Vernetztes Kinderspielzeug

Datenrisiko in Kinderhand?

MARKTWÄCHTER
DIGITALE WELT

Untersuchung der Verbraucherzentralen

August 2018

verbraucherzentrale

Herausgeber
Verbraucherzentrale NRW e.V.
Mintropstr. 27
40215 Düsseldorf
Tel. (0211) 3809 0
Fax. (0211) 3809 172
marktwaechter@verbraucherzentrale.nrw

Text: Dr. Ricarda Moll, Lisa Scheibel, Miriam Rusch-Rodosthenous

Stand: Juni 2018

Vernetztes Kinderspielzeug

Datenrisiko in Kinderhand?

INHALT

1. Hintergrund

Auf dem deutschen wie internationalen Markt sind Spielzeuge für Kinder[1] verfügbar, die durch die Integration technischer Elemente neue Formen spielerischer Interaktivität ermöglichen sollen. Diese können durch zwei verschiedene technische Hardware-Elemente realisiert werden, die alleine oder in Kombination im Spielzeug integriert sein können.

1. Sensorik: Durch die Integration von Sensoren, Kameras oder Mikrofonen kann das betreffende Produkt Informationen aus der Umgebung registrieren. Unter Umständen können allein hierdurch interaktive Funktionen im Produkt realisiert werden.
2. Funkschnittstelle: Durch die Integration einer Funkschnittstelle[2] ist das Produkt zur Übertragung der aufgezeichneten Daten in der Lage. Diese Eigenschaft macht es zu einem *vernetzten Spielzeug*. Die Daten werden in der Regel via Bluetooth an ein mobiles Endgerät gesendet, wo die Weiterverarbeitung mit Hilfe einer installierten App stattfindet. Diese Weiterverarbeitung kann die Übertragung von Daten an Hersteller-Server beinhalten. Andere Produkte sind WLAN-fähig und können somit ohne den Zwischenschritt zum Endgerät Daten an externe Server senden.

Risiken für die Privatsphäre des Kindes können sich ergeben, sobald der Gegenstand vernetzt ist, d.h. über eine Funkschnittstelle verfügt, da hierdurch die Übertragung von Daten an Dritte möglich wird. Eine zusätzliche Ausstattung mit Sensoren kann zudem die Sensibilität der übertragenen Daten erhöhen.

Das vorliegende Papier gibt einen komprimierten Überblick über die betreffenden Produkte und damit verbundene potenzielle Problemfelder mit Bezug zu Datenschutz und Datensicherheit. Für den Marktüberblick (Abschnitt 2) wurde eine offene Online-Recherche durchgeführt.[3] In diese wurden auf dem deutschen Markt führende Online-Shops der Spielwarenbranche einerseits (z.B. *toysRus*, *mytoys.de*)[4] und der Technikbranche andererseits einbezogen (z.B. *Saturn*, *Mediamarkt*).[5] Für den Überblick über die mit der Nutzung verbundenen Problembereiche (Abschnitt 3) wurden Untersuchungen aus den letzten zwei Jahren hinzugezogen, die im Rahmen universitärer Forschung, privaten Prüfinstituten oder Verbraucherschutzorganisationen durchgeführt wurden.[6]

2. Marktüberblick

Vernetztes Spielzeug liegt im Trend: Auf der diesjährigen 69. internationalen Spielwarenmesse in Nürnberg wurden technisch ausgestattete Spielzeuge auf einer 400m^2 großen Aktionsfläche ausgestellt.[7] Das Marktforschungsinstitut *Juniper Research* prognostiziert dem Markt der vernetzten

[1] Kinderspielzeug ist abzugrenzen von Produkten, die zwar von Kindern (mit) genutzt werden, deren Zweck sich jedoch primär an die Bedürfnisse der Eltern richten, wie beispielsweise Baby-Assistenzsysteme (sog. *Babytech*) oder Kinder-GPS-Uhren. Beide werden in der Regel zur Überwachung des Kindes durch die Eltern verwendet. Kinderspielzeug hingegen betont die spielerische Aktivität durch das Kind als Hauptelement und -zweck des Produktes.

[2] In der Regel handelt es sich hierbei um Bluetooth oder WLAN, teilweise auch NFC oder RFID.

[3] Recherchezeitraum: 01.10. -30.11.2017; die Recherche wurde im Nachgang iterativ aktualisiert.

[4] VuMa Touchpoints (2018a).

[5] VuMa Touchpoints (2018b).

[6] Spielzeuge, die im Zuge dieser Studien auffällig wurden, wurden auch in den Überblick mit einbezogen, wenn sie nicht auf dem deutschen Markt verfügbar waren.

