Bundesrat **Drucksache 64/17**

27.01.17

In - Fz - G - Wi

Gesetzentwurf
der 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

A. Problem und Ziel

Am 8. August 2016 trat die 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 (ABl. L 194 vom 19. Juli 2016, S. 1; im Folgenden: NIS-Richtlinie) in Kraft. Mit der Richtlinie wurden ein einheitlicher europäischer Rechtsrahmen für den EU-weiten Aufbau nationaler Kapazitäten für die Cyber-Sicherheit, eine stärkere Zusammenarbeit der Mitgliedstaaten der Europäischen Union sowie Mindestsicherheitsanforderungen an und Meldepflichten für bestimmte Dienste geschaffen. Ziel ist es, einheitliche Maßnahmen festzulegen, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen in der Europäischen Union erreicht werden soll (Artikel 1 Absatz 1 der NIS-Richtlinie). Die NIS-Richtlinie ist gemäß ihrem Artikel 25 Absatz 1 bis zum 9. Mai 2018 in nationales Recht umzusetzen. Gemäß Artikel 5 Absatz 1 der NIS-Richtlinie ermitteln die Mitgliedstaaten bis zum 9. November 2018 für jeden in Anhang II der Richtlinie genannten Sektor und Teilsektor die Betreiber wesentlicher Dienste mit einer Niederlassung in ihrem Hoheitsgebiet.

Fristablauf: 10.03.17
besonders eilbedürftige Vorlage gemäß Artikel 76 Absatz 2 Satz 4 GG

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

B. Lösung

Die europarechtlichen Vorgaben wurden bezüglich der Betreiber wesentlicher Dienste, in Deutschland die sogenannten Kritischen Infrastrukturen gem. § 2 Absatz 10 BSIG, im Wesentlichen bereits durch das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl. I S. 1324) in deutsches Recht umgesetzt. Daher sind im Rahmen einer Anpassung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) sowie einer Anpassung einzelner für bestimmte Branchen der Kritischen Infrastrukturen vorrangiger Spezialgesetze (des Atomgesetzes (AtG), des Energiewirtschaftsgesetzes (EnWG) und des Fünften Buches Sozialgesetzbuch – Gesetzliche Krankenversicherung (SGB V)) nur wenige Anpassungen erforderlich.

Zur Umsetzung der Vorgaben der NIS-Richtlinie werden die Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Überprüfung der Einhaltung der technischen und organisatorischen Sicherheitsanforderungen, die Nachweispflicht der Betreiber nach § 8a BSIG und die Regelungen in § 8b BSIG um Vorgaben für das Verfahren bei grenzüberschreitenden Vorfällen erweitert. Ergänzend werden Regelungen zu Mobilen Incident Response Teams (MIRTs) aufgenommen, mit denen das BSI andere Stellen bei der Wiederherstellung ihrer IT-Systeme unterstützen wird. Zudem wird das BSIG um eine Definition der digitalen Dienste sowie um spezielle Regelungen zu Sicherheitsanforderungen, zu Meldepflichten und zur Aufsicht im Hinblick auf die Anbieter digitaler Dienste ergänzt; die Bußgeldvorschriften in § 15 werden entsprechend angepasst.

Die in Artikel 5 der NIS-Richtlinie vorgesehene Ermittlung der Betreiber wesentlicher Dienste wird über die im geltenden Recht bereits vorgesehene Rechtsverordnung nach § 10 Absatz 1 BSIG vorgenommen. Ergänzt wird eine Ermächtigung zum Erlass von Rechtsverordnungen zur Umsetzung der in Artikel 16 der NIS-Richtlinie vorgesehenen Durchführungsrechtsakte.

Die nach § 8c BSIG vorrangigen Spezialgesetze werden entsprechend den im BSIG mit Bezug auf den Betrieb Kritischer Infrastrukturen enthaltenen Regelungen angepasst, soweit sie die Anforderungen der NIS-Richtlinie bezüglich der Betreiber wesentlicher Dienste bisher unterschreiten.

Neu eingeführt werden Regelungen bezüglich der digitalen Dienste Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste in das BSIG.

Zusätzlich werden mit dem Gesetzentwurf erforderliche Klarstellungen, Bereinigungen und Anpassungen bei den Unterstützungsaufgaben des BSI vorgenommen.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein zusätzlicher Erfüllungsaufwand.

E.2. Erfüllungsaufwand für die Wirtschaft

Für die Betreiber von Energieversorgungsnetzen und Energieanlagen, für bestimmte Telekommunikationsanbieter, für die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik), deren Gesellschafter die Spitzenverbände der Leistungserbringer und Kostenträger im nationalen Gesundheitswesen sind, sowie für sonstige Betreiber Kritischer Infrastrukturen entsteht ein Erfüllungsaufwand von maximal 8,66 Millionen Euro.

Für die Anbieter digitaler Dienste resultiert darüber hinaus durch die Verpflichtung zur Einhaltung eines Mindestniveaus an IT-Sicherheit und die Einführung von Meldepflichten für bestimmte IT-Vorfälle Erfüllungsaufwand. Dieser Aufwand kann im Voraus nicht quantifiziert werden, da das erforderliche Sicherheitsniveau und Meldeschwellen erst durch Durchführungsrechtsakte der Kommission festgelegt werden.

Der Kreis der verpflichteten Anbieter kann derzeit nicht konkret eingegrenzt und eine entsprechende Zahl meldepflichtiger Anbieter digitaler Dienste benannt werden, da hierzu keine Erhebungen vorliegen. Es wird jedoch geschätzt, dass von den Regelungen für digitale Dienste in Deutschland zwischen 500 und 1.500 Unternehmen betroffen sein werden. Die konkrete Anzahl hängt jedoch auch von späteren Festsetzungen der Durchführungsakte der Kommission ab. Der Aufwand für die Umsetzung von Maßnahmen zur Sicherung technischer Einrichtungen für einzelne Anbieter kann im Voraus nicht quantifiziert werden, da das erforderliche Sicherheitsniveau erst durch Durchführungsrechtsakte der Kommission festgelegt werden wird. Da Informationstechnik für Anbieter von digitalen Diensten das Kerngeschäft darstellt, und diese zudem bereits durch datenschutzrechtliche Vorgaben zur Gewährleistung eines hinreichenden Niveaus an Datensicherheit verpflichtet sind, ist allerdings davon auszugehen, dass das IT-Sicherheitsniveau bei digitalen Diensten bereits hohen Anforderungen genügt.

Auch die Anzahl der meldepflichtigen Vorfälle und der hierdurch für einzelne Anbieter resultierende Aufwand sind abhängig von der Festlegung konkreter Schwellenwerte und Meldevorgaben in Durchführungsrechtsakten der Kommission. Unter der Annahme, dass pro Betreiber und Jahr sieben Meldungen eines schweren Sicherheitsvorfalls erfolgen, und unter Ansatz einer Kostenschätzung von 660 Euro pro Meldung ergeben sich Gesamtkosten für die Meldepflicht digitaler Dienste in Höhe von rund 4,6 Mio. Euro. Kostenmindernd wird sich voraussichtlich auch hier auswirken, dass aufgrund datenschutzrechtlicher Vorgaben Meldestrukturen bereits vorhanden sein müssen.

Davon Bürokratiekosten:

Einzig die Meldepflichten für digitale Dienste und bestimmte Energieversorgungsnetzbetreiber stellen eine Informationspflicht dar, wodurch die Bürokratiekosten um rund 11,76 Millionen Euro steigen.

Die Belastungen sind nicht im Rahmen der One in, one out-Regel der Bundesregierung zu kompensieren, da diese Änderungen aus einer 1:1-Umsetzung der verbindlichen Mindestvorgaben der Richtlinie (EU) 2016/1148 resultieren.

E.3 Erfüllungsaufwand für die Verwaltung

Der Verwaltung entsteht für die Erfüllung der im Gesetz vorgesehenen zusätzlichen Aufgaben ein Aufwand von insgesamt 185,5 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 14,216 Millionen Euro.

Davon ist beim BSI ein Erfüllungsaufwand in Höhe 181,5 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 13,909 Millionen Euro und beim Bundesministerium des Innern (BMI) ein Erfüllungsaufwand in Höhe von 4 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 420.000 Euro zu berücksichtigen. Beim BSI werden in geringem Umfang zusätzliche Sachkosten entstehen, die aus dem Haushalt des BSI getragen werden können.

Der Bedarf an Personalmitteln sowie Planstellen und Stellen soll finanziell und stellenmäßig im jeweiligen Einzelplan ausgeglichen werden.

Der Erfüllungsaufwand für die Länder und Kommunen ist derzeit nicht bezifferbar.

F. Weitere Kosten

Betreibern Kritischer Infrastrukturen können im Sonderfall nach § 8a Absatz 3 Satz 3 BSIG Kosten entstehen, soweit berechtigte Zweifel an der ordnungsgemäßen Einhaltung der ihnen obliegenden Sicherheitsanforderungen bestehen, die eine zusätzlich Überprüfung vor Ort erforderlich machen.

Bundesrat **Drucksache 64/17**

27.01.17

In - Fz - G - Wi

Gesetzentwurf
der 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

Bundesrepublik Deutschland
Die Bundeskanzlerin

Berlin, 27. Januar 2017

An die
Präsidentin des Bundesrates
Frau Ministerpräsidentin
Malu Dreyer

Sehr geehrte Frau Präsidentin,

hiermit übersende ich gemäß Artikel 76 Absatz 2 Satz 4 des Grundgesetzes den von der Bundesregierung beschlossenen

> 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

mit Begründung und Vorblatt.

Fristablauf: 10.03.17
besonders eilbedürftige Vorlage gemäß Artikel 76 Absatz 2 Satz 4 GG

Der Gesetzentwurf ist besonders eilbedürftig, um die Richtlinie des Europäischen Parlaments und des Rates zeitnah in deutsches Recht umzusetzen.

Federführend ist das Bundesministerium des Innern.

Die Stellungnahme des Nationalen Normenkontrollrates gemäß § 6 Absatz 1 NKRG ist als Anlage beigefügt.

Mit freundlichen Grüßen
Dr. Angela Merkel

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[1]

Vom …

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1
Änderung des BSI-Gesetzes

Das BSI-Gesetz in der Fassung der Bekanntmachung vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 3 Absatz 6 des Gesetzes vom 18. Juli 2016 (BGBl. I S. 1666) geändert worden ist, wird wie folgt geändert:

1) § 2 wird wie folgt geändert:

   a) Nach Absatz 10 folgender Absatz 11 eingefügt:

   „(11) Digitale Dienste im Sinne dieses Gesetzes sind Dienste im Sinne von Artikel 1 Absatz 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1), und die

   1. es Verbrauchern oder Unternehmern im Sinne des Artikels 4 Absatz 1 Buchstabe a beziehungsweise Buchstabe b der Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die alternative Beilegung verbraucherrechtlicher Streitigkeiten und zur Änderung der Verordnung (EG) Nr. 2006/2004 und der Richtlinie 2009/22/EG (Richtlinie über alternative Streitbeilegung in Verbraucherangelegenheiten) (ABl. L 165 vom

[1] Dieses Gesetz dient der 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 (ABl. L 194 vom 19.7.2016, S.1).

18.6.2013, S. 63) ermöglichen, Kaufverträge oder Dienstleistungsverträge mit Unternehmern entweder auf der Website dieser Dienste oder auf der Website eines Unternehmers, die von diesen Diensten bereitgestellte Rechendienste verwendet, abzuschließen (Online-Marktplätze);

2. es Nutzern ermöglichen, Suchen grundsätzlich auf allen Websites oder auf Websites in einer bestimmten Sprache anhand einer Abfrage zu einem beliebigen Thema in Form eines Stichworts, einer Wortgruppe oder einer anderen Eingabe vorzunehmen, die daraufhin Links anzeigen, über die der Abfrage entsprechende Inhalte abgerufen werden können (Online-Suchmaschinen);

3. den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen (Cloud-Computing-Dienste),

und nicht zum Schutz grundlegender staatlicher Funktionen eingerichtet worden sind oder für diese genutzt werden."

b) Nach Absatz 11 wird folgender Absatz 12 eingeführt:

„Anbieter digitaler Dienste" im Sinne dieses Gesetzes ist eine juristische Person, die einen digitalen Dienst anbietet."

2) § 3 Absatz 1 Satz 2 wird wie folgt geändert:

a) Nummer 13 Buchstabe b) wird wie folgt geändert:
Nach dem Wort "Verfassungsschutzbehörden" werden die Wörter "und des Militärischen Abschirmdienstes" und nach dem Wort "der Länder" die Wörter "beziehungsweise dem Gesetz über den Militärischen Abschirmdienst" eingefügt.

b) Nach Nummer 13 wird folgende Nummer 13a eingefügt:
„13a. auf Ersuchen der zuständigen Stellen der Länder Unterstützung dieser Stellen in Fragen der Abwehr von Gefahren für die Sicherheit in der Informationstechnik;".

c) Nummer 17 wird wie folgt geändert:

Die Angabe „und 8b" wird durch die Angabe „bis 8c" und der Punkt am Ende wird durch die Wörter „und digitaler Dienste;" ersetzt.

d) Folgende Nummer 18 wird angefügt:

„18. Unterstützung bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen nach § 5a."

3) § 5 wird wie folgt geändert:

a) Absatz 5 wird wie folgt geändert:

aa) In Satz 2 Nummer 2 werden nach dem Wort "Verfassungsschutz" die Wörter "sowie an den Militärischen Abschirmdienst, wenn sich diese Tätigkeiten gegen Personen, Dienststellen oder Einrichtungen im Geschäftsbereich des Bundesministeriums der Verteidigung richten." eingefügt.

bb) Es wird folgende Nummer 3 angefügt:

„3. zur Unterrichtung über Tatsachen, die einen internationalen kriminellen, terroristischen oder staatlichen Angriff mittels Schadprogrammen oder vergleichbaren schädlich wirkenden informationstechnischen Mitteln auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland erkennen lassen, an den Bundesnachrichtendienst.“

b) Absatz 6 wird wie folgt geändert:
aa) Satz 1 wird wie folgt geändert:

aaa) In Nummer 3 werden nach dem Wort "Länder" die Wörter "sowie an den Militärischen Abschirmdienst" und nach dem Wort "Bundesverfassungsschutzgesetzes" die Wörter "beziehungsweise § 1 Absatz 1 des Gesetzes über den Militärischen Abschirmdienst" eingefügt.

bbb) Es wird folgende Nummer 4 angefügt:

„an den Bundesnachrichtendienst, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand Straftaten nach § 3 Absatz 1 Nummer 8 des Artikel 10-Gesetzes plant, begeht oder begangen hat und dies von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland ist.“

bb) In Satz 5 wird nach der Angabe „Nummer 3“ die Angabe „und Nummer 4“ eingefügt.

4) Nach § 5 wird folgender § 5a eingefügt:

„§ 5a

Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen

(1) Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Stelle des Bundes oder eines Betreibers einer Kritischen Infrastruktur um einen herausgehobenen Fall, so kann das Bundesamt auf Ersuchen der betroffenen Stelle oder des be-

troffenen Betreibers die Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind. Soweit das Bundesamt erste Maßnahmen zur Schadensbegrenzung und Sicherstellung des Notbetriebes vor Ort ergreift, werden hierfür keine Gebühren oder Auslagen für die Tätigkeit des Bundesamtes erhoben. Hiervon unberührt bleiben etwaige Kosten für die Hinzuziehung qualifizierter Dritter.

(2) Ein herausgehobener Fall nach Absatz 1 liegt insbesondere dann vor, wenn es sich um einen Angriff von besonderer technischer Qualität handelt oder die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems von besonderem öffentlichem Interesse ist.

(3) Das Bundesamt darf bei Maßnahmen nach Absatz 1 personenbezogene oder dem Fernmeldegeheimnis unterliegende Daten erheben und verarbeiten, soweit dies zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich und angemessen ist. Die Daten sind unverzüglich zu löschen, sobald sie für die Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems nicht mehr benötigt werden. Wenn die Daten in Fällen des Absatzes 4 an eine andere Behörde zur Erfüllung von deren gesetzlichen Aufgaben weitergegeben worden sind, darf das Bundesamt die Daten abweichend von Satz 2 bis zur Beendigung der Unterstützung dieser Behörden weiterverarbeiten. Eine Nutzung zu anderen Zwecken ist unzulässig. § 5 Absatz 7 ist entsprechend anzuwenden. Im Übrigen sind die Regelungen des Bundesdatenschutzgesetzes anzuwenden.

(4) Das Bundesamt darf Informationen, von denen es im Rahmen dieser Vorschrift Kenntnis erlangt, nur mit Einwilligung des Ersuchenden weitergeben, es sei denn, die Informationen lassen keine Rückschlüsse auf die Identität des Ersuchenden zu oder die Informationen können entsprechend § 5 Absatz 5 und 6 übermittelt werden. Zugang zu den in Verfahren nach Absatz 1 geführten Akten wird Dritten nicht gewährt.

(5) Das Bundesamt kann sich bei Maßnahmen nach Absatz 1 mit der Einwilligung des Ersuchenden der Hilfe qualifizierter Dritter bedienen, wenn dies zur rechtzeitigen oder vollständigen Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich ist. Die hierdurch entstehenden Kosten hat der Ersuchende zu tragen. Das Bundesamt kann den Ersuchenden auch auf qualifizierte Dritte verweisen. Das Bundesamt und vom Ersuchenden oder vom Bundesamt nach Satz 1 beauf-

tragte Dritte können einander bei Maßnahmen nach Absatz 1 mit der Einwilligung des Ersuchenden Daten übermitteln. Hierfür gilt Absatz 3 entsprechend.

(6) Soweit es zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems erforderlich ist, kann das Bundesamt vom Hersteller des informationstechnischen Systems verlangen, an der Wiederherstellung der Sicherheit oder Funktionsfähigkeit mitzuwirken.

(7) In begründeten Einzelfällen kann das Bundesamt auch bei anderen als den in Absatz 1 genannten Einrichtungen tätig werden, wenn es darum ersucht wurde und es sich um einen herausgehobenen Fall im Sinne des Absatzes 2 handelt.

(8) Im Falle von Anlagen oder Tätigkeiten, die einer Genehmigung nach dem Atomgesetz bedürfen, ist in Fällen der Absätze 1, 4, 5 und 7 vor Tätigwerden des Bundesamtes das Benehmen mit den zuständigen atomrechtlichen Aufsichtsbehörden des Bundes und der Länder herzustellen. Im Falle von Anlagen oder Tätigkeiten, die einer Genehmigung nach dem Atomgesetz bedürfen, haben bei Maßnahmen des Bundesamtes nach § 5a die Vorgaben aufgrund des Atomgesetzes Vorrang.“

5) In § 7a Absatz 1 Satz 1 werden die Wörter „Nummer 1, 14 und 17“ durch die Wörter „Nummer 1, 14, 17 und 18“ ersetzt.

