Deutscher Bundestag **Drucksache 19/7698**

19. Wahlperiode 12.02.2019

Antrag

der Abgeordneten Manuel Höferlin, Jimmy Schulz, Stephan Thomae, Grigorios Aggelidis, Renata Alt, Christine Aschenberg-Dugnus, Jens Beeck, Nicola Beer, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg, Dr. Marco Buschmann, Karlheinz Busen, Britta Katharina Dassler, Hartmut Ebbing, Dr. Marcus Faber, Daniel Föst, Otto Fricke, Thomas Hacker, Katrin Helling-Plahr, Markus Herbrand, Torsten Herbst, Katja Hessel, Dr. Christoph Hoffmann, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Gyde Jensen, Dr. Christian Jung, Dr. Marcel Klinge, Pascal Kober, Carina Konrad, Konstantin Kuhle, Alexander Graf Lambsdorff, Ulrich Lechte, Michael Georg Link, Oliver Luksic, Till Mansmann, Alexander Müller, Frank Müller-Rosentritt, Dr. Martin Neumann, Bernd Reuther, Dr. Wieland Schinnenburg, Matthias Seestern-Pauly, Frank Sitta, Judith Skudelny, Bettina Stark-Watzinger, Dr. Marie-Agnes Strack-Zimmermann, Benjamin Strasser, Katja Suding, Linda Teuteberg, Michael Theurer, Manfred Todtenhausen, Dr. Andrew Ullmann, Gerald Ullrich, Johannes Vogel (Olpe), Sandra Weeser, Nicole Westig, Katharina Willkomm und der Fraktion der FDP

Digitalisierung ernst nehmen – IT-Sicherheit stärken

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest:

1. Die IT-Sicherheit ist die Achillesferse des Informationszeitalters. Ihre Gewährleistung ist eine Kernherausforderung der Digitalisierung, der die Bundesregierung nicht ausreichend Beachtung schenkt. Vielmehr noch: Die Bundesregierung räumt der IT-Sicherheit gegenüber anderen Zielen nicht Priorität ein, sondern beteiligt sich - etwa um staatliche Zugriffe auf IT-Systeme zu ermöglichen - sogar noch an der Offenhaltung von Sicherheitslücken. Dies ist unverantwortlich: Die Digitalisierung führt dazu, dass nahezu alle Informationen auf informationstechnischen Geräten vorhanden sind und diese vernetzt über das Internet in unserem Leben eine immer größere Bedeutung einnehmen (bildlich: "Internet of Everything"). Dies bedeutet aber auch, dass die Gewährleistung von IT-Sicherheit entscheidend dafür ist, den unberechtigten Zugriff auf sensible Informationen wie personenbezogene Daten oder Unternehmensgeheimnisse zu verhindern. Angriffe auf informationstechnische Systeme können aber dazu dienen, diese zu steuern, und hierdurch erheblichen Schaden für Einzelne, Unternehmen oder auch gesamtgesellschaftlich zu verursachen. Die Gewährleistung von IT-Sicherheit ist daher für die Informationsgesellschaft ebenso wichtig wie der Brandschutz für Gebäude oder die Sicherheit im Straßenverkehr für die Fortbewegung. Damit die Menschen in die Chancen der Digitalisierung vertrauen, muss die IT-Sicherheit

ebenso strikt gewährleistet werden. Das Bundesverfassungsgericht hat diese Entwicklung schon 2008 vorweggenommen und das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme ("IT-Grundrecht") entwickelt (BVerfGE 120, 274 Rn. 201 ff.) und hiermit einen Gestaltungsauftrag an den Gesetzgeber formuliert, den dieser bisher nicht annähernd erfüllt hat. Dieser muss konsequent verwirklicht werden, anstatt die IT-Sicherheit in der Breite unter dem Deckmantel vermeintlicher Sicherheitsgewinne gezielt zu schwächen.