[7] https://www.spielwarenmesse.de/special/activity-area-tech2play/language/1/

Spielzeuge ein starkes Umsatzwachstum. Bis zum Jahr 2020 soll es auf 10 Milliarden Euro im Jahr steigen.[8]

Die Produkte des betreffenden Marktsegments lassen sich oberflächlich anhand ihrer optischen Erscheinung und ihrer Kernfunktionen unterscheiden (s. Tabelle 1 für einen Überblick). So gibt es zum Beispiel eine Reihe von *Figuren mit Spracherkennung*, deren Fokus auf der Kommunikation mit dem spielenden Kind liegt. Ein Beispiel hierfür ist die bekannt gewordene Puppe *MyFriendCayla*, die von der Bundesnetzagentur Anfang 2017 als unerlaubte Sendeanlage eingestuft wurde (s. Abschnitt 2.2). Daneben werden Spielzeuge angeboten, deren Hauptfunktion die ferngesteuerte Fortbewegung des Produkts ist (sog. *Remote Control Toys*). Hierunter fallen per App gesteuerte Autos (z.B. *Carrera GO plus*), aber auch Quadrokopter bzw. Drohnen (z.B. *Ryze Tello*).[9] Davon zu unterscheiden sind Spielzeuge, die die äußerliche Erscheinung eines Roboters haben und mit unterschiedlichen Spiel-Features ausgestattet sind, wie beispielsweise Gegenstände aufeinander stapeln (sogenannte *Robot Toys*). Der Spielzeugroboter *ANKI Cozmo* beispielsweise scannt mit Hilfe einer Kamera seine Umgebung, verfügt über eine eingebaute Gesichtserkennungs-Software und spielt mit den mitgelieferten Bauklötzen verschiedene interaktive Spiele.
Interaktive Lernspielzeuge können sich in ihrer Ausführung deutlich unterscheiden, gemeinsam haben sie die Absicht, eine (meist kognitive) Fähigkeit des Kindes zu fördern. In diese Kategorie fallen beispielsweise auch eigens für Kinder gestaltete Tablet Computer (Kindertablets), die zum Teil sowohl vernetzt als auch mit Sensoren ausgestattet sind (z.B. *Storio MAX 2.0*). Die Interaktivität des Spielzeugs kann auch ausschließlich über eingebaute Sensoren realisiert werden: So kommt die Produktgruppe der elektronischen Haustiere (sog. *Electronic Pets*), bei denen die Pflege des inszenierten Tiers im Vordergrund steht, in der Regel ganz ohne Vernetzung aus (z.B. *Hatchimals* von *Spin Master*).

Für die Beurteilung, ob ein Produkt ein potenzielles Risiko für die Sicherheit und Privatsphäre des Kindes darstellt, ist die Einteilung in derlei Produktkategorien jedoch nur bedingt zielführend, da es hinsichtlich ihres Vernetzungsgrads zum Teil große Unterschiede zwischen den Spielzeugen einer Produktkategorie geben kann. Anhand ihrer optischen Erscheinung ist nicht unbedingt auf den ersten Blick ersichtlich, über welche technischen Elemente die interaktiven Funktionen in das Spielzeug integriert sind. Zu dieser Unklarheit trägt darüber hinaus die Tatsachte bei, dass Produkte mit einer sehr unterschiedlichen Ausstattung an Hard- und Software oft gleichermaßen als *smart* vermarktet werden, zumal der Begriff nicht geschützt ist.

Insofern ist auch der Vernetzungsgrad des betreffenden Spielzeugs nicht unbedingt auf den ersten Blick ersichtlich. Diese Information ist jedoch von großer Relevanz, da sich durch die hiermit verbundene Datenübertragung andere Risiken ergeben, als es bei herkömmlichem Spielzeug der Fall ist. Im Folgenden werden vier Problembereiche geschildert, die mit der Datenübertragung im Kontext von vernetztem Spielzeug zusammenhängen.

[8] Juniper Research (2015), s. auch Bundesministerium für Justiz und Verbraucherschutz (BMJV, 2017).
[9] Die Nutzung von Drohnen durch Privatpersonen wirft eine Reihe von rechtlichen Fragen auf, die im Rahmen des vorliegenden Papiers nicht behandelt werden können.

Tabelle 1. Übersicht über verschiedene Produktgruppen im Marktsegment des vernetzten Spielzeugs.

