Deutscher Bundestag **Drucksache 19/10090**

19. Wahlperiode 13.05.2019

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Renate Künast, Tabea Rößner, Dr. Konstantin von Notz, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 19/9456 –

Datenschutz im Kinderzimmer – Digitales und vernetztes Spielzeug

Vorbemerkung der Fragesteller

„Intelligentes“, mit dem Internet verbundenes Spielzeug, sogenannte Smart Toys wie digitalisierte Roboter, Uhren, Teddybären oder Puppen sind mittlerweile weit verbreitet – auch auf dem bundesdeutschen Markt. Diese technischen Geräte können zum Teil sensorgesteuert selbständig auf Handlungen von Kindern reagieren.

Diese technischen Geräte werfen zahlreiche, ganz unterschiedlich gelagerte Rechtsfragen in den verschiedensten Rechtsbereichen auf, beispielsweise im Recht der IT-Sicherheit, im Verbraucherschutz- und Datenschutzrecht sowie im Haftungsrecht (vgl. etwa Hornung, VuR 2018, S. 41). Sogenannte Smart Toys zählen zu den Geräten des „Internet of Things“ (IoT) und teilen insoweit zahlreiche mit der IKT-Entwicklung sowie u. a. der Thematik „Smart Homes“ verbundene Fragen. Aufgrund der besonderen Verletzlichkeit von Kindern und der spezifischen grundrechtlichen Schutzanforderungen für Kinder stellen sich darüber hinaus noch deutlich weitergehende Fragen.

Als mit dem Internet verbundene Systeme können internetgestützte Sprachassistenzsysteme in gewissem Umfang Fragen der Kinder beantworten, manche ermöglichen ein ständiges Tracking des Aufenthaltsortes von Kindern. Zahlreiche Geräte erfassen alle Geräusche, Stimmen und Unterhaltungen in ihrer Umgebung, speichern diese und senden sie zur Analyse an zentrale, oft im Ausland liegende Server. Inwieweit es zur weiteren Verarbeitung und Auswertungen der erfassten Kommunikationen kommt, bleibt oftmals unklar.

Wiederholt wurden gravierende Sicherheitslücken bei entsprechenden Geräten festgestellt, die sich mit geringstem Aufwand von außen übernehmen und zu Missbrauchszwecken wie z. B. Identitätsdiebstahl einsetzen ließen (vgl. etwa Marktwächter VZBV NRW, www.marktwaechter.de/pressemeldung/kein-kinderspiel-vernetztes-spielzeug-birgt-risiken).

Klein- und Kleinstkinder werden mit digitalem Spielzeug ab den ersten Monaten ihres Lebens der Möglichkeit ständiger Erfassung und Beobachtung, auch durch unbefugte Dritte, unterworfen. Manipulative Zugriffe von außen im besonders geschützten Wohn- und Lebensbereich können das Recht auf Privatheit

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern, für Bau und Heimat vom 9. Mai 2019 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

und Unverletzlichkeit der Wohnung aushöhlen. Von ihrer IT-Sicherheit dürftig bis überhaupt nicht abgesicherte Massenprodukte können von außen leicht übernommen werden: damit kann die Ausspähung und Manipulation des privaten Wohnumfelds zum Kinderspiel werden. Je nach Produkt können nach Ansicht der Fragesteller Unbefugte über die Geräte Kommunikation von außen mit den Kindern aufnehmen. Auch unbeteiligte Dritte können dabei in ihren Grundrechten verletzt werden. Damit sind auch grundlegende Fragen des Rechts auf Integrität und Unverletzlichkeit informationstechnischer Systeme aufgeworfen.

Die Risiken dieser digitalisierten Spielzeuge für die Rechte aller davon Betroffenen, insbesondere aber der Kinder, sind zahlreich und gravierend. Den Staat trifft mit Blick auf die Persönlichkeitsentwicklung von Kindern und deren Persönlichkeitsrechte, aber auch mit Blick auf die Voraussetzungen einer demokratischen und rechtsstaatlich verfassten Gesellschaft eine umfassende Schutzpflicht.

Der Deutsche Bundestag hat sich bereits im März 2016 erstmalig aufgrund einer Kleinen Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN mit sogenannten Smart Toys und speziell der Puppe Cayla befasst (vgl. Bundestagsdrucksache 18/8317).

Spätestens mit dem Anfang 2017 nach § 90 des Telekommunikationsgesetzes ausgesprochenen Verbot der Spielzeugpuppe Cayla als unbefugte Sendeanlage sowie dem Verbot weiterer Produkte aus diesem Bereich durch die Bundesnetzagentur sind die Risiken „intelligenter“ Spielzeuge einer breiteren Öffentlichkeit bekannt geworden.