6) § 8a wird wie folgt geändert:

a) Absatz 3 wird wie folgt geändert:

aa) In Satz 3 werden die Wörter „eine Aufstellung“ durch die Wörter „die Ergebnisse“ ersetzt.

bb) Satz 4 wird durch die folgenden Sätze ersetzt:

„Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen. Es kann bei Sicherheitsmängeln im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.“

b) Nach Absatz 3 wird folgender Absatz 4 eingefügt:

„(4) Das Bundesamt kann beim Betreiber Kritischer Infrastrukturen die Einhaltung der Anforderungen nach Absatz 1 überprüfen; es kann sich bei der

Durchführung der Überprüfung eines qualifizierten unabhängigen Dritten bedienen. Der Betreiber Kritischer Infrastrukturen hat dem Bundesamt und den in dessen Auftrag handelnden Personen zum Zweck der Überprüfung das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücken und sonstigen Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Für die Überprüfung erhebt das Bundesamt Gebühren und Auslagen bei dem jeweiligen Betreiber Kritischer Infrastrukturen nur, sofern das Bundesamt auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Einhaltung der Anforderungen nach Absatz 1 begründeten."

c) Der bisherige Absatz 4 wird Absatz 5.

7) § 8b wird wie folgt geändert:

a) Absatz 2 Nummer 4 wird wie folgt geändert:

aa) In Buchstabe b wird das Wort „sowie" durch ein Komma ersetzt.

bb) In Buchstabe c wird das Wort „sowie" angefügt.

cc) Folgender Buchstabe d wird angefügt:

„d) die zuständigen Behörden eines anderen Mitgliedstaates der Europäischen Union über nach Absatz 4 oder nach vergleichbaren Regelungen gemeldete erhebliche Störungen, die Auswirkungen in diesem Mitgliedstaat haben,".

b) In Absatz 3 Satz 1 werden die Wörter „Kommunikationsstrukturen nach § 3 Absatz 1 Satz 2 Nummer 15" durch die Wörter „von ihnen betriebenen Kritischen Infrastrukturen" ersetzt.

c) Absatz 4 wird wie folgt geändert:

aa) Satz 1 wird wie folgt gefasst:

„Betreiber Kritischer Infrastrukturen haben die folgenden Störungen unverzüglich über die Kontaktstelle an das Bundesamt zu melden:

1. Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen geführt haben,

2. erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können.“

bb) Satz 2 wird wie folgt geändert:

aaa) Nach den Wörtern „Angaben zu der Störung“ werden die Wörter „, zu möglichen grenzübergreifenden Auswirkungen“ eingefügt.
bbb) Die Wörter „Branche des Betreibers“ werden durch die Wörter „erbrachten kritischen Dienstleistung und zu den Auswirkungen der Störung auf diese Dienstleistung“ ersetzt.

8) Nach § 8b wird folgender § 8c eingefügt:

„§ 8c
Besondere Anforderungen an Anbieter digitaler Dienste

(1) Anbieter digitaler Dienste haben geeignete und verhältnismäßige technische und organisatorische Maßnahmen zu treffen, um Risiken für die Sicherheit der Netz- und Informationssysteme, die sie zur Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen, zu bewältigen. Sie haben Maßnahmen zu treffen, um den Auswirkungen von Sicherheitsvorfällen auf innerhalb der Europäischen Union erbrachte digitale Dienste vorzubeugen oder die Auswirkungen so gering wie möglich zu halten.

(2) Maßnahmen zur Bewältigung von Risiken für die Sicherheit der Netz- und Informationssysteme nach Absatz 1 Satz 1 müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Dabei ist folgenden Aspekten Rechnung zu tragen:

1. der Sicherheit der Systeme und Anlagen,

2. der Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen,

3. dem Betriebskontinuitätsmanagement,

4. der Überwachung, Überprüfung und Erprobung,

5. der Einhaltung internationaler Normen.

Die notwendigen Maßnahmen werden durch Durchführungsrechtsakte der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 näher bestimmt.

(3) Anbieter digitaler Dienste haben jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung eines von ihnen innerhalb der Europäischen Union erbrachten digitalen Dienstes hat, unverzüglich dem Bundesamt zu melden. Die Voraussetzungen, nach denen Auswirkungen eines Sicherheitsvorfalls erheblich sind, werden durch Durchführungsakte der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 unter Berücksichtigung insbesondere der folgenden Parameter näher bestimmt:

1. die Zahl der von dem Sicherheitsvorfall betroffenen Nutzer, insbesondere der Nutzer, die den Dienst für die Bereitstellung ihrer eigenen Dienste benötigen;

2. die Dauer des Sicherheitsvorfalls;

3. das von dem Sicherheitsvorfall betroffene geographische Gebiet;

4. das Ausmaß der Unterbrechung der Bereitstellung des Dienstes;

5. das Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten.

Die Pflicht zur Meldung eines Sicherheitsvorfalls entfällt, wenn der Anbieter keinen ausreichenden Zugang zu den Informationen hat, die erforderlich sind, um die Auswirkung eines Sicherheitsvorfalls gemessen an den Parametern nach Satz 2 zu bewerten. Für den Inhalt der Meldungen gilt § 8b Absatz 3 entsprechend, soweit nicht Durchführungsakte der Kommission nach Artikel 16 Absatz 9 der Richtlinie (EU) 2016/1148 etwas anderes bestimmen. Über nach Satz 1 gemeldete Sicherheitsvorfälle, die Auswirkungen in einem anderen Mitgliedsstaat der Europäischen Union haben, hat das Bundesamt die zuständige Behörde dieses Mitgliedsstaats zu unterrichten.

(4) Liegen Anhaltspunkte dafür vor, dass ein Anbieter digitaler Dienste die Anforderungen des Absatzes 1 in Verbindung mit den Durchführungsrechtsakten der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 und des Absatzes 2 in Verbindung mit den Durchführungsrechtsakten der Kommission nach Artikel 16 Absatz 9 der Richtlinie (EU) 2016/1148 nicht erfüllt, kann das Bundesamt von dem Anbieter digitaler Dienste folgende Maßnahmen verlangen:

1. die Übermittlung der zur Beurteilung der Sicherheit seiner Netz- und Informationssysteme erforderlichen Informationen, einschließlich Nachweisen über ergriffene Sicherheitsmaßnahmen;

2. die Beseitigung von Mängeln bei der Erfüllung der in den Absätzen 1 und 2 bestimmten Anforderungen.

Die Anhaltspunkte können sich auch aus Feststellungen ergeben, die dem Bundesamt von den zuständigen Behörden eines anderen Mitgliedstaats der Europäischen Union vorgelegt werden.

(5) Hat ein Anbieter digitaler Dienste seine Hauptniederlassung, einen Vertreter oder Netz- und Informationssysteme in einem anderen Mitgliedstaat der Europäischen Union, so arbeitet das Bundesamt bei der Erfüllung der Aufgaben nach Absatz 4 mit der zuständigen Behörde dieses Mitgliedstaates zusammen. Diese Zusammenarbeit kann das Ersuchen umfassen, die Maßnahmen in Absatz 4 Satz 1 Nummer 1 und 2 zu ergreifen."

9) Der bisherige § 8c wird § 8d und wird wie folgt geändert:

a) In Absatz 1 Satz 2 werden nach der Angabe „Absatz 4" die Wörter „des Anhangs" eingefügt.
b) Dem Absatz 2 Nummer 2 werden die Wörter „soweit sie den Regelungen des § 11 des Energiewirtschaftsgesetzes unterliegen," angefügt.
c) Absatz 3 wird wie folgt geändert:
   aa) In Nummer 2 werden die Wörter „im Sinne des Energiewirtschaftsgesetzes" durch die Wörter „soweit sie den Regelungen des § 11 des Energiewirtschaftsgesetzes unterliegen," ersetzt.
   bb) In dem Satzteil vor Nummer 1 und in Nummer 5 werden jeweils die Wörter „Absatz 3 bis 5" durch die Angabe „Absatz 4" ersetzt.
d) Die folgenden Absätze 4 und 5 werden angefügt:

   „(4) § 8c Absatz 1 bis 3 gilt nicht für Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG. § 8c Absatz 3 gilt nicht für Anbieter,

   1. die ihren Hauptsitz in einem anderen Mitgliedstaat der Europäischen Union haben oder

   2. die, soweit sie nicht in einem Mitgliedstaat der Europäischen Union niedergelassen sind, einen Vertreter in einem anderen Mitgliedstaat der Europäischen Union benannt haben, in dem die digitalen Dienste ebenfalls angeboten werden.

   Für Anbieter nach Satz 2 gilt § 8c Absatz 4 nur, soweit sie in der Bundesrepublik Deutschland Netz- und Informationssysteme betreiben, die sie zur Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen."

10) Der bisherige § 8d wird § 8e und wird wie folgt geändert:

a) In Absatz 1 Satz 1 wird wie folgt geändert:
aa) Nach den Wörtern „§ 8a Absatz 2 und 3“ werden die Wörter „und § 8c Absatz 4“ und nach den Wörtern „§ 8b Absatz 4” die Wörter „und § 8c Absatz 4“ eingefügt.
bb) Nach den Wörtern „Kritischer Infrastrukturen“ werden die Wörter „oder des Anbieters digitaler Dienste“ eingefügt.
cc) Das Wort „wesentlicher“ wird durch das Wort „von“ ersetzt und die Wörter „zu erwarten ist“ durch die Wörter „eintreten kann“ ersetzt.

b) Absatz 2 wird wie folgt neugefasst:
„Zugang zu den Akten des Bundesamtes in Angelegenheiten nach den §§ 8a bis 8c wird bei Vorliegen der Voraussetzungen des § 29 des Verwaltungsverfahrensgesetzes nur gewährt, wenn schutzwürdige Interessen des betroffenen Betreibers Kritischer Infrastrukturen oder des Anbieters digitaler Dienste dem nicht entgegenstehen und durch den Zugang zu den Akten keine Beeinträchtigung von Sicherheitsinteressen eintreten kann.“

c) Folgender Absatz 3 wird angefügt:
„(3) Für Betreiber nach § 8d Absatz 2 und 3 gelten die Absätze 1 und 2 entsprechend.“

11) Dem § 10 wird folgender Absatz 4 angefügt:

„(4) Soweit die Durchführungsrechtsakte der Kommission nach Artikel 16 Absatz 8 und 9 der Richtlinie (EU) 2016/1148 keine abschließenden Bestimmungen über die von Anbietern digitaler Dienste nach § 8c Absatz 2 zu treffenden Maßnahmen oder über die Parameter zur Beurteilung der Erheblichkeit der Auswirkungen von Sicherheitsvorfällen nach § 8c Absatz 3 Satz 2 oder über Form und Verfahren der Meldungen nach § 8c Absatz 3 Satz 4 enthalten, werden diese Bestimmungen vom Bundesministerium des Innern im Einvernehmen mit den jeweils betroffenen Ressorts durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, getroffen.“

12) In § 11 wird die Angabe „§ 5“ durch die Wörter „die §§ 5 und 5a“ ersetzt.

13) Dem § 13 werden die folgenden Absätze 3 bis 5 angefügt:

„(3) Das Bundesamt übermittelt bis zum 9. November 2018 und danach alle zwei Jahre die folgenden Informationen an die Kommission:

1. die nationalen Maßnahmen zur Ermittlung der Betreiber Kritischer Infrastrukturen;

2. eine Aufstellung der im in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren, die nach § 2 Absatz 10 Satz 1 Nummer 2 wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistungen und deren als bedeutend anzusehenden Versorgungsgrad;

3. eine zahlenmäßige Aufstellung der Betreiber der in Nummer 2 genannten Sektoren, die in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren ermittelt werden, einschließlich eines Hinweises auf ihre Bedeutung für den jeweiligen Sektor.

Die Übermittlung darf keine Informationen enthalten, die zu einer Identifizierung einzelner Betreiber führen können. Das Bundesamt übermittelt die nach Satz 1 übermittelten Informationen unverzüglich dem Bundesministerium des Innern, dem Bundeskanzleramt, dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit.

(4) Sobald bekannt wird, dass eine Einrichtung oder Anlage nach § 2 Absatz 10 oder Teile einer Einrichtung oder Anlage eine wegen ihrer Bedeutung als kritisch anzusehenden Dienstleistung in einem der in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren in einem anderen Mitgliedstaat der Europäischen Union bereitstellt, nimmt das Bundesamt zum Zweck der gemeinsamen Ermittlung der Betreiber, die kritische Dienstleistungen in den in Anhang II der Richtlinie (EU) 2016/1148 genannten Teilsektoren erbringen, mit der zuständigen Behörde dieses Mitgliedstaats Konsultationen auf.

(5) Das Bundesamt übermittelt bis zum 9. August 2018 und danach jährlich an die Kooperationsgruppe nach Artikel 11 der Richtlinie (EU) 2016/1148 einen zusammenfassenden Bericht zu den Meldungen, die in Anhang II der Richtlinie (EU) 2016/1148 genannten Sektoren oder digitale Dienste betreffen. Der Bericht enthält auch die Zahl der Meldungen und die Art der gemeldeten Sicherheitsvorfälle sowie die ergriffenen Maßnahmen. Der Bericht darf keine Informationen enthalten, die zu einer Identifizierung einzelner Meldungen oder einzelner Betreiber oder Anbieter führen können.“

14) § 14 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) In Nummer 2 werden die Wörter „Satz 4 a) Nummer 1 oder b) Nummer 2“ durch die Angabe „Satz 5“ ersetzt.

bb) In Nummer 3 wird das Wort „oder“ am Ende durch ein Komma ersetzt.

cc) In Nummer 4 wird der Punkt am Ende durch ein Komma ersetzt.

dd) Die folgenden Nummern 5 bis 7 werden angefügt:

„5. entgegen § 8c Absatz 1 Satz 1 eine dort genannte Maßnahme nicht trifft,

6. entgegen § 8c Absatz 3 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vornimmt oder

7. einer vollziehbaren Anordnung nach § 8c Absatz 4

a) Nummer 1 oder

b) Nummer 2

zuwiderhandelt.“

b) Dem Absatz 2 wird folgender Satz angefügt:

„In den Fällen des Absatzes 1 Nummer 5 bis 7 wird die Ordnungswidrigkeit nur geahndet, wenn der Anbieter digitaler Dienste seine Hauptniederlassung nicht in einem anderen Mitgliedstaat der Europäischen Union hat oder, soweit er nicht in einem anderen Mitgliedstaat der Europäischen Union niedergelassen ist, dort einen Vertreter benannt hat und in diesem Mitgliedstaat dieselben digitalen Dienste anbietet.“

15) Folgender § 15 wird angefügt:

„§ 15

Anwendbarkeit der Vorschriften für Anbieter digitaler Dienste

Die Vorschriften, die Anbieter digitaler Dienste betreffen, sind ab dem 10. Mai 2018 anwendbar.“

Artikel 2
Änderung des Atomgesetzes

§ 44b des Atomgesetzes in der Fassung der Bekanntmachung vom 15. Juli 1985 (BGBl. I S. 1565), das zuletzt durch Artikel 1 des Gesetzes vom 26. Juli 2016 (BGBl. I S. 1843) geändert worden ist, wird wie folgt geändert:

1) In Satz 2 werden die Wörter „§ 8b Absatz 1, 2 und Absatz 7“ durch die Wörter „§ 8b Absatz 1, 2 Nummer 1 bis 3, Nummer 4 Buchstabe a) bis c) und Absatz 7“ ersetzt.
2) In Satz 4 werden nach den Wörtern „des Bundes und des Landes“ die Wörter „und an die von diesen bestimmten Sachverständigen nach § 20“ eingefügt.

Artikel 3
Änderung des Energiewirtschaftsgesetzes

Das Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 6 des Gesetzes vom 13. Oktober 2016 (BGBl. I S. 2258) geändert worden ist, wird wie folgt geändert:

1) § 11 Absatz 1c) wird wie folgt neu gefasst:

„(1c) Betreiber von Energieversorgungsnetzen und von solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, haben

1. Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage geführt haben,

2. erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer erheblichen Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage führen können,

über die Kontaktstelle unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik zu melden.

Die Meldung muss Angaben zu der Störung, zu möglichen grenzübergreifenden Auswirkungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache und der betroffenen Informationstechnik, enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat. Das Bundesamt für Sicherheit in der Informationstechnik hat die Meldungen unverzüglich an die Bundesnetzagentur weiterzuleiten. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben sicherzustellen, dass die unbefugte Offenbarung der ihnen nach Satz 1 zur Kenntnis gelangten Angaben ausgeschlossen wird. Zugang zu den Akten des Bundesamtes für Sicherheit in der Informationstechnik sowie zu den Akten der Bundesnetzagentur in Angelegenheiten nach den §§ 11 Absatz 1a bis Absatz 1c wird nicht gewährt. § 29 des Verwaltungsverfahrensgesetzes bleibt unberührt. § 8e Absatz 1 des BSI-Gesetzes ist entsprechend anzuwenden.“

2) § 95 wird wie folgt geändert:

a) In Absatz 1 werden nach Nummer 2 folgende Nummern 2a und 2b eingefügt:

„2a. entgegen § 11 Absatz 1a oder 1b den Katalog von Sicherheitsanforderungen nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig einhält,

2b. entgegen § 11 Absatz 1c eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vornimmt,“.

b) Absatz 5 wird wie folgt gefasst:

„(5) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist in den Fällen des Absatzes 1 Nummer 2b das Bundesamt für Sicherheit in der Informationstechnik, im Übrigen die nach § 54 zuständige Behörde.“

Artikel 4
Änderung des Fünften Buches Sozialgesetzbuch

Das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), das zuletzt durch

Artikel 2 des Gesetzes vom 11. Oktober 2016 (BGBl. I S. 2233) geändert worden ist, wird wie folgt geändert:

1) Dem § 291b wird folgender Absatz 8 angefügt:

„(8) Die Gesellschaft für Telematik legt dem Bundesamt für Sicherheit in der Informationstechnik auf Verlangen die folgenden Unterlagen und Informationen vor:

1. die Zulassungen und Bestätigungen nach den Absätzen 1a bis 1c und 1e einschließlich der zugrunde gelegten Dokumentation,

2. eine Aufstellung der nach den Absätzen 6 und 7 getroffenen Maßnahmen einschließlich der festgestellten Sicherheitsmängel und Ergebnisse der Maßnahmen und

3. sonstige für die Bewertung der Sicherheit der Telematikinfrastruktur sowie der zugelassenen Dienste und bestätigten Anwendungen erforderlichen Informationen.

Ergibt die Bewertung der in Satz 1 genannten Informationen Sicherheitsmängel, so kann das Bundesamt für Sicherheit in der Informationstechnik der Gesellschaft für Telematik verbindliche Anweisungen zur Beseitigung der festgestellten Sicherheitsmängel erteilen. Die Gesellschaft für Telematik ist befugt, Betreibern von zugelassenen Diensten und bestätigten Anwendungen nach den Absätzen 1a bis 1c und 1e, verbindliche Anweisungen zur Beseitigung festgestellter Sicherheitsmängel zu erteilen. Die Kosten der Überprüfung tragen

1. die Gesellschaft für Telematik, sofern das Bundesamt für Sicherheit in der Informationstechnik auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Sicherheit der Telematikinfrastruktur begründeten,

2. der Betreiber von zugelassenen Diensten und bestätigten Anwendungen nach den Absätzen 1a bis 1c und 1e, sofern das Bundesamt für Sicherheit in der Informationstechnik auf Grund von Anhaltspunkten tätig geworden ist, die berechtigte Zweifel an der Sicherheit der zugelassenen Dienste und bestätigten Anwendungen begründeten.“

2) § 307 wird wie folgt geändert

a) Nach Absatz 1 werden folgende Absätze 1a bis 1c eingefügt:

„(1a) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 291b Absatz 6 Satz 2 und 4 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vornimmt.

(1b) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 291b Absatz 8 Satz 2 einer verbindlichen Anweisung nicht, nicht vollständig oder nicht rechtzeitig Folge leistet.