Spielzeugkategorie	Beschreibung	Beispiele
Figuren mit Sprach-erkennung	Spielfiguren jeglicher Art, die in begrenztem Maße Dialoge mit dem Kind führen können oder anderweitig der Kommunikation dienen.	Hello Barbie (Mattell) My Friend Cayla (*Genesis*) My Friend Freddy (*Genesis*) iOue Robot (*Vivid*) Sphero Spiderman (*Sphero*)
Remote Control Toys	Im Vordergrund steht die ferngesteuerte Fortbewegung eines Fahrzeugs (Drohnen/Helikopter, Autos). Die Fernsteuerung kann mit einer App realisiert werden.	WowWee 15741 R.E.V. (*WowWee*) Carrera GO plus (*Carrera*) ANKI Overdrive (*ANKI*) Air Hogs (*Spin Master*) TobyRich Smartplane (*TobyRich*)
Robot Toys	Die Spielfigur nimmt die Gestalt eines Roboters an, der Roboter-typische Funktionen erfüllt (z.B. Gegenstände stapeln und transportieren).	ANKI Cozmo (*ANKI*) Sphero 2.0 - BB-8 "Star Wars" (*Sphero*) Silverlit Macrobot SL88045 (*Silverlit*) Hasbro Star Wars Droide (*Hasbro*)
Electronic Learning	Im Vordergrund steht die Förderung von Wissen und (kognitiven) Fähigkeiten des Kindes.	Interaktiver Globus (*Clementoni*) Storio MAX 2.0 (*VTech*)

3. Problempotenzial

Für die Nutzung eines vernetzten Spielzeugs müssen Eltern in der Regel persönliche Angaben über das Kind und sich selbst machen, beispielsweise im Zuge der Registrierung oder im Zuge der spielerischen Aktivitäten.[10] Zusätzlich entstehen je nach Produkt im Zuge der Nutzung weitere Daten, wie beispielsweise Gesprächsaufzeichnungen oder Fotos des Kindes, die Rückschlüsse auf das Kind zulassen. Die sich anschließende Frage in Bezug auf den Schutz und die Sicherheit der betreffenden Daten stellt sich im Kontext von vernetztem Spielzeug in einem besonderen Maße, da die primär betroffene Zielgruppe Kinder sind. Diese „verdienen bei ihren personenbezogenen Daten besonderen Schutz, da Kinder sich der betreffenden Risiken, Folgen und Garantien und ihrer Rechte bei der Verarbeitung personenbezogener Daten möglicherweise weniger bewusst sind“ (Erwägungsgrund 38 DS-GVO)[11]. Fälle im Frühwarnnetzwerk der Verbraucherzentralen[12] zeigen, dass gerade vernetzte Produkte für Kinder Unbehagen bei Verbrauchern in Bezug auf die damit verbundene Datenverarbeitung verursachen können. Die folgenden Problemfelder, die mit der Nutzung vernetzten Spielzeugs zusammenhängen, sollen einen Überblick über die besondere Verwundbarkeit geben, mit der Kindern den Risiken von mangelndem Datenschutz und mangelnder Datensicherheit gegenüberstehen.

Tabelle 2. Übersicht über vier potenzielle Problembereiche, die sich aus der Nutzung von vernetztem Spielzeug ergeben können.

Problempotenzial	Beschreibung
Physische Bedrohungen	Durch eine ungesicherte Bluetooth-Verbindung können auch fremde Personen Kontakt zum Kind aufnehmen.
Unerlaubtes Spionagegerät	Spielzeuge, die mit einem Mikrofon ausgestattet sind, können zum Abhören der häuslichen Umgebung missbraucht werden.
Profilbildung und Werbung	In Folge der Datensammlung kann dem Kind personalisierte Werbung angezeigt werden.
Identitätsdiebstahl	Durch unbefugten Zugriff auf die Daten des Kindes können Fremde die Identität des Kindes in unterschiedlichsten Kontexten vortäuschen.

3.1 Physische Bedrohungen

Gelangen Daten eines Kindes wie Name, Adresse oder Standort in die falschen Hände, kann dies im schlimmsten Fall zu unangemessener Kontaktaufnahme und Übergriffen durch Fremde führen.[13] Zahlreiche Produkte im Marktsegment vernetztes Spielzeug weisen erwiesenermaßen Sicherheitslücken auf, die derlei Risiken beinhalten. Insbesondere betroffen davon sind Produkte, die über eine Bluetooth-Schnittstelle verfügen, mit der sie eine Verbindung zu einem mobilen Endgerät herstellen.

[10] BeeSecure (2017).

[11] EU-Datenschutzgrundverordnung. Diese EU-Gesetzgebung ist seit dem 25.05.2018 anwendbar und betrifft den Umgang mit personenbezogenen Daten von EU-Bürgern.

[12] Das Frühwarnnetzwerk ist Teil der Marktbeobachtung, die im Projekt Marktwächter Digitale Welt durchgeführt wird. Besonders auffällige Verbraucherbeschwerden werden in einer neuen, zentralen Datenbank erfasst und von den Marktwächter-Experten kontinuierlich ausgewertet.

[13] Nelson (2016).