Die Digitalisierung macht vor den Kindern aller Altersgruppen insgesamt nicht halt, im Gegenteil. Kinder haben oftmals Zugang zu und nutzen in rasant zunehmendem Umfang Smartphones und andere digitale Geräte wie z. B. digitale Sprachassistenzsysteme. Ob und inwieweit die Bundesregierung sich zu dieser Entwicklung konstruktiv und problemangemessen verhält und ihrer Schutzverantwortung angemessen gerecht wird, ist insoweit von großer gesellschaftlicher Bedeutung.

Die Bundesregierung will sich zwar nach eigenen Angaben dafür einsetzen, auf Basis der Aktualisierung des EU Cybersecurity Acts (CSA) verpflichtende Mindestsicherheitsstandards für loT-Geräte zu etablieren (vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN zur Sicherheit und Konformität von loT-Geräten, Bundestagsdrucksache 19/9132, S. 3). Im aktuellen Trilog-Ergebnis zum CSA (vgl. http://data.consilium.europa.eu/doc/document/ST-15786-2018-INIT/en/pdf) werden mit Unterstützung der Bundesregierung nun allerdings nur freiwillige Zertifizierungen in Eigenregie der Hersteller nach vertikalen Zertifikationsschemata und mit selbst verliehenen Sicherheitssiegeln in Aussicht gestellt ohne Angabe von Sanktionsmaßnahmen bei Verstößen oder gar Haftungsregeln. Auch die Frage, inwieweit es im Zuge der Vorlage des „IT-Sicherheitsgesetzes 2.0“ der Bundesregierung zu verpflichtenden Mindeststandards und neuen Haftungsregelungen kommt, ist derzeit noch offen.

1. Verfügen die Bundesregierung und die ihr nachgeordneten Behörden inzwischen über aktualisierte Ergebnisse der Marktbeobachtung, die ihr eine Einschätzung der zahlreichen und zum Teil sehr unterschiedlich gelagerten Risiken der den deutschen Markt erreichenden Smart Toys erlauben, und wenn ja, wie lauten diese, und wenn nein, was unternimmt die Bundesregierung, um ein entsprechend differenziertes Bild zu erhalten (bitte nach Behörden aufschlüsseln)?

Die Bundesnetzagentur führt regelmäßig Internetrecherchen und anonyme Testkäufe durch, um Produkte zu prüfen oder geht Verbraucherbeschwerden nach. Im Hinblick auf die Risiken durch vernetztes Spielzeug wird auf die Pressemitteilung

der Bundesnetzagentur vom 7. Dezember 2018 hingewiesen (vgl. www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Allgemeines/Presse/Pressemitteilungen/2018/20181207_SmartToys.pdf;jsessionid=4F1D874C805F2CECEA03A7DCE0FF904B?__blob=publicationFile&v=3).

Im Übrigen wird auf die Antwort zu Frage 15 verwiesen.

2. Fällt nach Auffassung der Bundesregierung die Sicherheit von digitalem Spielzeug in die Zuständigkeit der Marktüberwachung nach dem Produktsicherheitsgesetz?

IT-Sicherheit (Sicherheit im Sinne von „security“) ist nicht Gegenstand der Anforderungen zur Gewährleistung von Sicherheit und Gesundheitsschutz im Produktsicherheitsgesetz bzw. in der Spielzeugverordnung. Somit fällt die IT Sicherheit von digitalem Spielzeug nicht in die Zuständigkeit der Marktüberwachungsbehörden. Im Übrigen wird darauf verwiesen, dass die Anforderungen an Produkte für Kinder weitgehend durch europäische Richtlinien bzw. Verordnungen geregelt sind.

3. Welche konkreten Positionen hat die Bundesregierung mit Blick auf die besonderen datenschutzrechtlichen Risiken von vernetzten „Smart Toys“ und anderen IoT-Geräten im Zusammenhang mit den Verhandlungen zur E-Privacy-Verordnung und der Aushandlung des Cybersecurity Acts vertreten, um ein sachgerechtes hohes Schutzniveau der Verbraucherinnen und Verbraucher sicherzustellen?

