# 4

# HEY, EINHORN: WIE UNS SPIELZEUG AUSSPIONIERT

Es ist weiß und kuschelig, hat rosa Pfoten, einen pfiffigen, 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, finsterer 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 »CloudPets« 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=lAOj0H5c6Yc*

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 Cyberkriminel-

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 runtergeladen, 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 »CloudPets« 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 Plüscheinhorn 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.