Die Ergebnisse verschiedener technischer Analysen zeigen, dass diese Bluetooth-Verbindung in der Regel nicht ausreichend abgesichert ist. So fehlen oft Authentifizierungsmechanismen: Will sich ein Smartphone mit dem Spielzeug verbinden, ist hierfür in vielen Fällen die Eingabe eines Passwortes oder Pin Codes nicht erforderlich. Wenn die Verbindung des eigentlich autorisierten Endgeräts unterbrochen ist, zum Beispiel bei ausgeschaltetem Smartphone oder zu großer Distanz zum Spielzeug, kann sich eine fremde Person ohne Eingabe eines Passwortes Zugriff auf das Spielzeug verschaffen. Eine ungesicherte Bluetooth-Verbindung durch mangelnde Authentifizierungsmechanismen wurde bei einer Reihe von vernetzten Spielzeugen festgestellt, darunter: *iQue Robot*[14] und *MyFriendCayla*[15] der Firma *Genesis*, *Spiral Toys' Cloudpets*[16], *Furby*[17], *MyFriendFreddy*[18], *Teksta Touka* (ein sprechender Spielzeugpapagei)[19], *WowWee Chip* oder dem *BB-8-Droiden*[20].

Sofern das Spielzeug über ein Mikrofon und einen Lautsprecher verfügt, kann es in der Folge unbemerkt als Bluetooth-Headset genutzt werden: Eine fremde Person, die sich innerhalb einer Distanz von – im Fall der bekannt gewordenen Puppe *Cayla* – bis zu zehn Metern zum Spielzeug befindet, könnte sich mit dem Spielzeug des Kindes per Bluetooth verbinden und sowohl mithören als auch mit dem Kind sprechen.[21] Unter Umständen ist dies auch möglich, wenn sich der potenzielle Angreifer außerhalb des Gebäudes befindet.[22] Die sich daraus ergebenden physischen Risiken liegen nahe: Ein Fremder, der auf der Straße steht und sich via Bluetooth mit dem Kind in Verbindung setzt, kann Urlaubspläne der Familie in Erfahrung bringen, die Anwesenheit der Eltern erfragen und das Kind überreden, ihm die Tür zu öffnen.

3.2 Verstecktes Spionagegerät

Eng verbunden mit der in Abschnitt 3.1 beschriebenen Problematik ist die Tatsache, dass vernetzte Spielzeuge, die mit einem Mikrofon ausgestattet sind, zum (unbemerkten) Abhören der häuslichen Umgebung genutzt werden können – auch wenn hiermit keine direkte physische Bedrohung für das Kind verbunden ist.

Verschärft wird dieser Sachverhalt bei Produkten, bei denen Kind und Eltern nur eingeschränkt Kontrolle darüber haben, *wann* das Gerät Gespräche aufzeichnet und überträgt. Dieses Problem entsteht auch in Zusammenhang mit anderen vernetzten Gegenständen wie Digitalen Sprachassistenten. Hier hatte eine Untersuchung des Marktwächters Digitale Welt gezeigt, dass die untersuchten Geräte auch Gespräche mitschneiden, wenn das hierfür notwendige Signalwort in abgewandelter Form genannt wird.[23]

[14] Forbruker Rådet (2017); Laughlin (2017); Stiftung Warentest (2017).
[15] Forbruker Rådet (2017); Munro (2015); Stiftung Warentest (2017).
[16] Laughlin (2017).
[17] Laughlin (2017).
[18] https://www.daserste.de/information/wirtschaft-boerse/plusminus/sendung/datenkraken-102.html
[19] Munro (2017).
[20] Lewis & Migliano (2017).
[21] Forbruker Rådet (2017, S. 31); Hessel (2016, S. 2).
[22] Hessel (2016, S. 2).
[23] Moll, Scheibel & Rusch-Rodosthenous (2017).

Im Fall der Puppe *Cayla* sollte das Leuchten ihrer Halskette anzeigen, dass das Mikrofon aktiv ist. Allerdings war diese Funktion nicht immer verlässlich, da sie entweder Geräte-abhängig von vornherein nicht funktionierte oder innerhalb der App ausgeschaltet werden konnte.[24]

Da die Aufzeichnungen der Puppe *Cayla* zusätzlich über die auf dem Endgerät installierte App an externe Server weitergeleitet wurden, stufte die Bundesnetzagentur (BNetzA) das Produkt im Februar 2016 als unerlaubte Sendeanlage ein[25] – also als verstecktes Spionagegerät.[26] Eltern, die die Puppe nach diesem Verbot nicht unschädlich machten, hätten sich strafbar machen können, da der Besitz derlei versteckter Spionagegeräte in Deutschland verboten ist. Auch wenn die BNetzA in diesem Fall nicht gegen Eltern vorging, kann der Besitz eines als unerlaubte Sendeanlage eingestuften Geräts prinzipiell mit Geld- oder Freiheitsstrafen sanktioniert werden.[27] Die Rückerstattung des Kaufpreises für Verbraucher gestaltet sich mitunter als schwierig – ein Problem, dass auch an den Marktwächter im Rahmen des Frühwarnnetzwerkes herangetragen wurde.