Für die Verarbeitung personenbezogener Daten ergeben sich die allgemeinen Anforderungen aus den Regelungen der EU-Datenschutz-Grundverordnung (DS-GVO), auch hinsichtlich der von den Verantwortlichen einer Datenverarbeitung zu gewährleistenden IT-Sicherheit (Artikel 32 DS-GVO). Die E-Privacy-VO soll auf dieser Grundlage ergänzende Regelungen für den Schutz von Privatsphäre und informationeller Selbstbestimmung sowie für die Gewährleistung des Telekommunikationsgeheimnisses bei der elektronischen Kommunikation enthalten. Damit ist sie ein sehr wichtiger Rechtsakt für den Schutz elementarer Grundrechte in der digitalen Welt. Die E-Privacy-Verordnung soll insbesondere zum Schutz der Privatsphäre auch die Anforderungen an das rechtmäßige Speichern von Informationen auf Endeinrichtungen und an das rechtmäßige Abrufen von Informationen von Endeinrichtungen durch Dritte regeln. Die Anforderungen an rechtmäßige Verarbeitung und Schutz der personenbezogenen Daten, die in solchen Informationen enthalten sein können, regelt die Datenschutz-Grundverordnung. „Smart Toys“ die an ein öffentliches Kommunikationsnetz angeschlossen sind, fallen – wie andere IoT-Geräte auch – als Endeinrichtungen uneingeschränkt in den Schutzbereich der E-Privacy-Verordnung. Hierzu bestehen keine besonderen Regelungen, da die E-Privacy-VO wie die Datenschutz-Grundverordnung technikneutral und nicht von der verwendeten Technik abhängig ausgestaltet ist, um eine Umgehung von Vorschriften zu vermeiden. Die Bundesregierung hat zu „Smart Toys“ deshalb keine spezifische Position im Rahmen der Verhandlungen zur E-Privacy-Verordnung vertreten. Zu IoT-Geräten insgesamt hat die Bundesregierung auf dem Ministerrat (Telekommunikation) am 4. Dezember 2018 folgende Position vertreten:

„Wegen der Reichweite des Artikels 8 hinsichtlich Arbeitswelt, IoT und vernetzten Geräten sieht Deutschland aber noch Beratungsbedarf. Deutschland hält es für wichtig, dass in der Ratsarbeitsgruppe darüber diskutiert wird, ob Ausnahmen vom Anwendungsbereich vorzusehen sind. Es soll sichergestellt werden, dass der

erforderliche Zugriff auf Endeinrichtungen nicht eingeschränkt wird, wenn dieser erforderlich ist, etwa für Zwecke der intelligenten Steuerung der Energieerzeugung und des Energieverbrauchs, beim automatisierten und vernetzten Fahren (insbesondere zur Ausführung sicherheitsrelevanter Funktionen und Software-Updates), im vitalen Interesse des Betroffenen, in der Gesundheitsversorgung, in der Arbeitswelt, in der intelligenten und vernetzten Herstellung von Gütern und Dienstleistungen."

4. Was hat die Bundesregierung bzw. speziell das federführende Bundesministerium für Wirtschaft und Energie konkret bewogen, im Rahmen ihrer Anpassung bundesdeutscher Rechtsvorschriften an die EU-Datenschutz-Grundverordnung (DSGVO) ihren bereits aufgenommenen Referentenentwurf zur Anpassung des Telekommunikationsgesetzes (TKG), nicht weiterzuverfolgen und auch im Rahmen der Vierten Änderung des Telekommunikationsgesetzes nicht für die erforderliche Klarheit hinsichtlich der geltenden Vorschriften zu sorgen?

Die Anpassung des Telekommunikationsgesetzes an die DSGVO wurde aus dem Gesetzentwurf für ein 2. Datenschutz-Anpassungsgesetz und Umsetzungsgesetz herausgenommen, weil innerhalb der Bundesregierung noch Beratungsbedarf im Hinblick auf die Ausgestaltung der Aufsicht durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit und die Bundesnetzagentur bestand. Dies galt insbesondere mit Blick auf die noch nicht erfolgte Positionierung innerhalb der Bundesregierung zur Ausgestaltung der Aufsicht in der zukünftigen E-Privacy-Verordnung und zu den Anforderungen der Datenschutz-Grundverordnung an die Aufsicht im Rahmen der E-Privacy-Verordnung. Zur Aufsicht hat die Bundesregierung auf dem Ministerrat (Telekommunikation) am 4. Dezember 2018 folgende Position vertreten: „Soweit die Verarbeitung personenbezogener Daten betroffen ist, sollte ein Gleichklang zwischen DSGVO und E-Privacy-VO bestehen." Auf dieser Grundlage soll die erforderliche Anpassung des Telekommunikationsgesetzes an die Datenschutz-Grundverordnung kurzfristig auf den Weg gebracht werden.

5. Teilt die Bundesregierung die Auffassung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (Stellungnahme gegenüber dem Innenausschuss des Deutschen Bundestages 19(4)151 vom 26. Oktober 2018), wonach durch die Nichtanpassung der Rechtsvorschriften insbesondere des Telemediengesetzes (TMG) und des Telekommunikationsgesetzes (TKG) erhebliche Rechtsunsicherheit hinsichtlich des anzuwendenden Rechts entstanden ist, welche auch den notwendigen Vollzug der Bestimmungen nachteilig beeinträchtigen könnte, und wenn nein, warum nicht?

Die erforderlichen Anpassungen des Telemediengesetzes und des Telekommunikationsgesetzes erfolgen gesondert und zeitnah neben dem bereits laufenden Gesetzgebungsvorhaben zur Anpassung des bereichsspezifischen Datenschutzrechts durch das Zweite Datenschutzanpassungs- und Umsetzungsgesetz EU (Bundestagsdrucksache 19/4674). Die Bundesregierung hat keine Erkenntnisse über eine erhebliche Rechtsunsicherheit in diesem Bereich. Die DSGOV findet seit dem 25. Mai 2018 – unabhängig von noch offenen Gesetzesvorhaben zur Anpassung an diese – unmittelbar Anwendung.

