Stimmen manipulieren

Ich möchte noch einen Schritt weitergehen und an das Szenario, dass Ihr Kind einem Fremden die Tür öffnen könnte, anknüpfen: Sie haben Ihr Kind schließlich so erzogen, dass es

3 vgl. <https://www.youtube.com/watch?v=LAQj0H5c6Yc>

Fremden keine Türen aufmachen soll – auch dann nicht, wenn es Schokolade gibt. Das Kind würde die Tür aber öffnen, wenn die Stimme wie die Mama oder die Tante Frida klingt und nicht wie ein Fremder. Und schon steht ein Unbekannter in Ihrer Wohnung und räumt sie aus oder entführt Ihr Kind.

Ich will dieses Szenario jetzt gar nicht weiter ausführen, weil ich Ihnen keine Angst machen will – aber technologisch ist es bereits möglich, Stimmen so zu manipulieren, dass diese wie eine bekannte Person klingen. Dazu wird zuerst die Stimme dieser Person gestohlen und im Anschluss für kriminelle Zwecke verwendet. Die Manipulation der Stimme selbst erfolgt mit einer Software, die über eine künstliche Intelligenz (KI) verfügt. Diese Software gibt es im Internet zum Runterladen. Die App heißt »Real Time Voice Cloning« und wurde dazu entwickelt, Stimmen zu klonen.⁴ Die Open-Source-App ist allerdings nicht die einzige Anwendung, mit der das technisch möglich ist. Auch das kalifornische Start-up modulate.ai arbeitet daran, Stimmen von Personen nachzubilden. Das Start-up trainiert sein Programm so, dass sich Stimmen so manipulieren lassen wie von den Nutzern gewünscht. Anders als reguläre Stimmfilter kann die Software bereits in Echtzeit das Alter, das Geschlecht und die Tonhöhe von Sprechern verändern.⁵ Was sich für Sie also wie Zukunftsmusik anhört, ist bereits seit einigen Jahren in Entwicklung und steht kurz davor, die Masse zu erreichen. Kriminelle haben diese Technik längst entdeckt und auch ausgenutzt: Ein CEO einer Firma überwies etwa 220.000 Euro, weil der vermeintliche Chef eines anderen Konzerns ihn dazu angewiesen hatte. Das hatte er allerdings nie: Seine Stimme war von Cyberkriminell-

4 vgl. <https://mixed.de/deepfake-audio-mit-dieser-app-lasst-ihr-jeden-alles-sagen/>

5 vgl. <https://www.derstandard.at/story/2000098708642/stimme-wie-obama-deepfake-ki-laesst-nutzer-klingen-wie-sie>

len gestohlen worden, die mit dieser Methode Geld erbeuten wollten.⁶

An dieser Stelle denken Sie jetzt bitte nicht: »Das kann mir nicht passieren!« oder »Ich bin kein Firmen-CEO, bei dem es Gelder in sechsstelliger Höhe zu erbeuten gibt. Ich bin doch nicht interessant genug!« Natürlich kann es auch Ihnen passieren: Wenn Sie, Ihre Freunde oder Familie das Spielzeug »CloudPets« nutzen, werden dabei Ihre Stimmen in die Cloud geschickt. Das heißt, die Sprachnachrichten, die Sie an Ihr Kind gesendet haben, werden auf Servern des Unternehmens Spiral Toy gespeichert und in einer Datenbank abgelegt. Hackt sich jemand in diese Datenbank ein, können Ihre Stimme und die Ihrer Freunde oder Familie ganz einfach gestohlen, manipuliert und für den oben beschriebenen Zweck missbraucht werden.