Nicht alle vernetzten Spielzeuge, die mit einem Mikrofon ausgestattet sind, erfüllen notwendigerweise den Tatbestand der unerlaubten Sendeanlage. Beispiele hierfür sind *Sphero's Spiderman* und *Cognitoys*[28]. Beide Spielzeuge zeichnen Sprache auf und sind zur Spracherkennung in der Lage. Bei diesen Produkten muss allerdings ein Knopf betätigt werden, um das Mikrofon zu aktivieren. Eltern und ihre Kinder haben somit mehr Kontrolle über die Aufnahmeaktivität und Datenverarbeitungs-prozesse des Spielzeugs.

3.3 Profilerstellung und Werbung

Selbst wenn keine vor dem Gesetz kriminellen Handlungen Grund für die entstehenden Bedrohungen sind, ist die Preisgabe von Daten über das Kind risikoreich. Denn die Daten können vom Hersteller oder Drittparteien, denen der Hersteller Zugriff auf die Daten gewährt, zur Profilbildung über das Kind genutzt werden. Das Profil kann in der Folge die Basis für auf das Kind zugeschnittene Werbung sein. Diese kann dem Kind auf Webseiten, in anderen Apps und mit Hilfe von Cross-Device-Tracking sogar auf anderen Geräten angezeigt werden.[29]

Dieses auch für Erwachsene existierende Problem der Profilbildung spitzt sich im Kontext des vernetzten Spielens durch Kinder aus mindestens zwei Gründen zu:

Erstens können im kindlichen Spiel expliziter als üblicherweise Informationen wie Wünsche, Träume und Fantasien offenbar werden. Werden diese von Mikrofonen und Sensoren aufgezeichnet und weitergegeben, lassen sich hierdurch besonders intime Einblicke in die Persönlichkeit des Kindes gewinnen. Dies ist insbesondere der Fall, wenn der Spielgegenstand getarnt ist als herkömmliches Spielzeug wie eine Puppe, bei der das Kind nicht damit rechnet, dass seine Gespräche „belauscht" werden. Werden diese Informationen für kommerzielle Zwecke wie Werbung genutzt, sind dem Ausmaß der Personalisierung nur noch wenige Grenzen gesetzt.

Zweitens lassen sich Kinder durch diese personalisierte Werbung besonders leicht beeinflussen, beispielsweise weil sie Werbung nicht in ähnlicher Weise als solche einordnen und bewerten können

[24] Hessel (2016); s. auch Forbruker Rådet (2017).
[25] nach § 90 TKG (Telekommunikationsgesetz).
[26] BNetzA (2017); Die Fragestellung, welche pädagogischen bzw. innerfamiliären Dynamiken die Möglichkeit der permanenten Überwachung des Kindes durch seine Eltern zur Folge hat, wird im vorliegenden Papier nicht behandelt.
[27] § 148 Abs. 1 Nr. 2 TKG; vgl. Hessel (2016, S. 5).
[28] S. z.B. Lewis & Migliano, (2017).
[29] Forbruker Rådet (2016, S. 22).

wie Erwachsene.[30] Selbst Jugendlichen, die auf Webseiten zwar klassische Werbung erkennen, fällt es schwer, als Artikel getarnte Werbung als solche zu identifizieren.[31] Aufgrund der Vulnerabilität dieser Verbrauchergruppe verschärft die DSGVO den Schutz personenbezogener Daten von Kindern insbesondere im Kontext der Profilbildung und Werbung (Erwägungsgrund 38).

Zusätzlich stellt sich auch in Bezug auf den Problembereich der Profilbildung und Werbung die Frage, inwieweit Eltern vor Kauf des Spielzeugs darauf aufmerksam werden können, wenn Anbieter sich das Recht vorbehalten, die Daten des Kindes zu kommerziellen Zwecken zu nutzen. Zum Umgang mit den erhobenen personenbezogenen Daten müssen Anbieter zwar in den Allgemeinen Geschäftsbedingungen (AGB) und/oder den Datenschutzerklärungen informieren, diese werden Eltern in der Regel jedoch erst präsentiert, wenn sie die App nutzen wollen, die für die Verwendung der Kernfunktionen des Spielzeugs erforderlich ist. Zusätzlich sind die in den Datenschutzerklärungen festgehaltenen Informationen oft schwierig geschrieben oder enthalten vage Formulierungen, was das Verstehen der tatsächlichen Inhalte zu einer zeitaufwändigen Herausforderung macht.[32] Fraglich ist zudem, inwieweit die in den AGB und Datenschutzerklärungen enthaltenen Informationen für eine realistische Risikoeinschätzung ausreichen.

