Deutscher Bundestag **Drucksache 18/11620**

18. Wahlperiode (zu Drucksache 18/11242)
22.03.2017

Unterrichtung

durch die Bundesregierung

Entwurf eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union

– Drucksache 18/11242 –

Stellungnahme des Bundesrates und Gegenäußerung der Bundesregierung

Stellungnahme des Bundesrates

Der Bundesrat hat in seiner 954. Sitzung am 10. März 2017 beschlossen, zu dem Gesetzentwurf gemäß Artikel 76 Absatz 2 des Grundgesetzes wie folgt Stellung zu nehmen:

1. Zu Artikel 1 Nummer 2 Buchstabe b – neu – (§ 3 Absatz 4 – neu – BSIG)

   In Artikel 1 ist Nummer 2 wie folgt zu fassen:

   ‚2. § 3 wird wie folgt geändert:

   a) Absatz 1 Satz 2 wird wie folgt geändert:

   aa) In Nummer 13 Buchstabe b werden nach dem Wort „Verfassungsschutzbehörden“ die Wörter „und des militärischen Abschirmdienstes“ und nach den Wörtern „der Länder“ die Wörter „beziehungsweise dem Gesetz über den militärischen Abschirmdienst“ eingefügt.

   bb) …<weiter wie Gesetzentwurf zu Artikel 1 Nummer 2 Buchstabe b>

   cc) In Nummer 17 wird die Angabe „und 8b“ durch die Angabe „bis 8c“ und der Punkt am Ende durch die Wörter „und digitaler Dienste;“ ersetzt.

   dd) …<weiter wie Gesetzentwurf zu Artikel 1 Nummer 2 Buchstabe d>

   b) Folgender Absatz wird angefügt:

   „(4) Das Bundesamt kann ersuchenden Dritten qualifizierte Sicherheitsdienstleister für die Bewältigung eines IT-Sicherheitsvorfalls benennen.“ ‘

   Begründung:

   Gemäß § 5a Absatz 5 Satz 3 BSIG-E kann das Bundesamt für Sicherheit in der Informationstechnik – statt selbst tätig zu werden – die ersuchende Stelle auf qualifizierte Dritte verweisen.

Es sollte klargestellt werden, dass auch andere Einrichtungen als die in § 5a BSIG-E genannten eine Auswahl von geeigneten Dienstleistern oder qualifizierten Dritten zur Lösung von Sicherheitsproblemen genannt bekommen können.

2. Zu Artikel 1 Nummer 4 (§ 5a Absatz 3 Satz 6 BSIG)

In Artikel 1 Nummer 4 § 5a Absatz 3 Satz 6 sind nach dem Wort „Bundesdatenschutzgesetzes“ die Wörter „und der landesdatenschutzrechtlichen Vorschriften“ einzufügen.

Begründung:

Einrichtungen der Landesverwaltungen, sofern sie Betreiber einer kritischen Infrastruktur im Sinne des Gesetzentwurfs sind, unterfallen § 5a BSIG-E. Deswegen sind auch die landesdatenschutzrechtlichen Vorschriften zu erwähnen.

3. Zu Artikel 1 Nummer 4 (§ 5a Absatz 7 Satz 2 – neu – BSIG-E)

In Artikel 1 Nummer 4 ist dem § 5a Absatz 7 folgender Satz anzufügen:

„Die Absätze 3 bis 6 finden in diesen Fällen entsprechende Anwendung.“

Begründung:

Es erscheint nicht ausgeschlossen, dass Einrichtungen der Landesverwaltung, die nicht bereits unter § 5a Absatz 1 BSIG-E fallen, unter die Ausnahmeregelung des § 5a Absatz 7 BSIG-E subsumiert werden können. In § 5a Absatz 7 BSIG-E sollte daher klarstellend festgeschrieben werden, dass auf diese Fälle § 5a Absatz 3 bis 6 BSIG-E entsprechend anzuwenden ist.

4. Zu Artikel 1 Nummer 6 Buchstabe a Doppelbuchstabe bb (§ 8a Absatz 3 Satz 4, 5 BSIG), Buchstabe b (§ 8a Absatz 4 BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob die Ausübung der Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik zur Vorlage von Dokumentationen und zur Durchführung von Überprüfungen von zusätzlichen einschränkenden Voraussetzungen abhängig gemacht werden sollte. Der Bundesrat bittet ferner um Prüfung, ob die Anforderungen an die Einschaltung eines qualifizierten unabhängigen Dritten präzisiert werden sollten.

