Bundesrat **Drucksache 16/21 (Beschluss)**

12.02.21

Stellungnahme
des Bundesrates

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

Der Bundesrat hat in seiner 1000. Sitzung am 12. Februar 2021 beschlossen, zu dem Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes wie folgt Stellung zu nehmen:

1. Zum Gesetzentwurf allgemein

   Der Bundesrat fordert den Bund auf, nicht nur die Kostenfolgen für die Bundesbehörden, sondern auch die der Landesverwaltung und insbesondere der Kommunen zu ermitteln.

   Begründung:

   Lediglich für die Bundesbehörden enthält die Gesetzesbegründung eine sehr differenziert gestaltete Darstellung der durch den Gesetzentwurf entstehenden Kosten. Für die Landesverwaltung und insbesondere die Kommunalverwaltungen und deren Zusammenschlüssen beispielsweise in Kommunalen Datenverarbeitungszentralen sind dagegen keine Kostenfolgen ermittelt worden.

   Für diese können sich jedoch aus den Anforderungen aus § 8a Absatz 1a und 3 Satz 1 BSIG-E und § 11 Absatz 1d und 1e EnWG-E Kosten durch Anforderungen des BSI sowie durch herzustellende Sicherheitsmaßnahmen ergeben.

Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0720-2946

juris Lex QS
20052024 ()

2. Zum Gesetzentwurf allgemein

a) Der Bundesrat begrüßt das mit dem IT-Sicherheitsgesetz 2.0 verfolgte Ziel, die IT-Sicherheit zum Schutze von Gesellschaft, Wirtschaft und Staat weiter zu erhöhen. Ein sicherer Cyberraum hat sich zu einer Grundbedingung für das gesellschaftliche und wirtschaftliche Zusammenleben entwickelt und ist daher von übergeordnetem Interesse.

b) Der Bundesrat fordert ein stärkeres gemeinsames Vorgehen von Bund und Ländern bei der Verbesserung der Abwehrfähigkeit im Bereich der Cybersicherheit durch eine engere Zusammenarbeit und Unterrichtungsverpflichtungen des Bundes gegenüber den Ländern, soweit der Aufgabenbereich des Bundes eröffnet ist, um die rasant wachsenden Herausforderungen im Cyberraum zu bewältigen.

c) Soweit die Neuregelungen, die auch auf eine Ausweitung des bestehenden Ordnungsrahmens im Bereich IT-Sicherheit abzielen, originäre Kompetenzen und Interessen der Länder berühren, insbesondere der Ermittlungs- und Sicherheitsbehörden im Bereich der digitalen Gefahrenabwehr sowie im Bereich der Datenschutzaufsicht über Telemedien, wird ein Nachbesserungsbedarf des IT-Sicherheitsgesetzes 2.0 gesehen.

3. Zum Gesetzesentwurf allgemein

Die unter die Vorgaben des BSIG fallenden Krankenhäuser und Universitätskliniken werden verpflichtet, zahlreiche Vorgaben an die IT-Sicherheit zu erfüllen. Es sind komplexe Anforderungen in den Bereichen Personal, Organisation und Betrieb umzusetzen. Nicht nur einmalige Installations- und Anschaffungskosten für Software sind zu berücksichtigen, sondern auch laufende Aufwendungen für Personal- als auch Sachkosten der Folgejahre. Diese Kosten werden über das Vergütungssystem der stationären Krankenversorgung nicht refinanziert.

Die Refinanzierung der in den betroffenen Krankenhäusern und Universitätskliniken entstehenden höheren Betriebskosten sollte durch die Einführung eines entsprechenden Zuschlags in § 5 Absatz 3 KHEntgG gesichert werden.

juris Lex QS
20052024 ()

4. Zu Artikel 1 Nummer 2 Buchstabe g (§ 3 Absatz 1 Satz 2 Nummer 20 BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob hinsichtlich der vom BSI künftig neu wahrzunehmenden Aufgabe, einen Stand der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte zu entwickeln, vorgesehen werden sollte, dass dabei eine enge Zusammenarbeit und Abstimmung mit den betroffenen Unternehmen oder ihren Verbänden zu erfolgen hat beziehungsweise diese entsprechend einzubeziehen sind.