6. Inwiefern teilt die Bundesregierung die Auffassung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (siehe ebenfalls die in Frage 4 angeführte Stellungnahme), wonach die Bundesnetzagentur (BNetzA) nicht den Anforderungen entspricht, die das europäische Recht an die Unabhängigkeit und Weisungsfreiheit der Datenschutzvorschriften kontrollierenden Stellen aufstellt (Artikel 8 Absatz 3 der Charta der Grundrechte der Europäischen Union; Artikel 16 Absatz 2 Satz 2 des Vertrags über die Arbeitsweise der Europäischen Union sowie dazu ergangene die eindeutige Rechtsprechung des Gerichtshofs der Europäischen Union), und wenn sie diese teilt, wann wird die Bundesregierung hier die Verhältnisse den entsprechenden Anforderungen anpassen?

Die Bundesregierung weist darauf hin, dass die weiterhin geltende ePrivacy-Richtlinie (Richtlinie 2002/58/EG) in Artikel 15a Absatz 3 die Überwachung und Durchsetzung der Einhaltung der gemäß dieser Richtlinie erlassenen innerstaatlichen Rechtsvorschriften jedenfalls auch den Regulierungsbehörden zuweist. Die Regelung wurde durch Artikel 2 der Richtlinie 2009/136/EG in die ePrivacy-Richtlinie eingefügt. Im Übrigen wird auf die Antwort zu Frage 4 verwiesen.

7. Teilt die Bundesregierung die Auffassung, dass der unabhängige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit vollständig mit der Aufgabe der Aufsicht über die Einhaltung der Datenschutzbestimmungen im Bereich der Telekommunikationsunternehmen betraut werden sollte und dazu gesetzlich die bisherigen Sanktionsmöglichkeiten der Bundesnetzagentur eingeräumt bekommen sollte, und wenn nein, warum nicht?

Auf die Antwort zu Frage 4 wird verwiesen. Die Bundesregierung befürwortet bei der Aufsicht über die Einhaltung von Datenschutzbestimmungen einen Gleichklang mit der DSGVO. Dies bedeutet eine vollständige Aufgabenwahrnehmung durch die unabhängige Datenschutzaufsichtsbehörde, in diesem Fall durch den Bundesbeauftragten für Datenschutz und Informationsfreiheit.

8. Teilt die Bundesregierung die Auffassung, dass die bisherige Beschränkung des Produktsicherheitsrechts auf das Schutzgut der körperlichen Integrität weder die besondere Gefahrenlage vernetzter Spielzeuge und anderer IoT-Geräte mit ihrer Vielzahl eingebauter Schwachstellen, noch die berechtigten Schutzerwartungen der Nutzerinnen und Nutzer abzubilden in der Lage ist (vgl. etwa Bäumerich, DVBl. 2019, S. 219, 224), und empfiehlt sich vor diesem Hintergrund ein zumindest bereichsbezogenes nationales oder europäisches Produktsicherheitsrecht für Software oder zumindest für sogenannte Smart Toys und wenn nein, warum nicht?

Embedded Software verfügt als unselbstständige, produktnahe Software über eine gesetzliche Fundierung im Produktsicherheitsgesetz ProdSG. Zu IT-Sicherheit im Sinne von „security“ in Spielzeug wird auf die Antworten zu den Fragen 2 und 3 verwiesen.

9. Sieht die Bundesregierung angesichts der bereits bekannt gewordenen Probleme bei vernetztem Spielzeug und anderen IoT-Geräten die Notwendigkeit, den Sicherheitsbegriff in der europäischen Spielzeugrichtlinie auszuweiten, so dass auch Gesundheit, IT-Sicherheit und Datenschutz zur Anforderung der Spielzeugsicherheit werden, und wenn nein, warum nicht?

10. Wirkt die Bundesregierung darauf hin oder hat sie bereits, wenn ja in welchem konkreten Kontext, darauf hingewirkt, dass die EU-Kommission eine Überarbeitung der Spielzeugrichtlinie mit dem Ziel der Einbeziehung von vernetzten digitalen Spielzeugen und anderen IoT-Geräten hinsichtlich typischer Risiken vornimmt, und wenn nein, warum nicht?

Die Fragen 9 und 10 werden zusammen beantwortet.

Die Bundesregierung hält eine Erweiterung der europäischen Spielzeugrichtlinie auf die Bereiche IT-Sicherheit und Datenschutz für nicht zielführend, sondern hält eine übergreifende Regelung, die auch andere Bereiche einbezieht für sinnvoller. Im Übrigen wird auf die Antworten zu den Fragen 2 und 3 verwiesen.