2. Die Verteilung der Aufgaben und Kompetenzen im Bund sowie zwischen Bund und Ländern ist nicht geeignet, diesen Herausforderungen zu begegnen. Kernproblem ist, dass das Bundesamt für die Sicherheit in der Informationstechnik (BSI) dem Bundesministerium des Innern, für Bau und Heimat (BMI) untersteht (§ 1 Satz 2 BSI-Gesetz) und damit dessen Rechts- und Fachaufsicht unterliegt. Da dem BMI zugleich auch das Bundeskriminalamt (BKA) und das Bundesamt für Verfassungsschutz (BfV) unterstehen, die ein Interesse an der Nutzung von Sicherheitslücken haben, um auf informationstechnische Erkenntnisse für ihre Aufgaben zugreifen zu können, besteht hier ein institutionalisierter Interessenkonflikt innerhalb desselben Ministeriums. Dieser führt dazu, dass sich das BSI nicht kompromisslos für die Gewährleistung der IT-Sicherheit einsetzen kann und seine Glaubwürdigkeit als Ansprechpartner für Unternehmen und IT-Sicherheitsforscher, die Sicherheitslücken melden möchten, erheblich leidet. Die zersplitterten Zuständigkeiten innerhalb der Bundesregierung im Bereich der Digitalisierung tragen noch zu einer Verstärkung der Problematik bei. Abhilfe kann hier ein federführendes und zugleich koordinierendes Digitalministerium schaffen. Das Digitalministerium setzt sich aus drei Säulen zusammen - 1. Säule: Geschäftsbereiche mit Federführung des Ministeriums, 2. Säule: Koordination von Fachvorhaben mit zuständigen Ministerien, 3. Säule: Think Tank für Innovationen im Bereich der Digitalisierung.

3. Die IT-Sicherheitsarchitektur ist im Rahmen einer Föderalismus-Kommission III, welche die Zuständigkeitsverteilung zwischen Bund und Ländern im Bereich der Inneren Sicherheit klärt, neu zu ordnen. Die Abwehr von Gefahren für die IT-Sicherheit liegt bisher als Teil der allgemeinen Gefahrenabwehr grundsätzlich bei den Polizeien. Die Rolle des Bundes und insbesondere des BSI ist hierbei zu stärken, insbesondere durch eine Eilkompetenz des BSI. Die Abwehr von Gefahren für die IT-Sicherheit sollte unterhalb der Schwelle der Landesverteidigung auch weiterhin als Gefahrenabwehr und Strafverfolgung begriffen werden, für die neben dem BSI in erster Linie Polizei und Strafverfolgungsbehörden zuständig sind.

4. Offensive Maßnahmen wie etwa eine aktive, digitale Gegenwehr, durch die beispielsweise Daten auf fremden Servern gelöscht werden oder sogar Hardware zerstört wird (sog. Hack Backs), sind keine geeigneten Instrumente, um die IT-Sicherheit zu sichern. Sie bergen vielmehr erhebliche Gefahren: Diese Maßnahmen nutzen selbst Sicherheitslücken aus, die hierfür geheimgehalten werden und während dieser Zeit für IT-Angriffe von Dritten auf Einzelne und Unternehmen ausgenutzt werden können. Zudem kann der Urheber eines Cyberangriffs meist nicht mit absoluter Sicherheit geklärt werden. Es besteht die Gefahr, dass es zu einem „Cyber-Kundus“ kommt, bei dem zivile Einrichtungen wie Krankenhäuser, Kindergärten und Kraftwerke in völlig unbeteiligten Ländern zur Zielscheibe einer Gegenoffensive gemacht und unschuldige Dritte getroffen werden, wenn zuvor deren Rechner gekapert worden sind. Nicht Hack Backs führen zu einem Mehr an Sicherheit, sondern ein besserer Schutz der Netze und Daten, sowie das Schließen von Sicherheitslücken.

5. Die Herausforderung der Gewährleistung der IT-Sicherheit durchzieht alle Lebensbereiche. Es ist daher illusorisch anzunehmen, dass der Staat in der Lage

wäre, allein durch Behörden die Erreichung dieses Ziels sicherzustellen. Vielmehr muss der Einzelne in die Lage versetzt werden, seine informationstechnischen Systeme, Daten, private Kommunikation und Geschäftsgeheimnisse selbst vor potentiellen Angreifern zu schützen. Er muss daher ein wirksames "Recht auf Verschlüsselung" seiner Daten haben (siehe hierzu Bundestags-Drucksache 19/5764). Kern dieses Rechts muss die Verpflichtung von Telekommunikations- und Telemedienanbietern sein, ihre Kommunikationsdienste verschlüsselt anzubieten (Ende-zu-Ende-Verschlüsselung).