Begründung:

Die Festlegung technischer Standards durch Fachgremien, an denen die Wirtschaft beteiligt ist, hat sich bewährt. Rein staatliche Festlegungen, wie der erweiterte Aufgabenkreis des BSI es vorliegend vorsieht, können mit der Geschwindigkeit des technischen Fortschritts nicht immer mithalten. Daher sollte geprüft werden, ob das BSI bei der Wahrnehmung seiner neuen Aufgaben die Expertise der Industrie einzuholen und zu berücksichtigen hat. Zu bedenken ist in diesem Zusammenhang ferner, dass eine nationale Festlegung des Stands der Technik sich als nicht sachgerecht erweisen könnte, da die relevanten IT-Produkte regelmäßig zumindest auch auf dem europäischen Binnenmarkt angeboten werden.

5. Zu Artikel 1 Nummer 3 (§ 4b Absatz 3 Nummer 5 – neu – BSIG)

In Artikel 1 Nummer 3 § 4b Absatz 3 Nummer 4 ist der Punkt am Ende durch ein Komma zu ersetzen und folgende Nummer anzufügen:

„5. Landesbehörden über die sie betreffenden Informationen zu unterrichten. Die Unterrichtung der Landesbehörden kann durch Weitergabe der entsprechenden Informationen an die von den Ländern nach Maßgabe des § 8b Absatz 2 Nummer 4 Buchstabe c benannte zentrale Kontaktstelle erfolgen.“

Begründung:

Die Aufnahme einer Informationspflicht soll sicherstellen, dass die im BSI an zentraler Stelle gesammelten Informationen über Sicherheitsrisiken in der Informationstechnik auch für die notwendige Arbeit der auf Landesebene zuständigen Stellen nutzbar gemacht werden können.

juris Lex QS
20052024 ()

6. Zu Artikel 1 Nummer 7 (§ 5c BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob und gegebenenfalls wie die dem BSI gemäß § 5c BSIG-E künftig zustehenden Auskunftsbefugnisse mit den bereits bestehenden Auskunftsrechten der Bundesnetzagentur nach dem Telekommunikationsgesetz harmonisiert werden könnten.

Begründung:

Der Gesetzentwurf lässt offen beziehungsweise nicht hinreichend erkennen, weshalb die nach dem TKG bereits bestehenden Auskunfts- und Meldepflichten von Telekommunikationsanbietern gegenüber der BNetzA nicht auch in Bezug auf die neuen Auskunftsbefugnisse des BSI genutzt werden könnten. Telekommunikations- und Telemediendiensteanbieter unterliegen bereits zahlreichen, zum Teil gleichgerichteten Auskunftspflichten gegenüber staatlichen Stellen. Auskunftspflichten gegenüber mehreren staatlichen Stellen mit gleichgerichteter Zielsetzung ziehen erhöhten Verwaltungsaufwand für die Unternehmen nach sich und erscheinen deshalb nicht erforderlich. Nach Möglichkeit sollte bestehenden Auskunftsrechten der Vorzug gegeben werden, um Dopplungen zu vermeiden. Zumindest sollte geprüft werden, ob die vorliegend vorgesehenen Pflichten der Telekommunikationsunternehmen und Telemediendiensteanbieter angesichts der bestehenden Auskunftsbefugnisse reduziert werden könnten, zum Beispiel, indem das BSI Daten über die BNetzA erhebt.

7. Zu Artikel 1 Nummer 7 (§ 5c Absatz 4 Satz 3 – neu – BSIG)

Dem Artikel 1 Nummer 7 § 5c Absatz 4 ist folgender Satz anzufügen:

„Die nach Landesrecht zuständigen Gefahrenabwehr-, Polizei- und Verfassungsschutzbehörden sowie die nach § 8b Absatz 2 Nummer 4 Buchstabe c benannte zentrale Kontaktstelle sind über betroffene Dritte und die ergriffenen Maßnahmen in ihrem Zuständigkeitsbereich unverzüglich zu unterrichten.“

Begründung:

Durch die Aufnahme einer Informationspflicht wird der Länderkompetenz für den Bereich der Gefahrenabwehr Rechnung getragen. Durch eine unverzügliche Information über betroffene Dritte und die ergriffenen Maßnahmen im Zuständigkeitsbereich eines Landes soll sichergestellt werden, dass die Koordination der nach Landesrecht zuständigen Gefahrenabwehr-, Polizei- und Verfassungsschutzbehörden sowie die Planung von Landesseite zu ergreifender Maßnahmen der Gefahrenabwehr in der erforderlichen Geschwindigkeit erfolgen kann.

juris Lex QS
20052024 ()

8. Zu Artikel 1 Nummer 7 (§ 5c Absatz 5 BSIG)

In Artikel 1 Nummer 7 § 5c Absatz 5 ist das Wort „kann“ durch das Wort „darf“ zu ersetzen.