Und jetzt raten Sie mal, was der Firma Spiral Toy, die dieses nette Spielzeug herstellt, passiert ist. Laut dem US-Sicherheitsexperten Troy Hunt sind dem Unternehmen 2,2 Millionen aufgenommene »CloudPets«-Sprachnachrichten von rund 820.000 registrierten Anwendern abhandengekommen.⁷ Die Sprachnachrichten waren in einer Datenbank abgelegt worden, die keinen Schutz geboten hatte. Man konnte damit von außen darauf zugreifen. Die Sprachnachrichten der Benutzer waren zwar jeweils mit Passwörtern geschützt, aber diese lauteten oft »1234« oder »susi123«. Daher möchte ich Sie an dieser Stelle daran erinnern, auf jeden Fall sichere Passwörter zu verwenden – auch wenn Sie denken, dass es sich beim erworbenen Einhorn doch »nur um Kinderspielzeug« handelt. Durch schlecht gewählte Passwörter dauerte es in diesem Beispiel nur wenige Sekunden, bis eine Software

6 vgl. <https://futurezone.at/digital-life/mit-deepfake-die-stimme-vom-chef-imitiert-220000-euro-ergaunert/400597388>

7 vgl. <https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/>

diese geknackt hatte und auf die Benutzerkonten mitsamt den gespeicherten Sprachnachrichten Zugriff hatte.

Die betroffenen Nutzer wurden damals von der Firma Spiral Toy zudem nicht darüber informiert, dass ihre Stimmen und Sprachdateien offen im Netz verfügbar waren. Auch nicht darüber, dass diese Nachrichten jeder runterladen und anhören konnte, der dazu Lust hatte – oder diese missbrauchen wollte. Laut Hunt sei das Unternehmen von einem Sicherheitsforscher-Kollegen mehrfach auf das Problem aufmerksam gemacht worden, doch es hatte mehrere Wochen lang nicht reagiert. Dabei saß die Firma Spiral Toy in Kalifornien, USA – ebenso wie der Sicherheitsforscher. Man sollte meinen, dass hier eine Kommunikation miteinander möglich sein sollte. Laut Hunt wurden die betroffenen Sprachdateien in der Zwischenzeit sehr häufig heruntergeladen, denn die offene Datenbank war ein gefundenes Fressen für Kriminelle. Es wurden damit auch Erpressungsversuche durchgeführt, wie der Sicherheitsforscher berichtete. Erst viel später wurde seitens des Unternehmens reagiert und die Datenbank vom Netz genommen.

Zur Beruhigung: Tatsächlich ist bis jetzt kein Fall bekannt, bei dem es durch eine gestohlene und im Anschluss gefälschte Stimme zu einer Kindesentführung oder einem Einbruchdiebstahl gekommen ist. Aber der Fall »CloudPets« zeigt, dass Sie mit einem vermeintlich niedlichen und harmlosen Spielzeug Ihr Kind gefährden können und auch sich selbst. Ich wollte Ihnen hier vor allem die Möglichkeiten aufzeigen, an die Sie wahrscheinlich nicht denken, wenn Sie Ihrem Kind dieses süße Kuscheltier mit Internet-Verbindung kaufen. Und mit Erpressungsversuchen, weil Ihre Daten in einer ungeschützten Datenbank im Internet landen, würde wohl erst einmal niemand rechnen.

Es gab zudem bereits mehr als den einen geschilderten Fall, bei denen etwa Unternehmen abgezockt worden sind, weil jemand mit der gestohlenen, manipulierten Stimme des

Firmenchefs angerufen und um eine Überweisung auf ein bestimmtes Konto gebeten hat. Der Mitarbeiter glaubte, er telefoniere gerade mit dem Chef – und hinterfragte die Anweisung nicht, frei nach dem Motto »der Chef hat immer recht«. Genauso wenig würde Ihr Kind zweifeln, wenn es Ihre Stimme aus dem Einhorn hört, die sagt, es solle die Wohnungstür öffnen, weil Sie sich ausgesperrt haben – außer es hört Sie zeitgleich im Nebenzimmer.

Unpassende Werbung

Jetzt haben Sie genug von vernetzten Einhörnern? Leider muss ich Sie enttäuschen, denn die Geschichte von »Cloud-Pets« ist noch immer nicht zu Ende. Die Firma hat nämlich auch noch ein Geschäftsmodell rund um seine App entwickelt, die ganz gut zu den Dingen passt, die Sie in den vorherigen Kapiteln bereits erfahren haben, nämlich die Tatsache, dass Sie das Produkt nicht wirklich besitzen. Sie haben zwar das vernetzte Plüschhorn käuflich erworben, aber wenn Sie die App nutzen wollen, haben Sie bei »CloudPets« zwei Optionen: Entweder Sie verwenden die »Gratis«-Version, bei der Sie Werbeeinblendungen sehen, oder Sie zahlen Geld für ein werbefreies Produkt.

