Deutscher Bundestag **Drucksache 19/28873**

19. Wahlperiode 21.04.2021

Entschließungsantrag

der Abgeordneten Manuel Höferlin, Stephan Thomae, Grigorios Aggelidis, Renata Alt, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Mario Brandenburg, Sandra Bubendorfer-Licht, Dr. Marco Buschmann, Dr. Marcus Faber, Daniel Föst, Otto Fricke, Thomas Hacker, Reginald Hanke, Peter Heidt, Torsten Herbst, Dr. Gero Hocker, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Daniela Kluckert, Pascal Kober, Konstantin Kuhle, Ulrich Lechte, Matthias Nölke, Dr. Wieland Schinnenburg, Matthias Seestern-Pauly, Frank Sitta, Hermann Otto Solms, Bettina Stark-Watzinger, Dr. Marie-Agnes Strack-Zimmermann, Benjamin Strasser, Katja Suding, Linda Teuteberg, Gerald Ullrich, Nicole Westig, Katharina Willkomm und der Fraktion der FDP

zu der dritten Beratung des Gesetzentwurfs der Bundesregierung
– Drucksachen 19/26106, 19/26921, 19/27035 Nr. 1.7, 19/28844 –

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

Der Bundestag wolle beschließen:

I. I. Der Deutsche Bundestag stellt fest:

Cyberkriminalität in ihren unterschiedlichen Ausprägungen und die dadurch bedingte allgemeine Bedrohungslage im Cyberraum für alle Bürgerinnen und Bürger, die sich im Netz bewegen, ist in den letzten Jahren verstärkt in den Fokus öffentlicher Aufmerksamkeit und medialer Berichterstattung gerückt. Beispiele sind Angriffe im Cyberraum auf prominente Ziele wie den Deutschen Bundestag (IVBB-Hack), auf die Europäische Arzneimittelagentur (EMA) oder eine Reihe von Krankenhäusern in Deutschland. Es wurden außerdem auch immer mehr massive Sicherheitslücken (z.B. Heartbleed, und Microsoft Exchange-Lücke) oder groß angelegte Malware- und Phishing-Kampagnen (z.B. Emotet, TrickBot und Ghostwriter) bekannt. An Bekanntheit gewonnen haben ebenfalls sogenannte „Doxing“-Vorfälle, die Veröffentlichung großer Mengen an Daten aus Datenleaks im Internet (z.B. Mastercard, Clearview AI und Facebook) oder kritische Angriffe auf Einzelziele, bei denen Datenabflüsse stattfanden (z.B. SolarWinds). Die Corona-Pandemie hat außerdem gezeigt, dass unter dem Deckmantel emotional aufgeladener Themen Cyberkriminalität mit altbekannten

Mitteln, aber aggressiverer Vorgehensweise stattfindet (vgl. Lagebild des Bundeskriminalamts, "Sonderauswertung Cybercrime in Zeiten der Corona-Pandemie", abrufbar unter: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeSonderauswertungCorona2019.html).

Das Ziel einer hundertprozentigen Sicherheit vor Gefahren im Cyberraum ist nicht erreichbar und damit auch nicht der richtige Denkansatz. Vielmehr sollte es darum gehen, nachhaltige Strukturen im IT-Sicherheitsbereich aufzubauen und eine umfassende Cybersicherheitskultur zu entwickeln, die es Staat, Wirtschaft und Gesellschaft ermöglicht, möglichst souverän mit den Bedrohungen im Cyberraum umzugehen und bei Cybervorfällen schnell wieder handlungsfähig zu werden. Dieses agile Verständnis von Cybersicherheit, das auf transparente Kommunikation und einen kooperativen Ansatz zwischen Staat, Wirtschaft und Gesellschaft setzt, lässt die Bundesregierung leider vermissen. Anstatt dessen befeuert sie selbst immer wieder Diskussionen darum, ob Sicherheitslücken zurückgehalten und von Sicherheitsbehörden ausgenutzt werden sollen oder bedient sich des Mythos der sogenannten „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung". Einen möglichst hohen Grad an Sicherheit kann es aber nur geben, wenn alle bekannten Sicherheitslücken geschlossen werden, der Staat diese nicht aus strategischen Gründen zurückhält und wenn die Bürgerinnen und Bürger aufgrund eines echten Rechts auf Ende-zu-Ende-Verschlüsselung vertraulich miteinander kommunizieren können (wie von der FDP-Fraktion in dem Antrag „Recht auf Verschlüsselung – Privatsphäre und Sicherheit im digitalen Raum stärken" auf Bundestags-Drs. 19/5764 gefordert).