6. Eine besondere Herausforderung ist die Gewährleistung der IT-Sicherheit von Hard- und Software bei Verbraucherprodukten, die zunehmend mit dem Internet verbunden und damit angreifbar sind. Verbraucher sind derzeit nur eingeschränkt in der Lage, die IT-Sicherheit von Verbraucherprodukten selbst einzuschätzen. Dies beginnt bereits bei der wesentlichen Frage, ob und für wie lange der Hersteller eines Produktes Updates zur Verfügung stellt, um Sicherheitslücken zu schließen. Wie auch bei anderen Verbraucherprodukten, sind daher Maßnahmen zu ergreifen, um Transparenz herzustellen und die Hersteller und Händler von Hard- und Software zur Vermeidung von Gefahren für die Rechtsgüter und Interessen von Verbrauchern und Dritten zu verpflichten.

7. IT-Sicherheit und Datenschutz sind untrennbar miteinander verwoben. Wer nicht weiß, welche Stelle welche Daten über ihn verarbeitet, kann auch nicht wirksam über ihren Schutz entscheiden. Die Datenschutz-Grundverordnung (DSGVO) enthält auch zur Datensicherheit (Art. 32 DSGVO) und zum Datenschutz durch Technik und technikfreundliche Voreinstellungen (privacy by design und default, Art. 25 DSGVO) wichtige Ansätze, die jedoch weiterentwickelt und konkretisiert werden müssen. Datenschutz muss bereits bei der Konstruktion von Hard- und Software mitgedacht werden; Datenschutz durch Technik, die Vorgabe datenschutzrechtlicher Voreinstellungen und ein Design, das den Nutzern in der Praxis eine eigenverantwortliche Ausübung ihres Rechts auf informationelle Selbstbestimmung ermöglicht, sollten daher bereits von den Herstellern berücksichtigt werden müssen. Neben den Datenschutzaufsichtsbehörden sollte eine wichtige Rolle bei der Aufklärung von Bürgerinnen und Bürgern sowie Unternehmen der Stiftung Datenschutz zukommen, ähnlich wie der Stiftung Warentest im Bereich von Verbraucherprodukten. Die Bundesregierung hat es seit Errichtung der Stiftung Datenschutz unterlassen, diese ausreichend finanziell auszustatten.

8. Das Strafrecht stellt bereits heute IT-Angriffe unter Strafe und kriminalisiert hierbei ungewollt teilweise auch erwünschte Verhaltensweisen, die der Aufdeckung und Schließung von Sicherheitslücken dienen sollen. Anstatt reflexartig Diskussionen über die Einführung neuer Straftatbestände zu führen, sollte der Gesetzgeber klarstellen, dass diese Handlungen nicht strafbar sind, wenn sie mit diesem Ziel erfolgen, und damit die Rechtsunsicherheit für IT-Sicherheitsforscher beseitigen. Generell sollten die Straftatbestände des IT-Strafrechts (v.a. §§ 201a ff., 303a, 303b StGB) auf ihre Systematik hin überprüft werden und ob sie die Integrität informationstechnischer Systeme bereits ausreichend schützen. Zudem sollten die Straftatbestände, welche Datenschutzverstöße unter Strafe stellen (§ 42 BDSG), in das Kernstrafrecht integriert werden, da sie bisher von den Staatsanwaltschaften kaum verfolgt werden.

II. Der Deutsche Bundestag fordert die Bundesregierung zu folgenden Maßnahmen auf, um die IT-Sicherheit in Deutschland zu stärken:

1. Aktuelle IT-Sicherheitsvorfälle (wie z.B. jüngst die Veröffentlichung von personenbezogenen Daten von Politikern) dürfen nicht missbraucht werden, um unter ihrem Deckmantel die staatlichen Ermittlungsbefugnisse auszuweiten und die

Grundrechte der Bürgerinnen und Bürger einzuschränken. So verstößt insbesondere die Vorratsdatenspeicherung von Telekommunikationsverbindungsdaten gegen die europäischen Grundrechte; die Bundesregierung muss das deutsche Recht endlich entsprechend anpassen (siehe hierzu den Gesetzentwurf der Fraktion der Freien Demokraten für ein Bürgerrechte-Stärkungsgesetz, Bundestags-Drucksache 19/204).

