Deutscher Bundestag **Drucksache 19/28872**

19. Wahlperiode 21.04.2021

Entschließungsantrag

der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Espendiller, Marc Bernhard, Marcus Bühl, Nicole Höchst, Stefan Keuter, Jörn König, Tobias Matthias Peterka, Martin Reichardt, Dr. Dirk Spaniel, Dr. Harald Weyel und der Fraktion der AfD

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. Der Deutsche Bundestag stellt fest:

1. Der vorliegende Reformentwurf des IT-Sicherheitsgesetzes wird dem Ziel einer Verbesserung der IT-Sicherheit in Deutschland in wesentlichen Teilen nicht gerecht. Es mangelt vor allem an klaren Schutzzielen, es mangelt an politischem Entscheidungswillen was die Zulässigkeit von staatsnahen Herstellern aus undemokratischen Ländern anbelangt und es mangelt an einer Evaluierung der bisherigen Regulierung im IT-Sicherheitsgesetz aus dem Jahr 2015, wie sie eigentlich gesetzlich vorgeschrieben ist.
2. Die Bundesregierung hat ferner in grob fahrlässiger Weise die Reform des IT-Sicherheitsgesetzes über einen Zeitraum von zwei Jahren verzögert und damit der Bundesrepublik Deutschland, seinen Bürgern und der Volkswirtschaft schweren Schaden zugefügt.
3. Der Bundesregierung und den Bundesministerien ist es trotz dieser zweijährigen, größtenteils intern geführten Debatte bis zu der Einbringung des Kabinettsentwurfes in das parlamentarische Verfahren nicht gelungen, einen aus ihrer eigenen Sicht konsistenten Referentenentwurf zu entwickeln.

   So wurde am 02.12.2020 ein ressortübergreifend nicht abgestimmter Diskussionsentwurf vorgelegt und bis zum 09.12.2020 um Stellungnahme gebeten (https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/entwurf-zweites-it-sicherheitsgesetz.html). Kurz vor Ablauf dieser Frist wurde am 09.12.2020 ein deutlich geänderter und weiterhin nicht ressortübergreifend abgestimmter Referentenentwurf verteilt, zu dem innerhalb von 27 Stunden Stellung

bezogen werden sollte.

Von 19.11.2020 bis 16.12.2020 alleine gab es fünf veröffentlichte Versionen mit teils umfangreicheren Anpassungen, die aber in Teilen wiederum nur einigen beteiligten Wirtschaftsverbänden bereitgestellt wurden (https://www.bundestag.de/resource/blob/825126/c932641828f11342efb2fbf372fa3dbc/A-Drs-19-4-741-C-data.pdf). Am 25.01.2021 wurde der Gesetzentwurf schließlich in das parlamentarische Verfahren eingebracht.

Das federführende Bundesministerium des Innern, für Bau und Heimat (BMI) hat es versäumt, eine angemessene Beteiligung der interessierten Kreise zu gewährleisten (https://www.bundestag.de/resource/blob/824768/a2d971d73d0e81c5eb1846e07f45b4f9/A-Drs-19-4-741-A-data.pdf, S.3), was zu einer nicht der gesamtgesellschaftlichen IT-Sicherheit dienenden Überfokussierung der Novelle auf die Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI) geführt hat.

4. Durch diese Verzögerung im deutschen Gesetzgebungsverfahren kommt es ferner auch zu einer derzeit parallel und damit unabgestimmten Aktualisierung der europäischen NIS-Richtlinie, die ebenfalls dem Schutz kritischer Infrastrukturen dienen soll und für die das deutsche IT-SiG 2.0 gut als Vorlage hätte dienen können. Eine europäische Harmonisierung insbesondere der vom IT-SiG 2.0 neu eingeführten Aspekte der Unternehmen von besonderem öffentlichen Interesse, der Siedlungsabfallentsorgung sowie des freiwilligen IT-Sicherheitskennzeichens sind dadurch zunächst nicht gewährleistet, obwohl es gerade hinsichtlich der Wirksamkeit dieser Regelungen einer internationalen Abstimmung bedarf. Eine Schädigung des Wirtschaftsstandortes Deutschland aufgrund von Wettbewerbsnachteilen deutscher Unternehmen ist dadurch geradezu vorprogrammiert, insbesondere für die genannten „Unternehmen von besonderem öffentlichen Interesse“ (§ 2 Abs. 14). Hinzu kommt schlechtesten falls erneuter Anpassungsaufwand für die Unternehmen bei einem künftig EU-abgestimmten IT-SiG 3.0.