Der vorliegende Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0), BT-Drs. 19/26106, lässt erkennen, dass die Bundesregierung es mit der IT-Sicherheit der Bevölkerung weiterhin nicht ernst genug meint und damit selbst schon zum Risiko für die IT-Sicherheit geworden ist. Eine Bekämpfung der Bedrohungen aus dem Cyberraum ist unmissverständlich an dem Ziel auszurichten, die Sicherheit für staatliche Strukturen, die Wirtschaft und die Bürgerinnen und Bürger im Cyberraum zu verbessern. Um diesem Ziel besser gerecht zu werden als der vorliegende Gesetzentwurf, hat die Fraktion der Freien Demokraten im Deutschen Bundestag zur Beratung des IT-Sicherheitsgesetzes 2.0 im Ausschuss für Inneres und Heimat mehrere Änderungsanträge eingebracht:

- Regelungen zur IT-Sicherheit der Mobilfunknetze beim 5G-Ausbau sind ihrem Wesen nach sinnvoller im Telekommunikationsgesetz zu regeln und sollten deshalb in den noch laufenden Beratungen zum Telekommunikationsmodernisierungsgesetz, Bundestags-Drucksache 19/26108, dorthin überführt werden. Der ewige Streit um die Beteiligung nicht vertrauensvoller Anbieter am 5G-Ausbau hat zu lange dazu geführt, die Beratungen des IT-Sicherheitsgesetzes 2.0 zu blockieren.
- Das Bundesamt für die Sicherheit in der Informationstechnik (BSI) wird in seiner Funktion als Meldestelle für Sicherheitslücken oder andere Risiken für die IT-Sicherheit gestärkt und immer mehr zu einer allgemeinen Meldestelle für die Sicherheit in der Informationstechnik ausgebaut. In diesem Rahmen muss das BSI für selbst detektierte oder ihm anderweitig bekannt gewordene Sicherheitslücken zur Weitergabe der Informationen an die Verantwortlichen verpflichtet werden und einen „koordinierten Offenlegungsprozess" zusammen mit den Verantwortlichen einleiten, wenn Dritte von Sicherheitslücken betroffen sind. Der koordinierte Offenlegungsprozess wird in einer Rechtsverordnung durch das Bundesministerium des Innern, für Bau und Heimat (BMI) nach Anhörung der Wirtschaftsverbände festgelegt.

- Die Meldepflichten gegenüber dem BSI in Bezug auf bekannt gewordene Informationen über Gefahren für die Sicherheit in der Informationstechnik, insbesondere zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und den dabei beobachteten Vorgehensweisen sollen auch auf die Bundesministerien und darunter liegenden Verwaltungsbehörden erstreckt werden.
- Wo Informationen über Sicherheitslücken durch verpflichtete Unternehmen gemeldet werden müssen, braucht es auch einen qualitativen Rückkanal an Informationen. Deshalb wird das BSI verpflichtet das kontinuierlich aktualisierte Lagebild zu Cyberbedrohungen in regelmäßigen Abständen an die meldenden Unternehmen zu übermitteln.
- Großflächig vorgesehene Ausnahmen von den durch das BSI festgelegten Mindeststandards der Sicherheit der Informations- und Kommunikationstechnik für das Auswärtige Amt werden aufgehoben. Die vorgesehe Ausnahme für den Geschäftbereich des Bundesministeriums der Verteidigung bleibt bestehen, da eine Verpflichtung besteht, ein vergleichbares Sicherheitsniveau in eigener Zuständigkeit sicherzustellen. Der lediglich empfehlende Charakter der Mindeststandards für Gerichte und Verfassungsorgane wird ebenfalls gestrichen.
- Das BSI wird durch die neu im BSI-Gesetz verankerten Anordnungsbefugnisse immer mehr zur Gefahrenabwehrbehörde für den Bereich der Cyber-Sicherheit. Aufgrund der Möglichkeit des Eingriffs in das IT-Grundrecht der Nutzerinnen und Nutzer muss jedoch aufgrund nicht vorgesehener, ausreichender Schutzmechanismen die Anordnungsbefugnis gegenüber Telekommunikationsdiensteanbietern, “technische Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene informationstechnische Systeme (zu verteilen)“ gestrichen werden.
- Die Selbsterklärung zur IT-Sicherheit durch die neue Kategorie von verpflichteten „Unternehmen im besonderen öffentlichen Interesse“ wird erleichtert, ohne neue Bürokratie aufzubauen. Dafür wird das im Gesetzentwurf vorgesehene Prinzip umgekehrt: das BSI hat Formulare als Arbeitshilfe einzuführen, die Unternehmen sind jedoch darin frei, ob sie diese verwenden oder die geforderte Selbsterklärung in freier Form übermitteln.
- Auch wenn nun bereits das IT-Sicherheitsgesetz 2.0 vorgelegt wurde, können aus einer Evaluierung des ersten IT-Sicherheitsgesetzes vom 17. Juli 2015 noch wertvolle Informationen gewonnen werden. Die Evaluierungsklausel im BSI-Gesetz ist deshalb beizubehalten und nicht zu streichen.