3.4 Identitätsdiebstahl

Bei Identitätsdiebstählen nutzen Fremde die personenbezogenen Daten von Verbrauchern dazu, deren Identität vorzutäuschen. Diese kann in sämtlichen Bereichen des Internets für ganz verschiedene Aktivitäten missbraucht werden.[33] Im Frühwarnnetzwerk der Verbraucherzentralen finden sich hierzu zahlreiche Beschwerden. In der Regel werden mit Hilfe der Verbraucherdaten Bestellungen getätigt, Abonnements gebucht oder Verträge abgeschlossen. Verbraucher selbst erfahren davon in der Regel erst durch Zahlungsaufforderungen oder Inkasso-Schreiben.

Identitätsdiebstahl ist insofern vor allem in Zusammenhang mit erwachsenen Verbrauchern ein bekanntes Problem. Gerade in Zusammenhang mit der kindlichen Identität verschärft sich das damit verbundene Risiko jedoch in besonderem Maße. Beispielsweise sind Daten von Kindern besonders attraktiv für Identitätsdiebstähle, weil ihre gestohlenen Daten für längere Zeit unbemerkt benutzt werden können, als dies bei Erwachsenen der Fall ist.[34] Die Identität des Kindes kann darüber hinaus dazu genutzt werden, um Kontakt mit anderen Kindern aufzunehmen, beispielsweise über Soziale Medien oder sogar in eigens für Kinder geschützten Räumen. *Ob* die Identität des Kindes missbraucht wurde, bekommen Eltern im Zweifelsfall nicht mit.

Die Voraussetzung für einen Diebstahl der Identität des Kindes ist, dass ausreichend personenbezogene Daten über das Kind in fremde Hände geraten, sodass die entsprechende Identität vorgetäuscht werden kann. Dies kann beispielsweise passieren, wenn Daten von Hersteller-Servern gestohlen werden. Im Kontext von vernetztem Spielzeug sind bislang zwei Fälle bekannt, in denen Daten gestohlen wurden, die Hersteller von vernetztem Spielzeug über ihre Kunden gespeichert hatten: Im November 2015 wurde bekannt, dass massenhaft Daten von Servern der chinesischen Firma *VTech*, die Technik-Gadgets für Kinder wie Tablets herstellt, gestohlen wurden. Die gestohlenen

[30] z.B. https://www.mediasmart.de/verein/medienpaedagogik/kinder-und-werbung/
[31] Wineburg et al. (2016).
[32] Z.B. Moll et al. (2017).
[33] https://ssl.marktwaechter.de/pressemeldung/identitaetsdiebstahl-der-digitalen-welt-weit-verbreitethttps://ssl.marktwaechter.de/pressemeldung/identitaetsdiebstahl-der-digitalen-welt-weit-verbreitet
[34] Nelson (2016).

Daten beinhalteten verschiedene sensible Informationen über das Kind wie seinen Namen, Geschlecht, Geburtstag und Fotos.[35] Zum anderen waren auch Informationen über die Eltern verfügbar, darunter Namen, E-Mail-Adressen, Passwörter und physische Adressen. Als besonders brisant wurde bewertet, dass es möglich war, die Informationen zum Kind mit den Eltern-Daten zu verbinden, sodass die vollständige Identität des Kindes offenbart wurde.[36] Betroffen von dem Datendiebstahl waren fast fünf Millionen Eltern sowie 200.000 Kinder. Damit wurde der *VTech*-Hack der viertgrößte bekannt gewordene Datendiebstahl überhaupt.

Im Februar 2017 wurde darüber hinaus bekannt, dass über zwei Millionen Sprachaufzeichnungen, die mit den *CloudPets* der Firma *Spiral Toys* aufgenommen worden waren, offen im Netz verfügbar waren. Die Datenbank, in der die Daten gespeichert waren, war noch nicht einmal durch ein Passwort geschützt und konnte somit von jedem eingesehen werden.[37] So hätten Fremde auf die Daten zugreifen können, was bereits in mehreren Fällen zu Lösegeldforderungen gegenüber den betroffenen Eltern geführt hat. Der Hersteller war auf die Lücke mehrfach aufmerksam gemacht worden, ohne eine Reaktion zu zeigen.

[35] Hunt (2015).

[36] Im Falle des *VTech*-Hacks hatte der verantwortliche Hacker angegeben, selbst die Daten nicht veröffentlichen zu wollen, es sei jedoch möglich, dass jemand anders die Sicherheitslücke zuvor schon ausgenutzt habe; Franceschi-Bicchierai (2015).

[37] Hunt (2017).

4. Zusammenfassung und Ausblick

Das vorliegende Papier beschreibt neben einem kurzen Marktüberblick verschiedene Problemfelder, die mit der Nutzung von vernetztem Spielzeug durch Kinder und ihre Eltern verbunden sind. Neben physischen Bedrohungen als Folge einer ungesicherten Bluetooth-Verbindung können einige Spielzeuge als unerlaubte Sendeanlage genutzt werden; die personenbezogenen Daten von Kindern und ihren Eltern können außerdem Identitätsdiebstählen zum Opfer fallen oder zur Profilbildung und personalisierter Werbung genutzt werden. Über die beschriebenen Risiken hinaus existieren eine Fülle weiterer Probleme im Kontext des vernetzten Spielens, wie beispielsweise zusätzlich entstehende Kosten durch In-App-Käufe oder die Bereitstellung von Updates für Firm- und Software, die die Sicherheit der im Zuge der Nutzung generierten Daten langfristig garantieren.