5. Die Antragsteller begrüßen grundsätzlich die geplante personelle und finanzielle Stärkung des BSI. Das BSI soll weiter zu einer starken Verbraucherschutzbehörde ausgebaut werden, z. B. durch den Betrieb einer IT-Hotline für Bürger, vergleichbar mit den 110/112-Notfallnummern. Allerdings ist der Gesetzentwurf, vermutlich aufgrund der mangelhaften Beteiligung aller interessierten Kreise, zu stark vom Staat her gedacht. Netzwerkförmigen Bedrohungen im Cyberraum kann nicht durch eine sternförmige Abwehrstrategie einzelner Behörden begegnet werden. Die zahlreichen Initiativen in Wirtschaft und Zivilgesellschaft im Bereich IT-Sicherheit sollten noch stärker mit dem regulatorischen Konzept des IT-Sicherheitsgesetzes verknüpft werden.

6. Die Antragsteller begrüßen die Etablierung eines freiwilligen IT-Sicherheitskennzeichens, das durch das BSI betrieben wird. Die Erfahrungen der etablierten normgebenden Institutionen wie DIN oder ETSI sollten jedoch zumindest berücksichtig oder die entsprechenden Institutionen als verantwortlich betrachtet werden.

7. Das IT-SiG.20 kann nur ein Baustein für mehr IT-Sicherheit sein. Die Sicherheit im Cyberraum ist in Bezug auf Wettbewerbsgleichheit und Wirksamkeit am besten durch einen harmonisierten Ansatz auf europäischer Ebene zu erreichen. Dazu gehört z. B. auch die zeitnahe und vollständige Umsetzung der EU-5G toolbox.

8. In einem früheren Entwurf der Novelle von Mai 2020 wurden dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) Aufgaben und weitere Personalstellen zugeteilt, um erstmalig in die Lage versetzt zu werden, auch für IT-Katastrophen Krisenreaktionspläne auszuarbeiten (https://intrapol.org/wp-content/uploads/2020/05/200507_BMI_RefE_IT-SiG20.pdf). Die mangelnde und

mangelhafte Befassung des BBK mit Digital-Themen wurde nicht zuletzt im Rahmen des bundesweiten Warntages sowie im Rahmen der Bekämpfung der Corona-Krise deutlich. Eine Ausweitung der gesetzlichen Aufgaben auch im Rahmen des IT-SiG 2.0 wäre ein erster Schritt zu der angekündigten Neuausrichtung des BBK gewesen (https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2021/03/neuausrichtung-bbk.html), der nun leider ausgeblieben ist.

9. Das Fehlen einer eindeutigen verpflichtenden Einführung eines Informationssicherheitsmanagementsystems (ISMS) und eines Business Continuity Managements (BCM) im Gesetzesentwurf ist nicht nachzuvollziehen.
10. Ebenfalls offen bleiben weiterhin Regulierungsthemen wie die aktive Cyberabwehr, die Cybersicherheitsarchitektur, der Umgang mit Schwachstellen und die Systematisierung und Konsolidierung des IT-Sicherheitsrechts.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. das BSI zu einer starken Verbraucherschutzbehörde auszubauen, z. B. durch den Betrieb einer IT-Sicherheitshotline für Bürger, vergleichbar mit den 110/112-Notfallnummern,
2. das BBK in die Lage zu versetzen, auch für IT-Katastrophen Krisenreaktionspläne auszuarbeiten,
3. bei der Umsetzung des freiwilligen Sicherheitskennzeichens und bei der Definition des Standes der Technik die Verfahrenskenntnisse und das technische Verständnis der etablierten normgebenden Institutionen wie DIN oder ETSI einzubeziehen,
4. bei der Umsetzung der Regelungen zur IT-Sicherheit verstärkt die zahlreichen Initiativen in Wirtschaft und Zivilgesellschaft im Bereich IT-Sicherheit einzubeziehen,
5. zu einer zeitnahen und engen Abstimmung der europäischen NIS-Richtlinie mit den durch das IT-SiG 2.0 novellierten Gesetzestexten zu gelangen,
6. für eine zeitnahe und vollständige Umsetzung der EU 5G-toolbox zu sorgen,
7. bei der weiteren Gestaltung des Ordnungsrahmens für IT-Sicherheit eine Konsolidierung der mittlerweile sehr zahlreichen IT-Sicherheitsgesetze, -verordnungen und -strategien herbeizuführen, da deren Zusammenwirken zu einer Komplexität führt, die IT-Sicherheit eher gefährdet, statt ihr zu dienen,
8. bei der weiteren Gestaltung des Ordnungsrahmens für IT-Sicherheit die Aspekte der aktiven Cyberabwehr sowie des Umgangs mit Schwachstellen eindeutig zu regulieren,
9. bei der weiteren Gestaltung des Ordnungsrahmens für IT-Sicherheit möglichst frühzeitig und umfänglich angemessen alle interessierten Kreise einzubeziehen,
10. die Gestaltung des Ordnungsrahmens für IT-Sicherheit in Zukunft einem verantwortlichen Bundesministerium für Digitalisierung und Cybersicherheit federführend zu übertragen.

Berlin, den 16. April 2021

Dr. Alice Weidel, Dr. Alexander Gauland und Fraktion