Deutscher Bundestag **Drucksache 19/28844**

19. Wahlperiode 21.04.2021

Beschlussempfehlung und Bericht

des Ausschusses für Inneres und Heimat (4. Ausschuss)

a) zu dem Gesetzentwurf der Bundesregierung
– Drucksachen 19/26106, 19/26921, 19/27035 1.7 –

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

b) zu dem Antrag der Abgeordneten Joana Cotar, Uwe Schulz, Dr. Michael Espendiller, weiterer Abgeordneter und der Fraktion der AfD
– Drucksache 19/26225 –

Evaluierung des IT-Sicherheitsgesetzes von 2015 nach Gesetzeslage umsetzen und Ergebnisse im IT-Sicherheitsgesetz 2.0 berücksichtigen

c) zu dem Antrag der Abgeordneten Uwe Schulz, Joana Cotar, Dr. Michael Espendiller und der Fraktion der AfD
– Drucksache 19/26226 –

IT-Sicherheitsgesetz 2.0 – Planungs- und Rechtssicherheit für Netzbetreiber herstellen

d) zu dem Antrag der Abgeordneten Dr. Konstantin von Notz, Tabea Rößner, Kerstin Andreae, weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 19/1328 –

IT-Sicherheit stärken, Freiheit erhalten, Frieden sichern

A. Problem

Zu Buchstabe a

Die Gewährleistung der Cyber- und Informationssicherheit ist ein Schlüsselthema für Staat, Wirtschaft und Gesellschaft. Gerade mit Blick auf die zunehmende Digitalisierung aller Lebensbereiche sind sie auf funktionierende Informations- und Kommunikationstechnik angewiesen – sei es für den Informationsaustausch, die Produktion, den Konsum, Dienstleistungen oder zur Pflege privater Kontakte. Voraussetzung hierfür ist eine sichere Infrastruktur.

Cyber-Angriffe stellen für Staat, Wirtschaft und Gesellschaft daher ein großes Gefahrenpotential dar. Die Angriffe werden qualitativ immer ausgefeilter und somit für alle Betroffenen auch gefährlicher. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet einen stetigen Anstieg von Schadprogrammen, jährlich kommen mehr als 100 Millionen neue Varianten hinzu. Die Schadsoftware „Emotet“ dominiert bereits seit Jahren die Gefährdungslage.

Vorfälle wie die Ransomware „WannaCry“ verdeutlichen die Situation. Mittlerweile werden Daten bei Ransomware-Angriffen nicht mehr nur verschlüsselt, sondern zudem vorher kopiert und ausgeleitet. Auch die Aufdeckung von Schwachstellen in Computerchips wie „Meltdown“ und „Spectre“ machen die Anfälligkeit für Sicherheitslücken besonders deutlich. Daneben hat der zu Beginn des Jahres 2018 in den Medien bekanntgewordene Angriff auf die Kommunikationsinfrastrukturen des Auswärtigen Amts deutlich gemacht, dass der Staat seine Schutzmaßnahmen anpassen muss.

Die zunehmende Verbreitung von „Internet of Things (IoT)“-Geräten verschärft die Situation zusätzlich. Diese Geräte werden teilweise nicht unter Sicherheitsaspekten entwickelt und lassen sich hierdurch zu großen Bot-Netzen zusammenschalten. Dieser Gefahr gilt es zu begegnen.

Insgesamt ist Cyber-Sicherheit nicht statisch, ein aktuelles Schutzniveau ist daher kein Garant für eine erfolgreiche Abwehr der Angriffe von morgen. Daher bedarf es einer ständigen Anpassung und Weiterentwicklung der Schutzmechanismen und der Abwehrstrategien.

Zu Buchstabe b

Die Fraktion der AfD fordert, eine Evaluierung mit einem vom Deutschen Bundestag bestellten wissenschaftlichen Sachverständigen zur aktuellen Reform

durchzuführen, um die Wirksamkeit der regulierenden Maßnahmen zu überprüfen und die IT-Sicherheit in Deutschland nachhaltig zu verbessern. Die Pflicht zur Evaluierung ergebe sich aus Artikel 10 des IT-Sicherheitsgesetzes.

Sie fordert die Bundesregierung daher auf, das Gesetzgebungsverfahren solange zu pausieren, bis eine Evaluierung zu dem Entwurf des IT-Sicherheitsgesetzes 2.0 unter Einbeziehung eines wissenschaftlichen Sachverständigen durchgeführt ist, um deren Ergebnisse in das Gesetzesvorhaben einfließen zu lassen.

Zu Buchstabe c

Die Fraktion der AfD ist der Auffassung, aufgrund der zunehmenden Digitalisierung von Verwaltung, Wirtschaft und Gesellschaft spiele die IT- und Cyber-Sicherheit eine übergeordnete Rolle. Vielerorts werde die Bevölkerung bereits mit einem 5G-Netz versorgt. Für die Produktpflege der Netzwerkkomponenten, wie die Durchführung von Software-Updates, Firmware-Updates und die Schließung von Sicherheitslücken, sei der Hersteller, nicht der Betreiber zuständig. Aufgrund dessen sei esvon großer Relevanz, dass die Hersteller der Netzwerkkomponenten keine missbräuchlichen Zugriffsmöglichkeiten auf Hard- und Software implementieren oder sonstige Handlungen vornehmen könnten, die Sabotage oder Spionage ermöglichten.

Die Fraktion der AfD fordert die Bundesregierung daher auf, eine politische Entscheidung darüber zu treffen, ob andere Länder grundsätzlich am Ausbau der 5G-Netze durch das Bereitstellen von Netzwerkkomponenten beteiligt werden dürfen. Zudem fordert sie, bei einem Ausschluss der Beteiligung am Ausbau der 5G-Netze durch andere Länder eine Kompensationsregelung für die Mobilfunknetzbetreiber gesetzlich zu regeln, um eine Planungs- und Rechtssicherheit für Mobilfunknetzbetreiber herzustellen.

Zu Buchstabe d

Die Fraktion BÜNDNIS 90/DIE GRÜNEN betont, die Stärkung der IT-Sicherheit sei eine zentrale Bedingung für eine erfolgreiche gesellschaftliche Gestaltung der Digitalisierung. Dabei habe auch die Schaffung von Vertrauen in digitale Angebote und Infrastrukturen eine grundlegende Bedeutung. Durch einen IT-Angriff auf das besonders gesicherte deutsche Regierungsnetz sei die Notwendigkeit einer Stärkung und Verbesserung der IT-Sicherheit deutlich geworden. Die bisherigen gesetzlichen Regelungen zum Schutz digitaler Infrastrukturen und Kommunikation seien unzureichend und schafften kein Vertrauen in digitale Angebote und Infrastrukturen.

Die Fraktion BÜNDNIS 90/DIE GRÜNEN fordert die Bundesregierung daher insbesondere auf, die IT-Sicherheit als verfassungsrechtliche Gewährleistungspflicht des Staates zu statuieren, indem sie die Schutzpflichten aus dem Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme als oberste Priorität für einen sicheren Umgang mit der Digitalisierung anerkennt.

B. Lösung

Zu Buchstabe a

Entsprechend dem Auftrag aus dem Koalitionsvertrag zwischen CDU, CSU und SPD für die 19. Legislaturperiode wird der mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl. I S. 1324) geschaffene Ordnungsrahmen durch das Zweite Gesetz

zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-Sicherheitsgesetz 2.0) erweitert. Schwerpunktmäßig werden folgende Änderungen vorgenommen:

– Verbesserung des Schutzes der IT der Bundesverwaltung u. a. durch weitere Prüf- und Kontrollbefugnisse des BSI und Festlegung von Mindeststandards durch das BSI.

– Schaffung von Befugnissen zur Detektion von Schadprogrammen zum Schutz der Regierungsnetze.

– Abfrage von Bestandsdaten bei Anbietern von Telekommunikationsdiensten, um Betroffene über Sicherheitslücken und Angriffe zu informieren.

– Befugnis für das BSI, Sicherheitslücken an den Schnittstellen informationstechnischer Systeme zu öffentlichen TK-Netzen zu detektieren sowie Einsatz von Systemen und Verfahren zur Analyse von Schadprogrammen und Angriffsmethoden.

– Schaffung einer Anordnungsbefugnis des BSI gegenüber Telekommunikations- und Telemedienanbietern zur Abwehr spezifischer Gefahren für die Informationssicherheit.

– Ausweitung der Pflichten für Betreiber Kritischer Infrastrukturen und weiterer Unternehmen im besonderen öffentlichen Interesse.

– Schaffung von Eingriffsbefugnissen für den Einsatz und Betrieb von kritischen Komponenten.

– Etablierung von Verbraucherschutz im Bereich der Informationssicherheit als zusätzliche Aufgabe des BSI.

– Schaffung der Voraussetzungen für ein einheitliches IT-Sicherheitskennzeichen, das die IT-Sicherheit der Produkte sichtbar macht.

– Überarbeitung des Bußgeldregimes.

Der Ausschuss für Inneres und Heimat hat beschlossen, den Gesetzentwurf im Wesentlichen um folgende Maßnahmen abzuändern und zu ergänzen:

– Das BSI nimmt als zentrale Stelle für Informationssicherheit auf nationaler Ebene seine beratenden Aufgaben gegenüber den Stellen des Bundes aufgrund „wissenschaftlich-technischer Erkenntnisse“ wahr.

– Die Bestimmung der Schutzziele der Informationssicherheit wird geschärft.

– Die Bereichsausnahmen bei der Kontrollbefugnis des BSI werden eingeschränkt auf Auslands-IT und die IT der Streitkräfte sowie des MAD.

– Die Befugnisse des BSI zur Entgegennahme von Informationen zu Schwachstellen und Meldung an betroffene IT-Hersteller werden ausgebaut.

– IT-Verantwortliche sollen unverzüglich über detektierte Sicherheitsrisiken informiert werden.

– Die Speicherdauer von pseudonymisierten Daten soll zur Analyse und Abwehr von Angriffen auf die Kommunikationstechnik des Bundes auf 18 Monate verlängert werden.

– Die Kontrollbefugnisse des BSI werden erleichtert, weil keine vorherige Absprache mehr mit den zu prüfenden Stellen des Bundes (Behörden und Ressorts) vorgesehen ist.

– Die Befugnis zur Bestandsdatenauskunft wird rechtstechnisch an das Gesetz zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020 (BGBl. 2021 I S. 448) angepasst.

– Das BSI kann nunmehr im Benehmen mit den Ressorts Mindeststandards verbindlich festlegen.

– Zu den Unternehmen im besonderen öffentlichen Interesse, die als Ergänzung zu den Betreibern Kritischer Infrastrukturen vom Anwendungsbereich des BSI-Gesetzes erfasst werden, sollen auch Zulieferer mit Alleinstellungsmerkmal für die nach ihrer Wertschöpfung größten Unternehmen in Deutschland zählen.

– Die Voraussetzungen für die Untersagung kritischer Komponenten wurden konkretisiert (bspw. Kontrolle des Herstellers durch Drittstaaten, Zuwiderlaufen gegen sicherheitspolitische Ziele).

– Die Frist zur Untersagung des erstmaligen Einsatzes kritischer Komponenten (Ex-ante-Untersagung) wurde auf zwei bzw. vier Monate verlängert.

– Das BMI entscheidet nun im Benehmen statt im Einvernehmen mit den Fachressorts und dem AA über den erstmaligen Einsatz.

– Einführung einer Pflicht des BMI, den Innenausschuss kalenderjährlich über die Anwendung des Gesetzes zu unterrichten.

Annahme des Gesetzentwurfs auf Drucksachen 19/26106, 19/26921 in geänderter Fassung mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen AfD, FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN.

Zu Buchstabe b

Ablehnung des Antrags auf Drucksache 19/26225 mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion der AfD.

Zu Buchstabe c

Ablehnung des Antrags auf Drucksache 19/26226 mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion der AfD.

Zu Buchstabe d

Ablehnung des Antrags auf Drucksache 19/1328 mit den Stimmen der Fraktionen der CDU/CSU, SPD und AfD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion der FDP.

C. Alternativen

Ablehnung des Gesetzentwurfs zu Buchstabe a und/oder Annahme der Vorlagen auf Buchstaben b bis d.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Zu Buchstabe a

Der unter E. dargestellte Erfüllungsaufwand wird voraussichtlich in vollem Umfang haushaltswirksam.

Der entsprechende Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen soll finanziell und stellenmäßig in den jeweils betroffenen Einzelplänen ausgeglichen werden.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Zu Buchstabe a

Es entsteht kein Erfüllungsaufwand für die Bürgerinnen und Bürger.

E.2 Erfüllungsaufwand für die Wirtschaft

Zu Buchstabe a

Der Wirtschaft entsteht für die Erfüllung der im Gesetz vorgesehenen zusätzlichen Aufgaben ein laufender Erfüllungsaufwand in Höhe von 21,64 Mio. Euro. Davon entfallen 3,86 Mio. Euro auf jährliche Personalkosten und rund 17,78 Mio. Euro auf jährliche Sachkosten. Hiervon entfallen wiederum 0,35 Mio. Euro auf Bürokratiekosten durch Informationspflichten. Der einmalige Erfüllungsaufwand in Form von einmaligen Personalkosten beläuft sich auf 0,04 Mio. Euro.

E.3 Erfüllungsaufwand der Verwaltung

Der Verwaltung entsteht für die Erfüllung der im Gesetz vorgesehenen zusätzlichen Aufgaben ein Aufwand von insgesamt 1.585,8 Planstellen/Stellen (705,5 hD; 782,30 gD; 98 mD) mit einem jährlichen Erfüllungsaufwand in Höhe von 202,23 Mio. Euro. Davon entfallen 133,12 Mio. Euro auf jährliche Personalkosten und 69,12 Mio. Euro auf jährliche Sachkosten. Durch die gesetzliche Änderung entstehen einmalige Sachkosten in Höhe von 31,7 Mio. Euro.

Davon entfallen auf

– das Bundesministerium des Innern, für Bau und Heimat (BMI) einschließlich seines Geschäftsbereichs 858 Planstellen/Stellen (552 hD; 303 gD; 3 mD) mit einem jährlichen Erfüllungsaufwand in Höhe von 129,26 Mio. Euro. Davon entfallen 78,95 Mio. Euro auf jährliche Personalkosten und 50,3 Mio. Euro auf jährliche Sachkosten. Durch die gesetzliche Änderung entstehen einmalige Sachkosten in Höhe von 28,06 Mio. Euro;

– den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) 15 Planstellen/Stellen (9 hD; 6 gD) mit einem jährlichen Erfüllungsaufwand in Höhe von 1,73 Mio. Euro. Davon entfallen 1,36 Mio. Euro auf jährliche Personalkosten und 0,37 Mio. Euro auf jährliche Sachkosten;

- das Auswärtige Amt (AA) einschließlich seines Geschäftsbereichs insgesamt 51 Planstellen/Stellen (14 hD; 29 gD; 8 mD) mit einem jährlichen Erfüllungsaufwand in Höhe von 5,85 Mio. Euro. Davon entfallen 3,88 Mio. Euro auf jährliche Personalkosten und 1,97 Mio. Euro auf jährliche Sachkosten. Zusätzlich entstehen einmalig Sachkosten in Höhe von 3,5 Mio. Euro;
- das Bundesministerium für Arbeit und Soziales (BMAS) einschließlich seines Geschäftsbereichs 15 Planstellen/Stellen (4 hD; 11 gD) mit einem jährlichen Erfüllungsaufwand in Höhe von 1,56 Mio. Euro. Davon entfallen 1,18 Mio. Euro auf jährliche Personalkosten und 0,37 Mio. Euro auf jährliche Sachkosten;
- das Bundesministerium der Finanzen (BMF) einschließlich seines Geschäftsbereichs 278 Planstellen/Stellen (20 hD; 247 gD; 11 mD) mit einem jährlichen Erfüllungsaufwand in Höhe von 26,71 Mio. Euro. Davon entfallen 19,8 Mio. Euro auf jährliche Personalkosten und 6,91 Mio. Euro auf jährliche Sachkosten;
- das Bundesministerium für Gesundheit (BMG) einschließlich seines Geschäftsbereichs 5 Planstellen/Stellen (3 hD; 2 gD) mit einem jährlichen Erfüllungsaufwand in Höhe von 0,58 Mio. Euro. Davon entfallen 0,45 Mio. Euro auf jährliche Personalkosten und 0,12 Mio. Euro auf jährliche Sachkosten;
- das Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) einschließlich seines Geschäftsbereichs 9,3 Planstellen/Stellen (0,5 hD; 7,8 gD; 1 mD) mit einem jährlichen Erfüllungsaufwand in Höhe von 0,91 Mio. Euro. Davon entfallen 0,64 Mio. Euro auf jährliche Personalkosten und 0,26 Mio. Euro auf jährliche Sachkosten. Zusätzlich entstehen einmalig Sachkosten in Höhe von 0,14 Mio. Euro;
- das Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit (BMU) einschließlich seines Geschäftsbereichs 32 Planstellen/Stellen (4 hD; 28 gD) mit einem jährlichen Erfüllungsaufwand in Höhe von 3,16 Mio. Euro. Davon entfallen 2,36 Mio. Euro auf jährliche Personalkosten und 0,8 Mio. Euro auf jährliche Sachkosten;
- das Bundesministerium für Verkehr und digitale Infrastruktur (BMVI) einschließlich seines Geschäftsbereichs 254,5 Planstellen/Stellen (85,5 hD; 109 gD; 60 mD) mit einem jährlichen Erfüllungsaufwand in Höhe von 25,88 Mio. Euro. Davon entfallen 19,56 Mio. Euro auf jährliche Personalkosten und 6,32 Mio. Euro auf jährliche Sachkosten;
- das Bundesministerium für Wirtschaft und Energie (BMWi) einschließlich seines Geschäftsbereichs 51 Planstellen/Stellen (4,5 hD; 32,5 gD; 14 mD) mit einem jährlichen Erfüllungsaufwand in Höhe von 4,71 Mio. Euro. Davon entfallen 3,44 Mio. Euro auf jährliche Personalkosten und 1,27 Mio. Euro auf jährliche Sachkosten;
- das Bundeskanzleramt (BKAmt) einschließlich seines Geschäftsbereichs 17 Planstellen/Stellen (9 hD; 7 gD; 1 mD) mit einem jährlichen Erfüllungsaufwand in Höhe von 1,9 Mio. Euro. Davon entfallen 1,48 Mio. Euro auf jährliche Personalkosten und 0,42 Mio. Euro auf jährliche Sachkosten.

Dezentral werden bei den nicht gesondert angeführten Ressorts für ein Ineinandergreifen des Sicherheitsmanagements und den erforderlichen Ausbau der Informationssicherheit in der Bundesverwaltung weitere Planstellen/Stellen mit Personalkosten und gegebenenfalls weitere Sachkosten erforderlich werden, die im jeweiligen Haushaltsaufstellungsverfahren geltend gemacht werden.

Darüber hinaus entsteht auch in der mittelbaren Bundesverwaltung bei Betreibern von Kritischen Infrastrukturen im Bereich der Sozialversicherung ein noch nicht abschließend quantifizierbarer Mehrbedarf an Personal- und Sachkosten, da u. a. eine Reihe von Vorschriften noch untergesetzliche Ausführungen erfordern.

Der Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen soll finanziell und stellenmäßig in den jeweiligen Einzelplänen ausgeglichen werden.

F. Weitere Kosten

Keine.