(1c) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig entgegen § 291b Absatz 8 Satz 3 einer verbindlichen Anweisung nicht, nicht vollständig oder nicht rechtzeitig Folge leistet.“

b) Folgender Absatz 4 wird angefügt:

„(4) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist in den Fällen der Absätze 1a bis 1c das Bundesamt für Sicherheit in der Informationstechnik.“

Artikel 5
Änderung des Telekommunikationsgesetzes

Das Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 1 und 12 des Gesetzes vom 4. November 2016 (BGBl. I S. 2473) geändert worden ist, wird wie folgt geändert:

§ 109 Absatz 5 wird wie folgt geändert:

In Satz 8 wird die Angabe „ § 8d“ durch die Angabe „§ 8e“ ersetzt.

Artikel 6
Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Zweck und Inhalt des Gesetzes

Am 8. August 2016 trat die 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 (ABl. L 194 vom 19. Juli 2016, S. 1; sog. NIS-Richtlinie) in Kraft. Mit der Richtlinie wurden ein einheitlicher europäischer Rechtsrahmen für den EU-weiten Aufbau nationaler Kapazitäten für die Cyber-Sicherheit, eine stärkere Zusammenarbeit der Mitgliedstaaten sowie Mindestsicherheitsanforderungen an und Meldepflichten für bestimmte Dienste geschaffen. Ziel ist es, einheitliche Maßnahmen festzulegen, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen in der Europäischen Union erreicht werden soll (Artikel 1 Absatz 1 der NIS-Richtlinie). Die Richtlinie ist gemäß Artikel 25 Absatz 1 bis zum 9. Mai 2018 in nationales Recht umsetzen. Gemäß Artikel 5 Absatz 1 der Richtlinie ermitteln die Mitgliedstaaten bis zum 9. November 2018 für jeden in Anhang II der Richtlinie genannten Sektor und Teilsektor die Betreiber wesentlicher Dienste mit einer Niederlassung in ihrem Hoheitsgebiet.

Die europarechtlichen Vorgaben werden im Rahmen einer Anpassung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) sowie einzelner für bestimmte Branchen der Kritischen Infrastrukturen vorrangiger Spezialgesetze (des Atomgesetzes (AtG), des Energiewirtschaftsgesetzes (EnWG) und des Fünften Buches Sozialgesetzbuch – Gesetzliche Krankenversicherung (SGB V)) umgesetzt.

Zur Umsetzung der Vorgaben der NIS-Richtlinie werden die Befugnisse des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur Überprüfung der Einhaltung der technischen und organisatorischen Sicherheitsanforderungen, die Nachweispflicht der Betreiber Kritischer Infrastrukturen nach § 8a BSIG und die Regelungen in § 8b BSIG um Vorgaben für das Verfahren bei grenzüberschreitenden Vorfällen erweitert. Zudem wird das BSIG um eine Definition der digitalen Dienste sowie um spezielle Regelungen zu Sicherheitsanforderungen, zu Meldepflichten und zur Aufsicht im Hinblick auf die Anbieter digitaler Dienste ergänzt; die Bußgeldvorschriften in § 15 werden entsprechend angepasst.

Die in Artikel 5 der NIS-Richtlinie vorgesehene Ermittlung der Betreiber wesentlicher Dienste wird über die im geltenden Recht bereits vorgesehene Rechtsverordnung

nach § 10 Absatz 1 BSIG zur Bestimmung der Kritischen Infrastrukturen vorgenommen. Ergänzt wird eine Ermächtigung zum Erlass von Rechtsverordnungen zur Umsetzung der in Artikel 16 der NIS-Richtlinie vorgesehenen Durchführungsrechtsakte.

Die nach § 8c BSIG vorrangigen Spezialgesetze werden entsprechend den im BSIG enthaltenen Regelungen mit Bezug auf den Betrieb Kritischer Infrastrukturen angepasst, soweit sie die Anforderungen der NIS-Richtlinie bezüglich der Betreiber wesentlicher Dienste bisher unterschreiten.

Zusätzlich werden mit dem Gesetzentwurf erforderliche Klarstellungen, Bereinigungen und Anpassungen bei den Unterstützungsaufgaben des BSI vorgenommen.

II. Gesetzgebungskompetenz des Bundes

Für die Änderungen des BSI-Gesetzes (Artikel 1), die den Schutz der Informationstechnik Kritischer Infrastrukturen betreffen, folgt die Gesetzgebungskompetenz des Bundes teilweise aus speziellen Kompetenztiteln:

- Luftverkehr: Artikel 73 Absatz 1 Nummer 6 des Grundgesetzes (GG),

- Eisenbahnen: Artikel 73 Absatz 1 Nummer 6a, Artikel 74 Absatz 1 Nummer 23 GG,

- Schifffahrt: Artikel 74 Absatz 1 Nummer 21 GG,

- Gesundheit: Artikel 74 Absatz 1 Nummer 19 GG,

- Telekommunikation: Artikel 73 Absatz 1 Nummer 7 GG und

- im Übrigen aus der Gesetzgebungskompetenz für das Recht der Wirtschaft (Artikel 74 Absatz 1 Nummer 11 GG).

Für die Änderung des Atomgesetzes (Artikel 2) ergibt sich die Gesetzgebungskompetenz des Bundes aus Artikel 73 Absatz 1 Nummer 14 GG.

Die Gesetzgebungskompetenz für die Änderung des Energiewirtschaftsgesetzes (Artikel 3) ergibt sich aus der Gesetzgebungskompetenz für das Recht der Wirtschaft (Artikel 74 Absatz 1 Nummer 11 GG).

Die Gesetzgebungskompetenz des Bundes für die Regelungen der Bußgeldvorschriften und Ordnungswidrigkeiten folgt aus Artikel 74 Absatz 1 Nummer 1 GG (Strafrecht). Die Änderungen im Telekommunikationsgesetz (Artikel 5) stützen sich auf die ausschließliche Gesetzgebungskompetenz des Bundes nach Artikel 73 Absatz 1 Nummer 7 GG.

Die Berechtigung des Bundes zur Inanspruchnahme der Gesetzgebungskompetenz aus Artikel 74 Absatz 1 Nummer 11 GG folgt aus Artikel 72 Absatz 2 GG. Eine bundesgesetzliche Regelung dieser Materie ist zur Wahrung der Wirtschaftseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich. Eine Regelung durch den Landesgesetzgeber würde zu erheblichen Nachteilen für die Gesamtwirtschaft führen, die sowohl im Interesse des Bundes als auch im Interesse der Länder nicht hingenommen werden können. Insbesondere wäre zu befürchten, dass unterschiedliche landesrechtliche Behandlungen gleicher Lebenssachverhalte (zum Beispiel unterschiedliche Anforderungen an die von den Betreibern Kritischer Infrastrukturen zu treffenden Sicherheitsvorkehrungen) erhebliche Wettbewerbsverzerrungen und störende Schranken für die länderübergreifende Wirtschaftstätigkeit zur Folge hätten.

III. Erfüllungsaufwand

1. Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein zusätzlicher Erfüllungsaufwand.

2. Erfüllungsaufwand für die Wirtschaft

Hinsichtlich des Erfüllungsaufwands für die Wirtschaft ist zu unterscheiden zwischen Betreibern von Energieversorgungsnetzen und Energieanlagen, bestimmten Telekommunikationsdiensteanbietern und Betreibern von Telekommunikationsnetzen, der Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik), sonstigen Betreibern Kritischer Infrastrukturen sowie Anbietern digitaler Dienste.

Die gematik ist eine GmbH, deren Gesellschafter die Spitzenverbände der Leistungserbringer und Kostenträger im deutschen Gesundheitswesen sind. Dies sind der GKV-Spitzenverband, die Bundesärztekammer, die Bundeszahnärztekammer, der Deutsche Apothekenverband, die Deutsche Krankenhausgesellschaft, die Kassenärztliche Bundesvereinigung sowie die Kassenärztliche Bundesvereinigung.

Der gematik entsteht Erfüllungsaufwand für

- das Betreiben einer Kontaktstelle und
- die Unterstützung des BSI bei der Prüfung der Erfüllung von Sicherheitsanforderungen, soweit dies vom BSI ergänzend verlangt wird.

Betreibern von Energieversorgungsnetzen und Energieanlagen, die als Kritische Infrastruktur im Sinne des BSI-Gesetzes eingestuft wurden (einschließlich der Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes), entsteht Erfüllungsaufwand

für das Betreiben einer Kontaktstelle. Ca. 1550 Betreibern von Energieversorgungsnetzen entsteht durch die Klarstellung von Meldepflichten an das BSI Aufwand, der bisher nicht berücksichtigt wurde. Bei einem Aufwand von 660 EUR pro Fall und höchstens 7 Fällen pro Anbieter und Jahr ergibt sich ein Aufwand von bis zu 7,16 Mio. EUR pro Jahr.

Bestimmten (öffentlichen) Telekommunikationsanbietern entsteht Erfüllungsaufwand für:

- das Betreiben einer Kontaktstelle.

Sonstigen Betreibern Kritischer Infrastrukturen entsteht Erfüllungsaufwand für

- die Unterstützung des BSI bei der Prüfung der Erfüllung von Sicherheitsanforderungen, soweit dies vom BSI ergänzend verlangt wird, und

die Angabe zusätzlicher Informationen im Falle eines grenzüberschreitenden Bezugs von Sicherheitsvorfällen mit erheblicher Auswirkung. Die Angabe zusätzlicher Informationen im Falle eines grenzüberschreitenden Bezugs von Sicherheitsvorfällen führt zu keinen relevanten Mehraufwänden, da das Bundesamt für Sicherheit in der Informationstechnik diese Informationen im Hinblick auf die Bewertung der potentiellen Auswirkungen auf Kritische Infrastrukturen in seinem Meldeformular bereits abfragt.

Ergänzende Prüfungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die zu zusätzlichem Erfüllungsaufwand für die gematik und die sonstigen Betreiber Kritischer Infrastrukturen führen, sind nicht als Regelfall, sondern lediglich im Einzelfall auf Stichprobenbasis bzw. bei begründetem Anlass durchzuführen. Unter der Annahme, dass das zuständige BSI aus der Gesamtheit von prognostizierten max. 2.000 KRITIS-Anlagen nicht mehr als 100 Anlagen pro Jahr vor Ort überprüft und dass eine Vor-Ort-Begleitung durch den KRITIS-Betreiber nicht mehr als bis zu 15.000 EUR kostet (der Schätzung zugrunde liegen bis zu 15 Personentage der Betreiber bei hohem Umfang sicherheitsrelevanter IT), wird der Gesamtaufwand auf maximal 1,5 Millionen EUR abgeschätzt.

Anbietern digitaler Dienste entsteht Erfüllungsaufwand

- für die Sicherung ihrer technischen Einrichtungen durch Maßnahmen unter Berücksichtigung des Stands der Technik,

- für die Einrichtung und Aufrechterhaltung von Verfahren für die Meldung von IT-Sicherheitsvorfällen mit erheblichen Auswirkungen an das BSI und

- durch die Benennung eines Vertreters in einem Mitgliedstaat in der Europäischen Union im Falle, dass sie nicht in einem Mitgliedstaat der Europäischen Union niedergelassen sind.

Für Anbieter digitaler Dienste wird die Verpflichtung zur Einhaltung eines Mindestniveaus an IT-Sicherheit dort zu Mehrkosten führen, wo kein hinreichendes IT-Sicherheitsniveau vorhanden ist. Der hierfür anfallende Aufwand hängt einerseits vom erforderlichen Sicherheitsniveau und andererseits vom jeweiligen Status quo des Normadressaten ab. Verlässliche Angaben zur Zahl der betroffenen Diensteanbieter, die nicht zwingend einen Sitz in einem Mitgliedstaat der EU haben müssen, liegen nicht vor. In einer ersten Annäherung auf der Grundlage der Ergebnisse der Verbändeanhörung am 19. Dezember 2016 wird von 500 bis 1.500 Anbietern mit mehr als 50 Mitarbeitern beziehungsweise einer Bilanzsumme, die 10 Millionen Euro überschreitet, ausgegangen, die ihren Sitz in Deutschland haben. Eine genauere Einschätzung der zahlenmäßig tatsächlich betroffenen Diensteanbieter ist bis zur Festlegung der Durchführungsakte der Kommission, mit denen der Umfang der Sicherheitsanforderungen für die jeweiligen Dienste weiter konkretisiert wird, nicht möglich. Zu den Anbietern digitaler Dienste können auch Bundesunternehmen zählen, soweit sie wirtschaftlich tätig sind und nicht zum Schutz grundlegender staatlicher Funktionen eingerichtet worden sind oder für diese genutzt werden. Unter den Anwendungsbereich fallen zudem Anbieter ohne Sitz in einem Mitgliedstaat der Europäischen Union, soweit sie einen Vertreter in Deutschland benennen. Es wird angenommen, dass diese Zahl relativ gering sein wird. Ferner können ausländische Anbieter zur Sicherung technischer Einrichtungen verpflichtet sein, soweit sie diese in Deutschland betreiben und die Einrichtung für das Angebot eines digitalen Dienstes sicherheitsrelevant ist. Grundsätzlich werden zudem auch alle anderen Diensteanbieter erfasst, die weder einen Sitz in einem Mitgliedstaat der Europäischen Union haben noch dort einen Vertreter benannt haben, aber im Inland entsprechende Dienste anbieten.

Der Aufwand für die Umsetzung von Maßnahmen zur Sicherung technischer Einrichtungen kann zudem auch bezogen auf einzelne Anbieter im Voraus nicht quantifiziert werden, da das erforderliche Sicherheitsniveau erst durch Durchführungsrechtsakte der Kommission festgelegt werden wird. Da Informationstechnik für Betreiber von digitalen Diensten das Kerngeschäft darstellt, und diese zudem durch datenschutzrechtliche Vorgaben bereits zur Gewährleistung eines hinreichenden Niveaus an Datensicherheit verpflichtet sind, ist allerdings davon auszugehen, dass an das IT-Sicherheitsniveau bei digitalen Diensten bereits hohe Anforderungen gestellt und diese bereits umgesetzt werden. Die Umsetzung der Vorgaben der Richtlinie (EU)

2016/1148 sollte danach keine zusätzlichen nennenswerten Kosten nach sich ziehen.

Für das Meldeverfahren ergibt sich der jährliche Erfüllungsaufwand aus

- der Anzahl der meldepflichtigen Unternehmen,
- der Anzahl der meldepflichtigen Vorfälle pro Jahr und pro Unternehmen sowie
- dem Aufwand pro Meldung.

Der Adressatenkreis der entsprechenden Verpflichtungen kann derzeit nicht konkret eingegrenzt und eine entsprechende Zahl meldepflichtiger Anbieter digitaler Dienste nicht benannt werden, da hierzu keine Erhebungen vorliegen. Auf der Grundlage der Ergebnisse der Verbändebeteiligung am 19. Dezember 2016 wird geschätzt, dass von den Regelungen für digitale Dienste in Deutschland zwischen 500 und 1.500 Unternehmen betroffen sein werden. Dies hängt jedoch auch von der späteren Schwellenwertfestsetzung der Durchführungsakte der Kommission ab. Unter der Annahme, dass pro Betreiber und Jahr sieben Meldungen eines schweren Sicherheitsvorfalls erfolgen und unter Ansatz einer Kostenschätzung von 660 Euro pro Meldung (vgl. Begründung zum Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl 2015, Teil I Nr. 31, S. 1324)) ergeben sich so Gesamtkosten für die Meldepflicht digitaler Dienste in Höhe von rund 4,6 Mio. EUR Euro. Kostenmindernd könnte sich auswirken, dass aufgrund datenschutzrechtlicher Vorgaben Meldestrukturen bereits vorhanden sein müssen.

Die Verpflichtung zum Betreiben einer Kontaktstelle wird bei ca. 300 Betreibern von öffentlichen Telekommunikationsnetzen, Energieversorgungsnetzen und Energieanlagen (einschließlich der Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes), die als Kritische Infrastruktur im Sinne des BSI-Gesetzes eingestuft wurden, sowie bei den Energieversorgungsnetzen und bei der gematik zu einem gewissen Mehraufwand führen, soweit dort noch keine entsprechende Kontaktstelle vorhanden ist. Die Kosten hierfür hängen von der konkreten Ausgestaltung der Erreichbarkeit durch den Betreiber ab. Faktisch sind diese Betreiber aber auch heute schon verpflichtet, Informationen zur IT-Sicherheit auszuwerten und in ihren Prozessen zu berücksichtigen, sodass der Mehraufwand im Wesentlichen in der formalen Benennung einer Kontaktstelle gegenüber dem BSI besteht.

3. Erfüllungsaufwand der Verwaltung

Der Verwaltung entsteht für die Erfüllung der im Gesetz vorgesehenen zusätzlichen Aufgaben ein Aufwand von insgesamt 185,5 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 14,216 Millionen Euro.

Davon ist beim BSI ein Erfüllungsaufwand in Höhe 181,5 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 13,909 Millionen Euro und beim Bundesministerium des Innern (BMI) ein Erfüllungsaufwand in Höhe von 4 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 420.000 Euro zu berücksichtigen. Beim BSI werden in geringem Umfang zusätzliche Sachkosten entstehen, die aus dem Haushalt des BSI getragen werden können.

Infolge des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl 2015, Teil I Nr. 31, S. 1324) erhielt das BSI Ressourcen als zentrale Anlaufstelle für Betreiber Kritischer Infrastrukturen. Der im Weiteren aufgeführte Erfüllungsaufwand entsteht darüber hinaus und aufgrund der Umsetzung der NIS-Richtlinie.

Als neue Aufgaben für das BSI kommen hinzu:

- Unterstützung der Kritischen Infrastrukturen und Bundesbehörden durch die Einrichtung von Mobile Incident Response Teams (MIRTs) (§ 5a BSIG):

In der heutigen Bedrohungslage sind präventive Schutz- und Abwehrmaßnahmen alleine nicht ausreichend, sondern müssen durch reaktive Maßnahmen ergänzt werden. Dazu zählt eine möglichst schnelle und sachkundige Zurückführung angegriffener Systeme und Netze in einen „sauberen“ Zustand, um die weitere Nutzbarkeit und Sicherheit der betroffenen Systeme und Netze sicherzustellen. Das BSI richtet hierzu Mobile Incident Response Teams (MIRTs) ein. Dadurch wird es möglich betroffenen Behörden der Bundesverwaltung, sowie weiterer Bedarfsträger wie andere Verfassungsorgane oder die Betreiber Kritischer Infrastrukturen, bei der Bewältigung von Sicherheitsvorfällen zu unterstützen. Zur Wahrnehmung dieser Aufgabe sind nach derzeitigem Stand ein Aufwuchs auf 63 Planstellen/Stellen zu realisieren.

- Neue Aufgaben und Befugnisse in Bezug auf Anbieter von Digitalen Diensten:

Durch die NIS-Richtlinie werden erstmalig die Anbieter von digitalen Diensten (Online-Marktplätze, Online-Suchmaschinen und Cloud Computing-Dienste, ca. 1000 Anbieter) innerhalb der EU verpflichtet, geeignete technische und organisatorische Maßnahmen zu treffen, um die Risiken der Netz- und Informationssysteme zu bewältigen. Dem BSI ist jeder erhebliche Sicherheitsvorfall zu melden und es erhält die Befugnis, Sicherheitskonzepte anzufordern, zu prüfen und die Beseitigung festgestellter Mängel zu verlangen.