Begründung:

Es handelt sich (auch ausweislich der Begründung) um eine Befugnisnorm für eine Datenverarbeitung. Rechtsförmlich ist dies in § 5c Absatz 5 BSIG-E mit der datenschutzrechtlich üblichen Formulierung „darf“ (vergleiche § 5a Satz 1 BSIG-E) zu regeln. Die bisherige Formulierung „kann“ impliziert hingegen Ermessen.

9. Zu Artikel 1 Nummer 10 (§ 7b Absatz 5 – neu – BSIG)

Dem Artikel 1 Nummer 10 § 7b ist folgender Absatz anzufügen:

„(5) Die nach Landesrecht zuständigen Gefahrenabwehr-, Polizei- und Verfassungsschutzbehörden sowie die nach § 8b Absatz 2 Nummer 4 Buchstabe c benannte zentrale Kontaktstelle sind über betroffene Dritte und die ergriffenen Maßnahmen in ihrem Zuständigkeitsbereich unverzüglich zu unterrichten.“

Begründung:

Der Ansatz, mithilfe staatlicher Instrumente zum Aufspüren von Sicherheitslücken und anderen Sicherheitsrisiken bei Einrichtungen des Bundes, KRITIS-Unternehmen, Digitalen Diensten und Unternehmen im besonderen öffentlichen Interesse einen Beitrag zur Erhöhung der Cybersicherheit zu leisten ist grundsätzlich zu unterstützen. Kritisch zu sehen ist allerdings, dass mit Blick auf die Aufgabenverteilung von Bund und Ländern im Bereich der Gefahrenabwehr mit der Übertragung dieser Befugnis auf eine Bundesbehörde die Sicherheitsinteressen der Länder berührt sein können. Durch die Aufnahme einer Informationspflicht wird der Länderkompetenz für den Bereich der Gefahrenabwehr Rechnung getragen. Durch eine unverzügliche Information über betroffene Dritte und die ergriffenen Maßnahmen im Zuständigkeitsbereich eines Landes soll sichergestellt werden, dass die Koordination der nach Landesrecht zuständigen Gefahrenabwehr-, Polizei- und Verfassungsschutzbehörden sowie die Planung von Landesseite zu ergreifender Maßnahmen der Gefahrenabwehr in der erforderlichen Geschwindigkeit erfolgen kann.

juris Lex QS
20052024 ()

10. Zu Artikel 1 Nummer 10 (§§ 7c, 7d BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob an Stelle der in den §§ 7c und 7d BSIG-E vorgesehenen neuen Anordnungsbefugnisse des BSI gegenüber Telekommunikations- und Telemediendiensteanbietern auf bestehende Anordnungsbefugnisse der BNetzA nach dem TKG zurückgegriffen werden könnte.

Begründung:

Der Gesetzentwurf lässt nicht hinreichend nachvollziehbar erkennen, weshalb es neuer Anordnungsbefugnisse zu Gunsten des BSI bedarf, anstatt die bereits bestehenden Befugnisse staatlicher Stellen wie zum Beispiel der BNetzA auch für das BSI nutzbar zu machen. Das bisherige Verfahren der Anordnungen durch die BNetzA hat sich bewährt, sollte beibehalten werden und auch in Bezug auf das BSI Anwendung finden. Der aktuell im Gesetzgebungsverfahren befindliche neue § 164 TKG (vergleiche BR-Drucksache 29/21) sieht Regelungen zu technischen und organisatorischen Schutzmaßnahmen durch Telekommunikationsanbieter vor und enthält bereits ein Anordnungsrecht der BNetzA und die Pflicht der BNetzA, das BSI über aufgedeckte Mängel zu informieren. Im Übrigen ist darauf hinzuweisen, dass die Anbieter mit ihren Systemen selbst am besten vertraut sind und ein großes Eigeninteresse daran haben, ihre IT-Sicherheit zu gewährleisten. Konkrete Hinweise auf Schwachstellen der IT durch das BSI sind deshalb wünschenswert. Die Beseitigung dieser Schwachstellen kann jedoch nur durch den Anbieter erfolgen, und behördliche Anordnungen sollten nur die ultima ratio sein.

