Deutscher Bundestag **Drucksache 19/662**

19. Wahlperiode 07.02.2018

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Konstantin Kuhle, Stephan Thomae, Jimmy Schulz, weiterer Abgeordneter und der Fraktion der FDP
– Drucksache 19/514 –

Verpflichtung Dritter für Maßnahmen der verdeckten Informationserhebung

Vorbemerkung der Fragesteller

Nach einer Meldung des RedaktionsNetzwerks Deutschland vom 30. November 2017 plant das Bundesministerium des Innern, die Industrie zu verpflichten, den Sicherheitsbehörden digitale Einfallstore für das Ausspionieren von privaten Autos, Computern, Unterhaltungs- sowie Haushaltsgeräten zu eröffnen (vgl. www.rnd-news.de/Exklusive-News/Meldungen/November-2017/De-Maiziere-will-Ausspaehen-von-Privat-Autos-Computern-und-Smart-TVs-ermoeglichen, letzter Abruf: 2. Januar 2018).

Dabei gehe es insbesondere um die gesetzliche Verpflichtung Dritter für Maßnahmen der verdeckten Informationserhebung nach den §§ 100c und 100f der Strafprozessordnung (StPO). So solle es etwa für Unternehmen und andere Entwickler künftig eine Auskunfts- und Mitteilungspflicht zur verdeckten Überwindung von Sicherheitssystemen geben. Das Bundesministerium des Innern hat weitreichenden Plänen zur Verpflichtung von Unternehmen und anderen Entwicklern widersprochen. Vielmehr gehe es lediglich um die Hersteller von Alarm- und Sicherheitssystemen (www.zeit.der/digital/datenschutz/2017-12/ueberwachung-wohnraum-de-maiziere).

In den freigegebenen Beschlüssen der 207. Sitzung der Innenministerkonferenz (IMK) am 7. und 8. Dezember 2017 heißt es zum Tagesordnungspunkt 22 (Handlungsbedarf zur gesetzlichen Verpflichtung Dritter für Maßnahmen der verdeckten Informationserhebung nach §§ 100c und 100f StPO):

„2. [Die IMK] stellt fest, dass die fortschreitende Entwicklung im Bereich der Fahrzeug- und Schlosstechnik die verfügbaren technischen Möglichkeiten zur verdeckten Überwindung dieser Systeme einschränkt. Dadurch können rechtlich zulässige Maßnahmen nicht umgesetzt werden.

3. Die IMK sieht unter Berücksichtigung der im Bericht aufgezeigten Szenarien und aus Gründen der Rechts- und Handlungssicherheit einen weitergehenden Prüfbedarf im Hinblick auf technische und rechtliche Lösungsmöglichkeiten zur Umsetzung der Maßnahmen der verdeckten Informationserhebung nach den §§ 100c und 100f StPO. Insbesondere soll dabei geprüft werden, ob und inwieweit Dritte beim verdeckten Öffnen und Überwinden von Diebstahlwarnanlagen zur Mitwirkung de lege lata und de lege ferenda verpflichtet werden können,

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 6. Februar 2018 übermittelt.

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

wobei es ausdrücklich nicht um den Einbau von sogenannten Hintertüren in informationstechnische Systeme geht. Die zu erarbeitenden Lösungen sollten technikoffen ausgestaltet sein.“

Die Berichte im Vorfeld sowie der Beschluss der Innenministerkonferenz haben in betroffenen Kreisen zu großer Verunsicherung geführt.

Auch das Thema „Internet der Dinge“ hat bei der 206. und 207. Sitzung der IMK eine Rolle gespielt. Die 206. Sitzung der IMK hatte die länderoffene Arbeitsgruppe Cybersicherheit beauftragt, die Intensivierung der Maßnahmen zur Verbesserung der Cybersicherheit bezogen auf das Internet der Dinge umfassend zu prüfen. Zur 207. Sitzung hat diese Arbeitsgruppe einen Sachstandsbericht veröffentlicht (verfügbar unter www.innenministerkonferenz.de/IMK/DE/termine/to-beschluesse/2017-12-07_08/anlage-zu-top-8.pdf?__blob=publicationFile&v=3, letzter Abruf: 2. Januar 2018).

In diesem Sachstandsbericht heißt es u. a., dass die IMK feststelle, „dass die massenhafte Verbreitung von mit dem Internet verbundenen Gebrauchsgeräten (Internet der Dinge) ohne ausreichende Sicherheitsvorkehrungen eine erhebliche Bedrohung für den Cyberraum darstelle“ und dass „eine Intensivierung der Maßnahmen zur Verbesserung der Cybersicherheit bezogen auf das Internet der Dinge“ erforderlich sei.