Den Verpflichtungen unterliegen nicht nur Anbieter digitaler Dienste mit Hauptsitz oder Vertretung in Deutschland, sondern zusätzlich auch Anbieter weltweit, soweit sie Dienste in einem Mitgliedstaat innerhalb der Europäischen Union anbieten. Die

Aufgaben des BSI bezogen auf diese Anbieter aus Drittstaaten ergeben sich hier soweit diese Netz- und Informationssysteme in Deutschland nutzen, sowie grundsätzlich im Rahmen der internationalen Zusammenarbeit und Koordinierung.

Das Meldewesen des BSI wird auf die Anbieter Digitaler Dienste ausgeweitet. Eingehende Meldungen nach § 8c Absatz 3 BSIG sind zu bewerten und ggf. entsprechende Produkte (z. B. Warnmeldungen, Lagebilder) zu erstellen und anzupassen.

Weiterhin müssen anlassbezogen die IT-Sicherheitskonzepte der Anbieter Digitaler Dienste angefordert und bewertet werden. Gleiches gilt für bekannt gewordene Anhaltspunkte sowie Feststellungen der zuständigen Behörden anderer Mitgliedstaaten nach § 8c Absatz 4 und 5 BSIG.

Zur Ausführung der neuen Aufgaben ist spezielles Hintergrundwissen in Bezug auf die jeweiligen digitalen Dienste, das europäische und internationale Regelungs- und Marktumfeld sowie die entsprechende technische Expertise (insbesondere zur Bewertung des Stands der Technik) zwingend erforderlich. Der erforderliche Personalbedarf in Höhe von 51 Planstellen/Stellen ermöglicht den Aufbau, die ständige Aktualisierung und Pflege der Wissensbasis und der notwendigen Fachexpertise als Grundlage für die geforderte Bewertung, Unterstützung und Zusammenarbeit sowie die operative Umsetzung der Aufgaben in Bezug auf die Anbieter Digitaler Dienste.

- Erweiterung der Befugnisse des BSI bezüglich KRITIS:

Die Erweiterung der Befugnisse zur Kontrolle der Umsetzung angemessener technischer und organisatorischer Vorkehrungen zur Vermeidung von Störungen der relevanten IT-Systeme nach § 8a Absätze 3 und 4 BSIG über die Betreiber Kritischer Infrastrukturen und der Telematik-Infrastruktur führt zu einem Bedarf von 20 Planstellen/Stellen.

- Ausdehnung der Meldepflichten auf alle Energienetze:

Aufgrund des Gesetzes wird der Kreis der meldepflichtigen Betreiber um ca. 1.600 Anlagenbetreiber (§ 11 Absatz 1c EnWG) ausgeweitet. Dies führt zu einem erheblichen Aufgabenzuwachs des BSI als Kontaktstelle für die Bereiche des TKG, EnWG und SGB V. Zur sachgerechten Durchführung der ausgedehnten Registrier- und Meldepflichten für Energienetze und -anlagen werden zusätzlich 21,5 Planstellen/Stellen benötigt.

- Ausbau der internationalen Zusammenarbeit mit den Kritischen Infrastrukturen (§ 8b BSIG) und der digitalen Dienste (§ 8c BSIG) sowie Berichtswesen (§ 13 BSIG)

Für die operative grenzüberschreitende Zusammenarbeit und zum Informationsaustausch über grenzüberschreitende IT-Störungen, der Erfüllung der Berichtspflichten gegenüber der Kommission, die Bestimmung der Kritischen Infrastrukturen mit grenzübergreifendem Versorgungsgebiet sowie die fachliche Unterstützung der Koordinierung und der Angleichung von Vorgaben auf europäischer Ebene benötigt das BSI insgesamt 9,5 Planstellen/Stellen.

- Erweiterung der Bußgeldvorschriften nach dem Gesetz über Ordnungswidrigkeiten (OWIG) für Anbieter Digitaler Dienste, Betreiber von Energienetzen und -anlagen, der Telematikinfrastruktur im Gesundheitswesen sowie damit zusammenhängender Dienste

Ein zusätzlicher Bedarf in Höhe von 10 Planstellen/Stellen entsteht, um die Verfolgung und Bearbeitung von Ordnungswidrigkeiten als zuständige Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 OWiG nach § 14 Absatz 1 BSIG, § 95 Absatz 5 Satz 2 EnWG und § 307 Absatz 4 SGB V auch im Bereich der Anbieter Digitaler Dienste, der Betreiber von Energienetzen und -anlagen und der Telematikinfrastruktur im Gesundheitswesen sowie damit zusammenhängender Dienste sicherzustellen.

- Unterstützung der Länder (§ 3 Absatz 1 und § 13a BSIG)

Mit der vorgesehenen Änderung von § 3 Absatz 1 und § 13a BSIG darf das BSI die Länder auf deren Ersuchen nunmehr umfassender unterstützen. Es handelt sich insoweit um einen spezialgesetzlich geregelten Fall der Amtshilfe, bei dem das BSI den Landesbehörden seine technische Expertise bei der Bewältigung ihrer (landes-) gesetzlichen Aufgaben zur Verfügung stellt. Hierfür entsteht ein Gesamtaufwand für die Einrichtung einer koordinierenden Geschäftsstelle von 6,5 Planstellen/Stellen.

Beim BMI entsteht ein Erfüllungsaufwand von insgesamt 4 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 420.000 Euro. Die zusätzlichen Aufgaben des BSI erfordern den Aufbau einer entsprechend qualifizierten und quantitativ ausreichenden Fachaufsicht. Des Weiteren werden durch die Umsetzung der Richtlinie vier neue Gremien auf EU-Ebene geschaffen, von denen drei (NIS-Expertengruppe, NIS-Committe, NIS-Kooperationsgruppe) durch BMI besetzt werden müssen.

Der Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen soll finanziell und stellenmäßig im jeweiligen Einzelplan ausgeglichen werden.

Den Länder und Kommunen entsteht Erfüllungsaufwand insbesondere durch die Anpassung der Aufsichtsbefugnisse des BSI und die Ausweitung von Registrierung und

Meldepflichten. Der den Länder und Kommunen entstehende Erfüllungsaufwand ist derzeit nicht bezifferbar.

IV. Weitere Kosten

Betreibern Kritischer Infrastrukturen können im Sonderfall nach § 8a Absatz 3 Satz 3 BSIG Kosten entstehen, soweit berechtigte Zweifel an der ordnungsgemäßen Einhaltung der ihnen obliegenden Sicherheitsanforderungen bestehen, die eine zusätzlich Überprüfung vor Ort erforderlich machen.

V. Gleichstellungspolitische Relevanz

Die Regelungen sind inhaltlich geschlechtsneutral und damit ohne gleichstellungspolitische Relevanz. § 1 Absatz 2 des Bundesgleichstellungsgesetzes, der verlangt, dass Rechts- und Verwaltungsvorschriften des Bundes die Gleichstellung von Frauen und Männern auch sprachlich zum Ausdruck bringen sollen, wurde in die Entwicklung der Gesetzesformulierung miteinbezogen. Gleichzeitig wurde aber auch die Diktion der jeweils zu ändernden Stammgesetze mitberücksichtigt.

VI. Nachhaltigkeit

Der Gesetzentwurf entspricht dem Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der nationalen Nachhaltigkeitsstrategie.

VII. Demographie-Check

Von dem Vorhaben sind keine demographischen Auswirkungen − d.h. Auswirkungen unter anderem auf die Geburtenentwicklung, Altersstruktur, Zuwanderung, regionale Verteilung der Bevölkerung oder das Generationenverhältnis − zu erwarten.

VIII. Vereinbarkeit mit europäischem Recht und völkerrechtlichen Verträgen

Der Gesetzentwurf ist mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen vereinbar. Er dient der Umsetzung der NIS-Richtlinie.

IX. Befristung und Evaluierung

Eine Befristung ist nicht vorgesehen, da der Gesetzentwurf der Umsetzung der NIS-Richtlinie dient, die unbefristet gilt. Der Gesetzentwurf soll anhand der Konzeption zur Evaluierung neuer Regelungsvorhaben gemäß dem Arbeitsprogramm bessere

Rechtsetzung der Bundesregierung vom 28. März 2012, Ziffer II. 3. maximal fünf Jahre nach Inkrafttreten evaluiert werden.

B. Besonderer Teil

Zu Artikel 1 (Änderung des BSI-Gesetzes)

Zu Nummer 1 (Änderung des § 2 BSIG)

Die ursprünglich in § 2 Absatz 9 BSIG enthaltene Definition des Begriffs „Datenverkehr“ ist entbehrlich, da dieser Begriff im BSIG nicht weiter verwendet wird. Die Einfügung eines neuen Absatzes 9 dient der Umsetzung der NIS-Richtlinie. Mit den Änderungen wird der Katalog in § 2 um eine neue Definition der digitalen Dienste gemäß Artikel 4 Nummer 5 und 6 sowie Nummer 17 bis 19 der NIS-Richtlinie ergänzt. Gleichzeitig wird der Anwendungsbereich der Vorgaben, die für die genannten Dienste gelten gemäß Artikel 18 der NIS-Richtlinie auf Anbieter eingegrenzt, die einen dieser Dienste innerhalb der Europäischen Union zur Nutzung bereitstellen. Die für digitale Dienste geltenden Vorgaben sind also unabhängig davon anwendbar, ob der Anbieter in einem der Mitgliedstaaten der Europäischen Union niedergelassen ist oder nicht. Dienste, die von einer natürlichen Person oder von Kleinstunternehmen oder kleinen Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission angeboten werden, sind von der Anwendung der Vorgaben ausgenommen. Damit wird Artikel 16 Absatz 11 der NIS-Richtlinie entsprochen, der den Anwendungsbereich der für digitale Dienste geltenden Regelungen entsprechend zwingend begrenzt. Die für Anbieter digitaler Dienste in den Artikeln 16 bis 18 der NIS-Richtlinie niedergelegten Mindestanforderungen und Meldepflichten gelten nach Artikel 1 Absatz 3 der NIS-Richtlinie nicht für Unternehmen, die den Anforderungen der Artikel 13a und 13b der Richtlinie 2002/21/EG unterliegen, Unternehmen, die ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen unterliegen daher nicht der Anwendung der für digitale Dienste anwendbaren Vorgaben.

Online-Marktplätze im Sinne des Absatz 9 Nr. 1 sind nur solche Online Dienste, die es Verbrauchern und Unternehmern im Sinne der Richtlinie Artikels 4 Absatz 1 Buchstabe a beziehungsweise Buchstabe b der Richtlinie 2013/11/EU über alternative Streitbeilegung in Verbraucherangelegenheiten ermöglichen, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmern abzuschließen, und dabei der endgültige Bestimmungsort für den Abschluss dieser Verträge sind (s. Erwägungs-

grund 15 der NIS-Richtlinie). Ausgenommen sind daher Online-Dienste, die lediglich den Zugang zu dritten Diensten vermitteln, bei denen ein Vertrag letztlich geschlossen werden kann, wie beispielsweise Online-Dienste, die Angebote für bestimmte Produkte oder Dienste bei verschiedenen Unternehmern lediglich vergleichen und den Nutzer anschließend an den bevorzugten Anbieter weiterleiten. Unternehmer des Absatz 9 Nr. 1 ist grundsätzlich jede natürliche oder juristische Person unabhängig davon, ob sie in privatem oder öffentlichem Eigentum steht, die zu Zwecken handelt, die ihrer gewerblichen, geschäftlichen, handwerklichen oder beruflichen Tätigkeit zugerechnet werden können. (s. Art. 4 der Richtlinie über alternative Streitbeilegung in Verbraucherangelegenheiten). Ausgenommen, sind allerdings nichtwirtschaftliche Dienstleistungen von allgemeinem Interesse, die vom Staat oder im Namen des Staates ohne Entgelt erbracht werden, unabhängig von der Rechtsform, durch die diese Dienstleistungen erbracht werden. Nichtwirtschaftliche Dienstleistungen sind Dienstleistungen, die nicht für eine wirtschaftliche Gegenleistung erbracht werden (s. Erwägungsgrund 13 der Richtlinie über alternative Streitbeilegung in Verbraucherangelegenheiten).

Online-Suchmaschinen im Sinne des Absatzes 9 Nr. 2 ermöglichen es Nutzern, Suchen grundsätzlich auf beliebigen in einer oder verschiedenen Sprachen verfassten Websites anhand einer Abfrage zu einem beliebigen Thema vorzunehmen. Ausgenommen sind daher Online-Dienste und Funktionen in IT-Anwendungen, die Suchen jeweils nur auf bestimmte Websites oder Domains ermöglichen. Hierzu zählen auch Online-IT-Verfahren der Verwaltung wie zum Beispiel IT-Verfahren des Bundes und der Länder inklusive der Kommunen, deren Kernaufgabe die Recherche in Datenbeständen anderer IT-Verfahren der vorgenannten Verwaltungen ist. die Angebote für bestimmte Produkte oder Dienste bei verschiedenen Unternehmern lediglich vergleichen und den Nutzer anschließend an den bevorzugten Anbieter weiterleiten (s. Erwägungsgrund 16 der NIS-Richtlinie)..

Cloud-Computing-Dienste im Sinne des Absatzes 9 Nr. 3 umfassen eine breite Palette von Tätigkeiten, die den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen. Zu diesen Rechenressourcen zählen Ressourcen wie Netze, Server oder sonstige Infrastruktur, Speicher, Anwendungen und Dienste. Skalierbar sind Rechenressourcen, die unabhängig von ihrem geografischen Standort vom Anbieter des Cloud-Computing-Dienstes flexibel zugeteilt werden können, um Nachfrageschwankungen zu bewältigten. Mit dem Begriff „elastischer Pool“ werden Cloud-Computing-Dienste auf solche Dienste beschränkt, die Rechenressourcen entsprechend der Nachfrage bereitstellen und freigegeben, so dass die für den Nutzer verfügbaren Ressourcen je nach Arbeitsaufkommen rasch auf- bzw. abgebaut werden können. Der Begriff „gemeinsam nutzbar“ wird verwen-

det, um Rechenressourcen zu beschreiben, die einer Vielzahl von Nutzern bereitgestellt werden, wobei jedoch die Verarbeitung für jeden Nutzer separat erfolgt, obwohl der Dienst von derselben elektronischen Einrichtung erbracht wird (s. Erwägungsgrund 17 der NIS-RL).

Mit Halbsatz 2 wird klargestellt, dass Dienste, die zum Schutz grundlegender staatlicher Funktionen eingerichtet worden sind oder für diese genutzt werden, keine digitalen Dienste im Sinne des Absatzes 11 Nummer 1 bis 3 sind. Ausgenommen ist daher zum Beispiel die Nutzung von Cloud-Diensten durch die Landes- oder Bundesverwaltung(z.B. die sogenannte „Bundescloud“). Diese Ausnahme ist auf Artikel 1 Absatz 6 der NIS-Richtlinie gestützt, nach dem Maßnahmen zum Schutz grundlegender staatlicher Funktionen, insbesondere Maßnahmen zum Schutz der nationalen Sicherheit, einschließlich Maßnahmen zum Schutz von Informationen, deren Preisgabe nach Erachten der Mitgliedstaaten der Europäischen Union ihren wesentlichen Sicherheitsinteressen widerspricht, und Maßnahmen zur Aufrechterhaltung von Recht und Ordnung, insbesondere zur Ermöglichung der Ermittlung, Aufklärung und Verfolgung von Straftaten, von der Richtlinie nicht berührt werden.

Zu Nummer 2 (Änderung des § 3 BSIG)

Mit der Einfügung einer neuen Nummer 13a in § 3 Absatz 1 Satz 2 BSIG wird der Tatsache Rechnung getragen, dass auch in den für die Gefahrenabwehr primär zuständigen Bundesländern vermehrt nichtpolizeiliche Stellen mit der Abwehr von IT-Gefahren befasst sind oder sein können. Generell ist für die Länder in § 3 Absatz 1 Satz 2 Nummer 14 BSIG lediglich eine Beratung oder Warnung in Fragen der Sicherheit in der Informationstechnik vorgesehen. Eine Unterstützung durch das BSI ist nach § 3 Absatz 2 BSIG auf die Sicherung der eigenen Informationstechnik der Länder beschränkt. Allein Polizeien oder Strafverfolgungsbehörden werden gemäß § 3 Absatz 1 Satz 2 Nummer 13 BSIG insoweit bei ihrer sonstigen Aufgabenwahrnehmung unterstützt. Mit der Änderung darf das Bundesamt die Länder auf deren Ersuchen nunmehr umfassender unterstützen. Es handelt sich insoweit um einen spezialgesetzlich geregelten Fall der Amtshilfe, bei dem das BSI den Landesbehörden seine technische Expertise bei der Bewältigung ihrer (landes-) gesetzlichen Aufgaben zur Verfügung stellt.

Mit der Ergänzung der Nummer 13 Buchstabe b) wird klargestellt, dass es auch zu den Aufgaben des Bundesamtes gehört, den Militärischen Abschirmdienst zu unterstützen der im Geschäftsbereich des Bundesministeriums der Verteidigung anstelle des Bundesamtes für den Verfassungsschutz die Aufgaben des Verfassungsschutzes wahrnimmt und damit Funktionsträger des Verfassungsschutzes ist. Er soll vom Bundesamt auf die gleiche Weise wie die übrigen Verfassungsschutzbehörden des

Bundes und der Länder unterstützt werden dürfen, wenn Angriffe auf die IT-Systeme des Bundesministeriums der Verteidigung bzw. der Bundeswehr in seinen gesetzlichen Aufgabenbereich fallen.

Die Änderung in Nummer 17 dient der Umsetzung der NIS-Richtlinie. Mit der Änderung werden die Aufgaben des BSI als zentrale Stelle für die Sicherheit in der Informationstechnik auf digitale Dienste nach § 2 BSIG erweitert.

Mit der Ergänzung der Nummer 18 werden Maßnahmen, die von sogenannten Mobile Incident Response Teams (MIRTs) durchgeführt werden, in den Aufgabenkatalog des BSI-Gesetzes aufgenommen. Mit den MIRTs soll das Bundesamt andere Stellen bei der Wiederherstellung ihrer IT-Systeme bei Cyber-Angriffen unterstützen. Die Sicherheit informationstechnischer Systeme von Stellen des Bundes und von Betreibern Kritischer Infrastrukturen gehört bereits heute zum Aufgabenkreis des Bundesamtes (§ 3 Absatz 1 Satz 2 Nummer 2 und § 3 Absatz 3 BSIG). Die Unterstützung von Stellen des Bundes und von Betreibern Kritischer Infrastrukturen ist hierin bereits enthalten. Da die Befugnisse der MIRTs aber nach dem in diesem Gesetzentwurf vorgesehenen § 5a Absatz 1 BSIG erstmals geregelt werden und in Ausnahmefällen auch anderen Einrichtungen zu Gute kommen sollen, wird die Aufgabe insgesamt noch einmal ausdrücklich festgeschrieben.