11. Zu Artikel 1 Nummer 10 (§ 7d Satz 1 BSIG)

Artikel 1 Nummer 10 § 7d Satz 1 ist wie folgt zu fassen:

„Das Bundesamt kann zur Abwehr drohender Gefahren, die sich erheblich auf die Integrität oder den ordnungsgemäßen Betrieb informationstechnischer Systeme oder auf sonstige schutzwürdige Belange einer Vielzahl von Nutzern auswirken können, gegenüber Diensteanbietern im Sinne des § 2 Satz 1 Nummer 1 des Telemediengesetzes diejenigen Maßnahmen anordnen, die zur Erfüllung der Verpflichtungen nach § 13 Absatz 7 des Telemediengesetzes erforderlich sind.“

Begründung:

Mit der geänderten Formulierung der Anordnungsbefugnis soll eine klare und vollzugstaugliche Rechtsgrundlage geschaffen werden, um einen effektiven Schutz der Nutzer von Telemedien, insbesondere den Schutz von Verbrauchern im Online-Handel vor Cybersicherheitsrisiken, sicherzustellen. Dabei sollen

juris Lex QS
20052024 ()

dem BSI auch Anordnungsbefugnisse eingeräumt werden, wenn Sicherheitslücken zu Schädigungen einer Vielzahl von Personen genutzt werden können, ohne dass dabei die informationstechnischen Systeme der betroffenen Personen selbst gestört werden müssen. Dies kann beispielsweise der Fall sein bei Sicherheitslücken, die ein Ausspähen sensibler Gesundheitsdaten oder von Daten für Zahlungsdienste ermöglichen. Die im Gesetzentwurf enthaltenen zusätzlichen Vorgaben auf Tatbestands- und Rechtsfolgenseite bergen die Gefahr von Rechtsunsicherheit und sind aufgrund des ohnehin im Verwaltungsrecht zu beachtenden Verhältnismäßigkeitsgrundsatzes entbehrlich.

12. Zu Artikel 1 Nummer 12 Buchstabe b (§ 8a Absatz 1a Satz 1 BSIG)

In Artikel 1 Nummer 12 Buchstabe b § 8a Absatz 1a Satz 1 sind die Wörter „des zwölften“ durch die Wörter „des vierundzwanzigsten“ zu ersetzen.

Begründung:

Für die Umsetzung der Vorgaben des § 8a Absatz 1a BSIG-E (Vorhaltung von Systemen zur Angriffserkennung) werden bei komplexen und größeren Kritischen Infrastrukturen wie den Universitätskliniken mehr als zwölf Monate benötigt, zumal bei Gesetzesverstößen hohe Bußgelder drohen.

13. Zu Artikel 1 Nummer 12 Buchstabe c (§ 8a Absatz 2 Satz 2 Nummer 2 BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren eine Regelung zu prüfen, die bei der Einholung des Benehmens nach § 8a Absatz 2 Satz 2 Nummer 2 BSIG verhindert, dass eine Vielzahl von Landesbehörden vor der Entscheidung über die Eignung von branchenspezifischen Sicherheitsstandards beteiligt werden muss.

Begründung:

Die derzeit geltende Benehmensregelung in § 8a Absatz 2 Satz 2 Nummer 2 BSIG führt dazu, 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 völlig unpraktikabel, zumal die Aufsichtsbehörden auch nicht immer die erforderliche fachliche Kompetenz besitzen, um die Wechselwirkung zwischen informationstechnischen und sonstigen sicherheitsrelevanten Belangen beurteilen zu können. Eine Lösung könnte darin bestehen, ein zwingendes Benehmenserfordernis auf die fachlich zuständigen Behörden und Stellen des Bundes, in der Regel Bundesoberbehörden, sowie in Rechtsvorschriften verankerte bundesweit tätige Fachgremien zu beschränken. Ergänzend könnte als Sollvorschrift

juris Lex QS
20052024 ()

in geeigneten Fällen eine Einbeziehung der in ihrem Zuständigkeitsbereich berührten obersten Landesbehörden vorgesehen werden, sofern hierfür ein Bedarf gesehen wird.