11. Inwiefern wirkt die Bundesregierung auf europäischer Ebene auf eine verpflichtende Drittzertifizierung für Spielzeug und andere IoT-Geräte hin, die neben anderen Sicherheitsaspekten auch IT-Sicherheits- und Datenschutzrisiken berücksichtigt, und wenn nein, warum nicht?

Der für IT-Zertifizierungen maßgebliche allgemeine Rechtsrahmen auf europäischer Ebene wird künftig durch den Cyber Security Act (CSA) bestimmt. Um vernetzte Spielzeuge oder andere IoT-Geräte künftig europäisch einheitlich zertifizieren zu können, bedarf es eines im Rahmen des CSA abgestimmten Schemas. Drittzertifizierungen könnten durch spezialgesetzliche Vorschriften verpflichtend vorgegeben werden. Konkrete Vorhaben dazu sind der Bundesregierung derzeit nicht bekannt. Unabhängig davon enthält die DS-GVO bereits Bestimmungen zur Einführung von Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, die dem Nachweis dienen, dass die für die Datenverarbeitung Verantwortlichen und die Auftragsverarbeiter bei der Verarbeitung von Daten die Bestimmungen der DSGVO einhalten (Artikel 42 f.).

12. Werden festgestellte Verstöße wie im Fall der Spielzeugpuppe „Cayla“ oder festgestellte Datenschutz- und IT-Sicherheitsmängel von den zuständigen Behörden an das europäische Schnellwarnnetzwerk RAPEX weitergegeben, und wenn ja, in wie vielen Fällen in den letzten drei Jahren (bitte konkret auflisten), und wenn nein, warum nicht?

Das europäische Schnellwarnnetzwerk RAPEX ist ein Instrument im Kontext der Regelungen zur Produktsicherheit. Datenschutz- und IT-Sicherheitsmängel von vernetztem Spielzeug fallen nicht in den Zuständigkeitsbereich der Marktüberwachungsbehörden. Dazu wird auf die Antwort zu Frage 2 verwiesen.

Bei der Spielzeugpuppe „Cayla“ wurden Verstöße gegen das Verbot missbräuchlicher Sende- oder Telekommunikationsanlagen nach § 90 TKG geahndet. Da es sich hier um eine rein nationale Rechtsnorm aus dem Telekommunikationsrecht handelt, fiel dieser Fall nicht in den Anwendungsbereich des RAPEX-Verfahrens.

13. Teilt die Bundesregierung den von der britischen Regierung für IoT-Produkte allgemein formulierten Anforderungskatalog (vgl. EPIC-Stellungnahme, S. 4, https://epic.org/comments/EPIC-Comments-EU-Toy-Safety-Directive.pdf), und wenn nein, welche vergleichbaren Sicherheits-Anforderungen sieht sie im Falle von „Smart Toys“ und anderen IoT-Geräten als einschlägig an?

Soweit sich diese von einer US-amerikanischen Nichtregierungsorganisation formulierten Anforderungen auf datenschutzrechtliche Aspekte der IT-Sicherheit beziehen, wird auf die Antworten zu den Fragen 2 und 3 verwiesen.

14. Wie bewertet die Bundesregierung das Vorgehen der Bundesnetzagentur (BNetzA) in Fällen, bei denen die Positionsdaten und weitere Informationen von mehreren Tausend Kindern abgegriffen werden können, aber offenbar keine systematische Prüfung der Produktpaletten und Intervention seitens der Bundesnetzagentur erfolgte (vgl. http://0x0000dead.de/Watchgate_TROOPERS2019.pdf)?

Die Inhalte des Berichtes sind der Bundesnetzagentur bekannt. Bei der dort angesprochenen Thematik handelt es sich nach Einschätzung der Bundesnetzagentur jedoch um ein IT-Sicherheitsproblem, da die genannten Vidimensio-Smartwatches nicht ausreichend gegen Hackingmaßnahmen geschützt sind. Die Bundesnetzagentur hat jedoch im Zusammenhang mit Verstößen gegen § 90 TKG für die Behebung von IT-Sicherheitsrisiken keine rechtliche Grundlage.

Der Hacker, der die IT-Sicherheitsprobleme ausnutzt und so die Kinderuhr angreift, um das Kind und dessen Umgebung abzuhören, kann dadurch vielmehr eine Straftat nach dem Strafgesetzbuch (StGB) begehen. In Betracht kommt eine Strafbarkeit nach § 201 StGB („Verletzung der Vertraulichkeit des Wortes“). Auch eine Strafbarkeit nach § 202a StGB („Ausspähen von Daten“) kann gegeben sein. Diese Straftaten sind allein durch die Staatsanwaltschaft zu verfolgen.