Zu Nummer 3 (Änderung des § 5 Absatz 5 und 6 BSIG)

Durch das zunehmende Bedrohungspotential im Cyber-Raum müssen auch die entsprechenden Weitergabebefugnisse von Informationen regelmäßig überprüft werden. Die Vorfälle der jüngsten Vergangenheit haben gezeigt, dass die bisherigen Befugnisse des BSI in diesem Zusammenhang den Anforderungen einer zunehmend digitalisierten Gesellschaft nicht mehr gerecht werden. Eine Informationsweitergabe über die Vorschriften des BVerfSchG ist nicht mehr zeitgemäß. Die hierdurch entstehende verzögerte Informationsweitergabe kann die Auswirkungen eines Cyber-Vorfalles erheblich steigern. Daher stellt die Stärkung des Informationsaustausches zwischen den relevanten Bundesbehörden auch eine Maßnahme der Cyber-Sicherheitsstrategie 2016 für Deutschland dar. Bei den Änderungen handelt es sich lediglich um die Möglichkeit zur Informationsweitergabe. Es wird keine Regelübermittlung eingeführt.

Durch die Änderung des § 5 Abs. 5 und 6 werden rechtsklare Regelungen für Übermittlungen vom Bundesamt an den Militärischen Abschirmdienst, der gleichermaßen Funktionsträger des Verfassungsschutzes ist, und an den Bundesnachrichtendienst geschaffen. Die Möglichkeit der Übermittlung des Bundesamts an den Militärischen Abschirmdienst schließt dabei insbesondere eine Lücke, die bei elektronischen An-

griffen auf den Geschäftsbereich des Bundesministeriums der Verteidigung besteht. Eine verzugslose und unmittelbare Überstellung von Daten zu Angriffen auf den Geschäftsbereich Bundesministeriums der Verteidigung ist hier für die Bearbeitung der IT-Abschirmung des Militärischen Abschirmdienstes unerlässlich und muss ohne Zeitverluste unmittelbar vom Bundesamt an den MAD erfolgen.

Dies ist auch für den BND notwendig. Der BND ist für die Erkennung und Begegnung von Angriffen aus dem Cyberraum zuständig (§§ 3 Abs. 1 Satz 1 Nr. 8, 5 Abs. 1 Satz 3 Nr. 8 G10). Sofern das BSI im Rahmen der Gefahrenabwehr entsprechende Informationen zu Angriffen i.S.d. § 5 Abs. 1 Satz 3 Nr. 8 G10 oder zu Straftaten nach § 3 Abs. 1 Satz 1 Nr. 8 G10 erhält, sind diese an den BND weiterzuleiten. Der BND nutzt diese Information im Rahmen seiner Zuständigkeit ebenfalls zur Gefahrenabwehr – eine Zweckänderung liegt insofern hier nicht vor.

Zu Nummer 4 (neuer § 5a BSIG - Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen)

Die NIS-Richtlinie sieht in Kapitel II in Verbindung mit Anhang 1 zur Richtlinie vor, dass die Mitgliedstaaten der Europäischen Union über angemessene technische und organisatorische Fähigkeiten zur Prävention, Erkennung, Reaktion und Abschwächung von Sicherheitsvorfällen und Risiken bei Netz- und Informationssystemen verfügen und wirksame und kompatible Fähigkeiten zur Bewältigung von Sicherheitsvorfällen und Risiken gewährleisten (s. Erwägungsgrund 34).

Mit dem neuen § 5a BSIG wird die rechtliche Grundlage näher konkretisiert, auf der das BSI die erforderlichen Maßnahmen zur Unterstützung und Wiederherstellung der Sicherheit oder Funktionsfähigkeit der von Cyber-Angriffen betroffenen informationstechnischen Systeme von Stellen des Bundes oder von Betreibern einer Kritischen Infrastruktur sowie (in Ausnahmefällen) von anderen Einrichtungen mit MIRTs treffen kann. Die notwendige Koordination mit anderen Behörden erfolgt unter Wahrung der verfassungsrechtlichen Grenzen im Nationalen Cyber-Abwehrzentrum.

Zwar kann das Bundesamt im Rahmen seiner ihm in § 3 BSIG zugewiesenen Aufgaben (vergleiche insbesondere § 3 Absatz 1 Satz 2 Nummer 1 und § 3 Absatz 3 BSIG) auf Einwilligungsbasis und nach allgemeinem Datenschutzrecht bereits jetzt von Cyber-Attacken betroffene Stellen des Bundes und Betreiber Kritischer Infrastrukturen mit MIRTs vor Ort unterstützen und beraten.

Es können im Rahmen einer Maßnahme der MIRTs aber auch Maßnahmen erforderlich werden, die nicht von einer Einwilligung der betroffenen Einrichtung abgedeckt werden, da sie mit Eingriffen in das Fernmeldegeheimnis verbunden sind. Dies ist etwa der Fall, wenn zur Wiederherstellung der betroffenen Systeme der Netzwerk-

verkehr der betroffenen Einrichtungen analysiert werden muss. Hierfür ist zum einen eine ausdrückliche rechtliche Grundlage erforderlich; zum anderen sind die entsprechenden Eingriffsschwellen und der Schutz personenbezogener Daten ausdrücklich zu regeln, um eine klare Rechtsgrundlage für die Maßnahmen der MIRTs zu schaffen.

Durch Absatz 1 soll das BSI mit MIRTs künftig verstärkt auch operative Unterstützung bei der Bewältigung von Sicherheitsvorfällen bei Stellen des Bundes und bei Betreibern Kritischer Infrastrukturen leisten können. Voraussetzung ist, dass es sich um einen herausgehobenen Fall handelt. Dabei wird das Bundesamt nur auf Ersuchen der betroffenen Einrichtung tätig, da die MIRTs primär der Unterstützung der betroffenen Einrichtung dienen. Deshalb soll der betroffenen Einrichtung die Entscheidung überlassen werden, ob sie die Dienste des Bundesamtes in Anspruch nimmt. Wegen des zunehmenden Bedrohungspotentials und des damit verbundenen herausragenden öffentlichen Interesses an der Sicherheit der von § 5a BSIG erfassten Betroffenen, werden erste Maßnahmen zur Schadensbegrenzung und Sicherstellung des Notbetriebes vor Ort nicht kostenpflichtig sein. Hierdurch wird gewährleistet, dass von einem Hilfeersuchen nicht aus Kostengründen abgesehen wird. Zur Klarstellung wird in Absatz 5 darauf hingewiesen, dass der Betroffene die Kosten für den Einsatz qualifizierter Dritter selbst zu tragen hat. Die Unterstützung des Bundesamtes dient alleine der schnellen Wiederherstellung der Sicherheit der betroffenen informationstechnischen Systeme und soll keine günstige Alternative zur Beauftragung kommerzieller IT-Dienstleister darstellen.

Aufgabe der MIRTs ist dabei zunächst die kurzfristige Unterstützung der betroffenen Einrichtung bei der Schadensbegrenzung und der Sicherstellung eines Notbetriebes vor Ort. Danach sollen die Betroffenen aber auch bei der forensischen Untersuchung des Vorfalles, der Beseitigung der Ursachen und damit der Wiederherstellung des Normalbetriebes unterstützt werden dürfen. Dies kann vor Ort oder aber z. B. auch im BSI erfolgen. Insbesondere forensische Arbeiten werden im Regelfall im BSI selbst erfolgen.

Die Möglichkeit eines Einsatzes der MIRTs des BSI entbindet die um Unterstützung ersuchenden Einrichtungen jedoch nicht von der Pflicht, sich eigenständig auf Sicherheitsvorfälle vorzubereiten. Insbesondere werden die MIRTs nur dann tätig, wenn die Stelle oder der Betreiber einer Kritischen Infrastruktur nicht mit eigenen Mitteln in der Lage ist, die Vorfälle zu bewältigen. Die Ausgestaltung als „Kann-Regelung“ stellt klar, dass eine Pflicht des BSI zum Tätigwerden nicht besteht. Hieraus folgt, dass ein Ersuchender keinen Anspruch auf ein Tätigwerden des BSI hat, sondern dem BSI ein Ermessensspielraum zusteht.

Die vom BSI zu ergreifenden Maßnahmen können unterschiedlicher Natur sein. Neben Analysen der betroffenen informationstechnischen Systeme und des Netzwerkverkehrs können dazu insbesondere auch aktive Sicherungsmaßnahmen gehören, wie etwa das Blockieren der Netzwerkverbindungen zu den Quellen der Gefährdung (z. B. zu den Kontrollservern des Angreifers oder zu den Ausgangspunkten von DDoS-Angriffen).

In Absatz 2 wird festgelegt, wann ein herausgehobener Fall vorliegt, bei dem um Unterstützung durch die MIRTs des Bundesamtes ersucht werden kann. Ein herausgehobener Fall liegt insbesondere dann vor, wenn es sich um einen Angriff von besonderer technischer Qualität handelt oder die zügige Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems im besonderen öffentlichen Interesse ist.

Angriffe besonderer Qualität liegen etwa dann vor, wenn zumindest der Verdacht auf sogenannte Advanced Persistent Threats besteht, die sich dadurch auszeichnen, dass Standardsicherheitsmaßnahmen zur Abwehr nicht ausreichen. Eine besondere Qualität kann auch sogenannten DDoS-Angriffen zugeschrieben werden, sofern sie mit einer außergewöhnlichen Bandbreite oder Technik ausgeführt werden. Wird zum Beispiel ein Verschlüsselungstrojaner eingesetzt, kann es sein, dass der erste Angriff als außergewöhnlich einzustufen ist; diese Einstufung würde aber für spätere Fälle nicht mehr gelten, wenn in diesen Fällen keine neuen Techniken verwendet wurden und Anleitungen zum Umgang mit den Vorfällen bereits verfügbar sind.

Ein besonderes öffentliches Interesse an der zügigen Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems wird immer dann anzunehmen sein, wenn dessen Ausfall oder Beeinträchtigung spürbare Auswirkungen auf das Gemeinwohl zum Beispiel im Sinne der Versorgung der Allgemeinheit mit kritischen Dienstleistungen, auf die Sicherheit oder auf die Arbeitsfähigkeit von Stellen des Bundes haben kann oder diese aus einem anderen Grund ein gegenwärtiges Anliegen der Allgemeinheit darstellen. Dies ist z. B. dann der Fall, wenn bei Betreibern Kritischer Infrastrukturen ein Ausfall droht, Einrichtungen, von denen potenzielle Gefahren für Leib und Leben der Bevölkerung ausgehen (z. B. Chemieanlagen), angegriffen werden oder staatliche IT-Systeme durch Angreifer kompromittiert sind und dadurch die Funktionsfähigkeit und Vertraulichkeit ihres Handelns nicht mehr sichergestellt ist.

In Absatz 3 ist der Umgang mit den personen- und kommunikationsbezogenen Daten geregelt, die das BSI bei seiner Unterstützung erheben und verarbeiten muss. Zur Analyse eines Cyber-Angriffes müssen Logdaten der betroffenen Systeme und Netze analysiert werden, um den Angriff und die Aktivitäten des Täters nachvollziehen zu

können. Üblicherweise verbleiben Täter nicht nur auf einem IT-System, sondern versuchen, sich im Netz des Angegriffenen auszubreiten. Die Aufklärung eines solchen Angriffs und die Bereinigung der infizierten Systeme können nur mittels umfassender Analyse der Log- und Kommunikationsdaten ermöglicht werden. Die personen- und kommunikationsbezogenen Daten, die das Bundesamt erhoben hat, sind nach Beendigung der Unterstützung zu löschen. Ausnahmen gelten nur dann, wenn die Daten mit Einwilligung der betroffenen Stelle oder entsprechend § 5 Absatz 5 oder 6 BSIG an eine andere Behörde zur Erfüllung ihrer gesetzlichen Aufgaben weitergegeben worden sind. Dies ist im Hinblick auf die Abstimmung des Bundesamtes mit den Sicherheitsbehörden notwendig, die ebenfalls entsprechende Vor-Ort-Teams aufbauen werden. Das in § 5 Absatz 7 und in § 8b Absatz 7 BSIG vorgesehene hohe Datenschutzniveau wird auf § 5a BSIG übertragen. Im Übrigen gelten zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten die Vorgaben des Bundesdatenschutzgesetzes. Für die Unterstützungsleistungen des BSI stellt § 5a BSIG eine Sondernorm dar, die sonstigen Regelungen vorgeht.

Nach Absatz 4 dürfen Informationen, von denen das BSI Kenntnis erlangt, von diesem nur mit Einwilligung des Ersuchenden übermittelt werden, es sei denn, die weiterzugebenden Informationen lassen keine Rückschlüsse auf die Identität des Ersuchenden zu oder die Informationen können entsprechend § 5 Absatz 5 und 6 BSIG übermittelt werden. Diese Regelung dient dem Schutz der Interessen der unterstützten Einrichtung. Sofern die Ergebnisse und Fakten bekannt würden, die bei der Analyse und Wiederherstellung der Sicherheit oder Funktionsfähigkeit der informationstechnischen Systeme erarbeitet wurden, könnten Angreifer daraus wertvolle Informationen für neue Angriffe auf die Sicherheit dieser Systeme erhalten. Außerdem setzt die Einschaltung des BSI das Zutrauen der zu unterstützenden Stellen in die vertrauliche Behandlung des Vorfalles voraus. Da sich allerdings aus den erhobenen und verarbeiteten Daten auch für Strafverfolgungsbehörden, Polizeien und Verfassungsschutzbehörden wichtige Erkenntnisse für ihre Aufgabenwahrnehmung ergeben können, werden zur Übermittlung dieser Daten die bereits bewährten Verfahren nach § 5 Absatz 5 und 6 BSIG übernommen. In diesem Zusammenhang begründen Angriffe, die eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Stelle des Bundes, eines Betreibers einer Kritischen Infrastruktur oder einer vergleichbaren Stelle im Sinne des Absatzes 7 nach sich ziehen, in der Regel zugleich auch den Anfangsverdacht der Begehung von Straftaten oder eine Gefahr für die öffentliche Sicherheit. Satz 3 regelt ferner, dass zum Schutz des öffentlichen Interesses an der Bewältigung der hier in Rede stehenden Sicherheitsvorfälle, der hierfür zu treffenden Maßnahmen sowie der schutzwürdigen Interessen der ersuchenden Stelle oder Einrichtung ein Zugang für Dritte (beispielsweise auf Grundlage des Informationsfreiheitsgesetzes) zu den Akten von Verfahren nach

§ 5a Absatz 1 BSIG ausgeschlossen wird. Soweit das BSI andere Behörden unterstützt, bleibt das Recht auf Informationszugang gegenüber diesen Behörden unberührt.

Absatz 5 stellt klar, dass das Bundesamt nicht nur mit eigenen Mitteln unterstützen kann, sondern mit Zustimmung des Ersuchenden und auf dessen Kosten auch auf externe Unterstützung zurückgreifen darf. Gerade im Hinblick auf die notwendige Verarbeitung personenbezogener und dem Fernmeldegeheimnis unterfallender Daten ist diese Klarstellung erforderlich. Die Einbindung Dritter durch das Bundesamt kann in verschiedenen Formen geschehen. Zum einen kann das Bundesamt selbst externe Experten und Dienstleister mit der Wahrnehmung bestimmter Tätigkeiten beauftragen. Zum anderen kann es aber auch Dritte einbinden, die von der ersuchenden Stelle bestimmt wurden. Es kann mit den Dritten auch Daten austauschen. Hierbei sind die Vorgaben des Absatzes 3 einzuhalten.

Unter den Begriff der Dritten fallen auch natürliche und juristische Personen, die sich im Rahmen einer IT-Sicherheitskooperation mit dem Bundesamt bereiterklärt haben, in Notfällen zu helfen, obwohl sie hierzu nicht verpflichtet sind. Dies werden in der Regel Spezialisten anderer Unternehmen sein, die diese im Wege der gegenseitigen Hilfe und Unterstützung entsenden. Mit dieser Möglichkeit zur Einbindung freiwilliger Helfer aus der Mitte der Wirtschaft wird der Gedanke von der Cyber-Sicherheit als gesamtgesellschaftlicher Aufgabe auch legislativ mit Leben gefüllt. Anders als bei § 3 Absatz 3 BSIG bezieht sich die Regelung im neuen § 5a Absatz 5 BSIG auch explizit nicht nur auf Dritte, die IT-Sicherheitsdienstleistungen anbieten, sondern generell auf qualifizierte Dritte. Dies trägt der Tatsache Rechnung, dass das Ziel der Unterstützung nicht nur die reine Absicherung ist, sondern die Wiederherstellung des sicheren (Regel-)Betriebs des informationstechnischen Systems. Dies gilt insbesondere bei Vorfällen mit Spezial-IT, zu der im BSI keine ausreichenden Fachkenntnisse für eine rasche Unterstützung vorliegen.

Anstelle der oder zusätzlich zur eigenen Unterstützung kann das Bundesamt betroffene Stellen auf qualifizierte Dritte verweisen, die bei der Wiederherstellung der Sicherheit der informationstechnischen Systeme herangezogen werden können. Hintergrund der Regelung ist, dass das Bundesamt nur begrenzte Ressourcen hat. Gleichzeitig fehlt den Betroffenen im akuten Notfall die Zeit für eine Marktsichtung. Daher besteht die Erwartung, dass das Bundesamt zumindest eine Auswahl geeigneter Dienstleister oder sonstiger qualifizierter Dritter benennen kann. Da entsprechende Daten beim Bundesamt ohnehin für die Unterstützung der Betreiber Kritischer Infrastrukturen nach § 3 Absatz 3 BSIG zusammengestellt werden müssen, sollen diese Daten auch im Übrigen Verwendung finden können. Die Auswahl des Dritten obliegt der betroffenen Stelle selbst.

In Anlehnung an § 8b Absatz 6 BSIG sieht § 5a Absatz 6 BSIG vor, dass das Bundesamt die Hersteller der betroffenen informationstechnischen Systeme auffordern kann, bei der Analyse und Wiederherstellung der Sicherheit oder Funktionsfähigkeit mitzuwirken. Insbesondere wenn die IT-Sicherheit durch eine Sicherheitslücke in der verwendeten Hard- oder Software gefährdet wird, kann in erster Linie der Hersteller des jeweiligen Produktes schnell und nachhaltig zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit beitragen – etwa durch das zeitnahe Bereitstellen eines Sicherheitspatches. Aus Gründen der Verhältnismäßigkeit darf der Hersteller nicht zur kostenlosen Mitwirkung herangezogen werden, wenn die ersuchende Stelle Soft- oder Hardware einsetzt, deren Supportzeitraum bereits abgelaufen ist, und der Hersteller das Ende des Supportzeitraumes rechtzeitig angekündigt hat. In diesem Fall hat die ersuchende Einrichtung dem Hersteller die entstandenen Kosten zu ersetzen. Die Mitwirkungspflicht des Herstellers bleibt davon unberührt.