14. Zu Artikel 1 Nummer 13 Buchstabe a Doppelbuchstabe bb (§ 8b Absatz 2 Nummer 4 Buchstabe c BSIG)

Artikel 1 Nummer 13 Buchstabe a Doppelbuchstabe bb ist wie folgt zu fassen:

‚bb) Nummer 4 wird wie folgt geändert:

aaa) Buchstabe a wird wie folgt gefasst:

„a) …< weiter wie Vorlage >…“

bbb) In Buchstabe c werden die Wörter „1 bis 3“ durch die Wörter „1 bis 3, insbesondere über Inhalte und Absender von Meldungen nach Absatz 4 mit möglichen Auswirkungen auf das jeweilige Land, dies gilt unabhängig davon, ob der Absender der Meldung der Aufsicht des Bundes oder des Landes untersteht,“ ersetzt.‘

Begründung:

Mit dieser Formulierung werden die in § 8b Absatz 2 Nummer 4 Buchstabe c BSIG vorgesehenen Informationspflichten konkretisiert. Eine Konkretisierung der Vorschrift ist geboten, um Informationsdefiziten auf Seiten der zuständigen Landesbehörden vorzubeugen.

15. Zu Artikel 1 Nummer 17 (§ 8f Absatz 7 Satz 3 – neu –, Absatz 8 Satz 3 – neu – BSIG)

Dem Artikel 1 Nummer 17 § 8f Absatz 7 und 8 ist jeweils folgender Satz anzufügen:

„Das Bundesamt hat die zuständigen Aufsichtsbehörden der Länder oder die nach § 8b Absatz 2 Nummer 4 Buchstabe c benannte Stelle über den Inhalt und den Absender von Meldungen nach Satz 1 mit möglichen Auswirkungen auf das jeweilige Land zu unterrichten, unabhängig davon, ob der Absender der Aufsicht des Bundes oder des Landes untersteht.“

juris Lex QS
20052024 ()

Begründung:

Gemäß § 8b Absatz 1 BSIG obliegt dem BSI die Aufgabe als zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik. Zur Wahrnehmung hat das BSI die Aufsichtsbehörden der Länder oder die von den Ländern benannte zentrale Kontaktstelle über die zur Erfüllung ihrer Aufgabe erforderlichen Informationen zu unterrichten. Diese Informationen sind für die Landesstellen von großer Bedeutung, um Informationsdefiziten vorzubeugen.

Zudem sind die Unternehmen von besonderem öffentlichen Interesse gem. § 8f Absatz 7 und 8 BSIG-E ebenfalls verpflichtet, Störungen dem Bundesamt zu melden. Der Wortlaut des § 8f BSIG-E spricht insoweit nicht von einer zentralen Meldestelle für Unternehmen von besonderem öffentlichem Interesse, sondern lediglich vom Bundesamt. Im Ergebnis kommt dem BSI jedoch auch für die Unternehmen nach § 2 Absatz 14 BSIG-E genau diese Funktion zu. Da den Unternehmen ebenso wie den KRITIS-Betreibern eine besondere Bedeutung zukommt, müssen die Länder ebenfalls über Störungen mit möglichen Auswirkungen auf das jeweilige Land unterrichtet werden, um einem Informationsdefizit vorzubeugen.

16. Zu Artikel 1 Nummer 19 (§ 9a Absatz 2 BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob dem BSI die Möglichkeit gegeben werden könnte, die Befugnis, die der Konformitätsbewertungsstelle nach § 9a Absatz 2 BSIG-E bei Erfüllung der gesetzlichen Voraussetzungen zu erteilen ist, mit Nebenbestimmungen zu versehen.

Begründung:

In der Praxis der Zulassung von Konformitätsbewertungsstellen hat sich gezeigt, dass Nebenbestimmungen zur Befugniserteilung eine wichtige Voraussetzung für eine wirksame Aufsicht darstellen. Eine Beschränkung der aufsichtlichen Möglichkeiten auf den Widerruf der Befugnis kann zu erheblichen Vollzugsproblemen führen, da bei Pflichtverstößen der Widerruf wegen der Intensität des Eingriffs oftmals unverhältnismäßig wäre, aber weder Anordnungsbefugnisse noch verwaltungsrechtliche Zwangsmittel auf Grundlage beispielsweise von Auflagen zur Verfügung stehen.