Beschlussempfehlung

Der Bundestag wolle beschließen,

a) den Gesetzentwurf auf Drucksachen 19/26106, 19/26921 mit folgenden Maßgaben, im Übrigen unverändert anzunehmen:

1. Artikel 1 wird wie folgt geändert:

a) Der Nummer 1 wird folgende Nummer 1 vorangestellt:

‚1. § 1 wird wie folgt gefasst:

„§ 1

Bundesamt für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat. Es ist die zentrale Stelle für Informationssicherheit auf nationaler Ebene. Aufgaben gegenüber den Bundesministerien führt das Bundesamt auf Grundlage wissenschaftlich-technischer Erkenntnisse durch.“ ‘

b) Die bisherige Nummer 1 wird Nummer 2 und wird wie folgt geändert:

aa) Dem Buchstaben a wird folgender Buchstabe a vorangestellt:

‚a) Absatz 2 wird wie folgt geändert:

aa) Die folgenden Sätze werden vorangestellt:

„Informationen sowie informationsverarbeitende Systeme, Komponenten und Prozesse sind besonders schützenswert. Der Zugriff auf diese darf ausschließlich durch autorisierte Personen oder Programme erfolgen. Die Sicherheit in der Informationstechnik und der damit verbundene Schutz von Informationen und informationsverarbeitenden Systemen vor Angriffen und unautorisierten Zugriffen im Sinne dieses Gesetzes erfordert die Einhaltung bestimmter Sicherheitsstandards zur Gewährleistung der informationstechnischen Grundwerte und Schutzziele.“

bb) In dem neuen Satz 4 wird das Wort „Unversehrtheit“ durch das Wort „Integrität“ ersetzt.‘ ‘

bb) Die bisherigen Buchstaben a und b werden die Buchstaben b und c.

cc) Der bisherige Buchstabe c wird Buchstabe d und Absatz 9a wird wie folgt gefasst:

„(9a) IT-Produkte im Sinne dieses Gesetzes sind Software, Hardware sowie alle einzelnen oder miteinander verbundenen Komponenten, die Informationen informationstechnisch verarbeiten.“

dd) Der bisherige Buchstabe d wird Buchstabe e.

ee) Der bisherige Buchstabe e wird Buchstabe f und wird wie folgt geändert:

aaa) In Absatz 13 Satz 1 in dem einleitenden Satzteil wird das Wort „die“ gestrichen.

bbb) In Absatz 13 Satz 1 Nummer 1 wird dem Wort „in“ das Wort „die“ vorangestellt.

ccc) In Absatz 13 Satz 1 Nummer 2 werden die Wörter „von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil“ durch die Wörter „bei denen“ ersetzt und werden die Wörter „dieser IT-Produkte“ gestrichen.

ddd) Absatz 13 Satz 1 Nummer 3 wird wie folgt gefasst:

„3. die auf Grund eines Gesetzes unter Verweis auf diese Vorschrift

a) als kritische Komponente bestimmt werden oder

b) eine auf Grund eines Gesetzes als kritisch bestimmte Funktion realisieren.“

eee) In Absatz 13 Satz 2 werden nach den Wörtern „eines Gesetzes“ die Wörter „unter Verweis auf diese Vorschrift“ eingefügt.

fff) Absatz 14 wird wie folgt gefasst:

„(14) Unternehmen im besonderen öffentlichen Interesse sind Unternehmen, die nicht Betreiber Kritischer Infrastrukturen nach Absatz 10 sind und

1. die Güter nach § 60 Absatz 1 Nummer 1 und 3 der Außenwirtschaftsverordnung in der jeweils geltenden Fassung herstellen oder entwickeln,

2. die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind oder die für solche Unternehmen als Zulieferer wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung sind oder

3. die Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung in der jeweils geltenden Fassung sind oder nach § 1 Absatz 2 der Störfall-Verordnung diesen gleichgestellt sind.

Die Unternehmen im besonderen öffentlichen Interesse nach Satz 1 Nummer 2 werden durch die Rechtsverordnung nach § 10 Absatz 5 bestimmt, in der festgelegt wird, welche wirtschaftlichen Kennzahlen maßgeblich dafür sind, dass ein Unternehmen

zu den größten Unternehmen in Deutschland im Sinne der Nummer 2 gehört und welche Alleinstellungsmerkmale maßgeblich dafür sind, dass Zulieferer für solche Unternehmen von wesentlicher Bedeutung sind.“

c) Die bisherige Nummer 2 wird Nummer 3 und wird wie folgt geändert:

aa) In dem Änderungsbefehl wird die Angabe „Satz 2“ gestrichen.

bb) Dem Buchstaben a wird folgender Buchstabe a vorangestellt:

‚a) Satz 1 wird wie folgt gefasst:

„Das Bundesamt fördert die Sicherheit in der Informationstechnik mit dem Ziel, die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und deren Verarbeitung zu gewährleisten.“ ‘

cc) Der bisherige Buchstabe a wird Buchstabe b und nach dem Wort „In“ wird die Angabe „Satz 2“ eingefügt.

dd) Der bisherige Buchstabe b wird Buchstabe c und nach dem Wort „Nach“ wird die Angabe „Satz 2“ eingefügt.

ee) Nach dem neuen Buchstaben c wird folgender Buchstabe d eingefügt:

‚d) Nach Satz 2 Nummer 12 wird folgende Nummer 12a eingefügt:

„12a. Beratung und Unterstützung der Stellen des Bundes in Fragen der Sicherheit in der Informationstechnik;“.‘

ff) Der bisherige Buchstabe c wird Buchstabe e und der Angabe „Nummer 14“ wird die Angabe „Satz 2“ vorangestellt.

gg) Der bisherige Buchstabe d wird Buchstabe f und nach dem Wort „Nach“ wird die Angabe „Satz 2“ eingefügt.

hh) Der bisherige Buchstabe e wird Buchstabe g und der Angabe „Nummer 17“ wird die Angabe „Satz 2“ vorangestellt.

ii) Der bisherige Buchstabe f wird Buchstabe h und nach dem Wort „In“ wird die Angabe „Satz 2“ eingefügt.

jj) Der bisherige Buchstabe g wird Buchstabe i und wird wie folgt gefasst:

‚i) Dem Satz 2 werden die folgenden Nummern 19 und 20 angefügt:

„19. Empfehlungen für Identifizierungs- und Authentisierungsverfahren und Bewertung dieser Verfahren im Hinblick auf die Informationssicherheit;

20. Beschreibung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte unter Berücksichtigung

bestehender Normen und Standards sowie Einbeziehung der betroffenen Wirtschaftsverbände.“ ‘

d) Die bisherige Nummer 3 wird Nummer 4 und wird wie folgt geändert:

aa) § 4a wird wie folgt geändert:

aaa) Absatz 2 Satz 2 wird aufgehoben.

bbb) Die Absätze 5 und 6 werden wie folgt gefasst:

„(5) Ausgenommen von den Befugnissen nach den Absätzen 1 bis 3 sind Kontrollen der Auslandsinformations- und -kommunikationstechnik im Sinne des § 9 Absatz 2 des Gesetzes über den Auswärtigen Dienst, soweit sie ausschließlich im Ausland belegen ist oder für das Ausland oder für Anwender im Ausland betrieben wird. Die Bestimmungen für die Schnittstellen der Kommunikationstechnik des Bundes im Inland bleiben davon unberührt. Näheres zu Satz 1 regelt eine Verwaltungsvereinbarung zwischen dem Bundesministerium des Innern, für Bau und Heimat und dem Auswärtigen Amt.

(6) Die Befugnisse nach den Absätzen 1 bis 3 gelten im Geschäftsbereich des Bundesministeriums der Verteidigung nicht für die Kontrolle der Informations- und Kommunikationstechnik, die von den Streitkräften für ihre Zwecke oder dem Militärischen Abschirmdienst genutzt wird. Nicht ausgenommen ist die Informations- und Kommunikationstechnik von Dritten, insbesondere von IT-Dienstleistern, soweit sie nicht ausschließlich für die Zwecke der Streitkräfte betrieben wird. Die Bestimmungen für die Schnittstellen der Kommunikationstechnik des Bundes bleiben von den Sätzen 1 und 2 unberührt. Näheres regelt eine Verwaltungsvereinbarung zwischen dem Bundesministerium des Innern, für Bau und Heimat und dem Bundesministerium der Verteidigung.“

bb) § 4b wird wie folgt geändert:

aaa) In Absatz 2 Satz 1 wird das Wort „kann“ durch das Wort „nimmt“ und das Wort „entgegennehmen“ durch das Wort „entgegen“ ersetzt.

bbb) Absatz 3 Nummer 2 wird wie folgt gefasst:

„2. die Öffentlichkeit oder betroffene Kreise gemäß § 7 zu warnen und zu informieren,“.

e) Die bisherige Nummer 4 wird Nummer 5 und Buchstabe a wird wie folgt gefasst:

‚a) Absatz 2 wird wie folgt gefasst:

„(2) Protokolldaten nach Absatz 1 Satz 1 Nummer 1 dürfen über den für die automatisierte Auswertung nach Absatz 1 Satz 1 Nummer 1 erforderlichen Zeitraum hinaus,

längstens jedoch für 18 Monate, gespeichert werden, soweit tatsächliche Anhaltspunkte dafür bestehen, dass diese im Falle der Bestätigung eines Verdachts nach Absatz 3 Satz 2 zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich sein können. Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Auswertung der nach diesem Absatz gespeicherten Daten nur automatisiert erfolgt und dass ein Zugriff auf Daten, die länger als drei Monate gespeichert sind, nur beim Vorliegen tatsächlicher Erkenntnisse über die Betroffenheit des Bundes mit einem Schadprogramm erfolgt. Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist. Eine nicht automatisierte Verarbeitung ist nur nach Maßgabe der nachfolgenden Absätze zulässig. Soweit hierzu die Wiederherstellung pseudonymisierter Protokolldaten erforderlich ist, muss diese durch die Präsidentin oder den Präsidenten des Bundesamtes oder die Vertretung im Amt angeordnet werden. Die Entscheidung ist zu dokumentieren.“ ‘

f) Die bisherigen Nummern 5 und 6 werden die Nummern 6 und 7.

g) Die bisherige Nummer 7 wird Nummer 8 und Absatz 1 wird wie folgt gefasst:

„(1) Das Bundesamt darf zur Erfüllung seiner gesetzlichen Aufgabe nach § 3 Absatz 1 Satz 1 Nummer 1, 2, 14, 17 oder 18 von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes) Auskunft verlangen. Die Auskunft nach Satz 1 darf nur verlangt werden zum Schutz der Versorgung der Bevölkerung in den Bereichen des § 2 Absatz 10 Satz 1 Nummer 1 oder der öffentlichen Sicherheit, um damit eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme

1. einer Kritischen Infrastruktur oder

2. eines Unternehmens von besonderem öffentlichem Interesse

abzuwenden, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, das auf die informationstechnischen Systeme bestimmbarer Infrastrukturen oder Unternehmen abzielen wird, und die in die Auskunft aufzunehmenden Daten im Einzelfall erforderlich sind, um die Betroffenen nach Absatz 4 vor dieser Beeinträchtigung zu warnen, über diese zu informieren oder sie bei deren Beseitigung zu beraten oder zu unterstützen.“

h) Die bisherige Nummer 8 wird Nummer 9 und in Buchstabe b wird in Satz 4 die Angabe „Satz 4“ durch die Angabe „Satz 3“ ersetzt.

i) Die bisherige Nummer 9 wird Nummer 10.

j) Die bisherige Nummer 10 wird Nummer 11 und wird wie folgt geändert:

aa) § 7b Absatz 3 wird wie folgt geändert:

aaa) In Satz 1 werden die Wörter „und stehen überwiegende Sicherheitsinteressen nicht entgegen“ gestrichen und wird nach dem Wort „Verantwortlichen“ das Wort „unverzüglich“ eingefügt.

bbb) Folgender Satz 5 wird angefügt:

„Das Bundesamt legt die Weiße Liste nach Absatz 1 Satz 3 der Bundesbeauftragten oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vierteljährlich zur Kontrolle vor.“

k) Die bisherige Nummer 11 wird Nummer 12 und Buchstabe a wird wie folgt geändert:

aa) Absatz 1 wird wie folgt geändert:

aaa) In Satz 1 wird das Wort „Einvernehmen“ durch das Wort „Benehmen“ ersetzt.

bbb) Die folgenden Sätze werden angefügt:

„Das Bundesamt berät die in Satz 1 genannten Stellen auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards. Für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach Satz 1 empfehlenden Charakter. Für die Verpflichtung nach Satz 1 gilt die Ausnahme nach § 4a Absatz 6 entsprechend.“

bb) In Absatz 1a werden die Sätze 5 bis 7 aufgehoben.

l) Die bisherige Nummer 12 wird Nummer 13 und wird wie folgt geändert:

aa) In Buchstabe b wird das Wort „zwölften“ durch die Angabe „24.“ ersetzt.

bb) Nach Buchstabe c wird folgender Buchstabe d eingefügt:

‚d) In Absatz 2 Satz 3 Nummer 2 werden die Wörter „oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde“ gestrichen.‘

cc) Die bisherigen Buchstaben d und e werden die Buchstaben e und f.

m) Die bisherigen Nummern 13 und 14 werden die Nummern 14 und 15.

n) Die bisherige Nummer 15 wird Nummer 16 und wird wie folgt gefasst:

‚16. § 8d wird wie folgt geändert:

a) In Absatz 1 Satz 1 wird die Angabe „2003/361/EC“ durch die Angabe „2003/361/EG“ ersetzt.

b) Nach Absatz 1 wird folgender Absatz 1a eingefügt:

„(1a) § 8f ist nicht anzuwenden auf Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG. Artikel 3 Absatz 4 des Anhangs zu der Empfehlung ist nicht anzuwenden."

c) In Absatz 3 in dem einleitenden Satzteil wird die Angabe „§ 8b Absatz 4" durch die Wörter „§ 8b Absatz 4 und 4a" ersetzt.'

o) Die bisherigen Nummern 16 bis 18 werden die Nummern 17 bis 19.

p) Die bisherige Nummer 19 wird Nummer 20 und wird wie folgt geändert:

aa) In § 9a Absatz 2 werden die Wörter „Das Bundesamt erteilt auf Antrag Konformitätsbewertungsstellen, die im Anwendungsbereich der Verordnung (EU) 2019/881 sowie des § 9 dieses Gesetzes tätig werden, eine Befugnis" durch die Wörter „Das Bundesamt kann auf Antrag Konformitätsbewertungsstellen, die im Anwendungsbereich der Verordnung (EU) 2019/881 sowie des § 9 dieses Gesetzes tätig werden, eine Befugnis erteilen" ersetzt.

bb) § 9b wird wie folgt gefasst:

„§ 9b

Untersagung des Einsatzes kritischer Komponenten

(1) Der Betreiber einer Kritischen Infrastruktur hat den geplanten erstmaligen Einsatz einer kritischen Komponente gemäß § 2 Absatz 13 dem Bundesministerium des Innern, für Bau und Heimat vor ihrem Einsatz anzuzeigen. In der Anzeige sind die kritische Komponente und die geplante Art ihres Einsatzes anzugeben. Satz 1 gilt für einen Betreiber einer Kritischen Infrastruktur nicht, wenn dieser den Einsatz einer anderen kritischen Komponente desselben Typs für dieselbe Art des Einsatzes bereits nach Satz 1 angezeigt hat und ihm dieser nicht untersagt wurde.

(2) Das Bundesministerium des Innern, für Bau und Heimat kann den geplanten erstmaligen Einsatz einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur im Benehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt bis zum Ablauf von zwei Monaten nach Eingang der Anzeige nach Absatz 1 untersagen oder Anordnungen erlassen, wenn der Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt. Bei der Prüfung einer voraussichtlichen Beeinträchtigung der öffentlichen Ordnung oder Sicherheit kann insbesondere berücksichtigt werden, ob

1. der Hersteller unmittelbar oder mittelbar von der Regierung, einschließlich sonstiger staatlicher Stellen oder Streitkräfte, eines Drittstaates kontrolliert wird,
2. der Hersteller bereits an Aktivitäten beteiligt war oder ist, die nachteilige Auswirkungen auf die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland oder eines anderen Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages oder auf deren Einrichtungen hatten, oder
3. der Einsatz der kritischen Komponente im Einklang mit den sicherheitspolitischen Zielen der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrages steht.

Vor Ablauf der Frist von zwei Monaten nach Anzeige nach Absatz 1 ist der Einsatz nicht gestattet. Das Bundesministerium des Innern, für Bau und Heimat kann die Frist gegenüber dem Betreiber um weitere zwei Monate verlängern, wenn die Prüfung besondere Schwierigkeiten tatsächlicher oder rechtlicher Art aufweist.

(3) Kritische Komponenten gemäß § 2 Absatz 13 dürfen nur eingesetzt werden, wenn der Hersteller eine Erklärung über seine Vertrauenswürdigkeit (Garantieerklärung) gegenüber dem Betreiber der Kritischen Infrastruktur abgeben hat. Die Garantieerklärung ist der Anzeige nach Absatz 1 beizufügen. Aus der Garantieerklärung muss hervorgehen, wie der Hersteller sicherstellt, dass die kritische Komponente nicht über technische Eigenschaften verfügt, die spezifisch geeignet sind, missbräuchlich, insbesondere zum Zwecke von Sabotage, Spionage oder Terrorismus auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können. Das Bundesministerium des Innern, für Bau und Heimat legt die Einzelheiten der Mindestanforderungen an die Garantieerklärung im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt durch Allgemeinverfügung fest, die im Bundesanzeiger bekannt zu machen ist. Die Einzelheiten der Mindestanforderungen an die Garantieerklärung müssen aus den Schutzzielen der Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur folgen und die Vermeidung von Gefahren für die öffentliche Sicherheit und Ordnung, insbesondere im Sinne von Absatz 2 Satz 2, adressieren, die aus der Sphäre des Herstellers der kritischen Komponente, insbesondere dessen Organisationsstruktur, stammen. Die Sätze 1 und 2 gelten erst ab der Bekanntmachung der Allgemeinverfügung nach Satz 5 und nicht für bereits vor diesem Zeitpunkt eingesetzte kritische Komponenten. Soweit Änderungen der Allgemeinverfügung erfolgen, sind diese für bereits nach diesem Absatz abgegebene Garantieerklärungen unbeachtlich.

(4) Das Bundesministerium des Innern, für Bau und Heimat kann den weiteren Einsatz einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen oder Anordnungen erlassen, wenn der weitere Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt, insbesondere, wenn der Hersteller der kritischen Komponente nicht vertrauenswürdig ist. Absatz 2 Satz 2 gilt entsprechend.

(5) Ein Hersteller einer kritischen Komponente kann insbesondere dann nicht vertrauenswürdig sein, wenn hinreichende Anhaltspunkte dafür bestehen, dass

1. er gegen die in der Garantieerklärung eingegangen Verpflichtungen verstoßen hat,
2. in der Garantieerklärung angegebene Tatsachenbehauptungen unwahr sind,
3. er Sicherheitsüberprüfungen und Penetrationsanalysen an seinem Produkt und in der Produktionsumgebung nicht im erforderlichen Umfang in angemessener Weise unterstützt,
4. Schwachstellen oder Manipulationen nicht unverzüglich, nachdem er davon Kenntnis erlangt, beseitigt und dem Betreiber der Kritischen Infrastruktur meldet,
5. die kritische Komponente auf Grund von Mängeln ein erhöhtes Gefährdungspotenzial aufweist oder aufgewiesen hat, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können oder
6. die kritische Komponente über technische Eigenschaften verfügt oder verfügt hat, die spezifisch geeignet sind oder waren, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können.