Ich habe mir die »Gratis«-Version der App ein wenig genauer angesehen und dabei festgestellt, dass die Werbung nicht nur im Eltern-Teil der App eingeblendet wird, sondern auch in dem Teil der App, die Ihrem Kind vorbehalten ist. Denn auch Kinder können vom selben Gerät oder ihrem eigenen Handy – je nachdem, ab welchem Alter sie damit ausgestattet werden – auf die App zugreifen und selbst Nachrichten an das Einhorn schicken. In der Nutzeroberfläche der App, die für das Kind freigegeben war, wurde mir nicht altersgerechte Werbung eingeblendet.

Ergo: Einmal sah ich, eingeloggt als Kind namens »Cayla« (die App fragte selbstverständlich auch Namen und Alter des

Kindes ab) eine Werbung für Alkohol, dann sah ich eine Werbung für eine bestimmte Aktie, ein andermal wurde mir eine Anzeige mit expliziten »Casual Dating«-Angeboten und viel nackter Haut angezeigt. Logisch, denken Sie sich. Wahrscheinlich treibt sich Frau Wimmer auch privat auf solchen Seiten herum und informiert sich laufend über eine Aktie nach der anderen. Doch bei den Anzeigen hat es sich nicht um personalisierte Werbeeinblendungen gehandelt, die nur für Erwachsene, die sich für diese Dinge interessieren mögen, gedacht sind, sondern explizit um Einblendungen im Menü für Kinder. Das heißt, auch Ihr Kind hätte diese Art von Werbung bei der Benutzung der Gratis-App zu Gesicht bekommen.

Na und, denken Sie? Aber wollen Sie wirklich, dass Ihr Kind bei der Benutzung einer Spielzeug-App vielleicht irrtümlich auf derartige Anzeigen draufklickt? Was wäre, wenn gleich die erste Kontaktperson nicht jugendfrei antwortet? Wollen Sie das noch immer?

Werbung mag Sie als Erwachsene vielleicht nicht immer und überall stören. Aber Apps, die für Kinder gedacht sind, sollten bereits von Beginn an werbefrei konzipiert sein. Und Unternehmen, die mit derartigen Methoden zusätzliches Geld verdienen wollen, haben niemals das Wohl von Kindern im Visier, sondern lediglich ihren eigenen Profit.

Ratschläge für Eltern

Was können Sie nun aus diesem schönen, langen Beispiel alles lernen? Sehr viel, würde ich sagen. Dieses Horror-Beispiel steht symptomatisch für viele der Probleme, die vernetztes Spielzeug mit sich bringt. Ein guter Rat für Eltern ist deshalb, sich bereits vor der Anschaffung eines neuen Spielzeugs darüber zu informieren, ob dieses mit dem Internet verbunden werden kann oder gar muss, um zu funktionieren.

STICHWORTVERZEICHNIS

A

Abhören 149
Abo-Modell 45
ADAC 126
Adtech 181
AGB 125, 178
Albrecht, Jan Philipp 241
Alexa 24, 129–130, 149
 Bestellungen 136
 Datenspeicherung 132
 Überwachung 134
Algorithmen
 Werbenetzwerke 176
Algorithmwatch 245
Allgemeinen Geschäftsbedingungen *siehe* AGB
Alternative
 datenschutzfreundliche 177
Always On 10
Amazon 27, 89, 129
Amazon Dash Replenishment Service 8
Amazon Echo 133
Amazon Prime 103
Amnesty International 171
Ampel 124
Anderson, Ross 22, 113, 120, 122, 239