Begründung:

§ 8a Absatz 3 Satz 4 und 5 und Absatz 4 BSIG-E räumt dem Bundesamt für Sicherheit in der Informationstechnik Ermessen bei der Ausübung seiner Befugnisse zur Vorlage von Dokumentationen und zur Durchführung von Überprüfungen ein, ohne dass dieses Ermessen an bestimmte Voraussetzungen geknüpft ist. Diese anlasslosen Überprüfungen widersprechen dem bisherigen kooperativen Ansatz, wonach sich Betreiber von kritischen Infrastrukturen in eigener Verantwortung nach dokumentierten Standards selbst schützen. Es sollte daher geprüft werden, ob die Ausübung der neuen Befugnisse von zusätzlichen einschränkenden Voraussetzungen abhängig gemacht werden sollte. Zur Wahrung der Geschäfts- und Firmengeheimnisse der Betreiber erscheint es zudem erforderlich zu prüfen, ob die Anforderungen an die Einschaltung eines qualifizierten unabhängigen Dritten präzisiert werden sollten, um der Gefahr zu begegnen, dass ein Mitbewerber des Betreibers zur Überprüfung herangezogen wird.

5. Zu Artikel 1 Nummer 8 (§ 8c BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahrens zu prüfen, ob es Überschneidungen zwischen den Pflichten von Anbietern digitaler Dienste gemäß § 8c BSIG-E und von Diensteanbietern gemäß § 13 Absatz 7 TMG gibt, und gegebenenfalls eine klarstellende Regelung zu treffen.

Begründung:

Sowohl § 8c BSIG-E als auch § 13 Absatz 7 TMG statuieren Pflichten für „Anbieter digitaler Dienste“ sowie für „Diensteanbieter“. Beide Vorschriften ähneln sich nicht nur in Bezug auf die Begrifflichkeit,

sondern auch in Bezug auf die darin geregelten Anforderungen, etwa die Pflicht zur Ergreifung geeigneter und verhältnismäßiger technischer und organisatorischer Maßnahmen (§ 8c Absatz 1 Satz 1 BSIG-E) und zum Schutz der geschäftsmäßig angebotenen Telemedien durch technische und organisatorische Vorkehrungen (§ 13 Absatz 7 TMG). Das Verhältnis der Regelungen zueinander sollte daher im weiteren Gesetzgebungsverfahren klargestellt werden.

6. Zu Artikel 1 Nummer 9 Buchstabe c Doppelbuchstabe bb (§ 8d Absatz 3 BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob eine Regelung gefunden werden kann, die es ermöglicht, dass Unternehmen, die bereits auf Grund spezialgesetzlicher Normen eine Kontaktstelle benannt haben, von der durch § 8d Absatz 3 BSIG-E bewirkten Ausweitung der Verpflichtung zur Benennung einer Kontaktstelle ausgenommen werden können.

Begründung:

Bisher müssen keine Kontaktstellen von den in § 8d Absatz 3 BSIG-E genannten Betreibern benannt werden. Mit der vorgesehenen Änderung wird die Verpflichtung zur Benennung einer Kontaktstelle in § 8b Absatz 3 BSIG aus europarechtlichen Gründen hingegen auf diese Betreiber ausgedehnt. Da die betroffenen Unternehmen auf Grund spezialgesetzlicher Normen zumeist bereits Kontaktstellen unterhalten, etwa zur Bundesnetzagentur, sollte zur Vermeidung von Doppelregulierungen und Doppelzuständigkeiten im Interesse der Rechtssicherheit geprüft werden, ob von einer Ausdehnung der Kontaktstellenpflicht Abstand genommen werden kann.

7. Zu Artikel 1 Nummer 9 Buchstabe d (§ 8d Absatz 4 Satz 3 BSIG)

Der Bundesrat bittet, im weiteren Gesetzgebungsverfahren zu prüfen, ob eine Regelung gefunden werden kann, die klarstellt, dass Anbieter gemäß § 8d Absatz 4 Satz 3 BSIG-E, die in der Bundesrepublik Deutschland Netz- und Informationsdienste betreiben, die sie zur Bereitstellung der Dienste innerhalb der Europäischen Union nutzen, nicht gegenüber mehreren Behörden berichtspflichtig sind.

Begründung:

Die Formulierung des § 8d Absatz 4 Satz 3 BSIG-E erscheint unklar. Danach soll § 8c Absatz 4 BSIG-E auch dann gelten, wenn Anbieter mit Hauptsitz in einem anderen Mitgliedstaat der Europäischen Union „in der Bundesrepublik Deutschland Netz- und Informationssysteme betreiben, die sie im Rahmen der Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen“. Dies begegnet Bedenken, da das in der umzusetzenden Richtlinie (EU) 2016/1148 angelegte Sitzlandprinzip bei zu weitgehender Auslegung des § 8d Absatz 4 Satz 3 BSIG-E untergraben würde mit der Folge, dass die betroffenen Anbieter gegenüber mehreren Behörden berichtspflichtig wären. Der hierdurch entstehenden Rechtsunsicherheit für die Betreiber sollte durch eine entsprechende Klärung vorgebeugt werden.