(6) Wurde nach Absatz 4 der weitere Einsatz einer kritischen Komponente untersagt, kann das Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt

1. den geplanten Einsatz weiterer kritischer Komponenten desselben Typs und desselben Herstellers untersagen und
2. den weiteren Einsatz kritischer Komponenten desselben Typs und desselben Herstellers unter Einräumung einer angemessenen Frist untersagen.

(7) Bei schwerwiegenden Fällen nicht vorliegender Vertrauenswürdigkeit nach Absatz 5 kann das Bundesministerium des Innern, für Bau und Heimat den Einsatz aller kritischen Komponenten des Herstellers im Einvernehmen mit

den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen.“

cc) § 9c Absatz 3 wird wie folgt gefasst:

„(3) Die IT-Sicherheitsanforderungen, auf die sich die Herstellererklärung bezieht, ergeben sich aus einer Norm oder einem Standard oder aus einer branchenabgestimmten IT-Sicherheitsvorgabe, die die jeweilige Produktkategorie umfasst, sofern das Bundesamt in einem Verfahren, das durch Rechtsverordnung nach § 10 Absatz 3 geregelt wird, festgestellt hat, dass die Norm oder der Standard oder die branchenabgestimmte IT-Sicherheitsvorgabe geeignet ist, ausreichende IT-Sicherheitsanforderungen für die Produktkategorie abzubilden. Ein Anspruch auf diese Feststellung besteht nicht. Liegt keine Feststellung nach Satz 1 vor, ergeben sich die IT-Sicherheitsvorgaben aus einer vom Bundesamt veröffentlichten Technischen Richtlinie, die die jeweilige Produktkategorie umfasst, sofern das Bundesamt eine solche Richtlinie bereits veröffentlicht hat. Wird ein Produkt von mehr als einer oder einem bestehenden, als geeignet festgestellten Norm, Standard, branchenabgestimmten IT-Sicherheitsvorgabe oder Technischen Richtlinie umfasst, richten sich die Anforderungen nach der oder dem jeweils spezielleren bestehenden, als geeignet festgestellten Norm, Standard, branchenabgestimmten IT-Sicherheitsvorgabe oder Technischen Richtlinie.“

q) Die bisherige Nummer 20 wird Nummer 21 und wird wie folgt geändert:

aa) In Buchstabe a werden die Wörter „§ 9a Absatz 1 Satz 1“ durch die Angabe „§ 9c“ ersetzt und werden das Komma und die Wörter „der beizufügenden Unterlagen und der Verwaltungsgebühren“ durch die Wörter „und der beizufügenden Unterlagen“ ersetzt.

bb) Buchstabe b wird wie folgt geändert:

aaa) Im Änderungsbefehl werden die Wörter „Die folgenden Absätze 5 und 6 werden“ durch die Wörter „Folgender Absatz 5 wird“ ersetzt.

bbb) In Absatz 5 wird das Wort „Betreiber“ durch das Wort „Unternehmen“ ersetzt.

ccc) Dem Absatz 5 werden die folgenden Sätze angefügt:

„Unter den Voraussetzungen nach Satz 1 kann das Bundesministerium des Innern, für Bau und Heimat durch Rechtsverordnung bestimmen, welche Alleinstellungsmerkmale maßgeblich dafür sind, dass Zulieferer für Unternehmen, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören, von wesentlicher Bedeutung im Sinne des § 2 Absatz 14 Satz 1 Nummer 2 sind.“

ddd) § 10 Absatz 6 wird aufgehoben.

r) Die bisherige Nummer 21 wird Nummer 22.

s) Nach der neuen Nummer 22 wird folgende Nummer 23 eingefügt:

‚23. § 13 wird wie folgt geändert:

aa) Absatz 2 Satz 2 wird wie folgt gefasst:

„§ 7 Absatz 1a ist entsprechend anzuwenden.“

bb) Nach Absatz 2 wird folgender Absatz 3 eingefügt:

„(3) Das Bundesministerium des Innern, für Bau und Heimat unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Ausschuss für Inneres und Heimat des Deutschen Bundestages über die Anwendung dieses Gesetzes. Es geht dabei auch auf die Fortentwicklung des maßgeblichen Unionsrechts ein.“

cc) Die bisherigen Absätze 3 bis 5 werden die Absätze 4 bis 6.‘

t) Die bisherigen Nummern 22 und 23 werden die Nummern 24 und 25.

2. Artikel 2 wird wie folgt geändert:

a) Nummer 2 Buchstabe b Doppelbuchstabe bb wird wie folgt gefasst:

‚bb) Nach Satz 3 wird folgender Satz eingefügt:

„Kritische Komponenten im Sinne von § 2 Absatz 13 des BSI-Gesetzes dürfen von einem Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotential nur eingesetzt werden, wenn sie vor dem erstmaligen Einsatz von einer anerkannten Zertifizierungsstelle überprüft und zertifiziert wurden.“ ‘

b) In Nummer 3 Buchstabe a wird die Angabe „Nummer 8“ durch die Angabe „Nummer 7“ ersetzt.

c) Nummer 3 Buchstabe b wird wie folgt gefasst:

‚b) Folgende Nummer 8 wird angefügt:

„8. an das Bundesamt für Sicherheit in der Informationstechnik zum Schutz der Versorgung der Bevölkerung in den Bereichen des § 2 Absatz 10 Satz 1 Nummer 1 des BSI-Gesetzes oder der öffentlichen Sicherheit, um damit eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme einer Kritischen Infrastruktur oder eines Unternehmens im besonderen öffentlichen Interesse abzuwenden, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, das auf die informationstechnischen Systeme bestimmbarer Infrastrukturen oder Unternehmen abzielen wird, und die in die Auskunft aufzunehmenden Daten im Einzelfall erforderlich sind, um den Betreiber der betroffenen Kritischen Infrastruktur

oder das betroffene Unternehmen im besonderen öffentlichen Interesse vor dieser Beeinträchtigung zu warnen, über diese zu informieren oder bei deren Beseitigung zu beraten oder zu unterstützen.“ ‘

d) Folgende Nummer 4 wird angefügt:

‚4. § 113 Absatz 5 wird wie folgt geändert:

a) In Nummer 8 wird der Punkt am Ende durch ein Komma ersetzt.

b) Folgende Nummer 9 wird angefügt:

„9. das Bundesamt für Sicherheit in der Informationstechnik zum Schutz der Versorgung der Bevölkerung in den Bereichen des § 2 Absatz 10 Satz 1 Nummer 1 des BSI-Gesetzes oder der öffentlichen Sicherheit, um damit eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme einer Kritischen Infrastruktur oder eines Unternehmens im besonderen öffentlichen Interesse abzuwenden, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, das auf die informationstechnischen Systeme bestimmbarer Infrastrukturen oder Unternehmen abzielen wird, und die in die Auskunft aufzunehmenden Daten im Einzelfall erforderlich sind, um den Betreiber der betroffenen Kritischen Infrastruktur oder das betroffene Unternehmen im besonderen öffentlichen Interesse vor dieser Beeinträchtigung zu warnen, über diese zu informieren oder bei deren Beseitigung zu beraten oder zu unterstützen.“ ‘

3. In Artikel 3 § 11 Absatz 1d und 1e wird jeweils das Wort „zwölften“ durch die Angabe „24.“ ersetzt.;

b) den Antrag auf Drucksache 19/26225 abzulehnen;

c) den Antrag auf Drucksache 19/26226 abzulehnen;

d) den Antrag auf Drucksache 19/1328 abzulehnen.

Berlin, den 21. April 2021

Der Ausschuss für Inneres und Heimat

Andrea Lindholz
Vorsitzende

Christoph Bernstiel Berichterstatter	**Sebastian Hartmann** Berichterstatter	**Joana Cotar** Berichterstatterin
Manuel Höferlin Berichterstatter	**Petra Pau** Berichterstatterin	**Dr. Konstantin von Notz** Berichterstatter

Bericht der Abgeordneten Christoph Bernstiel, Sebastian Hartmann, Joana Cotar, Manuel Höferlin, Petra Pau und Dr. Konstantin von Notz

I. Überweisung

Zu Buchstabe a

Der Gesetzentwurf auf **Drucksache 19/26106** wurde in der 206. Sitzung des Deutschen Bundestages am 28. Januar 2021 an den Ausschuss für Inneres und Heimat federführend sowie an den Verteidigungsausschuss, den Ausschuss Digitale Agenda, den Ausschuss für Recht und Verbraucherschutz, den Ausschuss für Verkehr und digitale Infrastruktur und den Haushaltsausschuss zur Mitberatung überwiesen. Die Unterrichtung durch die Bundesregierung zur Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung auf **Drucksache 19/26921** wurde am 26. Februar 2021 gemäß § 80 Absatz 3 der Geschäftsordnung mit Nummer 1.7 auf Drucksache 19/27035 an die beteiligten Ausschüsse überwiesen. Der Parlamentarische Beirat für nachhaltige Entwicklung beteiligte sich gutachtlich (Ausschussdrucksache 19(4)710).

Zu Buchstabe b

Der Antrag auf **Drucksache 19/26225** wurde in der 206. Sitzung des Deutschen Bundestages am 28. Januar 2021 an den Ausschuss für Inneres und Heimat federführend sowie an den Ausschuss für Recht und Verbraucherschutz und den Ausschuss für Digitale Agenda zur Mitberatung überwiesen.

Zu Buchstabe c

Der Antrag auf **Drucksache 19/26226** wurde in der 206. Sitzung des Deutschen Bundestages am 28. Januar 2021 an den Ausschuss für Inneres und Heimat federführend sowie an den Ausschuss Digitale Agenda, den Ausschuss für Verkehr und digitale Infrastruktur und den Ausschuss für Recht und Verbraucherschutz zur Mitberatung überwiesen.

Zu Buchstabe d

Der Antrag auf **Drucksache 19/1328** wurde in der 26. Sitzung des Deutschen Bundestages am 19. April 2018 an den Ausschuss für Inneres und Heimat federführend sowie an den Ausschuss für Verkehr und digitale Infrastruktur, den Ausschuss für Menschenrechte und humanitäre Hilfe, den Ausschuss Digitale Agenda, den Ausschuss für Bildung, Forschung und Technikfolgenabschätzung, den Verteidigungsausschuss, den Ausschuss für Wirtschaft und Energie und den Ausschuss für Recht und Verbraucherschutz zur Mitberatung überwiesen.

II. Stellungnahmen der mitberatenden Ausschüsse

Zu Buchstabe a

Der **Verteidigungsausschuss** hat in seiner 86. Sitzung am 21. April 2021 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen AfD, FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN die Annahme des Gesetzentwurfs auf Drucksachen 19/26106, 19/26921 empfohlen.

Der **Ausschuss Digitale Agenda** hat in seiner 79. Sitzung am 21. April 2021 mit den Stimmen der Fraktionen der CDU/CSU und SPD der CDU/CSU und SPD gegen die Stimmen der Fraktionen AfD, FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN die Annahme des Gesetzentwurfs auf Drucksachen 19/26106, 19/26921 empfohlen.

Der **Ausschuss für Recht und Verbraucherschutz** hat in seiner 143. Sitzung am 21. April 2021 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen AfD, FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN die Annahme des Gesetzentwurfs auf Drucksachen 19/26106, 19/26921 empfohlen.

Der **Ausschuss für Verkehr und digitale Infrastruktur** hat in seiner 110. Sitzung am 21. April 2021 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen AfD, FDP, DIE LINKE. und

BÜNDNIS 90/DIE GRÜNEN die Annahme des Gesetzentwurfs auf Drucksachen 19/26106, 19/26921 empfohlen.

Der **Haushaltsausschuss** hat in seiner 96. Sitzung am 21. April 2021 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen AfD, FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN die Annahme des Gesetzentwurfs auf Drucksachen 19/26106, 19/26921 empfohlen. Seinen Bericht nach § 96 der Geschäftsordnung wird er gesondert abgeben.

Zu Buchstabe b

Der **Ausschuss für Recht und Verbraucherschutz** hat in seiner 143. Sitzung am 21. April 2021 mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion der AfD die Ablehnung des Antrags auf Drucksache 19/26225 empfohlen.

Der **Ausschuss Digitale Agenda** hat in seiner 79. Sitzung am 21. April 2021 mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion der AfD die Ablehnung des Antrags auf Drucksache 19/26225 empfohlen.

Zu Buchstabe c

Der **Ausschuss Digitale Agenda** hat in seiner 79. Sitzung am 21. April 2021 mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion der AfD die Ablehnung des Antrags auf Drucksache 19/26226 empfohlen.

Der **Ausschuss für Verkehr und digitale Infrastruktur** hat in seiner 110. Sitzung am 21. April 2021 mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion der AfD die Ablehnung des Antrags auf Drucksache 19/26226 empfohlen.

Der **Ausschuss für Recht und Verbraucherschutz** hat in seiner 143. Sitzung am 21. April 2021 mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion der AfD die Ablehnung des Antrags auf Drucksache 19/26226 empfohlen.

Zu Buchstabe d

Der **Ausschuss für Verkehr und digitale Infrastruktur** hat in seiner 110. Sitzung am 21. April 2021 mit den Stimmen der Fraktionen der CDU/CSU, SPD und AfD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion der FDP die Ablehnung des Antrags auf Drucksache 19/1328 empfohlen.

Der **Ausschuss für Menschenrechte und humanitäre Hilfe** hat in seiner 79. Sitzung am 21. April 2021 mit den Stimmen der Fraktionen der CDU/CSU, SPD und AfD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion der FDP die Ablehnung des Antrags auf Drucksache 19/1328 empfohlen.

Der **Ausschuss Digitale Agenda** hat in seiner 79. Sitzung am 21. April 2021 mit den Stimmen der Fraktionen der CDU/CSU, SPD und AfD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion der FDP die Ablehnung des Antrags auf Drucksache 19/1328 empfohlen.

Der **Ausschuss für Bildung, Forschung und Technikfolgenabschätzung** hat in seiner 70. Sitzung am 21. April 2021 mit den Stimmen der Fraktionen der CDU/CSU, SPD und AfD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion der FDP die Ablehnung des Antrags auf Drucksache 19/1328 empfohlen.

Der **Verteidigungsausschuss** hat in seiner 86. Sitzung am 21. April 2021 mit den Stimmen der Fraktionen der CDU/CSU, SPD und AfD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion der FDP die Ablehnung des Antrags auf Drucksache 19/1328 empfohlen.

Der **Ausschuss für Wirtschaft und Energie** hat in seiner 115. Sitzung am 21. April 2021 mit den Stimmen der Fraktionen der CDU/CSU, SPD und AfD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion der FDP die Ablehnung des Antrags auf Drucksache 19/1328 empfohlen.

Der **Ausschuss für Recht und Verbraucherschutz** hat in seiner 143. Sitzung am 21. April 2021 mit den Stimmen der Fraktionen der CDU/CSU, SPD und AfD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion der FDP die Ablehnung des Antrags auf Drucksache 19/1328 empfohlen.

III. Beratungsverlauf und Beratungsergebnisse im federführenden Ausschuss

Der Ausschuss für Inneres und Heimat hat in seiner 119. Sitzung am 10. Februar 2021 zu den Vorlagen zu Buchstaben a bis c einstimmig sowie in seiner 32. Sitzung am 12. Dezember 2018 zur Vorlage zu Buchstabe d mit den Stimmen der Fraktionen FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktionen der CDU/CSU, SPD und AfD beschlossen, eine öffentliche Anhörung durchzuführen.

Die öffentliche Anhörung zu den Vorlagen zu Buchstaben a bis c, an der sich sechs Sachverständige beteiligt haben, hat der Ausschuss für Inneres und Heimat in seiner 124. Sitzung am 1. März 2021 durchgeführt. Die öffentliche Anhörung zur Vorlage zu Buchstabe d hat der Ausschuss für Inneres und Heimat in seiner 48. Sitzung am 8. April 2019 mit sechs Sachverständigen durchgeführt. Die Beratung in dieser öffentlichen Anhörung erfolgte gemeinsam mit den Vorlagen auf den Drucksachen 19/7698 und 19/7705. Hinsichtlich des Ergebnisses der Anhörungen wird auf die Protokolle der 48. und 124. Sitzung verwiesen (19/48 sowie 19/124).

Zu Buchstabe a

1. Der Ausschuss für Inneres und Heimat hat den Gesetzentwurf auf Drucksachen 19/26106, 19/26921 in seiner 134. Sitzung am 21. April 2021 abschließend beraten und empfiehlt die Annahme des Gesetzentwurfs in der aus der Beschlussempfehlung ersichtlichen Fassung mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen AfD, FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN.

Die Änderungen entsprechen dem Änderungsantrag der Fraktionen der CDU/CSU und SPD auf Ausschussdrucksache 19(4)811, der zuvor mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen AfD und DIE LINKE. bei Stimmenthaltung der Fraktionen FDP und BÜNDNIS 90/DIE GRÜNEN angenommen wurde.

Darüber hinaus hat der Ausschuss für Inneres und Heimat einen Antrag der Fraktionen der CDU/CSU und SPD auf Ausschussdrucksache 19(4)812 mit dem Titel „Deutschlands Cybersicherheit stärken“ mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen AfD und DIE LINKE. bei Stimmenthaltung der Fraktionen FDP und BÜNDNIS 90/DIE GRÜNEN angenommen und damit beschlossen:

I. Der Ausschuss für Inneres und Heimat des Deutschen Bundestages stellt fest:

Der Gesetzentwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme („IT-Sicherheitsgesetz 2.0“) ist ein wesentlicher Schritt für die Stärkung der Netz- und Informationssicherheit in Deutschland. Mit dem IT-Sicherheitsgesetz 2.0 wird der rechtliche Rahmen gestärkt. Der Gesetzentwurf umfasst Maßnahmen im Bereich der Wirtschaft zum Schutz Kritischer Infrastrukturen einschließlich kritischer Komponenten und weiterer Unternehmen im besonderen öffentlichen Interesse, zum Schutz der Verbraucherinnen und Verbraucher sowie zum Schutz der Bundesverwaltung.

Die digitale Transformation wird durch eine weiter steigende Durchdringung von Informations- und Kommunikationstechnologie ermöglicht. Unvermeidbare Folge der Digitalisierung ist dabei, dass die Anzahl der Schwachstellen in Soft- wie Hardware weiter ansteigt. Fehlerfreie Produkte können nicht gewährleistet werden – auch bei intensiven Tests ist es nicht möglich, alle Fehler zu entdecken. Die Information der betreffenden Stellen und Unternehmen über Sicherheitslücken ist daher ein wichtiger Baustein bei der Gewährleistung von IT-Sicherheit: insbesondere die Sicherheit von IT-Produkten kann verbessert werden, wenn Hersteller Informationen über entdeckte Sicherheitslücken erhalten und diese die Informationen nutzen, um Fehler zu beheben.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist auf Bundesebene die kompetente nationale Stelle zur Förderung der Sicherheit in der Informationstechnik. Zu den Aufgaben des BSI gehört es, Informationen über Sicherheitsrisiken zu sammeln, auszuwerten und die gewonnenen Erkenntnisse anderen Stellen zur Verfügung zu stellen (§ 3 Absatz 1 Satz 2 Nummer 2 BSI-Gesetz). Ferner berät und warnt das Bundesamt Hersteller, Vertreiber und Anwender in Fragen der IT-Sicherheit (§ 3 Absatz 1 Satz 2 Nummer 14 BSI-Gesetz). Mit § 7

Absatz 1 Satz 1 Buchstabe a BSI-Gesetz hat das BSI die Befugnis, die Öffentlichkeit und betroffene Fachkreise, insbesondere Hersteller, vor Sicherheitslücken in informationstechnischen Produkten und Diensten zu warnen.