2. Die Bundesregierung muss sich endlich mit der gebotenen Priorität der Organisation der IT-Sicherheit in Deutschland widmen. Für die IT-Sicherheit sind auf Bundesebene momentan zu viele Bundesministerien und Bundesämter gleichzeitig zuständig. Im Zweifelsfall will jedoch keiner die Verantwortung übernehmen. Es müssen klare Kompetenzabgrenzungen vorgenommen werden, ohne dabei unnötige Doppelstrukturen zu erreichen. Gleichzeitig müssen die Sicherheitsbehörden über klar definierte Meldeketten und Berichtswege kommunizieren und das Nationale Cyberabwehrzentrum (NCAZ) als Kooperations- und Informationsplattform ausgebaut werden.

- Um den bestehenden Interessenskonflikt im BMI aufzulösen, der sich aus der Inkaufnahme einiger Sicherheitslücken zu Ermittlungszwecken und der gleichzeitigen Zuständigkeit für den wirksamen Schutz der IT-Infrastruktur ergibt, und das Vertrauen in die Neutralität des BSI zu stärken, muss das BSI aus der Zuständigkeit des BMI herausgelöst werden.
- Nach seiner neuen organisatorischen Zuordnung soll das BSI als zentrale Stelle für Fragen der IT-Sicherheit in der Informationsgesellschaft weiter etabliert werden. Um die Funktion als zentrale Meldestelle effektiv ausüben zu können, sind die bestehenden Meldeverpflichtungen und dahingehenden Verwaltungsvorschriften auf ihre Vollständigkeit zu prüfen. Das BSI muss über alle Sicherheitslücken, die staatlichen Stellen bekannt werden, informiert werden. Insbesondere eine mögliche Verpflichtung von privaten Stellen in Bezug auf Sicherheitslücken oder IT-Sicherheitsvorfälle soll unter Beachtung des risikobasierten Ansatzes geprüft werden. Perspektivisch soll das BSI auch durch die Hersteller von Hard- und Software über Sicherheitslücken informiert werden, wenn von diesen Lücken für Einzelne oder gesamtgesellschaftlich erhebliche Risiken ausgehen.
- Das BSI übernimmt darüber hinaus das zentrale Schwachstellenmanagement. Alle Schwachstellen, die dem BSI gemeldet werden oder die dem BSI im Rahmen der Wahrnehmung der zu seinem Aufgabenbereich gehörenden Unterstützungsleistungen bekannt geworden sind, werden im eigenen Zuständigkeitsbereich versucht, selbst zu schließen. Über Sicherheitslücken im Zuständigkeitsbereich Dritter, die dem BSI bekannt geworden sind, informiert das BSI diese Dritten. Gemäß des Grundsatzes der „responsible disclosure“ ist das BSI berechtigt, Sicherheitslücken zu veröffentlichen, wenn die Sicherheitslücken nicht in angemessener Zeit geschlossen werden oder die Nutzer hiervor gewarnt werden. Es ist zu prüfen, in welchen Fällen über kritische Infrastruktur hinaus das BSI die Befugnis erhalten sollte, die Schließung von Sicherheitslücken, aufgrund der gravierenden Gefahren, die von ihnen ausgehen, und das Aufspielen von Updates anzuordnen.
- Neben dem Schutz der Informationstechnik des Bundes, und somit der Netze der Bundesverwaltung, soll der Aufgabenkatalog des BSI um die Möglichkeit erweitert werden, den Schutz der Informationstechnik der Verfassungsorgane zu übernehmen, wenn diese darum bitten.

- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) soll bei seiner Aufgabenerfüllung nicht nur auf die Beratungsleistungen des BSI zurückgreifen können. Bei IT-Sicherheitsvorfällen, die in die Zuständigkeit des BSI fallen, und bei denen in nicht unerheblichem Maße personenbezogene Daten betroffen sind, ist der ebenfalls zuständige BfDI von Anfang an hinzuzuziehen.
- Um sich auf Landesebene noch besser zu vernetzen, sollen die Bemühungen des BSI, deutschlandweit Verbindungsbüros aufzubauen, durch den Bund unterstützt werden.
- Bei der Beschaffung der Informationstechnik des Bundes darf nicht allein das Kriterium der Wirtschaftlichkeit ausschlaggebend sein, das Kriterium der IT-Sicherheit muss ein wesentlich stärkeres Gewicht erhalten.
- Die im Zuständigkeitsbereich des BSI liegenden Stellen des Bundes müssen Notfallpläne für IT-Sicherheitsvorfälle verschiedener Stufen erstellen und diese regelmäßig zum Gegenstand von Übungen machen. Das BSI soll darüber hinaus auch durch unangekündigte Penetrationstests die Sicherheit der informationstechnischen Systeme in seinem Zuständigkeitsbereich regelmäßig überprüfen. Nötigenfalls muss eine explizite Rechtsgrundlage hierfür geschaffen werden.
- Um- und Neubauten von kritischer Infrastruktur müssen grundsätzlich ein Cyber-Sicherheitskonzept beinhalten, um Fördergelder zu erhalten.
- Das Nationale Cyberabwehrzentrum (NCAZ) beim BSI, welches momentan nur auf Basis von Kooperationsvereinbarungen zwischen den beteiligten Bundesbehörden operiert, muss auf eine gesetzliche Grundlage gestellt werden. Die personellen und finanziellen Kapazitäten des NCAZ sollen genau wie das ebenfalls beim BSI angesiedelte Nationale IT-Lagezentrum so aus den Etats der zuständigen Ressorts ausgestaltet sein, dass eine Besetzung des NCAZ rund um die Uhr möglich ist. Als federführende Behörde, welche die Kooperation im NCAZ koordiniert, soll das BSI für relevante IT-Sicherheitsvorfälle mit einer Eilkompetenz ausgestattet werden, welche beispielsweise die Anordnung von Sicherheitsupdates oder der (temporären) Entfernung von Daten oder Websites aus dem Internet ermöglicht.
- Die Bundesregierung muss die Umsetzung der Cybersicherheits-Strategien von 2011 und 2016 evaluieren. Künftig sollen starre Cyber-Sicherheitsstrategien durch agile Umsetzungsstrategien ersetzt werden, die mit klaren Zielen versehen sind und die mindestens jährlich zu evaluieren und fortzuschreiben sind.
- Der im Rahmen der Umsetzung der ersten Cyber-Sicherheitsstrategie der Bundesregierung eingesetzte Nationale Cyber-Sicherheitsrat soll in die dritte Säule des neu zu schaffenden Digitalministeriums eingegliedert werden und weiter zu einer Plattform und einem Think Tank zur Diskussion zukünftiger IT-Sicherheitsfragen ausgebaut werden.
- Alle Behörden, die mit der IT-Sicherheit befasst sind, müssen im Rahmen der verfügbaren Haushaltsmittel ausreichend personell und finanziell ausgestattet werden. Insbesondere die Gewinnung von geeignetem IT-Personal muss im Vordergrund stehen. Als kurz- und mittelfristige Maßnahmen sollen hierfür insbesondere die Möglichkeiten des Personal-Pooling und das Ausschöpfen bestehender Anreiz-Instrumente (wie etwa des Personalgewinnungszuschlags im BBesG) geprüft werden. Als langfristige Maßnahmen müssen die betroffenen Behörden mehr Personal selbst ausbilden und es sind sowohl für

IT-Personal als auch für Ermittlungspersonal die Möglichkeit des Direkteinstieg in bestimmte Tätigkeitsfelder und die Schaffung entsprechender Laufbahnen zu prüfen.

3. Die Bundesregierung soll sich dafür einsetzen, gemäß des Vorschlags der FDP-Bundestagsfraktion (siehe hierzu Bundestags-Drucksache 19/7424) eine Föderalismus-Kommission III einzusetzen. Die neu einzusetzende Föderalismus-Kommission III soll sich auch mit der Frage der Zusammenarbeit zwischen Bund und Ländern im Bereich der IT-Sicherheit beschäftigen. Es sind etwa die Zuständigkeitsverteilung und das Selbsteintrittsrecht der relevanten Bundesbehörden in unklaren Fällen zu klären, da die Abwehr von Gefahren zur Zeit grundsätzlich bei den Landespolizeibehörden liegt.