ANDI 211
Android 169
Android Things 143
Anonymisierung 179
App 169
 vorinstallierte 169
App Store 169
Apple 156, 169
 Überwachung 159
Apple Watch 157
Apple-ID 157
App-Store 174
Arbeitskreis Vorratsdatenspeicherung 258
Arbeitsmarktchancen 244
Assistant 129
Austrian Standards 240
Auto 112
Autopilot 115

B

Baby-Cam 87
Barbie 84
Bauriedl, Sybille 214
Beckedahl, Markus 23, 132, 153
Behördenzugriff 146
Bertelsmann-Stiftung 245
Big Brother Award 23, 144
Big Brother Watch UK 133

Big Data 220
 Big-Tech 200
 Bühr, Peter 80, 91, 230, 246
 Bitkom 33
 Bloatware 170
 Bloody Health Collective 174
 Bluetooth 79, 201
 BMW i3 125
 Botnet 104
 Mirai 105
 Boykott
 unterstützen 235
 Bria, Francesca 221
 Brodnig, Ingrid 43
 BSI 102
 Bundeskartellamt 188
 Bundestrojaner 64
 Bürgerbeteiligung 223
 Bus
 selbstfahrender 234

C

Casino 102
 Caspar, Johannes 152
 Cayla 76
 CCC *siehe* Chaos Computer Club
 Cech, Florian 233
 CERT 7
 Chaos Communication Congress 26, 54
 Chaos Computer Club 66, 202
 Chiffrier-Tastatur 185
 China 64
 Christl, Wolfie 40, 181

Chrysler 113
 CIA 144
 Click Here to Kill Everybody 260
 Cloud 44
 CloudPets 69
 Common Voice 166
 Computer Emergency Response Team *siehe* CERT
 Connected Car 113
 Autopilot 115
 Lebensdauer 121
 Reparatur 121
 Unfall 115
 Contact Tracing 192
 Cookies 52
 Corona 191
 Russland 193
 Südkorea 193
 Tschechien 194
 Corona-App
 Fehlfunktionen 203
 Nutzen 205
 Sicherheitsstandard 198
 Coronavirus
 Übertragung 192
 Corona-Warn-App 201
 Privatsphäre 202
 Cortana 154
 Covid-19 191, 195
 Crowdfunding 44
 Cyberattacke 226
 Cyberkriminelle 52, 155
 Cybersecurity Act 238
 Cybersicherheitsgesetz 96
 Cybertrap 107

D**Daten**

sammeln 125

weitergeben 172

Wert 175

Datenhändler 52

Datenhoheit 143, 222

Datenlecks 19

Datenmissbrauch 55

Datennutzung

vor Gericht 147

Datensammelwut 177

Datensammlung 36

Datenschutz 15

Datenschutzbehörde 161

Irland 162

Datenschutzgrundverordnung 30, 63, 161–162, 183

Datenschutzkonformität 238

Datenschutzskandal 171

Datensensible 181

Datensparsamkeit 190

Datenspeicherung 132

Datenübertragung

unverschlüsselte 60

Datenverbindungen

unsichere 94

Datenverknüpfung 29

DDoS-Angriff 104

Decode 222

Deep Speech 167

Demokratie

fördern 237

Device Care 171

Diensthandy 207

Digitalcourage 259

Digitale Assistenzwanze 149

Digitale Gesellschaft 257

Digitaler Humanismus 233, 236

Digitalisierung 229

Drip 174

DSGVO *siehe* Datenschutzgrundverordnung

DynDNS 105

EEcho *siehe* Amazon Echo

Einhorn 78

Electronic Frontier Foundation 171

Eltern 77

Emberlight 44

epicenter.works 197

Eschbach, Andreas 109

Ethik der Algorithmen 245

EuGH *siehe* Europäischer Gerichtshof

Europäischer Gerichtshof 163

EU-Wettbewerbsbehörde 188

F

Facebook 18, 27

Prozess 163

Fahrassistentensystem 118

Fairfield, Joshua A.T. 46

Filesharing 61

Firmware 19

Fitbit 38, 40

Fitnessarmband 31

Foitik, Gerry 197

Forbrukerrådet 72, 183

Forgo, Nikolaus 206
 Forum Informationsfreiheit
 259
 Frauenberger, Christoph 223
 FREDI 89
 Freiwilligkeit 197, 206–207
 Full Self-Driving-Capability
 119
 Fußgängerampel 24