Mit dem IT-Sicherheitsgesetz 2.0 wird die Kompetenz des BSI, über Sicherheitslücken oder andere Sicherheitsrisiken zu informieren, gestärkt. Das BSI darf auf Grundlage von § 7 BSI-Gesetz künftig nicht nur Warnungen aussprechen, sondern auch allgemeine Informationen übermitteln. Diese Befugnis soll nunmehr ausdrücklich auch dem Verbraucherschutz und der Verbraucherinformation dienen. Mit Blick darauf sind nach § 7 Absatz 1 Satz 1 Nummer 1 Buchstabe d des Gesetzentwurfs auch Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten Gegenstand der Warn- und Informationsbefugnis. Zudem wird das BSI als allgemeine Meldestelle für die IT-Sicherheit ausgestaltet (§ 4b BSI-Gesetz des Gesetzentwurfs). Informationen über Sicherheitslücken, Schadprogramme oder sonstige Informationen können dem BSI anonym gemeldet werden. Diese Informationen soll das BSI nutzen, um die Öffentlichkeit und betroffene Kreise, wozu Hersteller, Vertreiber oder Anwender gehören, zu warnen und zu informieren. Im Sinne einer verantwortungsbewussten Offenlegung (Responsible Disclosure) sind Hersteller rechtzeitig vor Veröffentlichung einer Warnung zu informieren.

Es besteht ein anhaltender Trend, dass Angreifer modulare Schadprogramme für cyber-kriminelle Massenaufgriffe auf Privatpersonen, Unternehmen und andere Institutionen nutzen (vgl. Bundesamt für Sicherheit in der Informationstechnik, Die Lage der IT-Sicherheit in Deutschland 2020, S. 9). Typischerweise besteht diese Software aus einer initialen „Hintertür“, die genutzt wird, um weitere Schadfunktionen nachzuladen. Das Verhalten dieser Software lässt sich aus der Ferne steuern. Insbesondere in Verbindung mit Erpressungs-Software (Ransomware) enthält diese Schadsoftware auch Funktionen zu ihrer eigenen Deinstallation, aber auch Funktionalitäten eines Bot-Netzes sind häufig in derartiger Software enthalten. Ein bekanntes Beispiel der jüngeren Vergangenheit ist die „Emotet“ genannte Schadsoftware. Diese diente sowohl als Türöffner für Erpressung durch Verschlüsselung als auch zum unberechtigten Kopieren von Daten. Insbesondere der Bekämpfung solcher Schadprogramme dient die Anordnungsbefugnis nach § 7c Absatz 1 Satz 1 Nummer 2 des Entwurfs des BSI-Gesetzes. Auf Grundlage dieser Befugnis kann das BSI Telekommunikationsdiensteanbieter zur Mitwirkung bei der Bereinigung betroffener Datenverarbeitungssysteme von einem konkret benannten Schadprogramm verpflichten. Dabei knüpft die Befugnis an hohe tatbestandliche Hürden an. Das BSI kann Maßnahmen nur zur Abwehr konkreter erheblicher Gefahren für die Verfügbarkeit, Unversehrtheit und Vertraulichkeit der in § 7c Absatz 2 des Entwurfs des BSI-Gesetzes genannten Informations- und Kommunikationssysteme und -dienste anordnen. Zur Verfahrenssicherung ist vor Anordnung einer etwaigen Maßnahme das Einvernehmen mit der Bundesnetzagentur und dem oder der Beauftragten für den Datenschutz und die Informationsfreiheit herzustellen. Aufgrund des Zwecks und der technischen Durchführung sind Maßnahmen auf Grundlage von § 7c Absatz 1 Satz 2 Nummer 2 des Entwurfs des BSI-Gesetzes wertungsmäßig und technisch nicht mit Maßnahmen zu vergleichen, die dem Urteil des Bundesverfassungsgerichts zur Online-Durchsuchung zugrunde liegen (BVerfG, Urteil vom 27.2.2008 – 1 BvR 370/07, 1 BvR 595/07). Während es in dem Urteil um heimliche Infiltration eines informationstechnischen Systems ging, um sich Kenntnisse von Kommunikationsinhalten zu verschaffen, geht es bei der Befugnis nach § 7c Absatz 1 Satz 1 Nummer 2 des Entwurfs des BSI-Gesetzes darum, Schadprogramme zu deaktivieren, die sich – unter Verletzung der Integrität und Vertraulichkeit – auf einem befallenen IT-System befinden. Zudem werden weder zur Durchführung von Maßnahmen Zugangsbeschränkungen überwunden, noch werden Systeme manipuliert, um in den aus dem Persönlichkeitsrecht abgeleiteten Schutzbereich der Integrität und Vertraulichkeit informationstechnischer Systeme einzugreifen. Vielmehr wird die vorangehend von Cyber-Kriminellen durch Aufbringen einer Schadsoftware beeinträchtigte Integrität und Vertraulichkeit der informationstechnischen Systeme durch Maßnahmen nach § 7c Absatz 1 Satz 1 Nummer 2 des Entwurfs des BSI-Gesetzes wiederhergestellt.

Zum Schutz der IT-Sicherheit Kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse gehört neben technischen und organisatorischen Vorkehrungen auch der Einsatz vertrauenswürdiger Mitarbeiter in den sicherheitsrelevanten Bereichen. Den Unternehmen stehen derzeit häufig keine geeigneten Mittel zur Verfügung, die Vertrauenswürdigkeit des Personals zum Beispiel im Rahmen des Einstellungsprozesses zu überprüfen.

Als zentrale Meldestelle für Betreiber Kritischer Infrastrukturen erstellt das BSI ein Lagebild zur Sicherheit in der Informationstechnik Kritischer Infrastrukturen gemäß § 8b Absatz 2 Nummer 3 BSIG und unterrichtet die Betreiber über die sie betreffenden Informationen. Der Informationsfluss besteht aus allgemeinen Informationen in Form von Lagebildern sowie speziellen Handlungsanweisungen zu Prävention, Detektion und Reaktion zu Cyber-Angriffen, die den Betreibern Kritischer Infrastrukturen durch das BSI zur Verfügung gestellt werden. Damit das

BSI die Lagebilder und spezialisierten Handlungsanweisungen erstellen kann, ist es auch auf Meldungen der Betreiber Kritischer Infrastrukturen z. B. zu Cyber-Angriffen angewiesen.

Der sichere und souveräne Betrieb Kritischer Infrastrukturen hängt auf Grund der voranschreitenden Digitalisierung und Vernetzung zunehmend von bestimmten kritischen Komponenten und damit auch von deren Herstellern ab. Dies gilt gerade für die zukünftigen Mobilfunknetze, die zunehmend das Rückgrat der digitalen Gesellschaft bilden werden. Damit spielen auch die „Vertrauenswürdigkeit" der Hersteller und mithin Gefahren, die aus der Sphäre der Hersteller kritischer Komponenten stammen können, eine besondere Rolle beim Schutz der öffentlichen Ordnung und Sicherheit. Im IT-Sicherheitsgesetz 2.0 wird mit dem neuen § 9b BSIG erstmals eine Möglichkeit geschaffen, den Einsatz kritischer Komponenten bestimmter Hersteller durch Anordnungen einzuschränken oder als Ultima Ratio zu untersagen, sofern der Einsatz voraussichtlich eine Gefahr für die öffentliche Ordnung und Sicherheit der Bundesrepublik Deutschland darstellt. Damit wird eine der Kernforderungen der sog. EU 5G Toolbox („Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures") umgesetzt, welche ausdrücklich Begrenzungen des Einsatzes sog. „high risk suppliers" in den 5G-Netzen fordert („Strategic measure 03").

Die Verabschiedung des IT-Sicherheitsgesetzes wird begleitet durch weitere wesentliche Maßnahmen zur Sicherstellung der Integrität von Mobilfunknetzen an anderer Stelle. So ist eine weitere Kernforderung der EU Toolbox die Verhinderung von Monokulturen in der Netztopologie („Strategic measure 05"). Dies ist durch den Einsatz von Komponenten möglichst vieler Hersteller sicherzustellen.

Vor diesem Hintergrund ist die Entscheidung der Bundesregierung, im Rahmen des Konjunktur- und Zukunftspaketes zwei Milliarden Euro in die Entwicklung künftiger Netztechnologien zu investieren, nicht nur als eine wirtschaftspolitische Maßnahme, sondern auch als ein Beitrag zur Sicherheit unserer Mobilfunknetze zu begrüßen.

Maßnahmen nach § 9b BSIG können im Einzelfall dazu führen, dass die betroffenen Betreiber Kritischer Infrastrukturen kritische Komponenten nicht wie beabsichtigt – oder nicht wie bereits erfolgt weiter – in ihren Kritischen Infrastrukturen einsetzen können. Damit handelt es sich bei Maßnahmen nach § 9b BSIG im Einzelfall um Begrenzungen der Eigentümerbefugnisse in Form von Inhalts- und Schrankenbestimmungen. Im Rahmen der Ausarbeitung des § 9b BSIG wurde daher sorgfältig und umfangreich geprüft, ob sich diese Regelung in den Grenzen hält, bei denen die Begrenzungen der Eigentümerbefugnisse als Ausfluss der Sozialgebundenheit des Eigentums (Artikel 14 Absatz 2 GG) entschädigungslos hinzunehmen sind.

In Anbetracht der möglichen Szenarien, in denen es zu einer Anordnung oder einer Untersagung in Bezug auf den Einsatz kritischer Komponenten kommen kann, und unter Berücksichtigung und Abwägung der Interessen der betroffenen Unternehmen sowie den Interessen der Allgemeinheit an dem sicheren Betrieb Kritischer Infrastruktur und deren Rolle für das Gemeinwohl ist eine Entschädigung im Rahmen der verfassungsrechtlichen Vorgaben nicht notwendig.

Dabei wurden auch die zurechenbaren Verantwortungssphären mit in die Ab-wägung einbezogen. Die Betreiber der Kritischen Infrastrukturen haben jeweils die Gesamtverantwortung für den sicheren Betrieb inne. Da die Betreiber dazu verpflichtet sind, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, strahlt diese Pflicht auch auf die angemessene Auswahl der Zulieferer der eingesetzten Komponenten aus. Derartige Abwägungen und Prüfungen bei Auswahl der Komponenten sind bei dem Betrieb Kritischer Infrastrukturen, die im Interesse der Allgemeinheit – und des Schutzguts der öffentlichen Sicherheit und Ordnung – „sicher" zu betreiben sind, auch aus eigenem wirtschaftlichen Interesse immer zu machen.

Für den Sektor der „öffentlichen Telekommunikationsnetze" – und nur für diesen Bereich wird mit dem IT-Sicherheitsgesetz 2.0 die Möglichkeit geschaffen, auch kritische Komponenten festzulegen – wurde bereits der Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 Telekommunikationsgesetz aktualisiert und um neue Anforderungen an den sicheren Betrieb der Netze erweitert (Bearbeitungsstand 29. April 2020, in Kraft seit dem 23. Dezember 2020; die Betroffenen hatten ab dem 11. August 2020 Gelegenheit zur Stellungnahme). Darin wird unter Punkt 3.1.3 des Kataloges ausdrücklich aufgeführt, dass die Bereitstellung von Telekommuni-

kationsdiensten oft nur unter Rückgriff auf Dritte erfolgen kann und Lieferanten und Erfüllungsgehilfen vor diesem Hintergrund eine wichtige Rolle einnehmen. Aus diesem Grund wird explizit gefordert, dass das pflichtige Unternehmen daher eine Bewertung der Zuverlässigkeit, Vertrauenswürdigkeit und Qualität des Erfüllungsgehilfen oder Lieferanten vornehmen muss.

Ferner wurde im Rahmen der Abwägung berücksichtigt, dass es die Regelung ermöglicht, dass neben der Untersagung des Einsatzes auch sonstige Anordnungen erlassen werden können, um die erkannten Gefahren – sofern als milderes Mittel ausreichend – abzuwehren. Im Rahmen der Ermessensentscheidung muss zudem auch die verfassungsimmanente Grenze der Verhältnismäßigkeit beachtet werden. Unverhältnismäßige Maßnahmen scheiden daher aus. Diese Ausgestaltung sorgt dafür, dass alle Aspekte des Betriebs der Kritischen Infrastruktur im Rahmen der Entscheidung nach § 9b BSIG-E in ausreichender Weise beachtet werden können.

Bei der Anwendung des § 9b – insbesondere bei der Untersagung des Einsatzes bereits eingebauter Komponenten – sind von der Bundesregierung die Auswirkungen auf die Funktionalität der betroffenen Kritischen Infrastruktur sowie volkswirtschaftliche und gesellschaftliche Folgewirkungen zu berücksichtigen. Dazu können u. a. die Auswirkungen auf die Ausbauziele im Mobilfunk sowie auf die Entwicklung von digitalen Innovationen in unserem Land zählen.

Da die technologische Entwicklung der kritischen Komponenten in dynamischer Weise voranschreitet und sich dadurch auch die Gefährdungslage mit Blick auf Kritische Infrastrukturen ändern kann, sollte aber auch fortlaufend geprüft werden, ob die zur Verfügung stehenden Maßnahmen weiterhin angemessen sind, um Gefahren für die öffentliche Ordnung und Sicherheit wirksam abzuwenden.

Auch kommt dem Staat die Aufgabe zu, den Einsatz von sicheren und vertrauenswürdigen kritischen Komponenten in geeigneter Weise zu fördern.

II. Der Ausschuss für Inneres und Heimat des Deutschen Bundestages fordert die Bundesregierung auf,

1. a) das BSI organisatorisch so aufzustellen, dass es die bestehenden und durch das IT-Sicherheitsgesetz 2.0 erweiterten Aufgaben und Befugnisse so nutzen kann, dass Hersteller effektiv über gemeldete oder detektierte IT-Schwachstellen durch das BSI informiert werden;

   b) zu prüfen, ob die für Hersteller bestehenden (insbesondere zivilrechtlichen) Pflichten zum Schließen von durch das BSI gemeldeten Sicherheitslücken ausreichen, damit Hersteller ihrer Verantwortung zur Behebung von Fehlern in IT-Produkten entsprechen;

2. im BSI technisch und organisatorisch sicherzustellen, dass bei der Durchführung von Maßnahmen auf Grundlage der Befugnis von § 7c Absatz 1 Satz 1 Nummer 2 des Entwurfs des BSI-Gesetzes rechtwidrige Eingriffe in das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme von vornherein ausgeschlossen sind;

3. die gesetzliche Einführung weiterer Möglichkeiten zur Überprüfung der Vertrauenswürdigkeit von Beschäftigten in besonders sicherheitskritischen Bereichen bei Betreibern Kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse zu prüfen;

4. zur Stärkung des Informationsflusses in beide Richtungen und zur Verbesserung des Lagebilds des BSI zu Kritischen Infrastrukturen, in der nächsten Legislaturperiode ein geeignetes System zu entwickeln und umzusetzen, mit dem spezialisierte technische Informationen zu Prävention, Detektion und Reaktion effizient und effektiv zwischen den zuständigen Behörden und den Betreibern Kritischer Infrastrukturen automatisiert ausgetauscht werden können;

5. a) die Anwendung des § 9b BSIG fortlaufend zu überwachen und zu prüfen, ob die Erfahrungen aus der Verwaltungspraxis Anlass zu einer Anpassung der gesetzlichen Rahmenbedingungen geben. Dabei ist auch zu prüfen, ob infolge solcher Anpassungen Entschädigungsregelungen geboten sind und gegebenenfalls, wie solche umgesetzt werden können;

b) die Bundesregierung soll ferner zur Stärkung der digitalen Souveränität der Bundesrepublik Deutschland den Einsatz von sicheren kritischen Komponenten in Kritischen Infrastrukturen, insb. in Telekommunikationsnetzen, im Einklang mit den Empfehlungen der EU 5G Toolbox, mit geeigneten Mitteln fördern.

2. Zuvor hat der Ausschuss für Inneres und Heimat Änderungsanträge der Fraktionen der AfD und FDP jeweils abgelehnt.

a) Die Änderungsanträge der Fraktion der AfD auf Ausschussdrucksachen 19(4)809 A bis C hat der Ausschuss jeweils mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion der AfD abgelehnt.

Der Änderungsantrag auf Ausschussdrucksache 19(4)809 A hat einschließlich Begründung folgenden Wortlaut:

Der Bundestag wolle beschließen:

Artikel 6 wird wie folgt geändert:

In Absatz 1 wird der einleitende Halbsatz vor Nummer 1 wie folgt gefasst:

„Das Bundesministerium des Innern, für Bau und Heimat berichtet dem Deutschen Bundestag unter Einbeziehung von wissenschaftlichem Sachverstand, der im Einvernehmen mit dem Deutschen Bundestag bestellt wird, …“

Begründung

Die Evaluierung der geplanten Gesetzesänderungen soll durch wissenschaftliche Sachverständige erfolgen, die nicht nur vom Bundesministerium des Innern, für Bau und Heimat, sondern die im Einvernehmen mit dem Deutschen Bundestag bestellt werden, um die parlamentarische Kontrollfunktion hinreichend zu gewährleisten. Damit wird ein Verfahren gewählt, dass auch bereits im aktuell noch gültigen IT-Sicherheitsgesetz vorgeschrieben ist.

Der Änderungsantrag auf Ausschussdrucksache 19(4)809 B hat einschließlich Begründung folgenden Wortlaut:

Der Bundestag wolle beschließen:

1. Artikel 1 Nummer 1 wird wie folgt geändert:

In §2 wird der unter e) neu angefügte Absatz 13 zur Definition Kritischer Komponenten nach dem Punkt 3b) präzisierend ergänzt: „Für den Bereich der Kritischen Infrastrukturen, die ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, legt beispielsweise § 109 Absatz 6 des Telekommunikationsgesetzes fest, dass die Bundesnetzagentur im Einvernehmen mit dem BSI und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit in einem Katalog von Sicherheitsanforderungen bestimmt, welche Funktionen in diesem Bereich kritisch im Sinne des BSIG sind. Komponenten, welche die in dem Katalog von Sicherheitsanforderungen aufgeführten Funktionen realisieren, sind damit kritische Komponenten im Sinne des § 2 Absatz 13 BSIG.“

2. Artikel 1 Nummer 2 wird wie folgt geändert:

In §3 wird die unter g) neu angefügte Nummer 20 um folgenden Halbsatz ergänzt: „…, im Rahmen der entsprechenden normgebenden Institutionen wie z. B. DIN, ETSI, etc.“

3. Artikel 1 Nummer 19 wird wie folgt geändert:

In §9c wird in Absatz (6) der 2. Satz wie folgt gefasst: „Das IT-Sicherheitskennzeichen muss in jedem Fall auch elektronisch veröffentlicht werden.“ Satz 3 „Wenn nach der Beschaffenheit des Produktes das Anbringen nicht möglich ist, muss die Veröffentlichung des IT-Sicherheitskennzeichens elektronisch erfolgen.“ wird dafür ersatzlos gestrichen.

4. Artikel 1 Nummer 1 wird wie folgt geändert:

In §2 Abs. 3 und Abs. 4 wird jeweils Satz 2 ersatzlos gestrichen.