In Absatz 7 wird dem BSI die Möglichkeit eingeräumt, in begründeten Einzelfällen auch andere Einrichtungen bei der Analyse und Wiederherstellung der Sicherheit oder Funktionsfähigkeit ihrer informationstechnischen Systeme zu unterstützen. Ein begründeter Einzelfall liegt dann vor, wenn (neben den sonstigen Voraussetzungen des Absatzes 1) ein vergleichbares öffentliches Interesse an der Behebung des Sicherheitsvorfalls besteht, auch wenn die betroffene Einrichtung nicht zu dem Adressatenkreis des Absatzes 1 zählt. Zwar soll der Einsatz der MIRTs primär auf den Adressatenkreis des Absatzes 1 beschränkt bleiben. Dem BSI soll aber die Möglichkeit eröffnet werden, ausnahmsweise auch in anderen Fallkonstellationen tätig werden zu können. Dies kann etwa dann der Fall sein, wenn Anlagen oder Systeme von Unternehmen, welche sich in der staatlichen Geheimschutzbetreuung befinden, angegriffen werden oder Anlagen oder Systeme von Organisationen betroffen sind, deren Ausfall oder Beeinträchtigung ähnlich weitreichende Auswirkungen hätte wie der Ausfall Kritischer Infrastrukturen. Solche Auswirkungen können etwa bei erfolgreichen Angriffen auf Unternehmen mit besonderem Sicherheitsbezug oder besonderem Gefahrenpotenzial (z. B. Unternehmen der chemischen Industrie) oder auf große Konzerne sowie deren Zulieferer eintreten. Durch die starke Vernetzung und moderne Just-in-Time-Lieferungen wirken sich erfolgreiche Angriffe nicht nur auf das unmittelbar angegriffene, sondern auf viele assoziierte Unternehmen aus. Aufgrund der erheblich schädigenden Auswirkungen von Betriebsausfällen auf die Wertschöpfung in der gesamten Bundesrepublik und des drohenden Verlusts einiger zehntausend Arbeitsplätze wäre das Gemeinwohl in ähnlich starkem Ausmaß gefährdet. In Betracht kommen aber auch Einrichtungen, deren besondere politische, wirtschaftliche oder gesellschaftliche Bedeutung im Fall eines erheblichen Angriffs staatliches Eingreifen erforderlich erscheinen lässt.

Mit dem neuen Absatz 8 wird eine angemessene Berücksichtigung von Aspekten der nuklearen Sicherheit durch die Einbeziehung der Aufsichtsbehörden gewährleistet. Eine Regelung ist notwendig, um die besonderen Belange im Atomrecht sowie der damit verbundenen Gewährleistung der nuklearen Sicherheit und nuklearen Sicherung von kerntechnischen Anlagen und Tätigkeiten sowie des Geheimschutzes zu berücksichtigen. Daher ist insbesondere in Fällen der Absätze 1, 4, 5 und 7 vor Tätigwerden des BSI das Benehmen mit den zuständigen atomrechtlichen Aufsichtsbehörden des Bundes und der Länder herzustellen, da unmittelbare Auswirkungen auf Sicherungsmaßnahmen nach dem Atomgesetz möglich sind. Da Sicherungsmaßnahmen auf Grundlage des Atomgesetzes in der Regel auch dem Geheimschutz unterliegen, ist auch aus diesem Grund das Benehmen mit den atomrechtlich zuständigen Aufsichtsbehörden herzustellen. Hierdurch soll eine gegenseitige Beeinflussung von jeweils in unterschiedlichen Rechtsgebieten zuständigen Behörden vermieden werden. Analog zu der mit Inkrafttreten des IT-Sicherheitsgesetzes vom 17. Juli 2015 (BGBl. I S. 1324) eingeführten Regelung im Energiewirtschaftsgesetz haben aus den oben genannten Gründen die Vorgaben aufgrund des Atomgesetzes zur nuklearen Sicherheit und nuklearen Sicherung kerntechnischer Anlagen und Tätigkeiten sowie des Geheimschutzes Vorrang.“

Zu Nummer 5 (Änderung des § 7a BSIG)

Im Rahmen der Analyse und Wiederherstellung der Sicherheit und Funktionsfähigkeit informationstechnischer Systeme nach § 5a BSIG muss das Bundesamt auch die Möglichkeit haben, diese Systeme vollständig zu untersuchen, erforderlichenfalls auch mittels Reverse-Engineering. Um Auslegungsfragen zur Reichweite der bestehenden Regelung vorzubeugen, wird dies mit der Änderung des § 7a Absatz 1 Satz 1 BSIG klargestellt.

Zu Nummer 6 (Änderung des § 8a BSIG)

Die Änderungen des § 8a Absatz 3 BSIG und der neu eingefügte Absatz 4 dienen der Umsetzung von Artikel 15 der NIS-Richtlinie. Nach Artikel 15 Absatz 2 der NIS-Richtlinie muss die zuständige Behörde die Umsetzung der organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit Kritischer Infrastrukturen maßgeblich sind, überprüfen und von den Betreibern Kritischer Infrastrukturen verlangen können, dass sie die zur Bewertung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen, einschließlich der dokumentierten Sicherheitsmaßnahmen, zur Verfügung stellen. Der Nachweis für eine wirksame Umsetzung der Sicherheitsmaßnahmen kann wie bisher durch einen qualifizierten Prüfer erbracht werden, der die Anforderungen nach Absatz 5 erfüllt. Für

diesen Fall ist in Artikel 15 Absatz 2 Buchstabe b) der NIS-Richtlinie vorgesehen, dass neben den Ergebnissen der Überprüfung durch einen qualifizierten Prüfer auch die diesen zugrunde gelegten Nachweise verlangt werden können.

Das BSI kann derzeit die von den Betreibern Kritischer Infrastrukturen zu treffenden Sicherheitsmaßnahmen nur überprüfen, soweit diese konkrete Mängel anzeigen. Nach Artikel 15 der NIS-Richtlinie muss dies zukünftig auch unabhängig hiervon möglich sein. Die Betreiber müssen derzeit zudem nur eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen (einschließlich der dabei aufgedeckten Sicherheitsmängel) vorlegen.

Mit den Änderungen in Absatz 3 Satz 3 und der Einfügung des neuen Satzes 4 wird die Nachweispflicht der Betreiber Kritischer Infrastrukturen entsprechend angepasst. Mit den Änderungen in Satz 3 wird klargestellt, dass die vorzulegende Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen auch die Ergebnisse ausweisen muss. Mit dem neuen Satz 4 wird dem BSI die Möglichkeit eröffnet, ergänzend die Vorlage der Dokumente, die die Maßnahmen nach Absatz 1 belegen und daher den Überprüfungen zugrunde gelegt wurden, zu verlangen. Eine Ausweitung der zweijährigen Nachweispflicht für die Betreiber ist hiermit nicht verbunden. Damit im Rahmen der Überprüfung durch die Betreiber nach Absatz 3 die Einhaltung der Anforderungen nach Absatz 1 hinreichend belegt werden kann, sollen der Überprüfung Dokumente z. B. zur Risikoanalyse ebenso zugrunde gelegt werden, wie z. B. solche zur Dokumentation der nach Absatz 1 ergriffenen konkreten Maßnahmen oder bereits vorgefundene Ergebnisse von Teilprüfungen (z. B. Zertifizierungen). Zu diesen Dokumenten zählen z. B. IT-Sicherheitskonzepte, Prozessdokumentationen, Continuity-Management- und Notfallkonzepte.

Mit dem neuen Absatz 4 wird dem BSI eine Befugnis zum Betreten der Einrichtungen des Betreibers Kritischer Infrastrukturen und zur Einsichtnahme in die für den Nachweis der Erfüllung der Anforderungen nach Absatz 1 relevante Dokumentation und zur Begutachtung der getroffenen Umsetzungsmaßnahmen beim Betreiber eingeführt. Das Bundesamt wird so in die Lage versetzt, unabhängig von der Anzeige konkreter Mängel durch den Betreiber zu bewerten, ob die Betreiber ihren Pflichten nach Absatz 1 der Vorschrift nachkommen. Der neue Absatz 4 dient damit ebenfalls der effektiven Umsetzung von Artikel 15 Absatz 1 und 2 der NIS-Richtlinie. Die Einräumung eines Betretungsrechts unter Wahrung der grundrechtlichen Anforderungen sowie der Verhältnismäßigkeit dient der Umsetzung des Auftrags an die Mitgliedstaaten nach Artikel 15 der NIS-Richtlinie, eine effektive Kontrolle der Einhaltung der Anforderungen nach Artikel 14 der NIS-Richtlinie sicherzustellen. Für die Betreiber stellt die Einsichtnahme vor Ort in der Regel eine geringere Belastung dar als die Vorlage der gesamten und umfassenden Dokumentation der Sicherheitsmaßnahmen. Das

Bundesamt wird gleichzeitig in die Lage versetzt, den notwendigen Umfang und die tatsächliche Umsetzung der einzuhaltenden Maßnahmen zu überprüfen. Von der Möglichkeit zur Einsichtnahme beim Betreiber soll unter anderem dann Gebrauch gemacht werden, wenn die Prüfung der vom Betreiber nach § 8a Absatz 3 Satz 1 vorgelegten Nachweise in begründeten Einzelfällen nicht ausreichend ist. Nach Satz 1 kann sich das Bundesamt bei der Prüfung der Einhaltung der Anforderungen nach Absatz 1 einer qualifizierten Stelle bedienen. Qualifizierte Stelle im Sinne der Vorschrift können unter anderem nach § 9 Absatz 3 BSIG anerkannte Stellen sein, soweit sie über die notwendige Expertise und Neutralität verfügen. Dies sind z. B. vom BSI zertifizierte IT-Sicherheitsdienstleister wie Penetrationstester oder Grundschutz-Auditoren. Da die Umsetzung der Anforderungen nach Absatz 1 und der entsprechende Nachweis in der Verantwortung des Betreibers liegen, ist es sachgerecht und verhältnismäßig, dass dieser nach Satz 3 in Fällen berechtigter Zweifel an der ordnungsgemäßen Einhaltung die Kosten für eine zusätzlich erforderliche Einsichtnahme trägt.

Zu Nummer 7 (Änderung des § 8b BSIG)

Die Einfügung eines neuen Buchstaben d in § 8b Absatz 2 Nummer 4 BSIG dient der Umsetzung von Artikel 14 Absatz 5 der NIS-Richtlinie, der die Unterrichtung der zuständigen Behörden in einem anderen Mitgliedstaat der Europäischen Union vorsieht, soweit ein gemeldeter Vorfall erhebliche Auswirkungen auf die Verfügbarkeit wesentlicher Dienste in diesem Mitgliedstaat hat. Zuständige Behörden in einem anderen Mitgliedstaat der Europäischen Union sind die zentralen Anlaufstellen im Bereich der Netz- und Informationssicherheit, die nach Artikel 8 Absatz 3 der NIS-Richtlinie jeder Mitgliedstaat der Europäischen Union zu benennen hat und die nach Artikel 8 Absatz 4 der NIS-Richtlinie als Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit dienen. Gemäß Artikel 8 Absatz 7 der NIS-Richtlinie veröffentlicht die Kommission eine Liste der benannten zentralen Anlaufstellen. Die Feststellung erheblicher Auswirkungen in einem anderen Mitgliedstaat erfolgt auf der Grundlage der Angaben des betroffenen Betreibers.

Die Änderung in Absatz 3 dient der Klarstellung. Die Pflicht zur Registrierung der Kontaktstellen betrifft ausschließlich Betreiber, die eine Kritische Infrastruktur im Sinne der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) betreiben.

Die Änderung in Absatz 4 Satz 1 dient der Umsetzung von Artikel 14 Absatz 3 und 4 der NIS-Richtlinie. Das Erheblichkeitskriterium bezieht sich danach nicht auf den Grad des IT-Vorfalls, sondern auf den Grad der Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur. Dies wird durch die Änderung nachgezogen.

Mit der Änderung des Absatzes 4 Satz 2 wird bei den zu meldenden Angaben statt auf die Branche des Betreibers auf die von ihm erbrachten kritischen Dienstleistungen Bezug genommen. Die Vorschrift wird damit an die Systematik der NIS-Richtlinie angepasst, nach deren Artikel 14 die Meldepflicht an Auswirkungen auf einzelne Dienste anknüpft; zudem wird die in § 10 Absatz 1 BSIG bereits entsprechend angelegte Systematik zur Bestimmung Kritischer Infrastrukturen abgebildet, die innerhalb der jeweiligen Sektoren nicht zwischen Branchen, sondern zwischen kritischen Dienstleistungen unterscheidet. Gleichzeitig wird der zu meldende Inhalt auf diejenigen Auswirkungen auf die Dienstleistungserbringung bezogen, die bereits zum Zeitpunkt der Meldung bekannt waren.

Die weiteren Änderungen in Absatz 4 Satz 2 dienen der Umsetzung des Artikels 14 Absatz 3 der NIS-Richtlinie. Darin ist vorgesehen, dass Meldungen der Betreiber Kritischer Infrastrukturen die Informationen enthalten müssen, die es der zuständigen Behörde ermöglichen, zu bestimmen, ob ein Sicherheitsvorfall grenzüberschreitende erhebliche Auswirkungen hat. Das BSI wird so in die Lage versetzt, seiner Verpflichtung zur Unterrichtung der zuständigen Behörden in einem anderen Mitgliedstaat der Europäischen Union nach Absatz 2 Buchstabe d nachzukommen. Betreiber sollten bei den Angaben zu erheblichen Auswirkungen in einem anderen Mitgliedstaat insbesondere die in Artikel 14 Absatz 3 der NIS-Richtlinie genannten Parameter berücksichtigen.

Zu Nummer 8 (Einfügen eines neuen § 8c BSIG - Besondere Anforderungen an Anbieter digitaler Dienste)

Der neu eingefügte § 8c BSIG dient der Umsetzung der Vorgaben der NIS-Richtlinie für Anbieter digitaler Dienste und der damit verbundenen Aufsicht durch das BSI. Mit Absatz 1 werden die Vorgaben des Artikels 16 Absatz 1 und 2 der NIS-Richtlinie umgesetzt.

Mit Absatz 2 werden die Vorgaben des Artikels 16 Absatz 3 und 4 der NIS-Richtlinie umgesetzt, mit denen eine Pflicht zur Meldung von Sicherheitsvorfällen, die erhebliche Auswirkungen auf die Bereitstellung eines digitalen Dienstes haben, eingeführt wird. Die Sätze 2 und 4 stellen klar, dass Form und Verfahren der Meldepflicht sowie die genauere Bestimmung der Parameter zur Feststellung, wann ein Sicherheitsvorfall erhebliche Auswirkungen auf die Bereitstellung eines digitalen Dienstes hat, gemäß Artikel 16 Absatz 8 und 9 der NIS-Richtlinie durch Durchführungsrechtsakte der Kommission näher bestimmt werden. Mit Satz 5 wird die Verpflichtung aus Artikel 16 Absatz 6 der NIS-Richtlinie umgesetzt. Danach sind zuständige Behörden eines anderen Mitgliedstaats der Europäischen Union über gemeldete Sicherheitsvorfälle zu unterrichten, soweit diese Auswirkungen in diesem Mitgliedstaat haben. Zuständige

Behörden eines anderen Mitgliedstaats der Europäischen Union sind die zentralen Anlaufstellen im Bereich der Netz- und Informationssicherheit, die nach Artikel 8 Absatz 3 der NIS-Richtlinie jeder Mitgliedstaat der Europäischen Union zu benennen hat und die nach Artikel 8 Absatz 4 der NIS-Richtlinie als Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit dienen. Gemäß Artikel 8 Absatz 7 der NIS-Richtlinie veröffentlicht die Kommission eine Liste der benannten zentralen Anlaufstellen.

Absatz 3 beinhaltet die in Artikel 17 der NIS-Richtlinie vorgesehene Befugnis zu Aufsichts- und Kontrollmaßnahmen, soweit Anbieter digitaler Dienste den in den Absätzen 1 und 2 vorgesehenen Pflichten nachweislich nicht oder nur unzureichend nachgekommen sind. Als Nachweise gelten auch Feststellungen, die dem BSI von den zuständigen Behörden eines anderen Mitgliedstaats der Europäischen Union vorgelegt werden. Auf diese Weise wird eine angemessene Kontrolle und Aufsicht für die Fälle sichergestellt, in denen der Ort der Hauptniederlassung und die Netz- und Informationssysteme, die im Rahmen der Bereitstellung der angebotenen digitalen Dienste genutzt werden, in unterschiedlichen Mitgliedstaaten der Europäischen Union belegen sind.

Anbieter digitaler Dienste unterliegen den Sicherheitsanforderungen, wenn sie einen digitalen Dienst zur Nutzung innerhalb der Bundesrepublik Deutschland bereitstellen oder, soweit sie einen digitalen Dienst ausschließlich in einem oder mehreren anderen Mitgliedstaat der Europäischen Union zur Nutzung bereitstellen, wenn sie ihren Hauptsitz in der Bundesrepublik Deutschland haben oder dort Netz- und Informationssysteme betreiben, die sie im Rahmen der Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen.

Zu Nummer 9 (Änderung und Neunummerierung des § 8d BSIG)

Mit den Änderungen in § 8d (neu) Absatz 1 BSIG wird ein redaktionelles Versehen bei dem Verweis auf die Empfehlung 2003/361/EC der Kommission korrigiert.

Mit der Ergänzung des Absatzes 2 Nummer 2 wird eine redaktionelle Klarstellung zur Reichweite der Ausnahme vorgenommen.

Die Änderung in Absatz 3 dient der Umsetzung von Artikel 5 Absatz 5 sowie Artikel 9 Absatz 1 in Verbindung mit Anhang 1 Absatz 2 Buchstabe a der NIS-Richtlinie. Bisher müssen Kontaktstellen nicht von den in § 8d (neu) Absatz 3 Nummer 1 bis 4 genannten Betreibern benannt werden. Mit der Änderung in Absatz 3 wird die Verpflichtung zur Benennung einer Kontaktstelle in § 8b Absatz 3 BSIG auf diese Betreiber ausgeweitet. Die Änderung dient dazu, die Bereitstellung der nach Artikel 5 Absatz 7 Buchstabe c der NIS-Richtlinie geforderten Informationen der Betreiber zu ermögli-

chen und eine Ausgabe von Warnungen bzw. die Verbreitung von Informationen gemäß Artikel 9 in Verbindung mit Anhang 1 Absatz 2 Buchstabe a sicherzustellen. Eine Übermittlung von Daten, die eine Identifizierung einzelner Betreiber ermöglichen, findet nicht statt. Zusätzlich wird den spezialgesetzlich zur Meldung verpflichteten Betreibern die Möglichkeit eingeräumt, eine gemeinsame Ansprechstelle nach § 8b Absatz 5 BSIG zu benennen.

Anbieter digitaler Dienste unterliegen den Sicherheitsanforderungen, wenn sie einen digitalen Dienst zur Nutzung innerhalb der Bundesrepublik Deutschland bereitstellen oder, soweit sie einen digitalen Dienst ausschließlich in einem oder mehreren anderen Mitgliedstaaten der Europäischen Union zur Nutzung bereitstellen, wenn sie ihren Hauptsitz in der Bundesrepublik Deutschland haben oder dort Netz- und Informationssysteme betreiben, die sie im Rahmen der Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen. Mit Absatz 4 wird klargestellt, dass die Meldepflichten nach dem neuen § 8c Absatz 2 dann nicht greifen, wenn Meldungen durch Anbieter bereits an die zuständige Behörde eines anderen Mitgliedstaats der Europäischen Union erfolgen, weil er dort seinen Hauptsitz oder, soweit er nicht in einem Mitgliedstaat der Europäischen Union niedergelassen ist, einen Vertreter in einem anderen Mitgliedstaat der Europäischen Union benannt hat, in dem die digitalen Dienste ebenfalls angeboten werden. Gleichzeitig wird klargestellt, dass der neue § 8c Absatz 3 für diese Anbieter nur gilt, soweit sie in der Bundesrepublik Deutschland Netz- und Informationssysteme betreiben, die sie im Rahmen der Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen. Der Gerichtsstand richtet sich nach den allgemeinen Vorschriften. Zur Bestimmung des Gerichtsstands ist danach an den Hauptsitz beziehungsweise an die Vertretung des Diensteanbieters anzuknüpfen; bei Anbietern aus Drittstaaten im Übrigen, wenn ein digitaler Dienst im Inland angeboten wird.