G

Gemeinwohlorientiert 246
 Geschäftsmodell 248
 Gesellschaft für Freiheits-
 rechte 256
 Gesichtserkennung 65, 194,
 216
 Gesundheitsdaten 31, 180
 Gewohnheiten 19
 GitHub 64
 Glühbirne 19, 53
 Google 27
 Google Assistant 151
 Google Home
 Standby 135
 Google Play Protect 170
 GPS 53, 193
 Greenberg, Andy 112
 Grindr 181
 Guardian 154
 Guidelines 232

H

Have I Been Pwned 96
 Herstellerhaftung 97
 Hessel, Stefan 82

HIV-Status 183
 Hmaidi, Antonia 217
 Hochwassererkennung 226
 Hue *siehe* Philips Hue
 Humanismus
 digitaler 236

I

Infrastruktur
 Sicherheit 225
 vernetzte 225
 Innovationsdruck 232
 Insecam 99
 Institut für Technikfolgenab-
 schätzung 123
 Internet of Things 14
 IoT-Geräte 14
 IoT-Gütesiegel 230
 ITS *siehe* Institut für Tech-
 nikfolgenabschätzung

J

Jeep Cherokee 113

K

Kaltheuner, Frederike 42
 Kamera 99
 Keen Security Labs 114
 Kernick, Phil 111
 Kind 79
 Kommunikationsapps 187
 Kontaktdaten 189
 Kosten-Nutzen-Analyse 215
 Krieger-Lamina, Jaro 123, 127
 Kühlschrank 7
 smart 100

L

Laimer, Christoph 214
 Lampe 20
 Laub, Iwona 197
 Le Bonniec, Thomas 159–
 160, 162
 Leith, Douglas 200
 Leutheusser-Schnarrenber-
 ger, Sabine 145
 LineageOS 186
 Lockdown 193
 Loosemore, Tom 199

M

McAfee 114
 Menstruations-App 172
 Mercedes 119
 Messenger-Apps 187
 Mi-Cam HD 98
 Microsoft 156
 Migräne 179
 Miller, Charlie 113
 Mirai 105
 Mitbestimmung der Bürger
 223
 Mitgestaltung 227
 Mobile Accessory Kit 143
 Mordprozess 146
 Mozilla 166
 Mozilla Foundation 42
 M-Sense 179
 Müller, Klaus 206
 Mydays 181

N

Nachhaltigkeitssiegel 230
 Neidhardt, Julia 235
 Nesbitt, Daniel 133

Nest 45
 Netzpolitischer Abend 257
 Neumann, Linus 202
 New Deal for Consumers 239
 Nicht-Regierungs-Organisa-
 tionen *siehe* NGO
 None of Your Business 162
 Notfallplan 9
 Notfall-Regelungen 195
 NOYB *siehe* None of Your Bu-
 siness
 NSA 144
 Nutzerprofile 140

O

O’Neil, Cathy 244
 ÖAMTC 126
 OEM 53, 97
 OK Cupid 181
 Open Data 222
 Open Knowledge Foundation
 174, 259
 Opt-Out 128
 Original Equipment Manu-
 facturer *siehe* OEM
 Ortungs-App 189
 Orwell, George 67
 Over-the-Air-Update 120

P

padeluun 145
 Pandemie
 Befugnisse 209
 Partizipations-Plattform 223
 Passwörter
 gute 95
 starke 57
 voreingestellt 100

PayPal 106
 Philips Hue 130
 Play Store 169
 Privacy by Default 154, 158
 Privacy International 23, 173
 Privacy Shield 163
 Private Gespräche 159
 Profiling 133, 140
 Project Alias 139
 Prototyping 224
 Public Shaming 216