8. Zu Artikel 2 Nummer 2 (§ 44b Satz 4 AtG)

In Artikel 2 ist Nummer 2 wie folgt zu fassen:

‚2. Satz 4 wird wie folgt gefasst:

„Das Bundesamt für Sicherheit in der Informationstechnik leitet diese Meldung unverzüglich an die zuständige Aufsichtsbehörde weiter.“ ‘

Begründung:

Bei einer Störung der nuklearen Sicherheit handelt es sich gerade unter dem Aspekt einer zeitnahen behördlichen Kenntnisnahme und Bewertung um eine reine Aufsichtsfrage und nicht um eine Genehmigungsfrage. Die Genehmigungsinhaber nach §§ 6, 7 und 9 AtG unterliegen der Aufsicht der Länder. Es ist auch allein Sache der Aufsichtsbehörden, die Sachverständigen nach § 20 AtG einzuschalten.

§ 44b AtG und §§ 8a ff. BSIG verfolgen im Schwerpunkt unterschiedliche Ziele. Bei den §§ 8a ff. BSIG geht es um die Sicherheit der Informationstechnik kritischer Infrastrukturen. Die in diesem Zusammenhang vorgesehenen Meldungen an das BSI dienen der Versorgungssicherheit in den Sektoren Energie,

Wasser, Ernährung und Telekommunikation. Von den Meldepflichten nach § 8b BSIG sind Kernkraftwerke und sonstige Energieanlagen ausgenommen (§ 8c Absatz 3 Nummer 2 und 3 BSIG). Für Energieanlagen, die durch die BSI-Kritisverordnung als kritische Infrastruktur bestimmt worden sind, gilt jedoch dieselbe Meldepflicht nach § 11 Absatz 1c EnWG. Da es sich bei Kernkraftwerken nach der Definition der BSI-Kritisverordnung um kritische Infrastrukturen handelt, unterfallen sie in den Fällen, in denen die Störung der IT zu einer Beeinträchtigung der Funktionsfähigkeit der Anlage geführt hat oder hätte führen können, ohnehin der Meldepflicht an das BSI.

Gegenäußerung der Bundesregierung

Die Bundesregierung äußert sich zur Stellungnahme des Bundesrates wie folgt:

Zu Nummer 1

Die Bundesregierung lehnt den Vorschlag ab.

Die Aufgabe des BSI zur „Beratung und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen“ ist bereits in § 3 Absatz 1 Nummer 14 BSIG beschrieben.

Zu Nummer 2

Die Bundesregierung lehnt den Vorschlag ab.

Das BSI ist eine Bundesbehörde, für deren Tätigkeit das Bundesrecht gilt. Darauf, dass für die Einrichtungen der Landesverwaltung die Regelungen des Landesdatenschutzrechts gelten, kommt es daher nicht an.

Zu Nummer 3

Die Bundesregierung lehnt den Vorschlag ab.

Die Ergänzung ist nicht erforderlich. Die Absätze 3 bis 6 kommen in den Fällen des Absatzes 7 nach dem Gesetzentwurf bereits unmittelbar zur Anwendung.

Zu Nummer 4

Die Bundesregierung hat auf Bitte des Bundesrats geprüft, ob die Ausübung der Befugnisse des BSI von zusätzlichen einschränkenden Voraussetzungen abhängig gemacht und die Anforderungen an die Einschaltung qualifizierter Dritter präzisiert werden sollten. Die Prüfung hat zu dem Ergebnis geführt, dass die in dem Gesetzesentwurf vorgesehenen Aufsichtsbefugnisse des BSI nicht weiter eingeschränkt werden sollten.

Mit den vorgesehenen Änderungen werden die Mindestvorgaben in Artikel 15 Absätze 1 und 2 der NIS-Richtlinie umgesetzt, nach denen die NIS-Behörde die Möglichkeit zu einer umfassenden Aufsicht und Kontrolle unabhängig von dem tatsächlichen Vorliegen von Fehlern oder Verstößen haben muss. Die neuen § 8a Absätze 3 und 4 BSIG – neu – ermöglichen im Zusammenspiel ein ausgewogenes und adressatengerechtes Vorgehen bei der Aufsicht.

Qualifizierte Dritte, die im Auftrag des BSI tätig werden, unterliegen bereits nach den geltenden Vorschriften denselben Vertraulichkeits- und Unabhängigkeitsanforderungen wie das BSI. Explizite Regelungen zur Wahrung von Geschäfts- und Firmengeheimnissen der Betreiber sind bisher nicht im BSIG vorgesehen. Insofern soll auch für den Einzelfall der Einschaltung qualifizierter Dritter nach § 8a BSIG – neu – keine Ausnahme geschaffen werden.