Schon bevor das IT-Sicherheitsgesetz 2.0 beschlossen und in Kraft getreten ist, werden die Eckpunkte für das IT-Sicherheitsgesetz 3.0 bereits auf europäischer Ebene verhandelt. Am 16. Dezember 2020 hat die EU-Kommission einen Entwurf für die Novelle der sogenannten „NIS-Richtlinie“ (Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union und zur Aufhebung der Richtlinie (EU) 2016/1148, COM(2020) 823 final) vorgelegt, die nach ihrer Fertigstellung zeitnah in deutsches Recht umzusetzen ist und eine erneute Änderung des IT-Sicherheitsgesetzes notwendigen machen wird.

II. Der Deutsche Bundestag fordert die Bundesregierung dazu auf,

die Vorbereitungen für ein IT-Sicherheitsgesetz 3.0 bereits heute zu beginnen und dabei die folgenden Punkte zu beachten und einzubeziehen:

- Um den bestehenden Interessenkonflikt aufzulösen, der sich daraus ergibt, dass das BSI im Geschäftsbereich des BMI belegen ist, muss das BSI aus der Zuständigkeit des BMI herausgelöst werden und ist im Idealfall als fachlich unabhängige Behörde einem noch zu gründenden Digitalministerium zu unterstellen. Der Konflikt zwischen den Interessen der ebenfalls im Geschäftsbereich des BMI liegenden Sicherheitsbehörden, die Sicherheitslücken gerne für ihre eigene Verwendung zurückhalten würden, und der gleichzeitigen Zuständigkeit des BSI für den wirksamen Schutz der IT-Sicherheit muss endlich aufgelöst werden.
- Die Konzeption des freiwilligen IT-Sicherheitskennzeichens im Entwurf des IT-Sicherheitsgesetzes 2.0 ist höchst fragwürdig und wird als reiner "Aufkleber" auf Soft- und Hardware die IT-Sicherheit von Produkten und damit den IT-Verbraucherschutz nicht verbessern. Hersteller von Hard- und Software sollten im Rahmen der Produkthaftung aber für Schäden haften, die fahrlässig durch IT-Sicherheitslücken verursacht werden, um zivilrechtliche Anreize für die Einhaltung von IT-Sicherheitsstandards zu setzen. Hierbei werden sie zum Ersatz der Schäden verpflichtet, die durch Sicherheitslücken typischerweise hervorgerufen werden (etwa Vermögensschäden, Beeinträchtigungen der Privatsphäre, Verlust von Daten, Offenlegung von Betriebsgeheimnissen). Gleichzeitig müssen Hersteller verpflichtet werden für die übliche Nutzungsdauer eines Produktes Updates zur Verfügung zu stellen und – sollte dies aus wirtschaftlichen Gründen über die Gewährleistungszeit hinaus nicht möglich sein – auf dem Produkt deutlich auf die Dauer der Gewährleistung der IT-Sicherheit hinzuweisen („Mindesthaltbarkeitsdatum").
- Meldepflichten für Sicherheitslücken und andere Bedrohungen der IT-Sicherheit durch KRITIS-Unternehmen, weitere verpflichtete Unternehmen und staatliche Stellen sowie die dadurch geschaffene Kommunikationsebene dieser Stellen mit dem BSI werden alleine nicht ausreichen, um eine agile und umfassende Cybersicherheitsstrategie zu entwickeln und so eine signifikante Erhöhung der Cybersicherheit für Staat, Wirtschaft und Gesellschaft zu erreichen. Es bedarf deshalb endlich auch einer umfassenden Wirtschaftsschutzstrategie, die nicht nur Gefahren für KRITIS-Unternehmen in den Blick nimmt, sondern sich um die Erhöhung der Cybersicherheit für die gesamte Wirtschaft bemüht. Aktuelle Vorfälle wie die Microsoft Exchange Lücke haben bewiesen, dass es Cybervorfälle geben kann, die gerade aufgrund der Tatsache, dass sie nicht nur KRITIS-Unternehmen oder staatliche Strukturen betreffen, eine besonders breitflächige und gefährliche Cyberbedrohungslage begründen.