Zu Nummer 10 (Änderung und Neunummerierung des § 8e BSIG)

Mit den Änderungen in § 8e (neu) Absatz 1 BSIG wird der Anwendungsbereich der zu Kritischen Infrastrukturen bestehenden Spezialregelung im Sinne von § 1 Absatz 3 des Informationsfreiheitsgesetzes auf Anbieter digitaler Dienste nach § 8c ausgeweitet. Damit soll dem Schutz der insbesondere im Meldeverfahren zu übermittelnden hochsensiblen Informationen hinreichend Rechnung getragen werden. Zugleich werden die Regelungen des Artikels 16 Absatz 7 der NIS-Richtlinie zur Wahrung der Vertraulichkeit der von den Betreibern und Anbietern gemeldeten Informationen umgesetzt.

Für den Bereich der Kritischen Infrastrukturen bestehen entsprechende Vorgaben in Artikel 14 Absatz 6 der NIS-Richtlinie. Mit der Neufassung des Absatzes 2 wird si-

chergestellt, dass die Sicherheit und Sicherung von Kritischen Infrastrukturen bei der Gewährleistung von Akteneinsichtsrechten nicht beeinträchtigt werden. Mit dem neu eingefügten Absatz 3 wird klargestellt, dass die Vertraulichkeitsregelungen auch für Betreiber gelten, die spezialgesetzlich geregelten Pflichten unterliegen.

Zu Nummer 11 (Änderung des § 10 BSIG)

Mit dem neuen § 10 Absatz 4 BSIG wird die Ermächtigung zum Erlass einer Rechtsverordnung geschaffen, soweit dies für die Umsetzung der Durchführungsrechtsakte der Kommission nach Artikel 16 Absatz 8 und 9 der NIS-Richtlinie erforderlich ist. Die Erforderlichkeit ist nur gegeben, wenn und soweit die Herstellung der vollen Anwendbarkeit und Durchführung der Kommissionsrechtsakte ergänzender nationalen Bestimmungen bedarf und der Anwendungsvorrang des Unionsrechts einer nationalen Regelung nicht entgegensteht. Die betreffenden Bestimmungen werden im Einvernehmen mit den betroffenen Ressorts festgelegt. Hierzu gehören die Ressorts, die in § 13 Absatz 3 genannt sind, sowie gegebenenfalls weitere betroffene Ressorts.

Zu Nummer 12 (Änderung des § 11 BSIG)

Die Änderung dient der Wahrung des Zitiergebotes nach Artikel 19 Absatz 1 Satz 2 GG im Hinblick auf die Eingriffe in das Fernmeldegeheimnis, die mit den Analyse- und Wiederherstellungsmaßnahmen des BSI nach § 5a BSIG einhergehen.

Zu Nummer 13 (Einfügung eines neuen § 13 Absatz 3 bis 5 BSIG)

Die neu in § 13 BSIG eingefügten Absätze 3 und 4 dienen der Umsetzung von Artikel 5 der NIS-Richtlinie.

Mit dem neuen Absatz 3 werden die Pflichten zur Berichterstattung an die Kommission im nationalen Recht festgeschrieben. Die in Absatz 3 Nummer 1 bis 3 genannten Informationen sind der Kommission gemäß Artikel 5 Absatz 7 der NIS-Richtlinie bis zum 9. November 2018 und danach alle zwei Jahre zu übermitteln, damit diese die Umsetzung der Richtlinie bewerten kann, insbesondere, ob die Mitgliedstaaten der Europäischen Union bei der Ermittlung der Betreiber Kritischer Infrastrukturen einen einheitlichen Ansatz verfolgen. Die Informationen nach den Nummern 1 und 2 beinhalten insbesondere die in der Verordnung nach § 10 Absatz 1 BSIG festgelegten Dienstleistungen und Schwellenwerte. Die nach Nummer 3 bereitzustellenden Informationen umfassen eine zahlenmäßige Zusammenfassung der Betreiber für jeden der in Anhang II zur NIS-Richtlinie genannten Sektoren, soweit dies nicht zu einer Identifizierbarkeit einzelner Betreiber, Einrichtungen oder Anlagen führt. Die Übermittlung von Listen einzelner Betreiber zu Einrichtungen oder Anlagen, die als Kritische Infrastrukturen eingestuft sind, ist ausgeschlossen. Soweit die Kommission

technische Leitlinien nach Artikel 5 Absatz 7 der NIS-Richtlinie erlässt, um zur Bereitstellung vergleichbarer Informationen beizutragen, sind diese nach Maßgabe der Artikel 1 Absatz 5 und 6 der NIS-Richtlinie zu berücksichtigen.

Mit Absatz 4 werden die Vorgaben des Artikels 5 Absatz 4 der NIS-Richtlinie umgesetzt, der eine gegenseitige Konsultationspflicht der Mitgliedstaaten der Europäischen Union vorsieht, soweit bestimmte Einrichtungen kritische Dienstleistungen in mehr als einem Mitgliedstaat erbringen. Die Neuregelung sieht vor, dass Konsultationen nach Bekanntwerden der grenzüberschreitenden Erbringung von Dienstleistungen aufgenommen werden müssen. Damit wird sichergestellt, dass die vorgesehene gegenseitige Information und Abstimmung zum frühestmöglichen Zeitpunkt beginnt.

Absatz 5 dient der Umsetzung der Berichtspflichten nach Artikel 10 Absatz 3 Satz 2 der NIS-Richtlinie, mit dem die Mitgliedstaaten der Europäischen Union verpflichtet werden, der mit Artikel 11 der NIS-Richtlinie einzurichtenden Kooperationsgruppe der Mitgliedstaaten bis zum 9. August 2018 und dann jährlich zu den eingegangenen Meldungen nach den Artikeln 14 und 16 der NIS-Richtlinie zu berichten. Die vorzulegenden Berichte müssen einen zusammenfassenden Überblick über die eingegangenen Meldungen, einschließlich der Anzahl der eingegangen Meldungen, sowie die Art der gemeldeten Sicherheitsvorfälle enthalten. Dabei ist die Vertraulichkeit der Meldungen und der Betreiber und Anbieter digitaler Dienste zu wahren. Kann die Vertraulichkeit der Meldungen und der Betreiber und Anbieter im Einzelfall aufgrund der Detailtiefe der zu übermittelnden Informationen oder aus sonstigen Gründen nicht gewährleistet werden, ist die Übermittlung entsprechend einzuschränken. Die vom BSI der Kooperationsgruppe der Mitgliedstaaten vorzulegenden Berichte enthalten teilweise Informationen, die für die Cyber-/IT-Sicherheit Deutschlands von grundsätzlicher Bedeutung sind. Das BMI als Aufsichtsbehörde über das BSI stellt daher vor der Einreichung des Berichts durch das BSI mit den jeweils inhaltlich betroffenen Ressorts Einvernehmen zu den Berichten her.

Zu Nummer 14 (Änderung des § 14 BSIG)

Die Änderungen dienen der Ausweitung der Bußgeldvorschriften auf die Anbieter digitaler Dienste und setzen insofern die Vorgaben des Artikels 21 der NIS-Richtlinie um, nach denen die Mitgliedstaaten der Europäischen Union wirksame, angemessene und abschreckende Sanktionen für Verstöße gegen die nach der Richtlinie erlassenen nationalen Bestimmungen vorsehen und die erforderlichen Maßnahmen treffen müssen, um deren Anwendung sicherzustellen. Die Bußgeldvorschriften sind anwendbar auf alle Anbieter, die digitale Dienste innerhalb der Bundesrepublik Deutschland anbieten, sofern sie nicht ihre Hauptniederlassung in einem anderen Mitgliedstaat der Europäischen Union haben oder, sofern sie nicht in einem anderen

Mitgliedstaat der Europäischen Union niedergelassen sind, dort einen Vertreter benannt haben und in diesem Mitgliedstaat dieselben digitalen Dienste anbieten.

Zu Nummer 15 (neuer § 15 BSIG - Anwendbarkeit der Vorschriften für Anbieter digitaler Dienste)

Mit der Vorschrift wird eine Übergangsregelung zur Anwendbarkeit der Vorschriften getroffen, die die Anbieter digitaler Dienste betreffen. Bezüglich der für diese geltenden Mindestanforderungen und Meldepflichten, der hierzu durchzuführenden Aufsicht und der Sanktionierung von Verstößen sieht die NIS-Richtlinie eine EU-weit einheitliche Regelung und Anwendung vor. Dies schließt auch Regelungen zur zuständigen Stelle und zur gerichtlichen Durchsetzung gegenüber den in der Regel grenzüberschreitend tätigen Anbietern ein. Die der Umsetzung der Artikel 16 bis 18 der NIS-Richtlinie dienenden §§ 8c und 10 Absatz 4 (Verordnungsermächtigung) und § 14 (Sanktionen) sind daher entsprechend der in Artikel 25 der NIS-Richtlinie vorgesehenen Umsetzungsfrist erst ab dem 10. Mai 2018 anwendbar.

Zu Artikel 2 (Änderung des § 44b des Atomgesetzes)

Die neu aufgenommene Regelung in § 8b Absatz 2 Nummer 4 Buchstabe d) BSI-Gesetz dient der Umsetzung von Artikel 14 Absatz 5 der Richtlinie (EU) 2016/1148, der die Unterrichtung der zuständigen Behörden in einem anderen Mitgliedstaat der Europäischen Union vorsieht, soweit ein gemeldeter Vorfall erhebliche Auswirkungen auf die Verfügbarkeit wesentlicher Dienste in diesem Mitgliedstaat hat. Diese Regelung gilt jedoch lediglich für die Dienste, die Gegenstand der EU-Richtlinie sind. Grenzüberschreitende Beeinträchtigungen, die auf Gründen der nuklearen Sicherheit beruhen, sind nicht Gegenstand der Richtlinie. Für diesen Bereich existieren bereits unter EURATOM, im Atomgesetz sowie in bi- und multilateraler Abkommen getroffene Vereinbarungen. Bei erheblichen Störungen in der Anlage eines Genehmigungsinhabers nach § 7 Absatz 1 Atomgesetz, insbesondere, wenn diese grenzüberschreitende Auswirkungen haben können, ist in der Regel davon auszugehen, dass zugleich Schutzziele der nuklearen Sicherheit und Sicherung verletzt sind. Gemäß der Atomrechtlichen Sicherheitsbeauftragten- und Meldeverordnung vom 14. Oktober 1992 (BGBl. I S. 1766) zuletzt geändert durch Artikel 1 der Verordnung vom 8. Juni 2010 (BGBl. I S. 755) sind durch Genehmigungsinhaber nach § 7 Absatz 1 Atomgesetz Störfälle, Unfälle und sonstige für die kerntechnische Sicherheit bedeutsame Ereignisse der zuständigen Aufsichtsbehörde zu melden. Die zugrundeliegenden Meldekriterien sind in Anlage 1 bis 5 der Atomrechtlichen Sicherheitsbeauftragten- und Meldeverordnung aufgeführt. Auf europäischer Ebene beste-

hen Vereinbarungen zur gegenseitigen Information im Falle einer radiologischen Notstandssituation: die Entscheidung des Rates vom 14. Dezember 1987 über Gemeinschaftsvereinbarungen für den beschleunigten Informationsaustausch im Fall einer radiologischen Notstandssituation (87/600/Euratom) und das Abkommen zwischen der Europäischen Atomgemeinschaft (Euratom) und Nichtmitgliedstaaten der Europäischen Union über die Teilnahme an Vereinbarungen in der Gemeinschaft für den schnellen Austausch von Informationen in einer radiologischen Notstandssituation (Ecurie) (2003/C 102/02). Durch die Einfügung in § 44b Satz 2 wird der Verweis zur entsprechenden Anwendung des § 8b Absatz 1, 2 und 7 für Meldeverpflichtungen nach § 44b des Atomgesetzes von kerntechnischen Anlagen (nicht nur Genehmigungsinhabern nach § 7 Absatz 1) dahingehend konkretisiert, dass die im BSI-Gesetz neu eingefügte Regelung in § 8b Absatz 2 Nummer 4 Buchstabe d) nicht anwendbar ist.

§ 44b Satz 4 wird dahingehend ergänzt, dass Meldungen gemäß § 44b, die dem Bundesamt zugegangen sind, nicht nur unverzüglich an die für die nukleare Sicherheit und Sicherung zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder weiterzuleiten sind, sondern auch an die von diesen Stellen bestimmten Sachverständigen nach § 20 Atomgesetz. Damit soll eine zeitnahe Auswertung solcher Meldungen durch die Sachverständigen ermöglicht werden, die in der Regel von den zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder beauftragt werden. Diese Ergänzung dient der Konkretisierung eines Verfahrens im Bereich des Meldewesens nach § 44b, welches in anderen atomrechtlichen Verfahren bereits praktiziert wird.

Zu Artikel 3 (Änderung des § 95 des Energiewirtschaftsgesetzes)

Zu Nummer 1 (Änderung des § 11 EnWG)

Betreiber von Energieversorgungsnetzen und Energieanlagen im Sinne des Energiewirtschaftsgesetzes unterliegen bereits nach den Vorgaben des § 11 EnWG den §§ 8a und 8b BSIG weitgehend vergleichbaren Anforderungen, die den Vorgaben des Artikels 14 Absatz 1 bis 3 der NIS-Richtlinie entsprechen. § 11 Absatz 1a EnWG stellt klar, dass die Telekommunikationssysteme und Datenverarbeitungssysteme der Netzbetreiber so zu schützen sind, dass ein sicherer Netzbetrieb garantiert ist. § 11 Absatz 1b EnWG enthält entsprechende Vorgaben für die Betreiber von Energieanlagen, die in der Rechtsverordnung nach § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden. Nach § 11 Absatz 1c EnWG unterliegen Betreiber von Energieversorgungsnetzen und von Energieanlagen oder Teilen davon, die

aufgrund der Rechtsverordnung gemäß § 10 Absatz 1 BSIG als Kritische Infrastruktur eingestuft wurden, einer Meldepflicht an das BSI als zentraler Meldestelle für Betreiber Kritischer Infrastrukturen. Die Bundesnetzagentur als für die Sicherheitsstandards des Netzbetriebs zuständige Behörde überwacht die Einhaltung der jeweiligen Sicherheitsstandards.

§ 11 Absatz 1c EnWG wird nun dahingehend geändert, dass Betreiber von Energieversorgungsnetzen sowie solche Energieanlagen, die durch Rechtsverordnung als Kritische Infrastruktur bestimmt worden sind, zukünftig dem BSI auch Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer erheblichen Beeinträchtigung geführt haben, unverzüglich melden. Diese Änderung in Absatz 1 c dient der Umsetzung von Art. 14 Absatz 3 und 4 der NIS-Richtlinie. Das Erheblichkeitskriterium bezieht sich danach nicht auf den Grad des IT-Vorfalls, sondern auf den Grad der Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur.

Ergänzend wird in § 11 Absatz 1c EnWG klargestellt, dass die Meldepflichten nach Absatz 1c Satz 1 für alle Betreiber von Energieversorgungsnetzen gelten sowie für solche Energieanlagen, die durch Rechtsverordnung als Kritische Infrastruktur bestimmt worden sind. Diese Änderung dient lediglich der Klarstellung der Adressaten der Verpflichtung. Inhaltlich wirkt sich diese rein redaktionelle Änderung nicht aus.

Zu Nummer 2 (Änderung des § 95 EnWG)

Im EnWG waren bisher keine Sanktionen bei Verstößen gegen die Einhaltung von Mindestanforderungen oder die Meldepflicht nach § 11 Absatz 1a bis 1c EnWG vorgesehen. Die Änderungen in § 95 Absatz 1 Nummer 2a und 2b EnWG dienen der Ausweitung der Bußgeldvorschriften auf die gemäß § 11 Absatz 1a und 1b EnWG zur Einhaltung von Sicherheitsanforderungen und Meldepflichten verpflichteten Betreiber und setzen insofern die Vorgaben des Art. 21 der NIS-Richtlinie um, nach denen die Mitgliedstaaten Sanktionen für Verstöße gegen die nach der Richtlinie erlassenen nationalen Bestimmungen vorsehen und die erforderlichen Maßnahmen treffen müssen, um deren Anwendung sicherzustellen. Mit der Änderung in Absatz 5 wird das BSI, an das die Meldungen nach § 11 Absatz 1c zu richten sind, als zuständige Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten bestimmt. Im Übrigen wird die Zuständigkeit der Bundesnetzagentur als zuständige Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten beibehalten.

Zu Artikel 4 (Änderung des Fünften Buches Sozialgesetzbuch)

Zu Nummer 1 (Änderung des § 291b SGB V)

Die gematik als Betreiber der Telematikinfrastruktur nach § 291a Absatz 7 SGB V sowie die Betreiber von Diensten der Telematikinfrastruktur im Hinblick auf die nach § 291b Absatz 1a und 1e SGB V zugelassenen Dienste und die Betreiber von Diensten, soweit sie die Telematikinfrastruktur für nach § 291b Absatz 1b SGB V bestätigte Anwendungen nutzen, unterliegen bereits nach § 291b umfassenden technischen und verfahrensmäßigen Vorgaben, die die Vorgaben des Artikels 14 Absatz 1 bis 3 der NIS-Richtlinie erfüllen. § 291b Absatz 1 SGB V enthält an die gematik gerichtete technische und funktionale Vorgaben, einschließlich der Vorgaben zur Erstellung eines Sicherheitskonzepts und zur Einbeziehung des BSI in die Festlegung der Vorgaben für den sicheren Betrieb der Telematikinfrastruktur.

In Absatz 1a ist das für einzelne Komponenten und Dienste erforderliche Zulassungsverfahren geregelt. In den Absätzen 1b bis 1e sind die weiteren Rahmenbedingungen für den Betrieb und die Nutzung der Telematikinfrastruktur geregelt, mit denen die Erfüllung des Auftrags der Gesellschaft für Telematik, den Betrieb und die Nutzung der Telematikinfrastruktur gegenüber den Betreibern von Diensten der Telematikinfrastruktur und den Betreibern von Diensten, die die Telematikinfrastruktur für nach § 291b Absatz 1b SGB V bestätigte Anwendungen nutzen, sicherzustellen, gewährleistet wird. In Absatz 6 Satz 2 bis 4 ist eine Pflicht zur Meldung erheblicher Störungen für die Betreiber vorgesehen. Zentrale Meldestelle ist das BSI; an das BSI hat die Gesellschaft für Telematik Meldungen der Betreiber von Diensten der Telematikinfrastruktur und der Betreiber von Diensten, die die Telematikinfrastruktur für nach § 291b Absatz 1b SGB V bestätigte Anwendungen nutzen, unverzüglich weiterzuleiten.