5. Artikel 1 Nummer 11 wird wie folgt geändert:

In Absatz 1 wird das Wort „Einvernehmen“ durch das Wort „Benehmen“ ersetzt

6. Artikel 1 Nummer 19 wird wie folgt geändert:

a) In §9b Absatz 2 wird Satz 5 wie folgt geändert: „Das Bundesministerium des Innern, für Bau und Heimat legt die Mindestanforderungen für die Garantieerklärung im Benehmen mit den betroffenen Ressorts...“.

b) In §9b Absatz 3 wird die Frist jeweils von „einem Monat“ auf „zwei Monate“ erweitert.

Begründung

Zu 1): Die präzisere Definition des Begriffs „Kritische Komponenten“ über einen Verweis auf §109 TKG im Gesetzestext selbst und nicht nur in seiner Begründung soll zu mehr Rechtssicherheit führen.

Zu 2): Die für das BSI neu geplante Aufgabe der „Entwicklung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte“ soll im Rahmen der etablierten normgebenden Institutionen erfolgen, um eine Beteiligung aller interessierten Kreise zu ermöglichen.

Zu 3): Die Veröffentlichung des IT-Sicherheitskennzeichens auf elektronischem Wege nur für den Fall, dass es sich nicht am Produkt anbringen lässt, ist aus Transparenz und Sicherheitsgründen unzureichend. Auch aus Gründen der Wettbewerbsgleichheit muss das IT-Sicherheitskennzeichen in jedem Fall elektronisch veröffentlicht werden.

Zu 4): Eine Herausnahme der „Kommunikationstechnik der Bundesgerichte, soweit sie nicht öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen, des Bundestages, des Bundesrates, des Bundespräsidenten und des Bundesrechnungshofes, soweit sie ausschließlich in deren eigener Zuständigkeit betrieben wird“ sowie der entsprechenden „Schnittstellen der Kommunikationstechnik“ aus dem Anwendungsbereich des BSI-G ist aus Gründen der IT-Sicherheit nicht nachzuvollziehen.

Zu 5) und 6a): Um das Verfahren zu vereinfachen und zu beschleunigen sowie um zu höherer IT- und Rechtssicherheit zu gelangen, sollte das BMI nicht im „Einvernehmen“ sondern lediglich im „Benehmen“ mit den betroffenen Ressorts handeln müssen.

Zu 6b): Aus Praktikabilitätsgründen wird die Frist zur Prüfung einer kritischen Komponente von dem Eingang der Anzeige bis zur Untersagung oder Anordnung von einem auf zwei Monate erweitert.

Der Änderungsantrag auf Ausschussdrucksache 19(4)809 C hat einschließlich Begründung folgenden Wortlaut:

Der Bundestag wolle beschließen:

Artikel 1 Nummer 19 wird wie folgt geändert:

In § 9b wird Absatz 4 wie folgt gefasst:

„Das Bundesministerium des Innern, für Bau und Heimat muss den Betrieb einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur im Benehmen mit den betroffenen Ressorts untersagen oder Anordnungen erlassen, wenn der Hersteller der kritischen Komponente sich als nicht vertrauenswürdig erwiesen hat oder bereits bei Anzeige nach Absatz 1 als nicht vertrauenswürdig bewertet wird“.

b. In § 9b wird in Absatz 5 als neue Ziffer 1 eingefügt:

„er bereits im Rahmen der Anzeige nach Absatz 1 vom Bundessicherheitsrat als nicht vertrauenswürdig (in Form eines staatsnahen Anbieters aus einem undemokratischen Land) bewertet wird, oder“. Die weiteren Ziffern werden entsprechend neu nummeriert. Die neuen Ziffern 2 bis 4 werden am Satzende um das Wort „oder“ ergänzt.

c. In § 9b wird in Absatz 5 der letzte Satz („Ein Verstoß nach Nummer 5 liegt nicht vor, wenn...“) nach der neuen Ziffer 6 ersatzlos gestrichen.

d. In § 9b wird in Absatz 5 eine Ziffer 3 ergänzt mit dem Wortlaut:

„eine Kompensationsregelung mit dem betroffenen Mobilfunknetzbetreiber aushandeln.“

e. In § 9b wird in Absatz 2 als letzter Satz ergänzt: „Eine Rückwirkung des Verbots in Satz 1 auf Bestandsnetze wird aus Gründen des Investitions- und Vertrauensschutzes ausgeschlossen.“

Begründung

In dem vorgelegten Entwurf eines IT-Sicherheitsgesetzes 2.0 bleiben zentrale Fragen zu entstehenden Kosten sowie zu Planungs-, Investitions- und Rechtssicherheit bezüglich der Verwendung von Netzwerkkomponenten genau so offen, wie Fragen nach dem Rückgriff auf das Bestandsnetz. So gehen Netzwerkbetreiber ein erhöhtes Kosten-Risiko ein, wenn sie derzeit Netzwerkkomponenten verwenden oder einbauen, die bei künftigen Prüfungen nach §9b untersagt werden könnten.

Es wurde von der Bundesregierung versäumt, im Rahmen des IT-Sicherheitsgesetzes 2.0 eine klare und endgültige politische Entscheidung darüber zu treffen, ob staatsnahe Netzwerksausrüster aus undemokratischen Ländern am Ausbau kritischer 5G Infrastruktur beteiligt werden dürfen. Die Netzwerkbetreiber müssen eine entsprechende Entscheidung der Behörde (Untersagungsvorbehalt) abwarten, bevor der Einsatz von kritischen Komponenten zum Beispiel aus China möglicherweise gestattet wird.

Mit zunehmender informationstechnischer Komplexität der eingesetzten kritischen Komponenten bleibt ein wesentlicher Teil der Beherrschbarkeit der Technologie im Rahmen der Produktpflege (Softwareupdates, Firmware-Updates, Schließen von Sicherheitslücken) beim Hersteller selbst oder in der weiteren Lieferkette und nicht beim Betreiber des Netzwerkes oder bei den Behörden. Daher und aufgrund der zu erwartenden stetigen Updates (Soft- oder Fimware) bieten weder eine Komponentenzertifizierung, noch hohe technische Sicherheitsanforderungen eine ausreichende Sicherheit dahingehend, dass die Hersteller keine missbräuchlichen Zugriffsmöglichkeiten auf Hard- und Software implementieren oder sonstige Handlungen vornehmen, die Sabotage oder Spionage ermöglichen (https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/entwurf-zweites-it-sicherheitsgesetz.pdf?__blob=publicationFile&v=1).

Ein maximaler Schutz hoheitlicher, personenbezogener, wissenschaftlicher und wirtschaftlich verwertbarer Daten und der damit einhergehenden digitalen Souveränität ist von übergeordneter Bedeutung. Insbesondere Softwarekomponenten bilden einen zentralen Bestandteil der 5G Netzwerke. Die Funktionalität dieser Komponenten kann nach einem abgeschlossenen Zulassungsverfahren unvermittelt über Updates angepasst werden und würde sich damit der Kontrolle der Behörden entziehen. Dieser zentrale Aspekt moderner Telekommunikationsnetze wird im vorliegenden Entwurf nicht hinreichend berücksichtigt.

Zu 1a): Die Änderung von einer „kann" in eine „muss"-Formulierung soll das Verfahren vereinfachen, beschleunigen sowie zu höherer IT- und Rechtssicherheit führen. Das BMI sollte aus den gleichen Gründen nicht im „Einvernehmen" sondern lediglich im „Benehmen" mit den betroffenen Ressorts handeln müssen. Aus den gleichen Gründen sollte die Möglichkeit der Untersagung bereits bei Anzeige nach Absatz 1 erfolgen können, wenn zu diesem Zeitpunkt bereits die eine Bewertung als nicht vertrauenswürdig vorliegt.

Zu 1b): Die Möglichkeit der Bewertung als nicht vertrauenswürdig durch den Bundessicherheitsrat soll auf ein bewährtes Verfahren im Rahmen der Ausfuhrkontrolle zurückgreifen. Auch dadurch soll es zu einem vereinfachten und beschleunigten Verfahren und damit zu höherer IT- und Rechtssicherheit kommen.

Zu 1c): Der nachträgliche Nachweis eines Herstellers, eine z. B. Sicherheitslücke nicht implementiert oder ordnungsgemäß beseitigt zu haben ist für einen wirksamen Ordnungsrahmen für IT-Sicherheit nicht zuträglich, da er die Verantwortung und damit den Handlungsdruck des federführenden Akteurs nahezu beseitigt.

Zu 1d und 1e): Die Einführung einer Kompensationsregelung für den betroffenen Mobilfunknetzbetreiber sowie der Bestandsschutz für Netzwerke soll zu mehr Planungs- und Investitionssicherheit führen.

b) Die Änderungsanträge der Fraktion der FDP auf Ausschussdrucksachen 19(4)813 A, B und H hat der Ausschuss jeweils mit den Stimmen der Fraktionen der CDU/CSU, SPD und AfD gegen die Stimmen der Fraktionen FDP und DIE LINKE. bei Stimmenthaltung der Fraktion BÜNDNIS 90/DIE GRÜNEN abgelehnt.

Den Änderungsantrag der Fraktion der FDP auf Ausschussdrucksache 19(4)813 C hat der Ausschuss mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen FDP und DIE LINKE. bei Stimmenthaltung der Fraktionen AfD und BÜNDNIS 90/DIE GRÜNEN abgelehnt.

Den Änderungsantrag der Fraktion der FDP auf Ausschussdrucksache 19(4)813 D hat der Ausschuss mit den Stimmen der Fraktionen der CDU/CSU, SPD und AfD gegen die Stimmen der Fraktionen FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN abgelehnt.

Die Änderungsanträge der Fraktion der FDP auf Ausschussdrucksachen 19(4)813 E und F hat der Ausschuss jeweils mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen AfD, FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN abgelehnt.

Den Änderungsantrag der Fraktion der FDP auf Ausschussdrucksache 19(4)813 G hat der Ausschuss mit den Stimmen der Fraktionen CDU/CSU, SPD, AfD und DIE LINKE. gegen die Stimmen der Fraktionen FDP und BÜNDNIS 90/DIE GRÜNEN abgelehnt.

Der Änderungsantrag auf Ausschussdrucksache 19(4)813 A hat einschließlich Begründung folgenden Wortlaut:

Der Ausschuss wolle beschließen,

den Gesetzentwurf auf BT-Drucksache 19/26106 mit folgenden Maßgaben zu ändern:

1. Artikel 1 Nr. 1 lit. e) wird wie folgt geändert:

§ 2 Absatz 13 BSIG-E wird aufgehoben.

2. Artikel 1 Nr. 19 wird wie folgt geändert:

§ 9b BSIG-E wird aufgehoben.

Begründung

Die Regelungen mit Berührungspunkten zum Mobilfunkstandard 5G sind aus dem Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme zu streichen. Systematisch fügt sich dieser Komplex wesentlich besser ein in das laufende Gesetzgebungsverfahren des "Gesetzes zur Umsetzung der Richtlinie (EU) 2018/1972 des Europäischen Parlaments und des Rates vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation (Neufassung) und zur Modernisierung des Telekommunikationsrechts (Telekommunikationsmodernisierungsgesetz) (BMWi)", BT-Drs. 19/26108. Es sollten weiterhin keine Definitionen eingeführt werden, die nicht bereits im Telekommunikationsgesetz (TKG) vorgesehen sind. Wohingegen eine Erweiterung des § 109 Absatz 6 TKG um neue Kategorien oder zumindest eine Angleichung sinnvoll erscheint. Hierbei dient die ausführende Rechtsverordnung als Anlage zum Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten (TK-Sicherheitskatalog) gemäß § 109 Absatz 6 TKG in Verbindung mit § 10 Absatz 1 BSI-Gesetz (BSIG) als Vorbild. Demzufolge ist vor Erlass eine "Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände" erforderlich.

Unabhängig von der Frage der systematischen Verortung der Vorgaben für den Einsatz von kritischen Komponenten im Sinne des § 2 Abs. 13 BSIG-E, wurden in der öffentlichen Anhörung des Ausschusses für Inneres und Heimat am 01.03.2021 zum vorliegenden Gesetzentwurf erhebliche verfassungsrechtliche Zweifel an der Regelung des § 9b BSIG-E geäußert. Dies bezog sich insbesondere auf den grundgesetzlich verankerten Vorbehalt des Gesetzes, der in Verbindung mit dem sogenannten Wesentlichkeitsgebot eine gesetzgeberische Entscheidung zu wesentlichen Regelungsfragen fordert, die bestimmt und daher für alle Betroffenen auch vorhersehbar sein müssen. Die gemäß § 9b Abs. 2 Satz 5 BSIG-E vorgesehene Auslagerung der Entscheidung über Mindestanforderungen für die geforderte Garantieerklärung unter Berücksichtigung überwiegender öffentlicher Interessen, insbesondere sicherheitspolitischer Belange, auf eine Allgemeinverfügung, die vom Bundesministerium des Innern, für Bau und Heimat, im Einvernehmen mit den betroffenen Ressorts abgestimmt wird, genügt diesem Anspruch nicht. Deshalb ist vor der Überführung der Regelungen zum Einsatz kritischer Komponenten in das Telekommunikationsmodernisierungsgesetz eine grundlegende Überarbeitung der vorgeschlagenen Regelungen erforderlich.

Der Änderungsantrag auf Ausschussdrucksache 19(4)813 B hat einschließlich Begründung folgenden Wortlaut:

Der Ausschuss wolle beschließen,

den Gesetzentwurf auf BT-Drucksache 19/26106 mit folgenden Maßgaben zu ändern:

1. Artikel 1 Nr. 3 werden folgende Sätze vorangestellt:

a) § 4 Absatz 3 wird wie folgt gefasst:

"Werden Bundesministerien oder anderen Bundesbehörden Informationen nach Absatz 2 Nummer 1 bekannt, unterrichten diese hierüber unverzüglich das Bundesamt."

b) § 4 Absatz 4 wird aufgehoben.

c) § 4 Absatz 5 wird aufgehoben.

d) § 4 Absatz 6 wird § 4 Absatz 4 und folgende Wörter angefügt:

", die öffentlich bekannt gemacht wird."

2. Der bisherige Artikel 1 Nr. 3 wird Artikel 1 Nr. 3 lit. e) und wie folgt geändert:

a) In § 4b Absatz 3 wird das Wort "soll" durch das Wort "nutzt" ersetzt und das Wort "nutzen" gestrichen.

b) Dem § 4b Absatz 3 wird folgende Nr. 5 angefügt:

"5. in allen gemeldeten Fällen von Sicherheitslücken darauf hinzuwirken, dass diese von den für ein informationstechnisches System Verantwortlichen geschlossen werden und in Koordination mit den Verantwortlichen einen koordinierten Offenlegungsprozess für die erkannte Sicherheitslücke einzuleiten, sofern hiervon auch Dritte betroffen sind."

c) § 4b Absatz 4 wird aufgehoben.

d) Der bisherige § 4b Absatz 5 wird § 4b Absatz 4.

3. Artikel 1 Nr. 11 lit. a) wird wie folgt geändert:

In § 8 Abs. 1a) BSIG-E wird Satz 6 wie folgt gefasst:

„Im gemäß § 4a Absatz 6 benannten Geschäftsbereich des Bundesministeriums der Verteidigung sind eigene Mindeststandards auf einem vergleichbaren Sicherheitsniveau der Mindeststandards für die Sicherheit der Informations- und Kommunikationstechnik umzusetzen. Abweichungen von den Mindeststandards sind in sachlich gerechtfertigten Einzelfällen nach vorheriger Risikoanalyse zulässig.“

Begründung

Ziffer 1

Die Unterrichtungspflichten gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (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, werden auch auf die Bundesministerien ausgeweitet.

Die formulierten Auffangnormen für Ausnahmen zur Unterrichtungspflicht gegenüber dem BSI sind nicht notwendig, da sie ohnehin auf bereits bestehende Rechtsregime und gesetzliche Regelungen verweisen.

Eine sachliche Begründung der Ausnahme von den neu geschaffenen Befugnissen des BSI zur Kontrolle der Sicherheit der Kommunikationstechnik für die Auslandsinformations- und Kommunikationstechnik gemäß § 9 Absatz 2 des Gesetzes über den Auswärtigen Dienst ist nicht ersichtlich. Die Gesetzesbegründung spricht nur von "besonderen Anforderungen an die im Ausland belegene Informations- und Kommunikationstechnik", denen Rechnung getragen werden müsse, ohne diese Anforderungen jedoch genauer zu benennen. Alternative Ansätze zur Kontrolle der Sicherheit der Kommunikationstechnik, die im Ausland belegen ist, werden nicht vorgeschlagen. Deshalb soll § 4 Abs. 5 BSIG-E ersatzlos aufgehoben werden. Im Gegensatz dazu wird die vorgeschlagene Ausnahme von den neu geschaffenen Befugnissen des BSI zur Kontrolle der Sicherheit der Kommunikationstechnik, die für die Bundeswehr und ihre Zwecke betrieben wird, sachlich begründet. Es wird zudem in der Gesetzesbegründung eine Kontrolle in eigener Verantwortung als Alternative beschrieben, jedoch im Normtext nur durch Verweis auf eine Verwaltungsvereinbarung verankert. Um hier Transparenz über das vereinbarte Verfahren zu schaffen, wird eine Verpflichtung zur Veröffentlichung der Verwaltungsvereinbarung in § 4 Abs. 6 S. 2 a.E. BSIG-E aufgenommen.

Ziffer 2

Umwandlung von einer Soll-Vorschrift in eine Verpflichtung des BSI. Genau wie in seiner Funktion als zentrale Stelle für die Sicherheit in der Informationstechnik kritischer Infrastrukturen (KRITIS) gemäß § 8b BSIG, wird das BSI auch in seiner neuen Funktion als allgemeine Meldestelle für die Sicherheit in der Informationstechnik

verpflichtet, Informationen an die für ein informationstechnisches System Verantwortlichen weiterzugeben. Außerdem wird eine neue Zielfunktion zur Verwendung der gemeldeten Informationen eingeführt. Das BSI wird somit verpflichtet in allen gemeldeten Fällen von Sicherheitslücken darauf hinzuwirken, dass diese von den für ein informationstechnisches System Verantwortlichen geschlossen werden und ein koordinierter Offenlegungsprozess für die erkannte Sicherheitslücke eingeleitet wird, sofern hiervon auch Dritte betroffen sind. Die formulierten Auffangnormen für Ausnahmen zur Unterrichtungspflicht gegenüber dem BSI sind nicht notwendig, da sie ohnehin auf bereits bestehende Rechtsregime und gesetzliche Regelungen verweisen.

Ziffer 3

Korrespondierend zu den Änderungen in Bezug auf die neuen Kontrollbefugnisse des BSI für die Sicherheit der Kommunikationstechnik soll auch die Verpflichtung der Bundeswehr zur Einhaltung der Mindeststandards der Sicherheit der Informations- und Kommunikationstechnik angepasst werden. Eine Ausnahme soll dergestalt beibehalten werden, dass eine Verpflichtung besteht, ein vergleichbares Sicherheitsniveau mit den vom BSI festgelegten Mindeststandards in eigener Zuständigkeit sicherzustellen.