Q

Qihoo 360 171
 Quintessenz 259

R

Real Time Voice Cloning 73
 Rebel City 221
 Rechtsdurchsetzung 241
 Recycling 212
 Regulierung 237
 Responsible Disclosure 123
 Ring 56
 Robert-Koch-Institut 191
 Roboterhund 48
 Rotes Kreuz 196
 Router 15

S

Safer Internet Day 86
 SaferInternet.at 86
 Samsung 171
 SAP 201
 Saubermacher 212
 Schmerold, Oliver 126
 Schneier, Bruce 22, 64, 97, 260

Schnittstelle
 Corona-App 199
 Schrems, Max 8, 162, 181, 258
 Schwarze Schafe 181
 SEC Consult 57
 Security 21, 227
 Security by Design 123
 Selbstfahrender Bus 234
 Sensible Daten 182
 Sensoren 229
 Server
 im Ausland 144
 Shenzhen Gwlltimes Technology 97
 Sicherheit 15
 Sicherheitsgurt 111
 Sicherheitslabel 90
 Sicherheitsstandards 111
 Sicherheitstipps 101
 Signal 187–188
 Signalwörter 134
 Siri 129, 156
 Auswertung deaktivieren 158
 Personenbezug 157
 unabsichtliche Aktivierung 156
 Skype 154
 Smart 247
 Smart City 211
 Barcelona 221
 China 216
 Deutschland 224
 Entwicklung 213
 Europa 217
 Kalifornien 215

Songdo City 221
 Wien 219
 Smart Home 52
 Smart Meter 25, 62
 Smart TV 250
 WLAN 251
 Smart Watch 31
 Smarte Ampeln 216, 219
 Smartphone
 Marktanteil 184
 Snips 231
 Snowden, Edward 26, 161,
 188, 194, 206
 Social-Credit 216
 Sonos 143
 Sony 47, 59
 Spielzeug 70
 Spiral Toy 69
 Sprachassistent
 Alternativen 166
 Verbreitung 165
 Spracherkennung 150
 Sprach-Snippets 152
 Stadtentwicklung 213
 Standard-Passwort 94
 Standortdaten 194
 Steckdose 19
 Steigerwald, Michael 45, 53,
 60
 Stimmabdruck 153
 Stimmbiometrie 153
 Stimmen manipulieren 72
 Stopp Corona App 196
 Straßenlampe 226
 Stromzähler 24

T

Tech for Good 246
 Telekommunikationsgesetz
 82
 Tesla Model S 114
 Tesla Model X 114
 Tinder 181
 Todesopfer 116
 Tracking 34
 Transkript 151
 Transparenz 220
 Trilemma 120
 Trustable Technology Mark
 230
 TU Wien 223, 233

U

Überwachung
 kommerzielle 52
 staatliche 61
 Überwachungskamera 17,
 87–88, 98
 Überwachungskapitalismus
 28, 41, 128
 Überwachungsstaat 198
 Überwachungstechnologien
 215
 Überwachungswerkzeuge
 195
 Universität Wien 206
 Use Case 214

V

Verbraucherzentrale 37, 164
 Verbraucherzentrale Bundes-
 verband 206

Verein für Konsumenten-
schutzhinformatiön 182
Verkehrsmanagement 219
Vernetzung 22
Versicherung 30
Viehböck, Stefan 58, 94
VKI *siehe* Verein für Konsu-
mentenschutzinformatiön
Volvo 119
Voreinstellungen 138
Vorratsdatenspeicherung
125, 153
Voßhoff, Andrea 132, 143
VPN-Dienst 185
Vtrust 53

W

Wanze 135
Wayca 231
Werbung
irreführende 117
nicht altersgerecht 76

personalisierte 141
Schwangerschaft 175
WhatsApp 65, 187
Whistleblower 154
Wikimedia Foundation 259
Winter, Susan J. 234
Wired 112
Wireshark 105
Wittpahl, Volker 186
WLAN-Netzwerk 19
Wohnbezirk 223
Wöhrl, Manfred 240

X

Xiaongmai 58

Z

Zahnbürste 28
Zuboff, Shoshana 27, 37
Zwei-Faktor-Authentifizie-
rung 57