Die Bundesnetzagentur hat im Mai 2018 einige Modelle der Firma Vidimensio („kleiner Affe“, „kleiner Pinguin“ und „kleiner Tiger“) dahingehend überprüft, ob ein Abhören mittels „SMS Commands“ und über die Apps „Find my kids“ sowie „Vidimensio GPS-Trackers“ möglich ist. Der Test fiel negativ aus. Im weiteren Verlauf wurden auch acht weitere Smartwatchmodelle der Firma Vidimensio auf einen Verstoß gegen § 90 Absatz 1 TKG getestet. Auch diese Modelle verfügen nicht über eine Abhörfunktion.

15. Hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) bereits oder plant es eigene Untersuchungen im Bereich der „Smart Toys“ oder anderer IoT-Produkte mit dem Ziel der Verbraucherunterstützung und Verbrauchersicherheit, und wenn nein, warum nicht?

Das Bundesamt für Informationstechnik (BSI) hat in der Vergangenheit bereits Untersuchungen von vernetztem Spielzeug und Smart Home Produkten vorgenommen, um die Sicherheit dieser zu beurteilen und Anwender bei Risiken informieren zu können. Im Zuge der im Koalitionsvertrag festgelegten Etablierung des digitalen Verbraucherschutzes als neue Aufgabe des BSI ist der Ausbau der Aktivitäten im Bereich der Marktbeobachtung und Sicherheitstests geplant. Das BSI als das Kompetenzzentrum in Deutschland für Fragen der Informations- und Cyber-Sicherheit ist ein wichtiger Gestalter des digitalen Verbraucherschutzes. Bereits jetzt arbeitet das BSI mit etablierten und anerkannten Partnern im Feld des Verbraucherschutzes zusammen.

Im März 2017 hat das BSI mit der Verbraucherzentrale Nordrhein-Westfalen ein sog. „Memorandum of Unterstanding“ (MoU) zur verstärkten Zusammenarbeit unterzeichnet. Im Bereich der „Smart Toys“ wurde im Frühjahr 2018 in Zusammenarbeit mit der Verbraucherzentrale Nordrhein-Westfalen der Spielzeugroboter „Anki Cozmo“ analysiert. Ziel der Untersuchung war, das Produkt auf seine Sicherheitseigenschaften zu untersuchen und ggf. vorhandene Schwachstellen zu identifizieren. Das Ergebnis wurde von der Verbraucherzentrale Nordrhein-Westfalen in einen entsprechenden Bericht eingearbeitet: www.marktwaechter.de/sites/default/files/downloads/bericht-vernetztes-spielzeug.pdf.

Zurzeit läuft ein weiteres Projekt mit der Verbraucherzentrale Nordrhein-Westfalen. Hierbei werden zwei IoT-Überwachungskameras sowie ein IoT-Rauchmelder und ein IoT-CO-Warner unterschiedlicher Hersteller auf ihre Sicherheitseigenschaften überprüft.

Das BSI arbeitet zudem an Mindestsicherheitsanforderungen, welche den übergeordneten Bereich der internetfähigen Endkundengeräte (kurz: IoT-Geräte) und damit auch „Smart Toys“ betreffen. Darunter fallen zum Beispiel die Technische Richtlinie BSI RT-03148 Sichere Breitband Router (www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03148/tr03148_node.html) und die inzwischen veröffentlichte DIN SPEC 27072. Gleichzeitig klärt das BSI Bürgerinnen und Bürger auf verschiedensten Kanälen über die Gefahren im Bereich der „Smart Toys“ auf. Beispielhaft wird auf die Veröffentlichung des Artikels „Smarte Spielzeuge – Lernhilfen oder Spione?“ und den dazugehörigen Videobeitrag (www.bsi-fuerbuerger.de/BSIFB/DE/DigitaleGesellschaft/IoT/SmartToys/SmartToys_node.html) verwiesen.

16. Wie viele Beschäftigte der Bundesnetzagentur sind mit der Sichtung und Kontrolle der in ihren Zuständigkeitsbereich fallenden „intelligenten“ Spielzeugprodukte und anderer IoT-Geräte befasst, und hält die Bundesregierung diese Ausstattung mit Blick auf Quantität und Qualität der Herausforderung für angemessen?

Für die Verfolgung von Verstößen gegen § 90 TKG werden derzeit 13 Beschäftigte in der Bundesnetzagentur eingesetzt. Weiterhin überwacht die Bundesnetzagentur elektrische und elektronische Geräte mit 102 Beschäftigten an zehn Standorten auf dem deutschen Markt nach dem Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln (EMVG) und dem Gesetz über die Bereitstellung von Funkanlagen auf dem Markt (FuAG). IT-Sicherheit fällt – wie in der Antwort zu Frage 2 ausgeführt – nicht in die Zuständigkeit der Marktüberwachungsbehörden.