Auch wenn in Deutschland die öffentliche und politische[38] Meinung zu vernetzten Spielzeugen – insbesondere nach dem Verbot der Puppe *Cayla* durch die BNetzA – möglicherweise skeptischer ist als im inner- und außereuropäischen Ausland und die Produktauswahl derzeit entsprechend geringer ist, bleibt das vernetzte Spielzeug auch hier ein relevantes Thema. So ist es ohne weiteres möglich, ein vernetztes Spielzeug zu produzieren, das zwar nicht als unerlaubte Sendeanlage genutzt werden kann, jedoch einen oder mehrere der anderen geschilderten Problembereiche betrifft.

Die geschilderten Probleme und Produktbeispiele sollten nicht zu dem Schluss führen, dass es nicht möglich ist, ein vernetztes Spielzeug zu nutzen, ohne dass derlei Risiken entstehen. So könnten Bluetooth-Verbindungen durchaus abgesichert werden; ebenso kann ein vernetztes Spielzeug ohne die Übertragung personenbezogener Daten auskommen. So wurden beispielsweise bei der Entwicklung eines Spielzeugroboters Datenschutz- und Datensicherheitsaspekte offensichtlich berücksichtigt. Der Roboter verarbeitet die erhobenen Daten lokal und schickt auf Wunsch des Nutzers keine personenbezogenen Daten wie den Namen des Nutzers an den Hersteller.[39] Zusätzlich nutzt der Roboter für die Verbindung mit dem Endgerät des Nutzers WLAN; das Endgerät kann sich bei aktiver WLAN-Verbindung mit dem Roboter nicht gleichzeitig auch mit externen Servern verbinden.

Die geschilderten Risiken sind prinzipiell auch in anderen Kontexten und für Verbraucher im Erwachsenenalter relevant, sie sind jedoch besonders brisant in Zusammenhang mit Kindern als besonders schützenswerte Verbrauchergruppe. Den Risiken in Zusammenhang mit Datenschutz und Datensicherheit sind Kinder zu immer früheren Zeitpunkten in ihrem Leben ausgesetzt: Bereits Säuglinge stehen im Fokus von neuen vernetzten Angeboten, die Eltern den Alltag und die Pflege des Kindes erleichtern sollen – zum Beispiel in Form von Puls messenden Babysöckchen, Bluetooth-Thermometern oder Windel-Voll-Alarm-Sensoren. Die sich stetig erweiternde Produktwelt bleibt somit Bestandteil der kontinuierlichen Marktbeobachtung des Marktwächters Digitale Welt.

[38] Z.B. Deutscher Bundestag (2016); Landtag NRW (2017).

[39] Bundesamt für Sicherheit in der Informationstechnik (BSI, 2018). Das betreffende Gutachten ist im Rahmen einer Zusammenarbeit zwischen dem BSI und der Verbraucherzentrale NRW entstanden (Memorandum of Understanding zur Förderung der Informationssicherheit von Verbraucherinnen und Verbrauchern vom 01.03.2017).

Quellen

BeeSecure (2017). Smart Toys – Multiple Facetten, multiple Risiken. Abgerufen von https://www.bee-secure.lu/sites/default/files/publications/Article%20Jouets%20connect%C3%A9s-DE.pdf [Stand: 05.06.2018]

BNetzA (2017). Bundesnetzagentur zieht Kinderpuppe „Cayla“ aus dem Verkehr. Abgerufen von https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/DE/2017/14012017_cayla.html [Stand: 30.05.2018]

BMJV (2017). Faktenblatt – Smartes Spielzeug. Abgerufen von http://www.bmjv.de/SharedDocs/Downloads/DE/PDF/Berichte/Faktenblatt_Smartes-Spielzeug.html [Stand: 06.06.2018]

BMJV (2017). Smart Toys – Worauf Verbraucherinnen und Verbraucher achten sollten. Abgerufen von http://www.bmjv.de/SharedDocs/Artikel/DE/2017/121117_Smart_Toys.html [Stand: 06.06.2018]

BSI (2018). Untersuchungsbericht Spielzeugroboter Anki Cozmo.