Zu Nummer 5

Die Bundesregierung hat auf Bitte des Bundesrates geprüft, ob es Überschneidungen zwischen den Pflichten von Anbietern digitaler Dienste gemäß § 8c BSIG – neu –und von Diensteanbietern gemäß § 13 Absatz 7 TMG gibt und eine klarstellende Regelung zu treffen ist. Die Prüfung hat zu dem Ergebnis geführt, dass eine weitere Abgrenzung der Vorschriften nicht vorgenommen werden sollte.

Die in Umsetzung von Artikel 16 NIS-RL in § 8c BSIG– neu – spezifisch vorgesehenen Pflichten beziehen sich auf Vorgaben zur Gewährleistung der Verfügbarkeit der digitalen Dienste. Demgegenüber verfolgen die Vorgaben in § 13 Absatz 7 TMG mit der Gewährleistung der informationellen Selbstbestimmung sowie der Vertraulichkeit und Integrität informationstechnischer Systeme der Nutzer eine andere Zielsetzung. Soweit unabhängig hiervon im Einzelfall nicht ausgeschlossen sein sollte, dass bestimmte, von Anbietern digitaler Dienste vorgenommene Schutzmaßnahmen gleichzeitig Anforderungen beider Vorschriften erfüllen, wird hierin keine Benachteiligung der Diensteanbieter gesehen.

Zu Nummer 6

Die Bundesregierung hat auf Bitte des Bundesrates geprüft, inwieweit Unternehmen, die bereits auf Grund spezialgesetzlicher Normen eine Kontaktstelle benannt haben, von der vorgesehenen Ausweitung der Verpflichtung zur Benennung einer Kontaktstelle ausgenommen werden können.

Die Prüfung hat zu dem Ergebnis geführt, dass von einer Ausdehnung der Kontaktstellenpflicht nicht Abstand genommen werden kann.

Der Bundesregierung sind vergleichbare spezialgesetzliche Pflichten nicht bekannt.

Zu Nummer 7

Die Bundesregierung hat auf Bitte des Bundesrates geprüft, ob eine Regelung gefunden werden kann, die klarstellt, dass Anbieter gemäß § 8d Absatz 4 Satz 2 – neu – des BSI-Gesetzes, die in der Bundesrepublik Deutschland Netz- und Informationsdienste betreiben, die sie zur Bereitstellung der Dienste innerhalb der Europäischen Union nutzen, nicht gegenüber mehreren Behörden berichtspflichtig sind.

Die Prüfung hat zu dem Ergebnis geführt, dass der Bitte zu einer Einengung der Voraussetzungen, nach dem Anbieter digitaler Dienste einer Berichtspflicht unterliegen, nicht entsprochen werden kann.

Die Vorgaben der NIS-Richtlinie zur Anwendbarkeit auf digitale Dienste gehen über das Sitzlandprinzip hinaus und sehen explizit vor, dass Anbieter digitaler Dienste Maßnahmen mehrerer Behörden unterliegen können. Dies gilt nach Artikel 17 Absatz 3 NIS-Richtlinie auch dann, wenn ein Anbieter digitaler Dienste seine Hauptniederlassung oder einen Vertreter in einem Mitgliedstaat hat, aber sich seine Netz- und Informationssysteme in einem oder mehreren anderen Mitgliedstaaten befinden.

Zu Nummer 8

Die Bundesregierung lehnt den Vorschlag ab.

Die Empfehlung fällt hinter die bereits in 2015 in Kraft gesetzte, aktuell gültige Fassung des § 44b Satz 4 AtG zurück. Die bisherige Regelung ist jedoch erforderlich. Die Weiterleitung von Meldungen vom BSI nicht nur an die zuständigen Genehmigungs- und Aufsichtsbehörden der Länder, sondern auch an die des Bundes, ermöglicht ein bundeseinheitliches Vorgehen in der gemeinsamen Bekämpfung von IT-Angriffen bzw. der Behebung von IT-Störungen.

Die im Gesetz-Entwurf vorgenommene Erweiterung des derzeit gültigen § 44b Satz 4 AtG dahingehend, dass auch Sachverständige nach § 20 AtG direkt in den Meldeprozess eingebunden sein können, dient der rechtlichen Klarstellung einer Praxis, die in anderen Bereichen des Atomrechts bereits etabliert ist. Die Weiterleitung der IT-Meldungen durch das BSI an Sachverständige nach § 20 AtG erfolgt nur, wenn diese Sachverständigen im Vorfeld von der jeweils zuständigen Genehmigungs- und Aufsichtsbehörde dem BSI gegenüber benannt worden sind.

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
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 0722-8333