Der Änderungsantrag auf Ausschussdrucksache 19(4)813 C hat einschließlich Begründung folgenden Wortlaut:

Der Ausschuss wolle beschließen,

den Gesetzentwurf auf BT-Drucksache 19/26106 mit folgenden Maßgaben zu ändern:

1. In Artikel 1 Nr. 10 wird § 7b Absatz 3 BSIG-E wie folgt gefasst:

"(3) Wird durch Maßnahmen gemäß Absatz 1 eine Sicherheitslücke oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt, sind die für das informationstechnische System Verantwortlichen darüber zu informieren. Das Bundesamt soll dabei auf bestehende Abhilfemöglichkeiten hinweisen und einen koordinierten Offenlegungsprozess für die erkannte Sicherheitslücke einleiten, sofern hiervon auch Dritte betroffen sind. Sind dem Bundesamt die Verantwortlichen nicht bekannt oder ist ihre Identifikation nur mit unverhältnismäßigem Aufwand oder über eine Bestandsdatenabfrage nach § 5c möglich, ist hilfsweise der betreibende Dienstleister des jeweiligen Netzes oder Systems unverzüglich zu benachrichtigen. Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Anzahl der gemäß Absatz 1 ergriffenen Maßnahmen."

2. In Artikel 1 Nr. 20 lit. c) wird § 10 BSIG-E folgender Absatz 7 angefügt:

"(7) Das Bundesministerium des Innern, für Bau und Heimat bestimmt nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände und im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, das Nähere über das Verfahren des koordinierten Offenlegungsprozesses nach § 4b Abs. 3 S. 1 Nr. 5 und § 7b Abs. 3 dieses Gesetzes."

Begründung

Ziffer 1

Die Änderung ist erforderlich, um vom Bundesamt für Sicherheit in der Informationstechnik (BSI) selbst detektierte Sicherheitslücken oder andere Risiken für die IT-Sicherheit konsequent an Verantwortliche zu melden. Ein "koordinierter Offenlegungsprozess" muss eingeleitet werden, wenn Dritte von Sicherheitslücken betroffen sind. Deshalb werden die entgegenstehenden "überwiegenden Sicherheitsinteressen" bei der Übermittlung von durch das BSI entdeckten Sicherheitslücken gestrichen. Durch die Neufassung des Absatzes wird vermieden, dass die im Gesetzentwurf vorgeschlagene Formulierung durch ihre Unklarheit zu einem Einfalltor für das Zurückhalten von Informationen durch das BSI werden kann.

Bei der Übermittlung der Information an die Verantwortlichen soll das BSI künftig jedoch nicht nur auf Abhilfemöglichkeiten hinweisen, sondern in Abstimmung mit den Verantwortlichen einen koordinierten Offenlegungsprozess für die Sicherheitslücken einleiten, sofern hiervon auch Dritte betroffen sind. Hierdurch wird sichergestellt, dass alle dem BSI bekannten Sicherheitslücken geschlossen werden oder die hiervon Betroffenen andere Maßnahmen zum Schutz ihrer informationstechnischen Systeme einleiten können.

Ziffer 2

Das Verfahren für den sowohl in § 4b Abs. 3 S. 1 Nr. 5 als auch in § 7b Abs. 3 BSIG-E benannten "koordinierten Offenlegungsprozess" wird nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände und im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie durch Rechtsverordnung geregelt. Als Vorbild für diese Regelung zur Einbeziehung dient § 10 Abs. 1 BSI-Gesetz (BSIG).

Der Änderungsantrag auf Ausschussdrucksache 19(4)813 D hat einschließlich Begründung folgenden Wortlaut:

Der Ausschuss wolle beschließen,

den Gesetzentwurf auf BT-Drucksache 19/26106 mit folgenden Maßgaben zu ändern:

In Artikel 1 Nr. 10 wird § 7c Abs. 1 wie folgt geändert:

1. Nr. 2 wird aufgehoben.

2. Nr. 1 wird ohne Nummerierung in S. 1 nach den Wörtern ", dass er" eingefügt.

3. In S. 2 werden die Wörter "nach Satz 1 Nummer 1 oder 2" gestrichen.

4. Die Sätze 3 und 4 werden aufgehoben.

Begründung

Durch die in § 7c Abs. 1 BSIG-E geschaffenen Anordnungsbefugnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI) wird das BSI immer mehr zur Gefahrenabwehrbehörde für den Bereich der Cyber-Sicherheit. Bisher sind die in § 109a Abs. 4-6 TKG vorgesehenen Maßnahmen für Telekommunikationsdiensteanbieter nicht verpflichtend. Es ist vielmehr in ihr Ermessen gestellt, ob sie etwa den Datenverkehr umleiten oder Telekommunikationsdienste einschränken, um Verletzungen des Schutzes personenbezogener Daten im Einzelfall abzuwenden.

Der vorgeschlagene § 7c BSIG-E konkretisiert in seinem Absatz 2 die Schutzziele für die angeordneten Maßnahmen. Da sich die Anordnungsbefugnis des § 7c Abs. 1 S. 1 Nr. 1 BSIG-E auf die bereits bestehenden Maßnahmen in § 109a Abs. 4-6 TKG bezieht, werden die Schutzziele künftig auch für die in § 109a Abs. 4-6 TKG vorgesehenen Maßnahmen gelten. Die Integrität, Vertraulichkeit und Verfügbarkeit informationstechnischer Systeme sind als neue Schutzziele daher grundsätzlich zu begrüßen.

Eine ähnliche Möglichkeit zur Konkretisierung der angeordneten Maßnahmen bietet der vorgeschlagene § 7c Abs. 1 S. 1 Nr. 2 BSIG-E jedoch nicht. Die Anordnung, dass ein verpflichteter Telekommunikationsdiensteanbieter "technische Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene informationstechnische Systeme verteilt" wird in der Gesetzesbegründung dahingehend konkretisiert, dass es sich um Befehle zum Aufspielen von Code zum Schließen von Sicherheitslücken (Patch) oder das Übersenden von Schlüsselworten, die beim Empfänger etwa zur automatischen Deinstallation von Programmen führen, handelt (S. 73 f.).

Es bleibt jedoch unklar, ob die Anordnung des BSI auch dahingeht, dass ein Patch auf einem Nutzersystem auch ausgeführt wird oder dass dieses dem Nutzer durch den Telekommunikationsdiensteanbieter nur angeboten werden muss. Ohne eine solche Konkretisierung kann auch die Gesetzesbegründung nicht überzeugen, die pauschal davon ausgeht, dass durch eine Anordnung des BSI kein Eingriff in die Integrität und Vertraulichkeit informationstechnischer Systeme (IT-Grundrecht) vorliegt. Aus Sicht der Antragsteller ist ein unmittelbarer Eingriff in das IT-Grundrecht der Nutzer weder durch die zu unklare Ausgestaltung der Anordnungsbefugnis noch durch die Gesetzesbegründung, die in diesem Punkt nicht zur Aufklärung führt, ausgeschlossen. Aufgrund der Möglichkeit des Eingriffs in das IT-Grundrecht der Nutzer müssen jedoch Schutzmechanismen formuliert werden und auch das Verfahren zur Anordnung näher beschrieben werden.

Überdies ist nicht ersichtlich, welchen zusätzlichen Schutz die Anordnungsbefugnis im Sinne der IT-Sicherheit liefern soll, den nicht auch eine Anordnung von Maßnahmen aus § 109a Abs. 4-6 TKG schon liefern kann. Eine mit klaren Voraussetzungen ausgestaltete Anordnungsbefugnis im Sinne einer Eilkompetenz des BSI, die mit der Verpflichtung von Herstellern zum Angebot von Updates während der üblichen Nutzungsdauer eines Produktes

einhergeht, wäre der IT-Sicherheit allgemein und dem IT-Grundrecht der Nutzerinnen und Nutzer deutlich zuträglicher (vgl. Antrag "Digitalisierung ernst nehmen – IT-Sicherheit stärken" der FDP-Fraktion, BT-Drs. 19/7698).

Der Änderungsantrag auf Ausschussdrucksache 19(4)813 E hat einschließlich Begründung folgenden Wortlaut:

Der Ausschuss wolle beschließen,

den Gesetzentwurf auf BT-Drucksache 19/26106 mit folgenden Maßgaben zu ändern:

In Artikel 1 Nr. 11 wird § 8 wie folgt geändert:

1. Absatz 1 S. 1 wird das Wort "Einvernehmen" durch das Wort "Benehmen" ersetzt.

2. In Absatz 1a werden die Sätze 6 und 7 aufgehoben.

Begründung

Die Begrifflichkeit "Einvernehmen" wird durch im "Benehmen" mit den Ressorts bei der Aufstellung von Mindeststandards für die IT-Sicherheit durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) ersetzt. Die Einführung der Verbindlichkeit für die durch das BSI festgelegten Mindeststandards für die Sicherheit der Informationstechnik des Bundes ist grundsätzlich zu begrüßen. Die in den Vorversionen des Gesetzentwurfs noch enthaltene Formulierung, dass diese Mindeststandards im Benehmen mit den Ressorts durch das BSI festzulegen sind, ist jedoch einem Einvernehmenserfordernis gewichen. Die Änderung stärkt die Position des BSI und stellt den Zustand der Vorversionen des Gesetzentwurfs wieder her.

Die Herausnahme der Bundesgerichte, soweit sie nicht öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen, des Bundestages, des Bundesrates, des Bundespräsidenten und des Bundesrechnungshofes aus dem Anwendungsbereich der aufgestellten Mindeststandards für die Sicherheit der Informationstechnik des Bundes zeigt einen Mangel an Aufarbeitung und Verständnis für die Reichweite und Folgen des Hacks der Folgen Regierungsnetze des IVBB -Hack aus (Informationsverbund Berlin-Bonn) aus dem Jahr 2017.

Abweichungen von den durch das BSI festgelegten Mindeststandards sind gemäß § 8 Abs. 1 S. 2 BSIG-E in sachlich gerechtfertigten Fällen zulässig und sind in solchen Fällen zu dokumentieren und zu begründen. Sollten also Abweichungen von den Mindeststandards durch die oben genannten Stellen vorgenommen werden, sind diese künftig zumindest durch die Dokumentation und Begründung im Einzelfall besser nachvollziehbar.

Der Änderungsantrag auf Ausschussdrucksache 19(4)813 F hat einschließlich Begründung folgenden Wortlaut:

Der Ausschuss wolle beschließen,

den Gesetzentwurf auf BT-Drucksache 19/26106 mit folgenden Maßgaben zu ändern:

In Artikel 1 Nr. 13 lit. a) wird § 8b Abs. 2 Nr. 3 wie folgt gefasst:

"3. das Lagebild bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen oder der Unternehmen im besonderen öffentlichen Interesse kontinuierlich zu aktualisieren und den nach diesem Gesetz verpflichteten Unternehmen regelmäßig in geeigneter und datenschutzkonformer Form zur Verfügung zu stellen und"

Begründung

Die bisherige Verpflichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) gemäß § 8b Abs. 2 Nr. 4a BSI-Gesetz (BSIG) zur unverzüglichen Unterrichtung der KRITIS-Betreiber über die sie betreffenden Informationen, die das BSI im Rahmen seiner Meldestellen-Funktion gesammelt hat und auch die Verpflichtung des BSI gemäß § 8b Abs. 2 Nr. 3 BSIG zur Erstellung und Aktualisierung eines Lagebildes wiegen die umfangreichen Meldeverpflichtungen der Unternehmen nicht auf. Seit Langem wird deshalb unternehmensseitig bereits ein qualitativer Rückkanal mit Informationen über die aktuelle Cyberbedrohungslage gefordert.

Die Änderung in § 8b BSIG-E zielt deshalb darauf ab, dass das BSI zum einen das Lagebild weiterhin aktuell zusammenstellt und es danach regelmäßig allen nach dem BSIG verpflichteten Unternehmen zur Verfügung stellt. Damit wird der Rückkanal mit Informationen nicht nur gegenüber den von einer bestimmten Information betroffe-

nen Unternehmen gewährleistet, sondern generell für alle nach dem Gesetz verpflichteten Unternehmen aufgebaut. Perspektivisch sollte zum anderen auch die Aktualität des Lagebildes noch genauer definiert werden, wobei ein tagesaktuelles Lagebild erstrebenswert ist.

Der Änderungsantrag auf Ausschussdrucksache 19(4)813 G hat einschließlich Begründung folgenden Wortlaut:

Der Ausschuss wolle beschließen,

den Gesetzentwurf auf BT-Drucksache 19/26106 mit folgenden Maßgaben zu ändern:

In Artikel 1 Nr. 17 wird § 8f Absatz 2 BSIG-E wie folgt gefasst:

"Das Bundesamt führt für die Selbsterklärung nach Absatz 1 Formulare ein, die zur Abgabe der Selbsterklärung verwendet werden können."

Begründung

Die jetzige Formulierung zur Abgabepflicht einer Selbsterklärung zur IT-Sicherheit durch Unternehmen im besonderen öffentlichen Interesse verpflichtet das Bundesamt für Sicherheit in der Informationstechnik (BSI) nicht, Formulare als Arbeitserleichterung für die verpflichteten Unternehmen zur Verfügung zu stellen. Gleichzeitig sind solche Formulare von den verpflichteten Unternehmen aber zu verwenden, sofern das BSI diese einführt. Die vorgeschlagene Änderung kehrt das Prinzip um. 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.

Der Änderungsantrag auf Ausschussdrucksache 19(4)813 H hat einschließlich Begründung folgenden Wortlaut:

Der Ausschuss wolle beschließen,

den Gesetzentwurf auf BT-Drucksache 19/26106 mit folgenden Maßgaben zu ändern:

- Artikel 6 Absatz 2 wird aufgehoben.

Begründung

Das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 enthält in seinem Art. 10 eine Evaluierungsklausel, die durch den vorliegenden Gesetzentwurf gestrichen werden soll. In der Begründung des Gesetzentwurfs (S. 98 f.) wird darauf verwiesen, dass die durch Art. 10 des IT-Sicherheitsgesetzes zu evaluierenden Vorschriften durch das vorliegende zweite IT-Sicherheitsgesetz teilweise wieder geändert werden sollen oder die ursprünglich vorgesehene Evaluierung mit der neu vorgesehenen Evaluierung in Art. 6 zusammengeführt werden könne. Zudem wird darauf verwiesen, dass mit dem Sektor der Siedlungsabfallentsorgung ein neuer KRITIS-Bereich hinzutrete, durch welchen eine fristgemäß im Sommer 2021 durchzuführende Evaluierung "zu einer unnötigen und unwirtschaftlichen Doppelevaluierung" führen würde. Die Evaluierung von IT-Sicherheitsmaßnahmen ist aus Sicht der Antragsteller niemals unnötig und im Rahmen eines agilen Verständnisses von Cybersicherheit auch dringend geboten. Wenn der neue Sektor der Siedlungsabfallentsorgung erst für die in Art. 6 neu vorgesehene Evaluierungsfrist vorgesehen werden soll, kann dies auch unabhängig von der Streichung der noch ausstehenden Evaluierung nach Art. 10 des IT-Sicherheitsgesetzes so festgelegt werden.

c) Darüber hinaus hat der Ausschuss für Inneres und Heimat einen Entschließungsantrag der Fraktion der AfD auf Ausschussdrucksache 19(4)810 mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion der AfD abgelehnt.

Der Entschließungsantrag auf Ausschussdrucksache 19(4)810 hat folgenden Wortlaut:

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 2.0 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.

Zu Buchstabe b

Der **Ausschuss für Inneres und Heimat** hat den Antrag auf Drucksache 19/26225 in seiner 134. Sitzung am 21. April 2021 abschließend beraten und empfiehlt die Ablehnung des Antrags mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion der AfD.

Zu Buchstabe c

Der **Ausschuss für Inneres und Heimat** hat den Antrag auf Drucksache 19/26226 in seiner 134. Sitzung am 21. April 2021 abschließend beraten und empfiehlt die Ablehnung des Antrags mit den Stimmen der Fraktionen CDU/CSU, SPD, FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN gegen die Stimmen der Fraktion der AfD.

Zu Buchstabe d

Der **Ausschuss für Inneres und Heimat** hat den Antrag auf Drucksache 19/1328 in seiner 134. Sitzung am 21. April 2021 abschließend beraten und empfiehlt die Ablehnung des Antrags mit den Stimmen der Fraktionen der CDU/CSU, SPD und AfD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN bei Stimmenthaltung der Fraktion der FDP.

IV. Begründung

1. Zur Begründung allgemein wird auf Drucksache 19/26106 verwiesen. Die vom Ausschuss für Inneres und Heimat auf Grundlage des Änderungsantrags der Fraktionen der CDU/CSU und SPD auf Ausschussdrucksache 19(4)811 vorgenommenen Änderungen begründen sich wie folgt:

Zu Nummer 1 (Artikel 1 – Änderungen des BSI-Gesetzes)

Zu Buchstabe a (§ 1)

Mit der Neufassung von § 1 BSI-Gesetz wird klargestellt, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) die zentrale Stelle für die Informationssicherheit auf nationaler Ebene ist. Es wird festgelegt, dass das BSI Aufgaben der Beratung und Unterstützung (siehe Begründung zu Artikel 1 Buchstabe c Doppelbuchstabe cc) als neutrale Stelle durchführt. Eine Änderung der Rechts- und Fachaufsicht des Bundesministeriums des Innern, für Bau und Heimat ist hiermit nicht verbunden.

Zu Buchstabe b (§ 2)

Doppelbuchstabe aa

Der Legaldefinition des Begriffs der Informationssicherheit wird mit der Änderung ein erläuternder Teil vorangestellt, um den Inhalt der Schutzziele der Informationssicherheit näher zu bestimmen. Im bisherigen § 2 Absatz 2 BSIG-G wird der Begriff Unversehrtheit durch den Begriff Integrität ersetzt, um im BSI-Gesetz ein einheitliches Verständnis des Schutzziels sicherzustellen.

Doppelbuchstabe bb

Es handelt sich um eine Folgeänderung.

Doppelbuchstabe cc

Es handelt sich um eine redaktionelle Klarstellung.

Doppelbuchstabe dd

Es handelt sich um eine Folgeänderung.

Doppelbuchstabe ee

In Absatz 13 wird die bisher vorhandene Verknüpfung mit der hohen Bedeutung der kritischen Komponente für das Gemeinwohl aus systematischen Gründen gestrichen. Das Gemeinwohl ist in den übrigen Voraussetzungen bereits inkorporiert. Durch die Ergänzung der Formulierung „unter Verweis auf diese Vorschrift“ wird klargestellt, dass kritische Komponenten oder Funktionen im Sinne dieses Gesetzes nur solche sind, die einen ausdrücklichen Verweis auf § 2 Absatz 13 BSI-Gesetz enthalten. Die Einordnung bestimmter Komponenten oder Funktionen als kritisch im Sinne des BSI-Gesetzes, ohne dass in Bezug auf diese Komponenten oder Funktionen eine ausdrückliche Bezugnahme auf § 2 Absatz 13 BSI-Gesetz erfolgt, ist daher nicht möglich. Dadurch wird Unklarheit darüber, ob Komponenten in Kritischen Infrastrukturen kritische Komponenten im Sinne des BSI-Gesetz sind, vermieden.

Mit der Neufassung von Absatz 14 werden die Unternehmen im besonderen öffentlichen Interesse durch wesentliche Zulieferer der nach ihrer inländischen Wertschöpfung größten Unternehmen in Deutschland ergänzt. Zu diesen Unternehmen gehören solche Zulieferer, die wegen ihrer Alleinstellungsmerkmale auf die Wertschöpfung der größten Unternehmen Einfluss haben, zum Beispiel, weil ein Ausfall der Zulieferung ihrer Produkte oder der Erbringung ihrer Dienstleistungen auch einen Ausfall der Wertschöpfung der größten Unternehmen bedeuten kann. Damit sind diese Zulieferer ebenfalls Unternehmen von besonderem öffentlichem Interesse.