17. Welchen Beitrag wird die Bundesregierung dafür leisten, dass auch die Datenschutzbehörden des Bundes und der Länder ihren gesetzlichen Verpflichtungen durch sachgerechte Ausstattung und finanzielle Ressourcen nachkommen können, die besonderen Risiken vernetzter Spielzeuge und vernetzter Produkte zu adressieren und die Durchsetzung des Datenschutzrechts zu gewährleisten?

Die Bundesregierung erachtet eine angemessene Ausstattung der unabhängigen Datenschutzbehörden des Bundes und der Länder für wichtig und notwendig, damit diese Behörden ihre nach der DSGVO festgelegten gesetzlichen Aufgaben effizient und wirkungsvoll ausführen können.

Die Datenschutzaufsichtsbehörden des Bundes und der Länder sind gemäß den EU-rechtlichen Vorgaben unabhängige Behörden. Etwaigen Personalbedarf müssen sie selbständig bei dem für die Aufstellung des Haushaltsplans zuständigen Finanzministerium anmelden. Für die Ausstattung der Datenschutzaufsichtsbehörden der Länder sind die Länder (und damit letztlich die Landesparlamente) zuständig.

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) bringt als unabhängige oberste Bundesbehörde seine Personal- und Sachmittelansätze in das Verfahren zur Aufstellung des Bundeshaushaltsplanes (Einzelplan 21) selbständig ein. Eine entsprechende Ausstattung des BfDI mit den erforderlichen Personal- und Sachmitteln muss der Deutsche Bundestag als Haushaltsgesetzgeber bewilligen.

18. Wie bewertet die Bundesregierung die Gefahr, dass unsichere „smarte“ Spielzeuge und andere IoT-Geräte zu Botnetzen verbunden werden, die wiederum für IT-Angriffe verwendet werden?

Diese Gefahr wird als hoch bewertet (siehe auch Botnetzlagebericht des BSI). In Deutschland sind mit dem Internet verbundene Geräte innerhalb eines internen Netzwerks in der Regel über einen Heim-Router ans Internet angebunden. Dadurch ist derzeit noch ein gewisser Schutz gegen Masseninfektionen gewährleistet. Falls vernetzte Geräte jedoch exponiert sind, womit zunehmend zu rechnen ist, und direkt mit dem Internet verbunden sind, können sie beispielsweise Malware aufgrund eines übernommenen Steuersystems nachladen. Die potentielle Gefahr steigt somit. Details zu dieser Einschätzung lassen sich auch dem Bericht zur Lage der IT-Sicherheit des BSI (www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html) entnehmen.

19. Wie bewertet die Bundesregierung die Gefahr, dass unsichere „smarte“ Spielzeuge und andere IoT-Geräte, die mit einer Videofunktion versehen sind, von Dritten übernommen werden und entsprechende Bildaufzeichnungen für verschiedene (kriminelle) Zwecke missbraucht werden können?

IoT-Geräte sind bei unzureichenden IT-Sicherheitsvorkehrungen der Gefahr einer Übernahme durch Dritte ausgesetzt. Geeignete Suchmaschinen oder entsprechende besondere Suchanfragen vereinfachen das Auffinden von offen erreichbaren oder von Schwachstellen betroffenen Geräten und erleichtern somit den unbefugten Zugriff. Zwar kann der Heimrouter, wie unter in der Antwort zu Frage 18 beschrieben, viele Angriffe verhindern, jedoch besteht weiterhin die Gefahr, dass IoT-Geräte, z. B. auch solche, die von Bürgerinnen und Bürgern bewusst als online-verfügbar konfiguriert wurden, übernommen werden.

20. Wie bewertet die Bundesregierung Gefahren, die dadurch entstehen, dass Kommunikationen über „smartes“ Spielzeug und andere IoT-Geräte auch auf Servern in Ländern gespeichert werden, in denen entsprechende gesetzliche Regelungen Sicherheitsbehörden und Nachrichtendiensten weitreichende Zugriffsrechte gewähren, beispielsweise in China und den USA?

Übermittlungen personenbezogener Daten in Länder außerhalb der Europäischen Union (sog. Drittländer) sind nur unter Einhaltung der in Kapitel V DSGVO niedergelegten Bedingungen wie auch der sonstigen Bedingungen der DSGVO zulässig (vgl. Artikel 44 Satz 1 DSGVO). Dies soll sicherstellen, dass das durch die DSGVO gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird (vgl. Artikel 44 Satz 2 DSGVO). Datenübermittlungen an Drittstaaten sind

danach nur zulässig, wenn ein sogenannter Angemessenheitsbeschluss nach Artikel 45 DSGVO vorliegt, wenn der für die Datenverarbeitung Verantwortliche oder Auftragsverarbeiter geeignete Garantien vorsieht und der betroffenen Person durchsetzbare und wirksame Rechtsbehelfe zur Verfügung stehen oder wenn eine Ausnahme nach Artikel 49 DSGVO gegeben ist. Zu den geeigneten Garantien zählen etwa rechtlich verbindliche interne Datenschutzvorschriften gemäß Artikel 47 DSGVO, der Einsatz von Standardvertragsklauseln oder genehmigte Verhaltensregeln zusammen mit verbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder Auftragsverarbeiters im Drittland. Die Einhaltung dieser Bedingungen hat jede verantwortliche Stelle, die personenbezogene Daten in Drittstaaten übermittelt, zu beachten. Durch Einhaltung dieser Bedingungen werden nach Auffassung der Bundesregierung die von den Fragestellern beschriebenen Gefahren deutlich begrenzt.

