19. April 2021

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)811

Änderungsantrag

der Fraktionen der CDU/CSU und der SPD

im Ausschuss für Inneres und Heimat des Deutschen Bundestages

zu dem von der Bundesregierung eingebrachten Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

– Drucksache 19/26106 –

Der Bundestag wolle beschließen,

den Gesetzentwurf auf Drucksache 19/26106 mit folgenden Maßgaben, im Übrigen unverändert, anzunehmen:

1. Artikel 1 wird wie folgt geändert:

   a) Der bisherigen Nummer 1 wird folgende Nummer 1 vorangestellt:

      ‚1. § 1 wird wie folgt gefasst:

      „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 wie folgt geändert:

      aa) Dem bisherigen Buchstaben a wird folgender Buchstabe a vorangestellt:

      ‚a) Absatz 2 wird wie folgt geändert:

      ‚aa) Es werden folgende Sätze 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) Im bisherigen Satz wird das Wort „Unversehrtheit“ durch das Wort „Integrität“ ersetzt.‘ ‘

      bb) Der bisherige Buchstabe a wird Buchstabe b.

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

aaa) In Absatz 13 Satz 1 wird nach dem Wort „IT-Produkte,“ 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 die Wörter „dieser IT-Produkte“ gestrichen.

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

aa) In Nummer 3 wird die Angabe „Satz 2" gestrichen.

bb) Dem bisherigen 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" 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 bisherigen Buchstaben b 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 der Angabe „Nummer 18" wird die Angabe „Satz 2" vorangestellt.

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

‚i) In 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 wie folgt geändert:

aa) § 4a Absatz 2 Satz 2 wird gestrichen.

bb) § 4a 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.“

cc) In § 4b Absatz 2 Satz 1 werden das Wort „kann“ durch das Wort „nimmt“ und das Wort „entgegennehmen“ durch das Wort „entgegen“ ersetzt.

dd) In § 4b Absatz 3 wird Nummer 2 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 geändert:

‚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 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 § 5c Absatz 1 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 Absatz 1a 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 wie folgt geändert:

aa) In § 7b Absatz 3 Satz 1 werden die Wörter „und stehen überwiegende Sicherheitsinteressen nicht entgegen“ gestrichen und nach dem Wort „Verantwortlichen“ das Wort „unverzüglich“ eingefügt.

bb) Nach § 7b Absatz 3 Satz 4 wird folgender Satz 5 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 in Buchstabe a wie folgt geändert:

aa) In § 8 Absatz 1 Satz 1 wird das Wort „Einvernehmen“ durch das Wort „Benehmen“ ersetzt.

bb) Dem § 8 Absatz 1 werden folgende 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.“

cc) In § 8 Absatz 1a werden die Sätze 5 bis 7 gestrichen.

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

aa) In Buchstabe b wird in § 8a Absatz 1a das Wort „zwölften“ durch die Angabe „24.“ ersetzt.

bb) Nach Buchstabe c wird folgender Buchstabe d eingefügt:

‚d) In Absatz 2 Satz 3 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 wie folgt gefasst:

‚16. § 8d wird wie folgt geändert:

a) In Absatz 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 der Empfehlung ist nicht anzuwenden.“

c) In § 8d Absatz 3 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 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 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, wen 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 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 Organisati-

onsstruktur, stammen. Satz 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 angegebenen 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 Nummer 1 bis 6 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 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 wie folgt geändert:

aa) In Buchstabe a wird in § 10 Absatz 3 die Angabe „§ 9a Absatz 1 Satz 1“ durch die Angabe „§ 9c“ ersetzt und es 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) In Buchstabe b werden die Wörter „Die folgenden Absätze 5 und 6 werden angefügt“ durch die Wörter „Folgender Absatz 5 wird angefügt“ ersetzt.

bbb) In § 10 Absatz 5 werden das Wort „Betreiber“ durch das Wort „Unternehmen“ ersetzt und am Ende folgende 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.“

ccc) § 10 Absatz 6 wird gestrichen.

r) Die bisherige Nummer 21 wird Nummer 22.

s) Nach der bisherigen Nummer 21 wird folgende Nummer 23 eingeführt:

‚23. § 13 wird wie folgt geändert:

a) Absatz 2 Satz 2 wird durch folgenden Satz 2 ersetzt:

„§ 7 Absatz 1a ist entsprechend anzuwenden.“

b) 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.“

c) 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:

‚d) 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) Der Nummer 3 wird folgende Nummer 4 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. 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 unterstützen.“ ‘

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

Begründung

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 öffentlichen 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).

Doppelbuchstaben ff bis ii

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)

Zu 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.

Zu 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)

Zu 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.

Zu 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)

Zu 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.

Zu 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.

Zu Doppelbuchstabe cc

Es handelt sich um eine Folgeänderung.

Zu Buchstabe m (§§ 8b bis c)

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)

Zu 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.

Zu 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 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.

Zu 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)

Zu 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.

Zu 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

Deutsches 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.