In der durch das Bundesministerium des Innern veröffentlichten Cyber-Sicherheitsstrategie für Deutschland 2016 heißt es ferner, das „Vertrauen zwischen Unternehmen und Behörden in Diskretion und Professionalität im Umgang mit sensiblen Sachverhalten“ spiele bei der Schaffung des notwendigen IT-Sicherheitsniveaus eine „wesentliche Rolle“.

Vorbemerkung der Bundesregierung

In ihrem Beschluss vom 8. Dezember 2017 erklärte die Ständige Konferenz der Innenminister und -senatoren der Länder (IMK), es bestehe Prüfbedarf im Hinblick auf technische und rechtliche Lösungsmöglichkeiten zur Umsetzung der Maßnahmen der verdeckten Informationserhebung nach den §§ 100c und 100f der Strafprozessordnung (StPO). Ihren Prüfauftrag richtete die IMK gemäß Ziffer 4 des Beschlusses an den Arbeitskreis Innere Sicherheit (AK II) und bat diesen, in Abstimmung mit der Justizministerkonferenz (JuMiKo) die geforderte Rechtsänderung zu prüfen und anschließend dem IMK-Vorsitzland sowie den A- und B-Sprecherländern zu berichten.

Der Prüfauftrag an den AK II und die JuMiKo betrifft das Eruieren technischer und rechtlicher Lösungsmöglichkeiten zur Umsetzung von Maßnahmen der akustischen Überwachung. Eine Verpflichtung Dritter zur Mitwirkung soll dabei insbesondere, aber nicht ausschließlich betrachtet werden. Die Betrachtung wird auch den Umfang etwaiger Mitwirkungspflichten und Möglichkeiten der technikoffenen Ausgestaltung umfassen, sowie alle damit im Zusammenhang stehenden Fragen.

Bereits der Beschluss der IMK führt aus, dass es im Rahmen der Prüfung ausdrücklich nicht um den Einbau von sogenannten Hintertüren in informationstechnische Systeme geht. Insofern steht nicht zu befürchten, dass es zu einer systematischen Schwächung der Sicherheit informationstechnischer Systeme kommt. Die Bundesregierung wird das Prüfungsergebnis der beauftragten Gremien abwarten und sich dazu im Anschluss positionieren.

1. Welcher gesetzgeberische Handlungsbedarf besteht aus Sicht der Bundesregierung, um Dritte zur Durchführung von Maßnahmen der verdeckten Informationserhebung nach den §§ 100c und 100f StPO im staatlichen Auftrag oder zur Ermöglichung solcher Maßnahmen zu verpflichten?

Nach § 100c StPO ist die Polizei unter engen Voraussetzungen befugt, auch ohne Wissen der Betroffenen das in einer Wohnung nichtöffentlich gesprochene Wort mit technischen Mitteln abzuhören und aufzuzeichnen (akustische Wohnraumüberwachung). § 100f StPO regelt eine vergleichbare Befugnis hinsichtlich des außerhalb von Wohnungen nichtöffentlich gesprochenen Wortes, beispielsweise in Kfz (akustische Überwachung außerhalb von Wohnraum).

Für beide Maßnahmen gilt, dass sie nur auf Antrag der Staatsanwaltschaft durch ein Gericht angeordnet werden dürfen. Bei der akustischen Wohnraumüberwachung ergeht die Anordnung durch die Strafkammer des zuständigen Landgerichts; sie kann bei Gefahr im Verzug auch durch den Vorsitzenden getroffen werden und tritt außer Kraft, wenn sie nicht binnen drei Werktagen von der Strafkammer bestätigt wird (§ 100e Absatz 2 StPO). Bei der akustischen Überwachung außerhalb von Wohnraum kann die Anordnung bei Gefahr im Verzug durch die Staatsanwaltschaft getroffen werden, muss aber binnen drei Werktagen vom Gericht bestätigt werden (§ 100e Absatz 1 i. V. m. § 100f Absatz 4 StPO).