21. Wie bewertet die Bundesregierung das aktuelle Trilog-Ergebnis zum Cybersecurity Act (CSA) (vgl. http://data.consilium.europa.eu/doc/document/ST-15786-2018-INIT/en/pdf) auch vor dem Hintergrund der eigenen Ankündigung, sich dafür einsetzen zu wollen, verpflichtende Mindestsicherheitsstandards für loT-Geräte zu etablieren (vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN zur Sicherheit und Konformität von loT-Geräten, Bundestagsdrucksache 19/9132, S. 3)?

Das Ergebnis des Trilogs zum CSA widerspricht nicht den in der Antwort auf die Kleine Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN zur Sicherheit und Konformität von loT-Geräten auf Bundestagsdrucksache 19/9132 dargestellten Absichten der Bundesregierung.

22. Hält die Bundesregierung freiwillige Zertifizierungen in Eigenregie der Hersteller nach vertikalen Zertifikationsschemata und mit selbst verliehenen Sicherheitssiegeln ohne tatsächliche Sanktionsmaßnahmen bei Verstößen oder gar Haftungsregeln für tatsächlich ausreichend?

Wenn ja, wie erklärt sich der Sinneswandel (vgl. ebd.)?

Eine Zertifizierung in Eigenregie ist nicht möglich. Hersteller können eine Erklärung abgeben, dass sie die Anforderungen bestimmter technischer Vorschriften oder Richtlinien einhalten. Hierbei ist nicht von einer Zertifizierung zu sprechen. Um der Diversität der einzelnen Gerätekategorien gerecht zu werden, ist die Verwendung spezifischer Vorschriften oder Richtlinien angezeigt. Dies dient vor allem der Schaffung besserer Transparenz für Verbraucher. Bei Nichteinhaltung der dargelegten Anforderungen, können ggf. wettbewerbsrechtliche Sanktionen drohen.

Vertikale Zertifizierungsschemata, wie sie der CSA ggf. vorsieht, sind besonders dann sinnvoll, wenn es produkt- oder bereichsspezifische Anforderungen gibt. Dies gilt vor allem dann, wenn sich im Rahmen eines Zertifizierungsvorhabens aufgrund der Höhe des erforderlichen Schutzniveaus gemäß der Assurance-Level Basic, Substantial, High immer spezifischere Anforderungen ergeben.

Die freiwillige Zertifizierung nach CSA ist darüber hinaus jedoch unabhängig von der möglichen Einführung europäisch einheitlicher Mindestsicherheitsanforderungen. Im Übrigen wird auf die Antwort der Bundesregierung zu den Fragen 1 und 2 der Kleinen Anfrage auf Bundestagsdrucksache 19/9132 verwiesen.

23. Wird die Bundesregierung im Zuge der Vorlage des „IT-Sicherheitsgesetzes 2.0“ neue, verpflichtende Mindeststandards und Haftungsregelungen vorlegen?

Falls ja, wie sehen diese konkret aus?

Falls nein, warum nicht?

Nach gegenwärtigem Sachstand ist nicht beabsichtigt, im Zuge der Vorlage eines „IT-Sicherheitsgesetzes 2.0“ verpflichtende Mindeststandards vorzusehen. Dies wäre vor dem Hintergrund eines möglichen Eingriffs in den EU-Binnenmarkt auch nicht zulässig. Auch neue Haftungsregelungen sind nicht beabsichtigt.

24. Inwiefern ist es nach Kenntnis der Bundesregierung deutschen Ermittlungsbehörden im Rahmen von Strafverfahren möglich, auf die aus intelligenten Spielzeugprodukten übertragenen (und auf Servern gespeicherten) Daten zuzugreifen, und wie viele solche Fälle sind der Bundesregierung bekannt (bitte nach Rechtsgrundlage aufschlüsseln)?

Das Bundeskriminalamt hat derzeit keine Möglichkeit auf Daten im Sinne der Fragestellung zuzugreifen. Darüber hinaus ist der Bundesregierung nicht bekannt, ob in von den Ländern geführten Strafverfahren Sachverhalte der geschilderten Art eine Rolle gespielt haben. Welche Rechtsgrundlagen anzuwenden wären, um entsprechende Daten zu erheben, hängt aber von den konkreten Umständen des jeweiligen Einzelfalls ab.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333