17. Zu Artikel 1 Nummer 19 (§ 9a Absatz 7 BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob dem BSI die Möglichkeit gegeben werden könnte, neben dem Widerruf der Befugnis nach § 9a Absatz 7 BSIG-E auch mit verwaltungsrechtlichen Anordnungen auf die Einhaltung der Zulassungsvoraussetzungen und Pflichten von Konformitätsbewertungsstellen hinwirken zu können.

juris Lex QS
20052024 ()

Begründung:

In der Praxis der Zulassung von Konformitätsbewertungsstellen hat sich gezeigt, dass Anordnungsbefugnisse eine wichtige Voraussetzung für eine wirksame Aufsicht darstellen. Eine Beschränkung der aufsichtlichen Möglichkeiten auf den Widerruf der Befugnis kann zu erheblichen Vollzugsproblemen führen, da bei Pflichtverstößen der Widerruf wegen der Intensität des Eingriffs oftmals unverhältnismäßig wäre und daneben keine aufsichtlichen Handlungsmöglichkeiten zur Verfügung stehen.

18. Zu Artikel 1 Nummer 19 (§ 9c BSIG)

a) Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren klarzustellen, in welchem Verhältnis die IT-Sicherheitskennzeichnung nach § 9c BSIG-E zur Cybersicherheitszertifizierung auf Grundlage der Verordnung (EU) 2019/881 steht und eine Mehrfachkennzeichnung von Verbraucherprodukten zum Aspekt der Cybersicherheit zu vermeiden.

b) Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren die Aufnahme materieller Vorgaben für die Verwendung des IT-Sicherheitskennzeichens in die gesetzliche Regelung des § 9c BSIG-E zu prüfen, um Klarheit darüber zu geben, welche Voraussetzungen für die Verwendung des IT-Sicherheitskennzeichens zu erfüllen sind und welche Aussage das IT-Sicherheitskennzeichen über das Cybersicherheitsniveau trifft.

c) Der Bundesrat bittet außerdem, im weiteren Gesetzgebungsverfahren zu prüfen, ob zur Stärkung der Bedeutung des IT-Sicherheitskennzeichens und zur Vermeidung einer Häufung von Siegeln der Aspekt des Datenschutzes einbezogen werden könnte.

Begründung:

Zu Buchstabe a:

Das Verhältnis zwischen der IT-Sicherheitskennzeichnung gem. § 9c BSIG-E und der Cybersicherheitszertifizierung auf Grundlage der Verordnung (EU) 2019/881 über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik ist unklar. Eine Mehrfachkennzeichnung ist aus Gründen der Verständlichkeit und Klarheit für den Verbraucher zu vermeiden.

Zu Buchstabe b:

Es besteht die Gefahr, dass aufgrund der Ausgestaltung der gesetzlichen Vorgaben in § 9c BSIG-E das IT-Sicherheitskennzeichen nur bedingt Gewähr für ein hohes Maß an Cybersicherheit bieten kann. Im Vergleich mit der Verordnung (EU) 2019/881 über die Zertifizierung der Cybersicherheit von Informa-

juris Lex QS
20052024 ()

tions- und Kommunikationstechnik fällt auf, dass, anders als dort in Artikel 51 geregelt, keine klaren Sicherheitsziele formuliert sind. Auch wenn das Bundesamt die Möglichkeit erhält, Technische Richtlinien zu erlassen, sollten die wesentlichen materiellen Vorgaben bereits im Gesetz selbst angelegt sein. Dies gilt umso mehr, als die Verwendung des IT-Sicherheitskennzeichens im Wesentlichen auf der Herstellererklärung beruht, die aber für sich genommen noch nichts über die tatsächliche IT-Sicherheit aussagt.

Zu Buchstabe c:

Es wäre wünschenswert, wenn die Verwendung des IT-Sicherheitskennzeichens die Einhaltung wesentlicher Grundsätze der DSGVO voraussetzte. Es wäre dem Verbraucher kaum zu vermitteln, wenn beispielsweise eine Gesundheits-App aufgrund einer sicheren Datenübermittlung ein IT-Sicherheitskennzeichen führen und damit beworben werden dürfte, jedoch bei der technischen Gestaltung der App weder eine informierte Einwilligung in die Datennutzung vorgesehen ist noch eine effektive, leicht auffindbare Möglichkeit des Widerrufs der datenschutzrechtlichen Einwilligung besteht.

19. Zu Artikel 1 Nummer 20 Buchstabe b (§ 10 Absatz 5 BSIG)

In Artikel 1 Nummer 20 Buchstabe b § 10 Absatz 5 ist das Wort „nicht“ zu streichen.

Begründung:

Mit dieser Formulierung werden föderale Aspekte sowie das grundgesetzliche Kompetenzgefüge bei der Bestimmung von Unternehmen im besonderen öffentlichen Interesse berücksichtigt.