Die Durchführung der so angeordneten Maßnahmen durch die Polizeibehörden setzt voraus, dass diese sich zunächst Zugang zu der Wohnung oder dem Kfz verschaffen. Die Art und Weise des unbemerkten Öffnens und Betretens der Wohnung oder des Kfz zum Zwecke der Installation der technischen Überwachungsmodule ist gesetzlich nicht ausdrücklich geregelt. Trotz Vorliegen aller Voraussetzungen kann die Polizei die Überwachungsmodule in Wohnungen oder Kfz nicht installieren, wenn moderne Schließeinrichtungen die unbemerkte Installation verhindern. Neben dem verdeckten Öffnen ist nämlich vermehrt das Überwinden von Sicherungs- und Alarmeinrichtungen notwendig, wofür in Abhängigkeit von der konkreten Sachlage die Mitwirkung des jeweiligen Herstellers notwendig werden kann. Die Gremien der IMK haben insbesondere bei Fällen der organisierten Kriminalität verschiedene Problemfälle identifiziert, in denen richterliche Beschlüsse zu Maßnahmen an Kfz nicht umgesetzt werden konnten. Aufgrund dieser Feststellungen muss daher geprüft werden, ob und welche Rechtsänderungen notwendig sind.

2. Sollte nach Auffassung der Bundesregierung eine neue Ermächtigungsgrundlage zur Verpflichtung Dritter zur Durchführung oder Ermöglichung von Maßnahmen der verdeckten Informationserhebung nach den §§ 100c und 100f StPO technikoffen ausgestaltet sein?

   Wenn ja, warum?

Bei der Gestaltung von Befugnisnormen der Strafverfolgung ist eine technikoffene Ausgestaltung unter Aufrechterhaltung aller rechtsstaatlichen Sicherungen in der Regel sinnvoll, um die Eingriffsermächtigungen nicht bei jeder neuen technischen Entwicklung entsprechend anpassen zu müssen.

3. Wie bewertet die Bundesregierung die Sorge, dass durch eine technikoffene Ausgestaltung der Verpflichtung Dritter zur Durchführung oder Ermöglichung von Maßnahmen der verdeckten Informationserhebung ein potenziell weitreichender Zugang auf private Gebrauchsgeräte möglich wird?

Ein weitreichender Zugang auf private Gebrauchsgeräte ist vom Prüfauftrag nicht umfasst.

4. Sollte eine neue Ermächtigungsgrundlage zur Verpflichtung Dritter zur Durchführung oder Ermöglichung von Maßnahmen der verdeckten Informationserhebung auf die Hersteller von Alarm- und Sicherheitssystemen beschränkt sein?

   Wenn ja, warum?

   Wenn nein, warum nicht?

Der Prüfauftrag der IMK beschränkt sich auf technische und rechtliche Maßnahmen nach den §§ 100c und 100f StPO. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

5. Wie kann eine gesetzliche Regelung zur Verpflichtung Dritter zur Durchführung oder Ermöglichung von Maßnahmen der verdeckten Informationserhebung nach Auffassung der Bundesregierung gleichzeitig technikoffen und auf die Hersteller von Alarm- und Sicherheitssystemen beschränkt sein?

Auf die Antwort zu Frage 4 und die Vorbemerkung der Bundesregierung wird verwiesen.

6. Welche Regelungen sollen nach Auffassung der Bundesregierung bei einer neuen Ermächtigungsgrundlage zur Verpflichtung Dritter zur Durchführung oder Ermöglichung von Maßnahmen der verdeckten Informationserhebung den Grundrechtsschutz durch Verfahren sicherstellen?

   Wie sollen bei einer solchen Maßnahme die Risiken berücksichtigt werden, die anderen Bürgerinnen und Bürgern durch das Unterlassen der Schließung von Sicherheitslücken drohen?

Eine Verpflichtung Dritter zur Durchführung von Maßnahmen der verdeckten Informationserhebung ist ebenso wenig wie eine staatlich angestrebte Unterlassung der Schließung von Sicherheitslücken in informationstechnischen Systemen Gegenstand des IMK-Beschlusses. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

7. Wie geht die Bundesregierung mit Informationen um, welche die IT-Sicherheit von Hard- oder Software betreffen?

   Werden diese Informationen verwendet, um den verdeckten Zugriff auf informationstechnische Systeme oder andere Geräte zu ermöglichen oder zu erleichtern?

   Werden diese Informationen umgehend an das Bundesamt für Sicherheit in der Informationstechnik (BSI) weitergeleitet?

   Wenn nicht, wer entscheidet dies und nach welchen Kriterien?

Aus Sicht der Bundesregierung sind diese Fragen im Zusammenhang so zu verstehen, dass der Umgang mit Informationen, welche die IT-Sicherheit von Hard- oder Software betreffen, im Rahmen der Aufgabenwahrnehmung der Strafverfolgungs- und Sicherheitsbehörden des Bundes gemeint ist.