- Es müssen einheitliche Meldewege zwischen den verschiedenen involvierten Behörden definiert werden und es soll ausgearbeitet werden wie der Aufbau der benötigten personellen und strukturellen IT-Kapazitäten auf allen Ebenen sichergestellt werden kann. Die Einbindung der jeweils zuständigen Datenschutzbeauftragten in die Meldewege ist zu prüfen, in jedem Fall soll jedoch eine beratende Hinzuziehung stattfinden, wenn personenbezogene Daten in nicht unerheblichem Umfang betroffen sind.
- Die Erweiterung des Zuständigkeitsbereichs der Zentralen Ansprechstellen Cybercrime (ZAC) ist zu prüfen. Daneben soll die organisatorische Aufhängung der jeweiligen Cybercrime-Zentren in den Bundesländern möglichst einheitlich aufgebaut werden.
- Für das NCAZ beim BSI, welches nun auf eine gesetzliche Grundlage gestellt wurde, soll die Föderalismus-Kommission III Regelungen für die Achtung des Trennungsgebotes erarbeiten, die gleichermaßen dem Bedürfnis der Kooperation und des Informationsaustauschs Rechnung tragen. Die Möglichkeit der anlassbezogenen Entsendung von Verbindungsbeamten (insbesondere von der jeweiligen Länder-Ebene) ist in die Ausarbeitung mit einzubeziehen.

4. Die Bundesregierung soll die Bedenken zur Attributionsproblematik sowie den Gefahren und den möglichen Folgen von Hack Backs ernstnehmen und die wider besseren Wissens stattfindende weitere Prüfung zur Schaffung einer rechtlichen Grundlage für Hack Backs umgehend einstellen. Sie soll ihre Bemühungen stattdessen auf effiziente Schutz- und Verteidigungssysteme konzentrieren. Wenn in Europa die Fähigkeiten gebündelt werden, kann Europa - ähnlich wie beim Datenschutz - auch bei der IT-Sicherheit eine Vorreiterrolle einnehmen und dadurch weltweite Standards setzen. Die Bundesregierung muss ihren Einfluss im Rat der EU deshalb dazu nutzen, langfristig ein Mandat für eine gemeinsame Europäische Cybersicherheitsagentur zu sichern. Außerdem soll sie sich dafür einsetzen, dass im Rahmen einer fortgesetzten gemeinsamen Cyber-Sicherheitsstrategie ein No-Spy-Abkommen zwischen den Mitgliedsstaaten abgeschlossen wird. Deutschland sollte seine Vorreiterrolle auch nutzen, um sich auf internationaler Ebene für eine völkervertragliche Regelungen zur Steigerung der IT-Sicherheit und zur Einhegung des Einsatzes von "Cyberwaffen" innerhalb und außerhalb bewaffneter Konflikte einzusetzen. Ein erster Ansatzpunkt könnte das Abkommen zwischen den USA und China sein, kritische zivile Infrastruktur nicht zu beeinträchtigen.

5. Die Bundesregierung muss die Nutzung von Verschlüsselung vorantreiben und hierzu:

- sich zum Schutz der Privatsphäre und zur Erhöhung der IT-Sicherheit für ein Recht auf Verschlüsselung einsetzen;

- in diesem Sinne Telekommunikations- und Telemedienanbieter verpflichten, ihre Kommunikationsdienste nach einer Übergangsfrist für zukünftige technische Systeme als Standard abhörsicher (Ende-zu-Ende verschlüsselt) anzubieten und sich im Rahmen der Verhandlungen zur E-Privacy-Verordnung auf europäischer Ebene hierfür einsetzen;
- die Weiterentwicklung von Verschlüsselungstechnologien, der Sicherheit von Speichersystemen und von qualifizierten Zugriffs- und Berechtigungslogiken konsequent vorantreiben;
- sich gegen gesetzliche Beschränkungen oder Verbote kryptographischer Sicherungssysteme aussprechen;
- den Einsatz von sogenannten Backdoors verurteilen und eine staatliche Beteiligung an digitalen Grau- und Schwarzmärkten für Sicherheitslücken ablehnen;
- die Verwendung von frei verfügbaren, offenen und einfach handhabbaren Protokollen sowie Verschlüsselungsstandards wie z. B. GPG vorantreiben.