Zu Buchstabe c (§ 3)

Doppelbuchstabe aa

Es handelt sich um eine Folgeänderung.

Doppelbuchstabe bb

Mit der Änderung in § 3 BSI-Gesetz wird dem Aufgabenkatalog die Zielbestimmung vorangestellt. Das BSI fördert bei der Erfüllung seiner Aufgaben das Ziel, die in § 2 Abs. 2 BSI-Gesetz bestimmten Schutzziele der Informationssicherheit zu gewährleisten.

Doppelbuchstaben cc und dd

Es handelt sich um Folgeänderungen.

Doppelbuchstabe ee

Mit der Zuweisung dieser Aufgabe wird klargestellt, dass das BSI den Bund, mithin die Bundesministerien und ihre nachgeordneten Geschäftsbereichsbehörden, in Fragen der IT-Sicherheit berät und unterstützt (vgl. Begründung zu Artikel 1 Buchstabe a).

Doppelbuchstabe jj

Mit der Änderung in Satz 2 Nummer 20 wird klargestellt, dass das BSI einen Stand der Technik beschreibt, statt diesen zu entwickeln. Es wird festgeschrieben, dass es zu den Aufgaben des BSI gehört, technische Richtlinien zu erstellen. Dabei werden die internationalen Standards und Normen sowie die maßgeblichen Akteure (Hersteller, Entwickler, Wirtschaft, Verbände usw.) einbezogen.

Zu Buchstabe d (§ 4a)

Doppelbuchstabe aa

Das Erfordernis der vorzeitigen Absprache wird im Sinne der Effektivität der Maßnahmen des BSI gestrichen.

Doppelbuchstabe bb

Die Änderung in § 4a Absatz 5 trägt dem Umstand Rechnung, dass besondere Anforderungen an die Informations- und Kommunikationstechnik (IKT) der Auslands-IT insbesondere in den Auslandsvertretungen bestehen. Es wird klargestellt, dass diese IKT von der Kontrollbefugnis ausgenommen ist, die Bestimmungen für die Schnittstellen zur Kommunikationstechnik des Bundes (vgl. § 5 BSI-Gesetz) unberührt bleiben. Näheres regelt eine Verwaltungsvereinbarung.

Die Änderung in § 4a Abs. 6 präzisiert die Reichweite der Ausnahme für die IKT der Streitkräfte und des Militärischen Abschirmdienstes. Es wird klargestellt, dass IT-Dienstleister nicht von der Kontrollbefugnis ausgenommen sind, sofern sie nicht für die unmittelbaren Zwecke der Streitkräfte (insb. Waffensysteme und Einsatztechnik) betrieben wird. Im Sinne des einheitlichen Schutzniveaus der IKT der Bundesverwaltung bleiben auch hier die Bestimmungen für die Schnittstellen des Bundes von der Ausnahme unberührt. In der Verwaltungsvereinbarung ist die Ausnahme näher zu regeln.

Doppelbuchstabe cc

Mit der Änderung wird klargestellt, dass das BSI zum einen befugt ist, Informationen entgegenzunehmen und zum anderen, dass die Entgegennahme nicht verweigert werden kann.

Doppelbuchstabe dd

Mit der Änderung wird die Befugnis der Reichweite von § 7 des Entwurfes des BSI-Gesetzes angepasst. Das BSI nutzt die gemeldeten Informationen, z. B. IT-Sicherheitslücken, somit, um die Öffentlichkeit und betroffene Kreise zu warnen und zu informieren. Betroffene Kreise können insbesondere Hersteller, Vertreiber und Anwender sein. Durch den Verweis auf § 7 BSI-Gesetz wird zudem sichergestellt, dass das Responsible Disclosure-Verfahren, d.h. die Einbindung der Hersteller vor der Veröffentlichung einer Sicherheitslücke, Anwendung findet.

Zu Buchstabe e (§ 5)

Die mögliche Dauer der Speicherung von Protokolldaten wird auf 18 Monate angehoben, um komplexen Cyberangriffen, d.h. insbesondere sog. Advanced Persistent Threats (APT-Angriffen), effektiver begegnen zu können. Ob der erhöhten Komplexität von technisch fortgeschrittenen APT-Angriffen bewegen sich Täter oftmals über Monate unentdeckt auf Zielsystemen. Aus diesem Grund ist es erforderlich, einen möglichst langfristigen Blick in Vergangenheit zu ermöglichen, um Angriffsvektoren aufklären zu können. Ohne sie ist eine Aufklärung

nur unzureichend oder gar nicht möglich. Diese Aufklärung und darauf aufbauende Präventionsmaßnahmen sind gerade auch zum Schutz personenbezogener Daten vor unberechtigtem Zugriff und Datenabflüssen zentral.

Auf die pseudonymisierten Protokolldaten in der Kommunikationstechnik des Bundes kann nur anlassbezogen zum Zwecke der Aufklärung oder aber der Widerlegung eines (vermuteten) Angriffs zugegriffen werden. § 5 BSIG sieht zudem eindeutige Regelungen zur Datensicherheit, Datenverwendung und zur Transparenz der Nutzung vor.

Zu Buchstabe f (§§ 5a und 5b)

Es handelt sich um eine Folgeänderung.

Zu Buchstabe g (§ 5c BSIG)

Es handelt sich um Folgeänderungen zum Gesetz zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020 (BGBl. I 2021 S. 448). Die Formulierung „drohende Gefahr“ in Absatz 1 wird entsprechend durch die Formulierung „zum Schutz“ ersetzt, im Übrigen erfolgen redaktionelle Folgeanpassungen.

Zu Buchstabe h (§ 7)

Es handelt sich um eine redaktionelle Richtigstellung.

Zu Buchstabe i (§ 7a)

Es handelt sich um eine Folgeänderung.

Zu Buchstabe j (§ 7b)

Doppelbuchstabe aa

Mit der Änderung wird festgelegt, dass die jeweiligen IT-Verantwortlichen unverzüglich über detektierte Sicherheitslücken und Sicherheitsrisiken zu informieren sind. Fehlende entgegenstehende Sicherheitsinteressen hat das BSI nicht vorab festzustellen.

Doppelbuchstabe bb

Mit der Änderung wird die datenschutzrechtliche Kontrolle bei der Überprüfung der Weißen Liste gestärkt. Der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit sind die sich aufgrund der Überprüfungen ergebenden Änderungen der Weißen Liste zur Kontrolle vierteljährlich vorzulegen.

Zu Buchstabe k (§ 8)

Doppelbuchstabe aa

Durch die Änderung wird die Effektivität der Befugnis zur Festlegung von Mindeststandards sichergestellt. Die Benehmensregelung entspricht der bestehenden Praxis von Konsultationsverfahren und verhindert, dass die Festlegung verbindlicher Mindeststandards durch ein einzelnes Veto verhindert wird. Es besteht über § 8 Absatz 1 Satz 2 des Entwurfes des BSI-Gesetzes die Möglichkeit, in sachlich gerechtfertigten Fällen von Mindeststandards abzuweichen.

Doppelbuchstabe bb und cc

Es handelt sich bei dieser Änderung um eine gebotene redaktionelle Richtigstellung. Die bisher in Absatz 1a verorteten Sätze werden an Absatz 1 angefügt, da dort die Befugnis für verbindliche Mindeststandards geregelt wird.

Zu Buchstabe l (§ 8a)

Doppelbuchstabe aa

Die Änderung trägt dem Umstand Rechnung, dass für die Umsetzung der Vorgaben des § 8a Absatz 1a des Entwurfes des BSI-Gesetzes (Vorhaltung von Systemen zur Angriffserkennung) bei komplexen und größeren Kritischen Infrastrukturen wie den Universitätskliniken mehr als zwölf Monate benötigt werden, zumal Gesetzesverstöße mit Bußgeldern belegt sind.

Doppelbuchstabe bb

Mit der Streichung wird dem Umstand Rechnung getragen, dass die derzeit geltende Benehmensregelung in § 8a Absatz 2 Satz 2 Nummer 2 BSIG dazu führt, dass bei bestimmten branchenspezifischen Sicherheitsstandards eine Vielzahl von Vollzugsbehörden auf Landesebene beteiligt werden muss, wenn sie als Aufsichtsbehörden fachlich betroffen sind. Gerade wenn die Aufsicht bei einzelnen Landesbehörden auf Ebene regionaler oder kommunaler Gebietskörperschaften liegt, ist eine derart weit gestreute Beteiligung nicht praktikabel, zumal die Aufsichtsbehörden auch nicht immer die erforderliche fachliche Kompetenz besitzen, um die Wechselwirkung zwischen informationstechnischen und sonstigen sicherheitsrelevanten Belangen beurteilen zu können.

Doppelbuchstabe cc

Es handelt sich um eine Folgeänderung.

Zu Buchstabe m (§§ 8b bis 8c)

Es handelt sich um eine Folgeänderung.

Zu Buchstabe n (§ 8d)

Bei der Änderung in Absatz 1 handelt es sich um eine redaktionelle Korrektur. Die Ergänzung des neuen Absatzes 1a stellt klar, dass für kleine und Kleinstunternehmen im Sinne der 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36) die Pflichten der Unternehmen im besonderen öffentlichen Interesse des § 8f nicht gelten.

Zu Buchstabe o (§ 8e)

Es handelt sich um eine Folgeänderung.

Zu Buchstabe p (§§ 9a, 9b, 9c)

Doppelbuchstabe aa (§ 9a)

Die Regelung wird als Kann-Vorschrift gestaltet, damit das BSI im Rahmen der Erteilung der Befugnis, als Konformitätsbewertungsstelle tätig zu werden, die Befugniserteilung mit Nebenbestimmungen, beispielsweise einer Befristung, versehen kann.

Doppelbuchstabe bb (§ 9b)

Zu Absatz 1

Der geplante erstmalige Einsatz kritischer Komponenten ist dem Bundesministerium des Innern, für Bau und Heimat vor Einsatz anzuzeigen. Gemeint ist damit jeweils der erstmalige Einsatz einer bestimmten Komponente – nicht eines Typs von Komponenten – durch einen bestimmten Betreiber. Daher muss jeder Betreiber den erstmaligen Einsatz einer kritischen Komponente anzeigen, selbst wenn der Einsatz desselben Typs bei einem anderen Betreiber bereits angezeigt und nicht untersagt wurde. Auch wenn demselben Betreiber gegenüber der Einsatz einer Komponente desselben Typs nicht untersagt wurde, muss dieser erneut eine Anzeige abgeben, wenn er eine weitere Komponente desselben Typs für eine andere Art des Einsatzes vorsieht als in dem zuvor nicht untersagten Fall. Eine Erleichterung enthält jedoch der neu eingefügte Satz 3. Danach muss derselbe Betreiber den Einsatz einer Komponente nicht anzeigen, wenn dieser Betreiber eine Komponente desselben Typs für dieselbe Art des Einsatzes bereits angezeigt hat und dies nicht innerhalb der Frist untersagt wurde. Dadurch wird unnötiger bürokratischer Aufwand verhindert.

Es sind nur nach Inkrafttreten dieser Regelung und der jeweiligen Regelung zur Bestimmung kritischer Komponenten eingebaute bzw. installierte Komponenten anzuzeigen. Eine Rückwirkung der Anzeigepflicht auf bereits vor Inkrafttreten dieser Regelung eingesetzte Komponenten besteht nicht.

Unter Art des Einsatzes ist die Funktion und Verortung in der Kritischen Infrastruktur (etwa Lokalisierung, Sicherheitsrelevanz, insbesondere mögliche Auswirkungen auf die Sicherheit der Kritischen Infrastrukturen, Funktionalität, Quantität des Einsatzes usw.) zu verstehen.

Die Voraussetzung der Zertifizierungspflicht wurde entfernt, da diese keinen selbstständigen Anwendungsbereich hatte. § 2 Absatz 13 legt über die dortigen Voraussetzungen fest, welche Komponenten über § 9b adressiert werden.

Mit der Änderung des § 109 Absatz 6 Satz 1 Nummer 3 TKG (Artikel 2, Änderungen des Telekommunikationsgesetzes) werden erstmals kritische Komponenten nach § 2 Absatz 13 festgelegt, indem die Bundesnetzagentur ermächtigt wird, kritische Funktionen im Sinne von § 2 Absatz 13 Satz 1 Nummer 3 Buchstabe b festzulegen. Soweit zukünftig eine derartige Notwendigkeit zur Festlegung von kritischen Komponenten in anderen Sektoren von Kritischen Infrastrukturen durch den Gesetzgeber erkannt wird, kann die Festlegung in entsprechender Weise im jeweils einschlägigen sektoralen Gesetz erfolgen.

Zu Absatz 2

Der neue Absatz 2 ist der vorherige Absatz 3, der vorgezogen wird, da diese Regelungen systematisch zur ex-ante Prüfung gehören.

Absatz 2 regelt die Befugnis des Bundesministeriums des Innern, für Bau und Heimat, den Einsatz einer kritischen Komponente im Einzelfall zu untersagen.

Die Eingriffsvoraussetzungen wurden von „überwiegenden öffentlichen Interessen, insb. sicherheitspolitischen Belangen“ auf „voraussichtliche Beeinträchtigungen der öffentlichen Sicherheit und Ordnung“ geändert. Dieser Maßstab wird bereits in § 5 Absatz 2 des Außenwirtschaftsgesetzes in Bezug auf die Prüfung von Erwerben inländischer Unternehmen durch unionsfremde Erwerber verwendet.

Daneben werden den Gefahrbegriff konkretisierende Fälle aufgeführt, welche bei der Prüfung nach Absatz 2 insbesondere berücksichtigt werden können.

Damit kann das Bundesministerium des Innern, für Bau und Heimat insbesondere bei der Prüfung berücksichtigen, ob der Hersteller unmittelbar oder mittelbar von der Regierung, einschließlich sonstiger staatlicher Stellen oder Streitkräfte, eines Drittstaates kontrolliert wird. Die Formulierung „unmittelbar oder mittelbar“ stellt dabei klar, dass nicht nur eine gesellschaftsrechtliche oder finanzielle Kontrolle, sondern auch sonstige Möglichkeiten wesentlicher Einflussnahme erfasst werden. Des Weiteren kann berücksichtigt werden, ob der Hersteller bereits an Aktivitäten beteiligt war, die nachteilige Auswirkungen auf die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland oder eines anderen Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages hatten. Darunter kann zum Beispiel die Mitwirkung an einem Cyber-Angriff auf Privatpersonen, Unternehmen oder Behörden in Deutschland oder einem der Mitgliedsstaaten der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages, einschließlich deren Einrichtungen, fallen. Ebenso kann berücksichtigt werden, ob der Einsatz der kritischen Komponente im Einklang mit den sicherheitspolitischen Zielen der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrages steht. Die Aufzählung ist nicht abschließend. Im Rahmen der sicherheitspolitischen Bewertung können daher alle für die öffentliche Sicherheit und Ordnung relevanten Aspekte berücksichtigt werden.

Das Bundesministerium des Innern, für Bau und Heimat berücksichtigt im Rahmen der Prüfung einer voraussichtlichen Beeinträchtigung der öffentlichen Sicherheit und Ordnung zusätzlich auch die nach Absatz 3 Satz 1 vorzulegende Garantieerklärung des Herstellers.

Für die Prüfung unter Einbindung beteiligter Behörden und gegebenenfalls der Erstellung eines Untersagungsbescheids einschließlich der erforderlichen Abstimmung innerhalb der Bundesregierung steht dem Bundesministerium des Innern, für Bau und Heimat nun ein Zeitraum von zwei Monaten zur Verfügung, um eine sachgerechte Prüfung zu ermöglichen. Das Bundesministerium des Innern, für Bau und Heimat kann die Frist gegenüber dem Betreiber um weitere zwei Monate verlängern, wenn die Prüfung besondere Schwierigkeiten tatsächlicher oder rechtlicher Art aufweist. Diese Möglichkeit entspricht § 14a Absatz 4 Satz 1 Außenwirtschaftsgesetz. Die Betreiber müssen eine entsprechende Entscheidung bis zum Ablauf der Frist abwarten, bevor der Einsatz gestattet ist (Untersagungsvorbehalt). Nach Ablauf der Frist ist der Einsatz automatisch gestattet, wenn dem Betreiber bis dahin keine Untersagung mitgeteilt wurde.

Die Notwendigkeit einer derartigen Untersagungsmöglichkeit ist der Tatsache geschuldet, dass mit zunehmender informationstechnischer Komplexität der eingesetzten kritischen Komponenten ein wesentlicher Teil der Beherrschbarkeit der Technologie im Rahmen der Produktpflege (Softwareupdates, Firmware-Updates, Schließen

von Sicherheitslücken) beim Hersteller selbst oder auch der weiteren Lieferkette verbleibt. Auf Grund der hohen Komplexität der kritischen Komponenten und der zu erwartenden stetigen Software/Firmware-Updates bieten etwa weder eine Komponentenzertifizierung noch hohe technische Sicherheitsanforderungen eine ausreichende Sicherheit dahingehend, dass die Hersteller keine missbräuchlichen Zugriffmöglichkeiten auf Hard- und Software implementieren, oder sonstige Handlungen vornehmen, die Sabotage oder Spionage ermöglichen. Geeignete technische Maßnahmen können derartige Risiken zwar minimieren beziehungsweise in den möglichen Auswirkungen abschwächen, die letztlich im Raum stehende Frage der Vertrauenswürdigkeit von Herstellern – in diesem Sinne – kann hierdurch jedoch nicht umfassend adressiert werden.

Die umfassende Prüfung derartiger Restrisiken muss über eine Risikobewertung in Bezug auf den Hersteller der kritischen Komponenten erfolgen. Absatz 2 dient damit auch der Umsetzung der Empfehlungen der sog. „EU 5G Toolbox“ („Cybersecurity of 5G Networks – EU Toolbox of risk mitigating measures“, dort „strategic measure SM03“), welche die Bewertung von Risikoprofilen der Hersteller und mögliche Restriktionen als eine der Schlüsselmaßnahmen zur Absicherung der 5G-Netze herausstellt.

Ferner wurde das Einvernehmen mit den übrigen betroffenen Ressorts in ein Benehmenserfordernis geändert.

Bei der Entscheidung durch das Bundesministerium des Innern, für Bau und Heimat sind die Vorgaben des § 28 Verwaltungsverfahrensgesetz über die Anhörung Beteiligter einzuhalten. Dabei kann der Hersteller der kritischen Komponenten nach den Vorgaben des § 13 Absatz 2 Verwaltungsverfahrensgesetz als Beteiligter hinzugezogen werden. Gleiches gilt für die Entscheidungen nach Absatz 4, 6 und 7.

Zu Absatz 3

Neben der bestehenden Pflicht, technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, müssen Betreiber Kritischer Infrastrukturen künftig auch eine Erklärung des Herstellers der kritischen Komponenten einholen. Darin erklärt der Hersteller, wie dieser sicherstellt, dass dessen Komponente über keine technischen Eigenschaften verfügt, die spezifisch geeignet sind, missbräuchlich, insbesondere zum Zwecke von Sabotage, Spionage oder Terrorismus auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können. Diese Aussage muss sich auf die Komponente selbst und ihr Zusammenspiel mit anderen Komponenten beziehen. Zudem hat der Hersteller in der Garantieerklärung weitere Zusicherungen und Angaben zu machen, die das Bundesministerium des Innern, für Bau und Heimat durch Allgemeinverfügung festlegen wird.