Der Umgang mit Sicherheitslücken, der Kauf, die Entwicklung und die Nutzung von Schwachstellen und Exploits durch Strafverfolgungs- und Sicherheitsbehörden des Bundes sind ein für die Bundesregierung relevantes Thema. Für die Bundesregierung gilt „Sicherheit durch Verschlüsselung“ und „Sicherheit trotz Verschlüsselung“. Beide Grundsätze sind in einem rechtsstaatlichen System vereinbar. Sicherheitslücken sind stets zu bewerten und auf ihr Schadenspotenzial hin

zu untersuchen. Die Bundesregierung setzt sich derzeit inhaltlich intensiv mit dieser Problematik auseinander. Die Überlegungen sollen in einen Prozess münden, bedürfen allerdings noch einer Konkretisierung.

Ergänzend wird auf die Antwort der Bundesregierung auf die Schriftliche Frage 10 der Abgeordneten Saskia Esken auf Bundestagsdrucksache 18/13667 vom 6. Oktober 2017 verwiesen.

Zur Frage, ob entsprechende Informationen verwendet werden, um den verdeckten Zugriff auf informationstechnische Systeme oder andere Geräte zu ermöglichen oder zu erleichtern, sowie, ob diese Informationen umgehend an das Bundesamt für Sicherheit in der Informationstechnik (BSI) weitergeleitet werden, wird auf die Antwort der Bundesregierung auf die Schriftliche Frage 10 der Abgeordneten Saskia Esken auf Bundestagsdrucksache 18/13667 vom 6. Oktober 2017 sowie auf die Antwort der Bundesregierung auf die Schriftliche Frage 10 des Abgeordneten Andrej Hunko auf Bundestagsdrucksache 18/13696 vom 23. Oktober 2017, auf die Antwort der Bundesregierung zu den Fragen 2, 26 bis 31 (VS-NfD) und 33 der Kleinen Anfrage der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Bundestagsdrucksache 18/13566 vom 13. September 2017 und auf die Antwort der Bundesregierung zu Frage 15 der Kleinen Anfrage der Fraktion DIE LINKE. auf Bundestagsdrucksache 18/13069 vom 6. Juli 2017 verwiesen.

8. Welche Sanktionen sollen nach Auffassung der Bundesregierung gegen solche Privaten verhängt werden können, die der Verpflichtung zur Durchführung oder Ermöglichung von Maßnahmen der verdeckten Informationserhebung nicht nachkommen?

Auf die Vorbemerkung der Bundesregierung und den darin erläuterten Prüfcharakter des in Bezug stehenden IMK-Beschlusses wird verwiesen.

9. Wie will die Bundesregierung sicherstellen, dass die technische Schaffung von Möglichkeiten der verdeckten Informationsgewinnung bei Privaten keine Zugriffsmöglichkeiten für Unbefugte eröffnet?

Auf die Antwort zu Frage 6 und die Vorbemerkung der Bundesregierung und den darin erläuterten Prüfcharakter des in Bezug stehenden IMK-Beschlusses wird verwiesen.

10. Mit welchen Maßnahmen gedenkt die Bundesregierung, die Einrichtungen der öffentlichen Verwaltung vor Zugriffen Unbefugter zu schützen, die gerade auf der Grundlage der technischen Schaffung von Möglichkeiten der verdeckten Informationsgewinnung bei Privaten entstehen?

Auf die Vorbemerkung der Bundesregierung und den darin erläuterten Prüfcharakter des in Bezug stehenden IMK-Beschlusses wird verwiesen.

11. Teilt die Bundesregierung die Feststellung der Innenministerkonferenz, dass eine Intensivierung der Maßnahmen zur Verbesserung der Cybersicherheit bezogen auf das Internet der Dinge notwendig ist?

    Welche Maßnahmen sind aus Sicht der Bundesregierung auf nationaler Ebene erforderlich?

    Welche Maßnahmen sind aus Sicht der Bundesregierung auf europäischer Ebene zu ergreifen?

Von einer massenhaften Verbreitung von mit dem Internet verbundenen Gebrauchsgeräten – „Internet der Dinge“ –, die keine Mindestsicherheitsanforderungen erfüllen, geht ein Risiko für die gesamte IT-Infrastruktur einschließlich unserer hochsensiblen Kritischen Infrastrukturen über die Landesgrenzen hinweg aus. Daher ist es gut und richtig, dafür Sorge zu tragen, dass diese vernetzbaren Geräte erstmals flächendeckende Mindestsicherheitsstandards aufweisen und diese dem Käufer auch transparent sind. Die Feststellung der IMK spiegelt diese Position.