6. Die Bundesregierung soll sich zu einer defensiven Cybersicherheitsstrategie bekennen. Das heißt, alle informationstechnischen Systeme müssen mit dem Gedanken „security by design“ gestaltet werden, dies schützt proaktiv gegen erfolgreiche Angriffe aus dem Cyberraum. Alle Programmierer und Administratoren müssen konstant weitergebildet werden, um auf dem aktuellen Stand der Technik zu sein. Dies gilt nicht nur im Bereich des Betriebs sondern auch in der Entwicklung und der Gestaltung sicherer Systeme. Dazu fordern wir eine bessere finanzielle Ausstattung der IT-Sicherheitsforschung, etwa durch die Einrichtung neuer Lehrstühle zur IT-Sicherheitsforschung und -lehre. Darüber hinaus ist die IT-Sicherheit von Hard- und Software, insbesondere von Verbraucherprodukten zu stärken, indem

- die Bundesregierung auf europäischer Ebene auf die Definition verbindlicher IT-Sicherheitsstandards als Basissicherheitsniveau hinwirkt, einschließlich der Verpflichtung zur Verschlüsselung von Kommunikation und Voreinstellungen für ausreichend sichere Passwörter;
- die Vorgabe gemacht wird, IT-Sicherheit bereits bei der Konstruktion von IT-Produkten zu berücksichtigen (security by design), einschließlich der Funktion, dass alle internetfähigen Geräte über einen Mechanismus zum Aufspielen von Updates verfügen müssen, über den Softwarelücken geschlossen werden können;
- klargestellt wird (insbesondere im Rahmen der Revision der Produkthaftungs-Richtlinie), dass die Hersteller von Hard- und Software für Schäden haften, die fahrlässig durch IT-Sicherheitslücken verursacht werden, um zivilrechtliche Anreize für die Einhaltung dieser Standards zu setzen. Hierbei sind sie auch zum Ersatz der Schäden verpflichtet sind, die durch Sicherheitslücken typischerweise hervorgerufen werden (Vermögensschäden, Beeinträchtigungen der Privatsphäre, Verlust von Daten, Offenlegung von Betriebsgeheimnissen);
- Hersteller verpflichtet werden, während der üblichen Nutzungsdauer eines Produktes Updates zur Verfügung zu stellen und - sollte dies wirtschaftlich über die Gewährleistungszeit hinaus nicht möglich sein - auf dem Produkt deutlich auf die Dauer der Gewährleistung der IT-Sicherheit hinzuweisen („Mindesthaltbarkeitsdatum“).

7. Die datenschutzrechtlichen Straftatbestände (§ 42 BDSG) sind in das Kernstrafrecht zu überführen und die §§ 202a ff. auf ihre Systematik hin zu überprüfen, hierbei ist das Schutzgut der Integrität informationstechnischer Systeme stärker zu berücksichtigen. Einerseits würde damit dem Umstand Rechnung getragen, dass der Wert von Daten in Zeiten der Digitalisierung auch für Kriminelle stetig steigt. Anderseits würde davon auch eine positive Signalwirkung für die Strafverfolgungsbehörden ausgehen. Außerdem ist die Stiftung Datenschutz durch einen Zuschuss aus dem Etat des BMI im Bundeshaushalt auskömmlich finanziell auszustatten, damit sie insbesondere ihrem Bildungsauftrag und der Förderung eines effizienten Privatsphärenschutzes nachkommen kann.

8. Die Bundesregierung muss das Auffinden und Schließen von Sicherheitslücken rechtlich eindeutig ermöglichen, indem sie einen Gesetzentwurf vorlegt, durch welchen

- im Urheberrecht (§§ 69d, 69e UrhG) klargestellt wird, dass Reverse Engineering, das mit dem Ziel des Auffindens und Schließens von Sicherheitslücken erfolgt, zulässig ist;
- in den §§ 202a ff. StGB die Strafbarkeit an die Intention der Handlung geknüpft wird, um sicherzustellen, dass Maßnahmen, die mit dem Ziel der Schließung von Sicherheitslücken oder zu Zwecken der Fort- und Weiterbildung erfolgen, nicht strafbar sind;
- in den Regelungen zum Schutz von Betriebsgeheimnissen (insb. § 17 UWG) sichergestellt wird, dass sie nicht der Offenlegung von Sicherheitslücken im Rahmen des "responsible disclosure" entgegenstehen, zumindest wenn die Offenlegung gegenüber dem BSI erfolgt;
- die Einführung eines neuen Tatbestands des digitalen Hausfriedensbruchs abgelehnt wird. Die bisherigen Diskussionen zur Einführung eines solchen Tatbestandes konnten nicht aufzeigen, welche Strafbarkeitslücken hierdurch geschlossen werden können, nahmen aber gleichzeitig die mögliche Kriminalisierung legalen Verhaltens in Kauf.

Berlin, den 12. Februar 2019

Christian Lindner und Fraktion