20. Zu Artikel 1 Nummer 22 (§ 14 Absatz 5 Satz 3 BSIG)

Artikel 1 Nummer 22 § 14 Absatz 5 Satz 3 ist zu streichen.

Begründung:

Die Erhöhung der Bußgelder von derzeit 100 000 Euro auf bis zu 2 Millionen Euro (beziehungsweise auf 20 Millionen Euro gemäß § 30 Absatz 1 OWiG) ist für Krankenhäuser und Universitätskliniken unverhältnismäßig und nicht tragbar.

juris Lex QS
20052024 ()

21. Zu Artikel 2 allgemein

a) Der Bundesrat begrüßt, dass die Bundesregierung angesichts der perspektivisch stetig zunehmenden Gefahrenlage im Bereich der Cybersicherheit und der stetig anwachsenden Komplexität der technologischen Herausforderungen, auch durch die zunehmende Softwarebasierung von Netzfunktionen in modernen Telekommunikationsnetzen, mit dem vorliegenden Gesetzentwurf ein ausdifferenziertes Wirkgefüge zur vorsorglichen und akuten Gefahrenabwehr vorgelegt hat.

b) Der Bundesrat sieht dabei die Notwendigkeit, dass dieses Zusammenwirken, insbesondere mit dem Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0), und der daraus folgenden Ausdifferenzierung behördlicher Zuständigkeiten nicht zu Lasten der fachbehördlichen Zuständigkeiten der Bundesnetzagentur gehen darf.

c) Der Bundesrat sieht mit einer gewissen Sorge, dass das ausdifferenzierte Wirkgefüge insbesondere des § 164 TKG-E aufgrund der strukturell notwendigen Entwicklungsoffenheit vor allem für die betroffenen Unternehmen beträchtliche Herausforderungen mit sich bringen kann. In diesem Kontext weist der Bundesrat auf den Bedarf einer mittelfristigen Evaluierung der zusammenwirkenden gesetzlichen Regelungen hin.

Begründung:

Die anwachsenden Gefahren im Bereich der Cybersicherheit stellen auch angesichts der allgemeinen technologischen Entwicklungsdynamik für die Telekommunikationsunternehmen eine große Herausforderung dar. Der von der Bundesregierung vorgelegte Entwurf des Telekommunikationsmodernisierungsgesetzes setzt diese Herausforderung im Zusammenwirken mit dem Entwurf für ein IT-Sicherheitsgesetz 2.0 in eine komplexe gesetzliche Regelung um. Auch aufgrund der Abstimmungsbedarfe auf europäischer Ebene zur Zertifizierung kritischer Komponenten unterliegen die resultierenden Maßnahmen einer besonderen Komplexität. In diesem Kontext erscheinen klare fachbehördliche Zuständigkeiten wie auch eine mittelfristige Evaluierung der Angemessenheit und Ausbalancierung der gesetzlichen Regelungen für die betroffenen TK-Unternehmen bedeutsam, um auch im Lichte dieser Herausforderungen Innovationen und Investitionen langfristig in Deutschland zu befördern.

juris Lex QS
20052024 ()

22. Zu Artikel 2 Nummer 2 Buchstabe b Doppelbuchstabe bb (§ 109 Absatz 2 Satz 3a TKG)

Artikel 2 Nummer 2 Buchstabe b Doppelbuchstabe bb Satz 3a ist wie folgt zu fassen:

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

Begründung:

Aus Gründen des Verwaltungsaufwandes und der Beschleunigung von Investitionen sollten die Überprüfung und die Zertifizierung der kritischen Komponenten weder in zwei voneinander getrennten Arbeitsschritten noch von zwei unterschiedlichen Institutionen erfolgen. Ferner sollte dabei aus Gründen des Investitionsschutzes eine Klarstellung erfolgen, dass eine Betriebserlaubnis für die Verwendung von kritischen Komponenten nur für einen in der Zukunft liegenden Zeitpunkt erteilt werden kann. Zudem ist sicherzustellen, dass die Wirtschaft, gerade kleine und mittlere Unternehmen, durch die beabsichtigten Änderungen insbesondere durch Zertifizierungsanforderungen nicht unverhältnismäßig belastet werden. Eine pauschale Verpflichtung von Unternehmen allein auf Grundlage der Nutzung kritischer Komponenten wie im vorliegenden Entwurf absehbar, ist abzulehnen.