Mit der Cybersicherheitsstrategie 2016 hat sich die Bundesregierung zum Ziel gesetzt, geeignete Vorschläge zu unterbreiten, damit der Verbraucher auf Basis eines einheitlichen Gütesiegels bei der Kaufentscheidung für neue IT-Produkte leicht und schnell feststellen kann, welches Angebot sicher ausgestaltet ist. Insoweit muss auch das Ergebnis der Verhandlungen zur Verordnung über die „EU-Cybersicherheitsagentur“ (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik („Rechtsakt zur Cybersicherheit“) in die weiteren Überlegungen einfließen. Das europäische Rechtsetzungsverfahren soll jedoch erst Ende 2018 abgeschlossen werden.

Ob in Bezug auf Cybersicherheitsaspekte ein zeitigeres rechtliches Handeln auf nationaler Ebene erforderlich und zulässig ist – vor dem Hintergrund der jetzt bekannt gewordenen IT-Sicherheitslücken Spectre und Meltdown – wird zurzeit geprüft.

Darüber hinaus hat die Bundesregierung in den vergangenen Jahren die Hersteller bereits im Rahmen der IT-Sicherheitsgesetzgebung kontinuierlich weiter in die Pflicht genommen. So wurde z. B. mit dem Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes vom 14. August 2009 (BGBl I S. 2821, www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%5b@attr_id='bgbl109s2821.pdf'%5d) in § 7 Absatz 2 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) geregelt, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) zur Erfüllung seiner Aufgaben unter Nennung der Bezeichnung des Herstellers vor Sicherheitslücken in informationstechnischen Produkten oder Diensten warnen kann.

Im Rahmen des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vom 17. Juli 2015 (IT-Sicherheitsgesetz – BGBl I S 1324, www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%5b@attr_id='bgbl115s1324.pdf'%5d) wurde in § 8b Absatz 6 BSIG geregelt, dass das BSI zum Schutz von Kritischen Infrastrukturen von Herstellern informationstechnischer Produkte und Systeme die Mitwirkung an der Störungsbeseitigung und -vermeidung verlangen kann. Eine vergleichbare Regelung enthält auch das Gesetz zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union vom 23. Juni 2017 (BGBl I 2017 S. 1885, www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&start=//*%5b@attr_id='bgbl117s1885.pdf'%5d)

in § 5a Absatz 6 BSIG. Danach kann das BSI im Rahmen eines Einsatzes der „Mobile Incident Response Teams“ (MIRTs) von Herstellern die Mitwirkung an der Wiederherstellung der IT-Sicherheit oder Funktionsfähigkeit ihrer Produkte und Systeme verlangen.

Bereits das geltende Produkthaftungsrecht gewährt Verbraucherinnen und Verbrauchern Schutz bei fehlerhafter Software. Bei den Verhandlungen über eine Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte wird im Zusammenhang mit der vertraglichen Haftung für IT-Sicherheitsmängel erörtert, unter welchen Voraussetzungen zu einer vertragsgemäßen Software auch deren Aktualisierung, einschließlich der Bereitstellung von (Sicherheits-) Updates gehört.

Die Europäische Kommission evaluiert derzeit die Wirksamkeit der Produkthaftungsrichtlinie im Hinblick auf neue technische Entwicklungen, d. h. insbesondere „Internet der Dinge“, fortschrittliche Roboter und automatisierte Systeme. Die Bundesregierung unterstützt diese Initiativen aktiv. Sie hat auch selbst Forschungsprojekte initiiert und unterstützt, um die mit der zunehmenden Digitalisierung und Vernetzung einhergehenden zivilrechtlichen Fragen insgesamt zu untersuchen.

12. Wie wäre aus Sicht der Bundesregierung eine allgemeine Auskunfts- und Mitteilungspflicht zur verdeckten Überwindung von Sicherheitssystemen mit dem Ziel der Verbesserung der Cybersicherheit vernetzter Geräte (Internet der Dinge) vereinbar?

Nach dem Verständnis der Bundesregierung beschränkt sich der Prüfauftrag der IMK auf Mitwirkungspflichten Dritter im Einzelfall. Von der Einführung einer allgemeinen Auskunfts- und Mitteilungspflicht zur verdeckten Überwindung von Sicherheitssystemen wird daher nicht ausgegangen.