Dabei muss der Hersteller seine Garantieerklärung in Bezug auf sein Endprodukt einschließlich aller ihm zugelieferten Teile abgeben, das heißt auch in Bezug auf die Lieferkette. Der bisherige Satz 2 (konnte gelöscht werden, da es sich um eine nicht notwendige Klarstellung gehandelt hat.

Daneben wurden die gesetzlichen Vorgaben an die Einzelheiten der Garantieerklärung in Hinblick auf die Konkretisierung des Gefahrenmaßstabes des Absatzes 2 geändert. Diese müssen aus den Schutzzielen der Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur folgen und die Vermeidung von Gefahren für die öffentliche Sicherheit und Ordnung adressieren, die aus der Sphäre des Herstellers der kritischen Komponente, insbesondere dessen Organisationsstruktur, stammen.

Zu Absatz 4

Absatz 4 regelt im Gegensatz zur ex-ante Prüfung nach Absatz 2 auch die Prüfung der Einhaltung der Vorgaben der Garantieerklärung, sowie die Möglichkeit einer Untersagung auf Grund voraussichtlicher Gefährdungen für die öffentliche Sicherheit oder Ordnung im laufenden Einsatz (ex-post Prüfung). Bei festgestellten Verstößen oder voraussichtlichen Beeinträchtigungen kann der weitere Einsatz einer Komponente untersagt werden (Rückbau). Die Pflichten aus der Garantieerklärung beziehen sich damit nicht allein auf den Zeitpunkt des Einsatzes, sondern müssen fortwährend, also gerade im Betrieb der Komponenten, eingehalten werden. Dies erfordert eine fortlaufende Bewertung der Vertrauenswürdigkeit, mithin vorliegender Erkenntnisse von Verstößen gegen die Garantieerklärung. Für Entscheidungen nach Absatz 4 bleibt – anders als bei Absatz 2 – das Einvernehmen mit den betroffenen Ressorts notwendig.

Die Voraussetzungen für eine ex-post Untersagung wurden an den Gefahrenmaßstab des Absatz 2 angepasst.

Zu Absatz 5

Absatz 5 listet beispielhaft Gründe auf, welche zu einer mangelnden Vertrauenswürdigkeit eines Herstellers führen können. Die Regelung wird in eine „kann"-Vorschrift geändert, damit ist auch bei Vorliegen von Anhaltspunkten nach den Nummern 1 bis 6 nicht zwingend von fehlender Vertrauenswürdigkeit des Herstellers auszugehen. Die Prüfung der Vertrauenswürdigkeit hat vielmehr unter Abwägung aller sicherheitsrelevanten Aspekte zu erfolgen. Nr. 5 wurde hinzugefügt, um die Vertrauensaspekte umfassend zu adressieren.

Zu den Absätzen 6 und 7

Die bisherige Voraussetzung der „wiederholten" Verstöße wurde durch das Merkmal der „schwerwiegenden Verstöße" ersetzt. Dies ist notwendig, da allein die Quantität von Verstößen kein adäquates Entscheidungsmerkmal ist.

Doppelbuchstabe cc (§ 9c)

Die Änderung ermöglicht die Berücksichtigung bestehender Normen und Standards als Grundlage für die IT-Sicherheitsanforderungen, soweit diese vom Bundesamt als geeignet festgestellt werden. Die weiteren Änderungen dienen dazu, einen Konflikt zwischen verschiedenen bestehenden Normen, Standards, branchenabgestimmten IT-Sicherheitsvorgaben und Technischen Richtlinien aufzulösen.

Zu Buchstabe q (§ 10)

Doppelbuchstabe aa

Mit dem Verweis auf § 9c wird in § 10 Absatz 3 eine redaktionelle Richtstellung vorgenommen.

Alle Gebührentatbestände im Zuständigkeitsbereich des Bundesministeriums des Innern, für Bau und Heimat werden in einer Gebührenverordnung (BMIBGebV) konzentriert. Die zusätzlichen Gebührentatbestände des Bundesamtes sollten daher in der BMIBGebV, nicht in der Verordnung nach § 10 Absatz 3 verankert werden.

Doppelbuchstabe bb

Hinsichtlich Absatz 5 handelt es sich um eine redaktionelle Anpassung sowie um eine Folgeänderung zu Nummer 1 Buchstabe b Doppelbuchstabe ee Dreifachbuchstabe fff.

Die Streichung von Absatz 6 ergibt sich daraus, dass das Vorhaben bereits ausreichend in § 166 Absatz 1 Satz 2 TKG-E (BT-Drs. 19/26108) berücksichtigt ist.

Zu Buchstabe r (§ 11)

Es handelt sich um eine Folgeänderung.

Zu Buchstabe s (§ 13)

Die Änderung von § 7 Absatz 2 Satz 2 ist eine Folgeänderung, die sich der bisherigen Nummer 8 Buchstabe a Doppelbuchstabe bb und Nummer 8 Buchstabe b ergibt.

Die Einfügung eines § 13 Absatz 3 verpflichtet das Bundesministerium des Innern, für Bau und Heimat (BMI) dazu, den Ausschuss für Inneres und Heimat des Deutschen Bundestages regelmäßig über die Anwendung des BSI-Gesetzes zu informieren. Dem Gesetzgeber wird damit ermöglicht, seiner Beobachtungs- und Nachbesserungspflicht nachzukommen.

Zu Buchstabe t (§§ 14, 14a)

Es handelt sich um eine Folgeänderung.

Zu Nummer 2 (Artikel 2 – Änderungen des Telekommunikationsgesetzes)

Zu Buchstabe a (§ 109)

Mit der Änderung wird klargestellt, dass sich diese Verpflichtung nur auf Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial bezieht und nicht wie im Gesetzentwurf bisher vorgesehen pauschal auf kritische Komponenten im Sinne des § 2 Absatz 13 BSI-Gesetzes. Die Klarstellung steht in Einklang mit Erwägungsgrund 95 der Richtlinie (EU) 2018/1972, der die Erforderlichkeit der Sicherstellung angemessener

Sicherheitsanforderungen entsprechend der spezifischen Art und wirtschaftlichen Bedeutung der Dienste bekräftigt. Der Änderungsvorschlag steht zudem in Einklang mit den Regelungen des § 164 Absatz 9 Satz 2 TKG-E (BT-Drs. 19/26108).

Zu den Buchstaben b, c und d (§ 113)

Es handelt sich wie bei Nummer 1 Buchstabe g um Folgeänderungen zum Gesetz zur Anpassung der Regelungen über die Bestandsdatenauskunft an die Vorgaben aus der Entscheidung des Bundesverfassungsgerichts vom 27. Mai 2020 (BGBl. I 2021 S. 448). Des Weiteren wird in § 113 Absatz 5 eine rechtstechnisch notwendige Ergänzung vorgenommen.

Zu Nummer 3 (Artikel 3 – Änderungen des EnWG)

Es handelt sich um eine Folgeanpassung zu Nummer 1 Buchstabe l Doppelbuchstabe aa.

2. Die **Fraktion der CDU/CSU** betont, die Koalition habe lange am IT-Sicherheitsgesetz gearbeitet. Inhaltlich seien die Beratungen teilweise überlagert worden um die Debatte zur Vergabe der 5G-Netze. Dieses Gesetz greife jedoch deutlich weiter und gehe über diese Frage hinaus. Durch die Reform führe man das IT-Sicherheitskennzeichen ein. Wichtig sei hierbei, voran zu gehen und nicht auf eine verpflichtende Einführung durch die Europäische Union zu warten. Das BSI werde zu einer echten Sicherheitsbehörde für alle Bürger/Innen ausgebaut und gestärkt. Darüber hinaus schaffe man weitreichende Zugriffsbefugnisse und Kontrollmechanismen, was eine erhebliche Aufwertung der IT-Sicherheit in Deutschland bedeute. Durch die Änderungsanträge habe man Einwände von Verbänden und Sachverständigen aufgegriffen und so etwa den ursprünglichen § 10 Absatz 6 des Entwurfs, der die Offenlegung von Schnittstellen behandelt habe, gestrichen und an weiteren Stellen nachgeschärft. Die in der öffentlichen Anhörung geäußerte Kritik zum geplanten § 9b habe man aufgegriffen und im parlamentarischen Verfahren grundlegend geändert. Durch die Änderungen schließe man einen Drittstaatseinfluss aus und nehme eine Kohärenz mit den Bündniszielen auf. Insgesamt stelle man klar, dass es sich um ein Sicherheitsgesetz handele, sodass der Beweismaßstab des Polizei- und Sicherheitsrechts gelte. Hierdurch schaffe man ein gutes IT-Sicherheitsgesetz und setze ein Zeichen für einen funktionierenden Parlamentarismus.

Die **Fraktion der SPD** hebt hervor, die nun zur Abstimmung gestellte Vorlage unterscheide sich wesentlich vom ursprünglichen Gesetzentwurf der Bundesregierung. Man sei stolz darauf, dass sich wesentliche Punkte, die die Fraktion zur Debatte gestellt habe, nun im Änderungsantrag wiederfänden. Die Hinweise aus der öffentlichen Anhörung habe man ernst genommen. Insgesamt lege man eine klare Aufgabendefinition für das BSI fest, welches auch finanzielle und personelle Aufstockungen erhält. Hierdurch werde vor allem der Verbraucherschutz gestärkt. Beim Schwachstellenmanagement gehe man im Sinne der IT-Sicherheit einen klaren Weg – Informationen seien anzunehmen und die Öffentlichkeit sowie weitere Kreise zu unterrichten. Durch die Änderungen beseitige man auch eine unsaubere Trennung zwischen technischer Frage von kritischen Komponenten und der entsprechenden Zertifizierung sowie der Vertrauenswürdigkeit von Herstellern. Das Parlament gebe der Bundesregierung klare Hinweise, anhand welcher Maßstäbe eine entsprechende und abgesenkte Prüfung, ab wann die Frage der Vertrauenswürdigkeit eines Herstellers beurteilt werden könne, vorgenommen werde. Zudem greife man die Kritik aus der Anhörung auf und regele das System der Einbeziehung verschiedener Ressorts in der Bundesregierung. Eine Evaluierung eines Gesetzes dürfe nicht darüber hinwegtäuschen, dass der Gesetzgeber auch unabhängig von Evaluierung stets tätig werden könne. Man implementiere eine Pflicht des BMI, dem Innenausschuss regelmäßig über den Stand der Cybersicherheit und die Fortentwicklung des Rechts zu berichten. Im parlamentarischen Verfahren habe man zahlreiche Kritikpunkte aufgenommen und dadurch das Gesetz in wesentlichen Teilen verbessert.

Die **Fraktion der AfD** macht deutlich, der Gesetzentwurf sei in der öffentlichen Anhörung selbst von Sachverständigen der Koalition inhaltlich zerrissen worden. Ein Sachverständiger habe sogar von einem „Unsicherheitsgesetz“ gesprochen. Dies sei ein bemerkenswerter Vorgang. Trotz mehrjähriger Beratungen sei schlussendlich nur ein zielloser Vorschlag ohne Strategie und ohne Einbindung von Wissenschaft und Zivilgesellschaft herausgekommen. Zudem bestünden verfassungsrechtliche Bedenken. Die AfD-Fraktion habe im parlamentarischen Verfahren zahlreiche Änderungsvorschläge unterbreitet. Dies unterscheide die Fraktion von den Grünen, die einen veralteten Antrag aus dem Jahr 2018 zur Abstimmung stellten. Besonders zu kritisieren sei die fehlende Evaluierung des IT-Sicherheitsgesetzes 1.0. Die Koalition unterlasse es, aus Erfahrungen zu lernen und zu analysieren, wo Verbesserungen und Anpassungen nötig seien. Das vorliegende Gesetz werde dem digitalen Verbraucherschutz in keinster Weise gerecht. Zudem treffe die Koalition keine politische Entscheidung darüber, ob staatsnahe

Netzwerkausrüster aus undemokratischen Ländern am Netzausbau der kritischen 5G-Infrastruktur beteiligt werden dürften. Diese Entscheidung fordere die AfD in ihren Änderungsanträgen. Zudem fordere man eine Definition kritischer Komponenten durch Verweis auf das TKG. Der Stand der Technik solle nicht nur vom BSI, sondern mit DIN, ISO, ETSI etc. entwickelt werden. Das BMI müsse kritische Komponenten bei nicht vertrauenswürdigen Herstellern untersagen. Eine Kann-Regelung reiche hier nicht. Zudem müsse das BSI zu einer starken Verbraucherschutzbehörde ausgebaut werden und solle Krisenreaktionspläne für IT-Katastrophen ausarbeiten. Es bedürfe zudem einer Konsolidierung der zahlreichen IT-Sicherheitsgesetze, da die gestiegene Komplexität die Sicherheit bedrohe. In eine bereits angestoßene Reform eines IT-Sicherheitsgesetzes 3.0 müssten frühzeitig und umfänglich alle interessierten Kreise einbezogen werden. Die Gestaltung des Ordnungsrahmens für die IT-Sicherheit müsse in Zukunft einem Bundesministerium für Digitalisierung und Cybersicherheit federführend übertragen werden.

Die **Fraktion der FDP** gesteht zu, der Entschließungsantrag der Koalition enthalte einige sinnvolle Regelungen. Diese hätte man jedoch unmittelbar als Änderungsantrag einbringen müssen. Zurecht seien Änderungen am ursprünglichen § 9b erfolgt. Insgesamt bleibe das IT-Sicherheitsgesetz Stückwerk, an dem wichtige Punkte fehlten, etwa die Steigerung der Cybersicherheit über die KRITIS-Infrastruktur hinaus. Insgesamt fehle ein agiles Verständnis von Cybersicherheit. Beim Thema Verschlüsselung und Offenlegung von Sicherheitslücken habe die Koalition gesetzlich nicht die richtigen Schlussfolgerungen gezogen, sondern gehe lediglich im Entschließungsantrag hierauf ein. Die Fraktion der FDP mache hierfür in ihren acht Änderungsanträgen entsprechende Vorschläge, auf die sie inhaltlich Bezug nehme. Der Vorschlag der Koalition, eine Evaluierung des IT-Sicherheitsgesetzes 2.0 vorzunehmen, sei angesichts der Tatsache, dass das IT-Sicherheitsgesetz 1.0 trotz gesetzlichem Auftrag noch nicht evaluiert sei, nicht ernst zu nehmen. Es gebe eine enorme inhaltliche Dissonanz zwischen dem Entschließungsantrag und dem zur Abstimmung gestellten Gesetzentwurf. Positiv hervorzuheben sei, dass die Kritik aus der öffentlichen Anhörung an § 9b aufgegriffen worden sei. Ob die nun getroffene Lösung ausreiche, sei jedoch zweifelhaft.

Die **Fraktion DIE LINKE.** weist darauf hin, der Sachverständige Manuel Atug der AG KRITIS habe in seiner Stellungnahme zur öffentlichen Anhörung darauf hingewiesen, dass durch diesen Gesetzentwurf eine eklatante Strategie- und Ziellosigkeit des Gesetzgebers im Cyberraum dokumentiert werde. Dieser Feststellung schließe man sich an. Teil einer sinnvollen und umsetzbaren Strategie bei der Stärkung der digitalen Sicherheit sei die enge Einbindung derjenigen, die tagtäglich daran arbeiteten – Wissenschaftler*innen, Netzaktivist*innen, Verbände und Unternehmen. Diese hätten unisono beklagt, nicht entsprechend einbezogen gewesen zu sein. Es sei unverantwortlich, in Zeiten des Fachkräftemangels in der IT-Sicherheit diesen Betroffenen derart vor den Kopf zu stoßen. Sinnvoll wäre es zudem, sich anzusehen, was mit den bisherigen Regeln des IT-Sicherheitsgesetzes erreicht worden sei, wo Defizite lägen und wo es Verbesserungsbedarf gebe. Hierfür müsste man ein Ziel definieren und dieses mittels Evaluation überprüfen. Das habe die Bundesregierung bislang versäumt und sich formal auf eine noch nicht abgelaufene Frist berufen. Jedoch sei es dem BMI unbenommen, vor einer weiteren Gesetzgebung bisherige Regelungen zu überprüfen. Eine solche Strategie müsse stringent und kohärent sein. Hieran mangele der Entwurf. Zwar würden Unternehmen eine Pflicht zur Meldung von Sicherheitslücken auferlegt, jedoch behalte sich der Staat vor, diese Sicherheitslücken öffentlich zu machen oder für andere Zwecke zu nutzen. Auch die Ausweitung der Verpflichtung für die Betreiber kritischer Infrastrukturen auf andere Unternehmen sei nicht stringent. Mit Unternehmen im besonderen öffentlichen Interesse werde eine Art „KRITIS light“ eingeführt, ohne dass den betroffenen Unternehmen vorher klar sei, ob sie schlussendlich hiervon umfasst seien. Dies sorge für weitere Unsicherheit. Auch beim Vorhaben eines IT-Sicherheitszertifikats fehle es an Stringenz. Ein solches Zertifikat gebe es bereits als EU-Richtlinie zu Cybersicherheitszertifikaten. Die Fraktion DIE LINKE. befürworte ausdrücklich eine europäische Lösung. In einem gemeinsamen Binnenmarkt mache alles andere keinen Sinn. Dass beide Zertifikate nur freiwillig seien, sei zu kritisieren. Es bedürfe eine obligatorische Zertifizierung. Es sei zudem unverständlich, dass die weit überwiegende Zahl der Wasserwerksbetreiber nicht unter die KRITIS-Verordnung fielen, da diese hierfür zu klein seien. Dies sei verantwortungslos. Aufgrund der vorgetragenen Kritikpunkte werde man das Gesetz ablehnen.

Die **Fraktion BÜNDNIS 90/DIE GRÜNEN** teilt die vorgetragenen Kritikpunkte der Fraktionen FDP und DIE LINKE. Bereits seit dem IT-Sicherheitsgesetz 1.0 bestehe enormer Nachbesserungsbedarf. Das IT-Sicherheitsgesetz 2.0 habe sich um Jahre verzögert. Stattdessen habe sich die Bundesregierung mit der Frage der Rolle von Huawei und dem 5G-Ausbau beschäftigt. Während alle Oppositionsfraktionen entsprechende Vorschläge unterbreitet hätten, sei von der Bundesregierung jahrelang nichts vorgelegt worden. Nun werde bereits vor Verabschiedung des vorliegenden Entwurfs über ein IT-Sicherheitsgesetz 3.0 debattiert. Die Zuständigkeiten innerhalb der

Bundesregierung im Bereich der IT-Sicherheit seien weiterhin unklar. Die IT-Sicherheitspolitik der Koalition gefährde die Grundrechte massiv. Es habe einhellige und breite Kritik an diesem Gesetzentwurf gegeben. Die öffentliche Anhörung habe ein verheerendes Zeugnis ausgestellt, selbst die Sachverständigen der Koalition hätten von einem „Unsicherheitsgesetz“ gesprochen. Hieran änderten auch die eingereichten Änderungsanträge nichts. Derweil gebe es weiterhin neue und massive Datenskandale durch Einflussnahme ausländischer Nachrichtendienste. Die Fraktion BÜNDNIS 90/DIE GRÜNEN habe bereits im Jahr 2018 entsprechende Vorschläge unterbreitet, die nicht aufgegriffen worden seien. Den Gesetzentwurf lehne man daher ab.

Berlin, den 21. April 2021

Christoph Bernstiel Berichterstatter	**Sebastian Hartmann** Berichterstatter	**Joana Cotar** Berichterstatterin
Manuel Höferlin Berichterstatter	**Petra Pau** Berichterstatterin	**Dr. Konstantin von Notz** Berichterstatter