Eine pauschale Verpflichtung zur Zertifizierung von Free-and-Open-Source-Software sowie eigenentwickelter Software im Bereich der Telekommunikation würde zu einem nachhaltigen Verlust von Innovationskraft führen, den Wettbewerb zum Nachteil kleinerer Anbieter erheblich beeinflussen und die Innovation stark beeinträchtigen.

Der Änderungsvorschlag beinhaltet insofern eine Klarstellung, dass sich diese Verpflichtung nur auf Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial beziehen soll und nicht wie im Gesetzentwurf bislang vorgesehen pauschal auf kritische Komponenten im Sinne des § 2 Absatz 13 BSIG. 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.

juris Lex QS
20052024 ()

23. Zu Artikel 2 Nummer 2 Buchstabe e Doppelbuchstabe aa (§ 109 Absatz 6 Satz 1 TKG)

In Artikel 2 Nummer 2 Buchstabe e Doppelbuchstabe aa §109 Absatz 6 Satz 1 sind die Wörter „Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten“ durch das Wort „Telekommunikationssystemen“ zu ersetzen.

Begründung:

Mit § 109 Absatz 6 TKG-E soll laut der Einzelbegründung die Richtlinie (EU) 2018/1972 umgesetzt werden. Artikel 1 Absatz 3 und 4 der Richtlinie stellt klar, dass die Richtlinie Datenschutzregelungen unberührt lässt. Außerdem sollen Maßnahmen, die von den Mitgliedstaaten für Zwecke der öffentlichen Ordnung und der öffentlichen Sicherheit ergriffen werden, unberührt bleiben. Insbesondere enthält die Richtlinie Sicherheitsvorgaben für die elektronische Kommunikation (vergleiche insbesondere Artikel 40 dieser Richtlinie), Telemedienanbieter können von den Vorgaben der Richtlinie insbesondere betroffen sein, wenn Auswirkungen von Sicherheitsvorfällen auf die elektronische Kommunikation zu befürchten sind.

Der aktuell vorliegende Gesetzentwurf würde dazu führen, dass einem Großteil der Telemedien durch die BNetzA im Einvernehmen mit dem BSI und der oder dem BfDI Vorgaben für die Verarbeitung personenbezogener Daten gemacht werden könnten, unabhängig davon, ob diese erforderlich sind, um Auswirkungen auf die elektronische Kommunikation zu vermeiden, und ohne dass eine Ausnahme für Zwecke der öffentlichen Ordnung und der öffentlichen Sicherheit (insbesondere für Polizeibehörden) vorgesehen wäre.

Für die Aufsicht über die Datenverarbeitung auf Telemedien sind zudem bisher nicht der BfDI, sondern ausschließlich die Landesdatenschutzaufsichtsbehörden zuständig. Die Regelung von Teilzuständigkeiten des BfDI würde ohne sachliche Notwendigkeit zu einer überschneidenden Kompetenzverteilung von Bundes- und Landesdatenschutzaufsichtsbehörden führen, was in der Praxis zu erheblichen Abgrenzungs- und Abstimmungsschwierigkeiten führen dürfte. Außerdem würden dadurch sogar Aufsichtszuständigkeiten der Bundesaufsichtsbehörde über öffentliche Stellen der Länder, welche Telemedien als Zugangsmöglichkeiten zur Öffentlichkeit nutzen, entstehen. Dies wäre insbesondere bei Polizeibehörden sowie den Parlamenten der Länder nicht zuletzt verfassungsrechtlich problematisch.

Außerdem ist aktuell ein eigener Gesetzentwurf der Bundesregierung in der Länderanhörung, der gerade den Zweck haben soll, alle Datenschutzregelungen einschließlich von Regelungen zur Datenschutzaufsicht zu Telekommunikations- und Telemediendiensten in einem eigenen Gesetz (Telekommunikations-Telemedien-Datenschutzgesetz) zu regeln, weshalb Regelungen im vorliegenden Gesetzentwurf entbehrlich sind. Die im Gesetzentwurf vorgesehen Regelungen wären im Telekommunikationsgesetz darüber hinaus fehl am Platz, weil

juris Lex QS
20052024 ()

es sich um Regelungen für Telemedien handelt; für diese besteht weiterhin parallel zum Telekommunikationsgesetz ein Telemediengesetz, welches bei Bedarf ergänzt werden könnte.

juris Lex QS
20052024 ()