Eine Unterscheidung zwischen der Sicherheit vernetzter Geräte und der Sicherheit informationstechnischer Systeme ist aus technischer Sicht nicht sinnvoll, wenngleich aus praktischer Sicht besonderer Verbesserungsbedarf bei Geräten für das Internet der Dinge besteht. Es ist Ziel der Bundesregierung, dass sich die Sicherheit aller informationstechnischen Systeme auf einem hohen Niveau befindet. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

13. Wie ist aus Sicht der Bundesregierung eine technikoffene Mitwirkungspflicht Privater beim verdeckten Öffnen und Überwinden von Diebstahlwarnanlagen mit dem Ziel der Verbesserung der Cybersicherheit vernetzter Geräte (Internet der Dinge) vereinbar?

Diebstahlwarnanlagen sind Sicherheitssysteme. Es wird daher auf die Antwort zu Frage 12 verwiesen.

14. Wie plant die Bundesregierung, das in der Cyber-Sicherheitsstrategie für Deutschland 2016 definierte Ziel, „Vertrauen zwischen Unternehmen und Behörden in Diskretion und Professionalität im Umgang mit sensiblen Sachverhalten bei der Schaffung des notwendigen IT-Sicherheitsniveaus“ zu gewährleisten, mit Blick auf das Internet der Dinge zu verwirklichen?

Insbesondere mit der „Allianz für Cybersicherheit“ und dem „UP KRITIS“ bestehen bereits zwei Plattformen, an denen Staat und Wirtschaft gleichermaßen partizipieren. Auf diesen Plattformen besteht bereits heute die Möglichkeit, sich zu sensiblen Sachverhalten mit der gebotenen Diskretion und Professionalität

auszutauschen. In den dort vorhandenen Unterstrukturen werden Sicherheitsmaßnahmen erarbeitet, diskutiert und können sodann individuell umgesetzt werden. Sicherheits- und Vorsorgeprozesse werden in Form von Übungen evaluiert, sowie Warn- und Informationsdienste etabliert.

Das BSI steht zudem in regelmäßigem Kontakt mit den relevanten Herstellern, um sich über die erforderlichen Mindestsicherheitsstandards auszutauschen.

Die Bundesregierung wurde im April 2017 durch den Bundestag aufgefordert, ein Gütesiegel für IT-Sicherheit auszuarbeiten. Dieses soll vor allem auch Mindestsicherheitsstandards für an das Internet angeschlossene Produkte (IoT-Devices) enthalten. Die Optionen für ein derartiges Gütesiegel werden derzeit geprüft.

15. Wie wäre aus Sicht der Bundesregierung eine allgemeine Auskunfts- und Mitteilungs- oder Mitwirkungspflicht zur verdeckten Überwindung von Sicherheitssystemen mit dem Ziel vereinbar, „Vertrauen zwischen Unternehmen und Behörden in Diskretion und Professionalität im Umgang mit sensiblen Sachverhalten bei der Schaffung des notwendigen IT-Sicherheitsniveaus“ zu gewährleisten?

Auf die Antwort zu Frage 12 wird verwiesen.

16. Wie ist aus Sicht der Bundesregierung eine technikoffene Mitwirkungspflicht Privater beim verdeckten Öffnen und Überwinden von Diebstahlwarnanlagen mit dem Ziel vereinbar, „Vertrauen zwischen Unternehmen und Behörden in Diskretion und Professionalität im Umgang mit sensiblen Sachverhalten bei der Schaffung des notwendigen IT-Sicherheitsniveaus“ zu schaffen?

Auf die Antwort zu Frage 13 wird verwiesen.

17. Welche verfassungsrechtlichen Grenzen bestehen aus Sicht der Bundesregierung für eine Verpflichtung Privater (u. a. Hersteller von Alarm- und Sicherheitssystemen sowie generell von anderer Hard- und Software, einschließlich vernetzter Geräte) zur Durchführung oder Ermöglichung verdeckter Maßnahmen der Informationserhebung?

Je nach Ausgestaltung sind insbesondere die Berufsfreiheit der zur Durchführung oder Ermöglichung verdeckter Maßnahmen der Informationserhebung zu verpflichtenden Privaten sowie die Grundrechte der von der Informationserhebung Betroffenen zu beachten. Im Übrigen wird auf die Vorbemerkung der Bundesregierung verwiesen.

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