Deutscher Bundestag (2016). Drucksache 18/8015 - Kleine Anfrage Fraktion BÜNDNIS 90/DIE GRÜNEN: Abhörpuppen – Datenschutz im Kinderzimmer. Abgerufen von http://dip21.bundestag.de/dip21/btd/18/080/1808015.pdf [Stand: 06.06.2018]

Forbruker Rådet (2016). #Toyfail – An analysis of consumer and privacy issues in three internet-connected toys. Abgerufen von https://fil.forbrukerradet.no/wp-content/uploads/2016/12/toyfail-report-desember2016.pdf [Stand: 05.06.2018]

Franceschi-Bicchierai, L. (2015). One of the largest hacks yet exposes data on hundreds of thousands of kids. Abgerufen von https://motherboard.vice.com/en_us/article/yp3z5v/one-of-the-largest-hacks-yet-exposes-data-on-hundreds-of-thousands-of-kids

Hessel, S. (2016). „My friend Cayla“ – eine nach §90 TKG verbotene Sendeanlage? Abgerufen von http://www.jurpc.de/jurpc/show?id=20170013 [Stand: 05.06.2018]

Hunt, T. (2015). When children are breached – inside the massive VTech hack. Abgerufen von https://www.troyhunt.com/when-children-are-breached-inside/ [05.06.2018]

Hunt, T. (2017). Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages. Abgerufen von https://www.troyhunt.com/data-from-connected-cloudpets-teddy-bears-leaked-and-ransomed-exposing-kids-voice-messages/ [Stand: 05.06.2018]

Juniper Research (2015). Smart Toys - Do toys dream of digital lives? Abgerufen von https://www.juniperresearch.com/press/press-releases/smart-toy-revenues-to-hit-%242-8bn-this-year [Stand: 06.06.2018]

Landtag NRW (2017). Drucksache 17/1402 - Antwort der Landesregierung auf die Kleine Anfrage 482 vom 2. November 2017 BÜNDNIS 90/DIE GRÜNEN - Von Roboflop zum Trojanerteddy – Smart Toys in NRW-Kinderzimmern (Drucksache 17/1072). Abgerufen von https://www.landtag.nrw.de/portal/WWW/dokumentenarchiv/Dokument/ MMD17-1402.pdf [Stand: 06.06.2018]

Laughlin, A. (2017). Safety alert: see how easy it is for almost anyone to hack your child’s connected

toys. Abgerufen von https://www.which.co.uk/news/2017/11/safety-alert-see-how-easy-it-is-for-almost-anyone-to-hack-your-childs-connected-toys/ [Stand: 30.05.2018]

Lewis & Miglano (2017). Assessment of the privacy and security of Smart Toys marketed to children. Abgerufen von https://www.top10vpn.com/wp-content/uploads/2018/02/Top10VPN-smart-toys-safety-report.pdf [Stand: 05.06.2018]

Moll, R., Scheibel, L. & Rusch-Rodosthenous, M. (2017). Amazon Alexa: Wann ist der Sprachassistent ganz Ohr? Ein Reaktions-Check. Verbraucherzentrale NRW e.V. (Hrsg.). Abgerufen von https://ssl.marktwaechter.de/sites/default/files/downloads/kurzbericht_amazon_alexa.pdf

Moll, R., Schulze, A., Rusch-Rodosthenous, M., Kunke, C., & Scheibel, L. (2017). Wearables, Fitness-Apps und der Datenschutz: Alles unter Kontrolle?. Verbraucherzentrale NRW e.V. (Hrsg.). Abgerufen von http://www.marktwaechter.de/digitale-welt/marktbeobachtung/wearables-und-fitness-apps

Munro, K. (2015). Making children's toys swear. Abgerufen von https://www.pentestpartners.com/security-blog/making-childrens-toys-swear/ [Stand: 29.05.2018]

Munro, K. (2017). Hacking a talking toy parrot. Abgerufen von https://www.pentestpartners.com/security-blog/hacking-a-talking-toy-parrot/ [Stand: 29.05.2018]

Stiftung Warentest (2017). Smart Toys: Wie vernetzte Spielkameraden Kinder aushorchen Abgerufen von https://www.test.de/Smart-Toys-Wie-vernetzte-Spielkameraden-Kinder-aushorchen-5221688-0/ [Stand: 05.06.2018]

VuMa Touchpoints (2018a). Ranking der beliebtesten Kauforte für Spielzeug und Spiele (Einkauf in den letzten 12 Monaten) in Deutschland in den Jahren 2014 bis 2017. https://de.statista.com/statistik/daten/studie/171501/umfrage/kauforte-fuer-spielzeug/

VuMa Touchpoints (2018). Ranking der beliebtesten technischen Kaufhäuser/Fachmärkte (Einkauf in den letzten 6 Monaten) in Deutschland in den Jahren 2014 bis 2017. Abgerufen von https://de.statista.com/statistik/daten/studie/171498/umfrage/in-den-letzten-6-monaten-besuchte-technische-fachmaerkte/

Wineburg, S., McGrew, S., Breakstone, J., & Ortega, T. (2016). Evaluating information: The cornerstone civic online reasoning. Stanford Digital Repository. Abgerufen von http://purl.stanford.edu/fv751yt5934 [Stand: 05.06.2018]