- Der personelle IT-Sicherheitsschutz ist ein bisher zu wenig beleuchteter Bereich im Rahmen von IT-Sicherheitsstrategien. Administratorinnen und Administratoren oder andere Mitarbeiterinnen und Mitarbeiter, die in Unternehmen weitgehende Zugriffsrechte auf die verwendeten IT-Systeme haben, gelangen dadurch in eine erhebliche Machtposition in Bezug auf die Funktionsfähigkeit eingesetzter IT-Systeme. Um IT-Sicherheitsrisiken durch den Faktor Mensch möglichst auszuschließen, muss datenschutzrechtlich und arbeitsrechtlich die Möglichkeit geschaffen werden, Mitarbeiterinnen und Mitarbeiter mit Zugriff auf besonders betriebskritische Stellen der IT-Infrastrukturen eines Unternehmens einer Überprüfung nach dem Sicherheitsüberprüfungsgesetz (SÜG) zu unterziehen. Eine Verpflichtung zur Sicherheitsüberprüfung solcher Mitarbeiterinnen und Mitarbeiter ist zumindest für den KRITIS-Bereich ebenfalls in Betracht zu ziehen.
- Die besten Kenntnisse über die Cybersicherheitslage besitzen diejenigen, deren Geschäft der Schutz vor Gefahren aus dem Cyberraum ist. Hersteller von Anti-

Viren-Programmen oder anderen Dienstleister im Bereich von IT-Sicherheitslösungen sollten deshalb mit ihrer Expertise besser in die Erstellung von Lagebildern zur Cybersicherheit eingebunden werden können. Und auch die Bemühungen privater Sicherheitsforschung zum Auffinden und Schließen von Sicherheitslücken sollten rechtlich eindeutig ermöglicht und nicht immer weiter erschwert werden. Hierfür sind beispielsweise Vorschriften im Urheberrecht zu ändern, um klarzustellen, dass sogenanntes „reverse engineering“ mit dem Ziel des Auffindens und Schließens von Sicherheitslücken zulässig ist; auch im Bereich des Schutzes von Betriebs- und Geschäftsgeheimnissen ist zu evaluieren, ob bestehende Vorschriften der Offenlegung von Sicherheitslücken im Rahmen eines koordinierten Offenlegungsprozesses entgegenstehen.

- Eine nachhaltige IT-Sicherheitsstrategie endet nicht mit dem Schließen einer Sicherheitslücke oder der erfolgreichen Abwehr einer erkannten Gefahr für ein IT-System. Vielmehr sind systematische Lehren aus bekannt gewordenen Angriffen und Sicherheitslücken und dem Umgang damit zu ziehen. Beispielsweise hat der Angriff auf das Sicherheitsunternehmen SolarWinds das Risiko sogenannter „supply chain“-Angriffe aufgezeigt. Ebenso hat etwa der IVBB-Hack, der unter anderem den Deutschen Bundestag betraf, Lücken in der Schutzstrategie für Verfassungsorgane offenbart. Künftige Novellen des IT-Sicherheitsgesetzes und Cybersicherheitsstrategien der Bundesregierung müssen sich stärker an dem Ziel orientieren, Lehren aus bekannten IT-Sicherheitsvorfällen zu ziehen.

Berlin, den 20. April 2021

Christian Lindner und Fraktion