Die gematik sowie die Betreiber von Diensten der Telematikinfrastruktur im Hinblick auf die nach § 291b Absatz 1a und 1e SGB V zugelassenen Dienste und Betreiber von Diensten, soweit sie die Telematikinfrastruktur für nach § 291b Absatz 1b SGB V bestätigte Anwendungen nutzen, unterliegen zudem bereits einer Aufsicht, die teilweise den Vorgaben des Artikel 15 der NIS-Richtlinie entspricht. Nach Artikel 15 Absatz 1 und 2 der NIS-Richtlinie muss die zuständige Behörde die Umsetzung der organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit Kritischer Infrastrukturen maßgeblich sind, überprüfen können und von den Betreibern Kritischer Infrastrukturen verlangen können, dass sie die zur Bewertung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen, einschließlich der Dokumentation der Sicherheitsmaßnahmen, zur Verfügung stellen. Der Nachweis für eine wirksame Umsetzung der Sicherheitsmaßnahmen kann wie bisher durch einen qualifizierten Prüfer erbracht werden, der die Anforde-

rungen nach Absatz 4 erfüllt. Für diesen Fall sieht die NIS-Richtlinie vor, dass neben den Ergebnissen der Überprüfung durch einen qualifizierten Prüfer auch die Nachweise verlangt werden können, die diesen Ergebnissen zugrunde gelegt worden sind. Artikel 15 Absatz 3 der NIS-Richtlinie sieht vor, dass die zuständige Behörde den Betreibern verbindliche Anweisungen zur Abhilfe der festgestellten Mängel erteilen kann.

Im Rahmen ihres Auftrags, den Betrieb und die Nutzung der Telematikinfrastruktur sicherzustellen, verfügt die gematik über umfassende Aufsichtsbefugnisse gegenüber den Betreibern von Diensten der Telematikinfrastruktur und den Betreibern von Diensten, die die Telematikinfrastruktur für nach § 291b Absatz 1b SGB V bestätigte Anwendungen nutzen. Hierzu zählen neben den in den Absätzen 6 und 7 genannten Befugnissen zu Maßnahmen zur Gefahrenabwehr und Überwachung auch die nähere Ausgestaltung der Zulassungsverfahren. Die gematik selbst unterliegt hinsichtlich der Umsetzung der für sie als Betreiber der Telematikinfrastruktur nach § 291a Absatz 7 SGB V geltenden Anforderungen und Meldepflichten allerdings nur einer eingeschränkten Aufsicht. Hierzu zählt insbesondere auch die Einbindung des BSI bereits bei der Erstellung von Vorgaben für den sicheren Betrieb der Telematikinfrastruktur, die nach Absatz 1 im Einvernehmen zu erfolgen hat, und der Zulassung von Komponenten und Diensten nach Absatz 1a.

Die Festlegung der Vorgaben und der Kriterien für das Bestätigungsverfahren für Betreiber von Diensten und Anwendungen für die Telematikinfrastruktur, sowie die Vornahme von Maßnahmen zur Gefahrenabwehr und Überwachung nach Absatz 6 und 7 erfolgen durch die gematik allerdings lediglich in Abstimmung mit dem BSI. „In Abstimmung“ bedeutet im Sinne der Vorschriften dabei, dass über ein Stellungnahmerecht hinaus ein Diskussionsprozess mit dem Ziel einer einvernehmlichen Lösung stattfindet. Die Einigung mit dem BSI stellt den Regelfall dar. Im Falle einer Entscheidung gegen die Auffassung des BSI durch die gematik ist diese Entscheidung gesondert und nachvollziehbar zu dokumentieren und zu begründen. Mit dem neuen § 291a Absatz 8 SGB V wird ergänzend sichergestellt, dass das BSI in diesen Fällen die Entscheidung prüfen und entsprechend den Vorgaben in Artikel 15 Absatz 3 der NIS-Richtlinie verbindliche Anweisungen zur Abhilfe der festgestellten Mängel erteilen kann. In Absatz 8 werden insbesondere Sicherheitsmängel betrachtet, die zu einer Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse führen können. Absatz 8 Satz 1 bezieht sich ausschließlich auf sicherheitsrelevante Informationen.

Zu Nummer 2 (Änderung des § 307 SGB V)

Der neu eingefügte § 307 Absatz 1a dient der Ausweitung der Bußgeldvorschriften auf die gemäß § 291b Absatz 6 Satz 2 und 4 SGB V zur Einhaltung von Meldepflichten verpflichteten Betreiber und setzt insofern die Vorgaben des Artikels 21 der NIS-Richtlinie um, nach denen die Mitgliedstaaten der Europäischen Union Sanktionen für Verstöße gegen die nach der Richtlinie erlassenen nationalen Bestimmungen vorsehen müssen und die erforderlichen Maßnahmen treffen müssen, um deren Anwendung sicherzustellen. Mit der Änderung in Absatz 4 wird das BSI, an das die Meldungen nach § 291b Absatz 6 Satz 4 SGB V zu richten sind, als zuständige Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten bestimmt. Die neu eingefügten Absätze 1b und 1c dienen der Ausweitung der Bußgeldvorschriften auf die Anweisungsempfänger gemäß des neuen Absatz 8 Satz 2 und 3.

Zu Artikel 5 (Änderung des § 109 Absatz 5 TKG)

Mit der Änderung wird der Verweis auf Vorschriften des BSIG angepasst (Folgeänderung aufgrund Neunummerierung im BSIG).

Zu Artikel 6 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten des Gesetzes.

Das Gesetz soll maximal fünf Jahre nach Inkrafttreten anhand der Konzeption zur Evaluierung neuer Regelungsvorhaben gemäß dem Arbeitsprogramm bessere Rechtsetzung der Bundesregierung vom 28. März 2012, Ziffer II. 3. evaluiert werden.

Anlage

Stellungnahme des Nationalen Normenkontrollrates gem. § 6 Absatz 1 NKRG

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 (NKR-Nr. 3970, BMI)

Der Nationale Normenkontrollrat hat den Entwurf des oben genannten Regelungsvorhabens geprüft.

I. Zusammenfassung

Bürgerinnen und Bürger	keine Auswirkungen
Wirtschaft	
Jährlicher Erfüllungsaufwand:	13,2 Mio. EUR
davon aus Informationspflichten:	*11,8 Mio. EUR (660 EUR pro Fall)*
Einmaliger Erfüllungsaufwand:	geringfügige Auswirkungen
Verwaltung	
Bund	
Jährlicher Erfüllungsaufwand:	14,3 Mio. EUR
Einmaliger Erfüllungsaufwand:	geringfügige Auswirkungen
Länder	geringfügige Auswirkungen
Umsetzung von EU-Recht	Dem NKR liegen keine Anhaltspunkte dafür vor, dass mit den vorliegenden Regelungen über eine 1:1-Umsetzung von EU-Recht hinausgegangen wird.
‘One in one out’-Regel	Aufgrund der 1:1-Umsetzung von EU-Recht stellt der jährliche Erfüllungsaufwand der Wirtschaft in diesem Regelungsvorhaben kein „In“ im Sinne der ‚One in one out‘-Regel der Bundesregierung dar.
Weitere Kosten	Betreibern kritischer Infrastrukturen können im Sonderfall Kosten in Form von Gebühren und Erstattungen an das BSI entstehen, soweit eine zusätzliche Überprüfung vor Ort erforderlich ist.

Evaluierung	Das Regelungsvorhaben wird anhand der Konzeption zur Evaluierung neuer Regelungsvorhaben gemäß des Arbeitsprogramms bessere Rechtsetzung der Bundesregierung spätestens fünf Jahre nach Inkrafttreten evaluiert. Normenkontrollrat und BMI stimmen darin überein, dass die Evaluierung dieses Regelungsvorhabens zusammen mit der Evaluierung des IT-Sicherheitsgesetzes durchgeführt werden sollte. Der Normenkontrollrat hält es für erforderlich, dabei insbesondere zu prüfen, ob die rechtlichen und untergesetzlichen Maßnahmen in angemessen Verhältnis zum gewonnen Grad an IT-Sicherheit stehen.

Das Ressort hat die Auswirkungen auf den Erfüllungsaufwand insgesamt nachvollziehbar dargestellt. Der Nationale Normenkontrollrat erhebt im Rahmen seines gesetzlichen Auftrags keine Einwände gegen die Darstellung der Gesetzesfolgen in dem vorliegenden Regelungsentwurf.

Der Normenkontrollrat gibt zu bedenken, dass dem BSI bereits durch das IT-Sicherheitsgesetz 220 Stellen zugewiesen wurden, die nun noch einmal um 181,5 Stellen aufgestockt werden. Da es sich im Wesentlichen um denselben Aufgabenraum handelt, regt der Normenkontrollrat an, noch stärker zu prüfen, wie die Aufgabenwahrnehmung so gestaltet werden kann, dass Synergieeffekte erschlossen und der Personalaufwuchs gedämpft werden können.

Neben der Regulierung durch EU- und Bundesrecht, werden Standards und Anforderungen der IT-Sicherheit maßgeblich durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) auf untergesetzlicher Ebene bestimmt. Der Normenkontrollrat hält es bezogen auf das gesamte Politikfeld IT-Sicherheit für erforderlich, dass BMI und BSI auch auf untergesetzlicher Ebene eine aufwandsbewusste Alternativenabwägung durchführen und auch untergesetzliche Maßnahmen bei der Evaluierung dieses Politikfeldes berücksichtigen, um unnötige und unverhältnismäßige Folgekosten zu vermeiden.

Der Normenkontrollrat sieht in der engen Einbeziehung der betroffenen Unternehmen und Verwaltungen bei der Ausgestaltung gesetzlicher, vor allem aber untergesetzlicher Bestimmungen eine besondere Chance, zu praktikableren Lösungen zu kommen, die gleichermaßen wirksam und effizient sind. Analog zu den positiven Erfahren, die zuletzt mit dem „Runden Tisch rechtskonforme E-Akte“ erzielt werden konnten, sollten BMI und BSI auch in anderen Bereichen der IT-Sicherheit Dialogformen mit den Betroffenen finden, die dabei helfen, bei der Definition technischer Richtlinien oder sonstiger untergesetzlicher Vorgaben ein hohes Maß an IT-Sicherheit zu gewährleisten ohne unverhältnismäßigen Aufwand zu verursachen.

II. Im Einzelnen

Im August 2016 trat die 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, die sog. NIS-RL in Kraft. Mit der Richtlinie wurden ein einheitlicher europäischer Rechtsrahmen für den EU-weiten Aufbau nationaler Kapazitäten für die Cyber-Sicherheit, eine stärkere

Zusammenarbeit der Mitgliedstaaten und Mindestanforderungen sowie Meldepflichten für bestimmte Dienste geschaffen. Ziel ist es, einheitliche Maßnahmen festzulegen, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen in der Europäischen Union erreicht werden kann.

Die europarechtlichen Vorgaben werden im Rahmen einer Anpassung des *Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)* sowie bestimmter – für einzelne Branchen mit kritischen Infrastrukturen vorrangiger – Spezialgesetze umgesetzt: *Gesetz über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (AtG), Gesetz über die Elektrizitäts- und Gasversorgung (EnWG), Fünften Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung (SGB V).*

Zur Umsetzung der NIS-RL werden die Befugnisse des BSI zur Überprüfung der Einhaltung der technischen und organisatorischen Sicherheitsanforderungen und die Nachweispflicht der Betreiber um Vorgaben für das Verfahren bei grenzüberschreitenden IT-Sicherheits-Vorfällen angepasst. Ergänzend werden Regelungen zu Mobilen Incident und Response Teams (MIRTs) aufgenommen, mit denen das BSI andere Stellen bei der Wiederherstellung ihrer IT-Systeme unterstützen soll. Zudem werden das BSIG um eine Definition der digitalen Dienste sowie spezielle Regelungen zu Sicherheitsanforderungen, Meldepflichten und Aufsicht im Hinblick auf die Anbieter digitaler Dienste ergänzt und Bußgeldvorschriften angepasst.

Ergänzt wird eine Ermächtigung zum Erlass von Rechtsverordnungen zur Umsetzung der in Art. 16 der Richtlinie (EU) 2016/1148 vorgesehenen Durchführungsrechtsakte. Zusätzlich werden mit dem Gesetzentwurf Klarstellungen, Bereinigungen und Anpassungen zu Unterstützungsaufgaben des BSI vorgenommen.

II.1 Erfüllungsaufwand

Das Ressort hat die Auswirkungen auf den Erfüllungsaufwands nachvollziehbar dargestellt. Die Angaben beruhen im Wesentlichen auf Schätzungen des BSI und Rückmeldungen aus der Verbändeanhörung. Sie orientieren sich zudem an vergleichbaren Aufwandsermittlungen, die bereits für das IT-Sicherheitsgesetz durchgeführt worden sind.

Bürgerinnen und Bürger

Bürgerinnen und Bürger sind nicht betroffen.

Wirtschaft

Die Wirtschaft ist durch die gesetzlichen Maßnahmen wie folgt betroffen:

- Den *Betreibern von Energieversorgungsnetzen und Energieanlagen*, bestimmten *Telekommunikationsanbietern* sowie der *Gesellschaft für Telematikanwendungen* entsteht Aufwand für das Betreiben einer Kontaktstelle. Die Verpflichtung trifft damit ca. 300 Betreiber und wird zu einem gewissen Mehraufwand führen, soweit dort noch keine entsprechende Kontaktstelle vorhanden ist. Diese Betreiber sind jedoch bereits heute schon verpflichtet, Informationen zur IT-Sicherheit auszuwerten und in ihren Prozessen zu berücksichtigen, sodass der Mehraufwand im Wesentlichen in der formalen Benennung einer Kontaktstelle gegenüber dem BSI besteht und insgesamt als marginal anzusehen ist.
- Den *Betreibern von Energieversorgungsnetzen und Energieanlagen* entsteht Aufwand durch die Ausweitung von Meldepflichten an das BSI auf alle Betreiber von Energieversorgungsnetzten (ca. 1.600); während bisher nur ca. 45 als tatsächliche KRITIS-Betreiber eingestufte Netzbetreiber betroffen waren. Bei einem Aufwand von 660 EUR pro Fall und 7 Fällen pro Anbieter und Jahr (Werte wurde im Rahmen des IT-Sicherheitsgesetzes vom 17. Juli 2015 ermittelt) ergibt sich für 1.555 zusätzlich Betroffene ein Aufwand von ca. 7,16 Mio. EUR pro Jahr.
- Der *Gesellschaft für Telematikanwendungen* und *sonstigen Betreibern Kritischer Infrastrukturen* entsteht Aufwand für die Unterstützung des BSI bei der Prüfung der Erfüllung von Sicherheitsanforderungen (Zugang gewähren, Unterlagen bereitstellen, Auskünfte erteilen). Diese Prüfungen erfolgen stichprobenartig bzw. im anlassbezogenen Einzelfall. Bei der Prüfung von ca. 100 Anlagen pro Jahr (ca. 2.000 Anlagen insgesamt) und bei einem Aufwand von geschätzt bis zu 35.000 EUR pro Fall entsteht ein Gesamtaufwand von 3,5 Mio. EUR pro Jahr.
- *Anbietern digitaler Dienste* entsteht Aufwand für die Sicherung ihrer technischen Einrichtungen entsprechend des Stands der Technik. Verlässliche Angaben zur Zahl der betroffenen Anbieter sowie zum Stand des derzeitigen Sicherheitsniveaus liegen nicht vor. In einer ersten Annäherung wird von 500 bis 1.500 betroffenen Anbietern ausgegangen, die ihren Sitz in Deutschland haben. Betroffen sind darüber hinaus auch ausländische Anbieter ohne Sitz in Deutschland. Deren Zahl konnte vom Ressort nicht geschätzt werden.
  Die konkrete Fallzahl und der eigentliche Aufwand für die Umsetzung von Maßnahmen zur Sicherung technischer Einrichtungen sind von der Definition bestimmter Schwellwerte (z.B. Ausfallzeiten, geografische Ausbreitung eines Störfalls) und vom konkret erforderlichen Sicherheitsniveau abhängig. Beides wird jedoch erst durch Durchführungsrechtsakte der Kommission festgelegt werden

(voraussichtlich im Laufe 2017). Da Informationstechnik für Betreiber von digitalen Diensten das Kerngeschäft darstellt, und diese zudem durch datenschutzrechtliche Vorgaben bereits zur Gewährleistung eines hinreichenden Niveaus an Datensicherheit verpflichtet sind, ist allerdings davon auszugehen, dass an das IT-Sicherheitsniveau bei digitalen Diensten bereits hohe Anforderungen gestellt, diese bereits umgesetzt und insofern keine nennenswerten zusätzlichen Kosten entstehen werden.
Aus Sicht des NKR ist es ausreichend, mögliche Aufwände im Zuge der Nachmessung des Erfüllungsaufwands zu erfassen, die vom Statistischen Bundesamt zwei Jahre nach Inkrafttreten turnusmäßig durchgeführt wird.

- *Anbietern digitaler Dienste* entsteht Aufwand für die Einrichtung und Aufrechterhaltung von Verfahren für die Meldung von erheblichen IT-Sicherheitsvorfällen an das BSI. Auch hier wird von ca. 1.000 betroffenen Anbietern ausgegangen. Bei einem Aufwand von 660 EUR pro Fall und 7 Fällen pro Anbieter und Jahr (Werte wurde im Rahmen des IT-Sicherheitsgesetzes vom 17. Juli 2015 ermittelt) ergeben sich Gesamtkosten für die Meldepflicht in Höhe von rund 4,6 Mio. EUR pro Jahr.
- Die Angabe zusätzlicher Informationen im Falle einer grenzüberschreitenden Wirkung von Sicherheitsvorfällen führt bei den *Betreibern Kritischer Infrastrukturen* (ca. 2.000) und den *Anbietern digitaler Dienste* (ca. 1.000) zu keinen relevanten Mehraufwänden, da diese Informationen vom BSI in der Praxis bereits abfragt werden.

Für Klein- und Kleinstunternehmen gelten gewissen Ausnahmen, die für diese Unternehmen zu einer insgesamt geringeren Belastung führen. Diese Ausnahmen sind bereits in der EU-Richtlinie vorgesehen und werden 1:1 ins deutsche Recht übernommen.

Betreibern kritischer Infrastrukturen können im Sonderfall nach § 8a Absatz 3 Satz 3 BSIG Kosten in Form von Gebühren und Erstattungen an das BSI entstehen, soweit berechtigte Zweifel an der ordnungsgemäßen Einhaltung der ihnen obliegenden Sicherheitsanforderungen bestehen, die eine zusätzlich Überprüfung des BSI vor Ort erforderlich machen.

Verwaltung Bund

Bereits durch das IT-Sicherheitsgesetz vom 17. Juli 2015 erhielt das BSI zusätzliches Personal für seine Funktion als zentrale Anlaufstelle für Betreiber Kritischer Infrastrukturen (220 Planstellen, ca. 16 Mio. EUR pro Jahr). Der im Weiteren aufgeführte Erfüllungsaufwand entsteht zusätzlich im Rahmen der Umsetzung der EU-Richtlinie. Es entstehen Personalaufwand in Höhe von jährlich rund 13,9 Mio. EUR (181,5 Stellen) sowie geringfügige Sachkosten.

Der Personalbedarf des BSI begründet sich im Wesentlichen wie folgt. Die Darstellung fasst eine detaillierte Personalbedarfsschätzung zusammen, die dem NKR vorgelegen hat:

- reaktive Maßnahmen für eine schnelle und sachkundige Zurückführung angegriffener Netze in einen „sauberen“ Zustand durch Mobile Incident Response Teams (MIRTs) und Unterstützung der Bundesbehörden bei der Bewältigung von Sicherheitsvorfällen: 63 Stellen
- Neue Aufgaben und Befugnisse in Bezug auf Anbieter von Digitalen Diensten und Ausweitung des BSI-Meldewesens auf diese Anbieter (u.a. Auswertung von Meldungen, Erstellung von Lagebildern und Warnungen, Auswertung von Sicherheitskonzepten der Anbieter) sowie Erweiterung der Grundlagenarbeit und Fachkompetenz im Bereich digitaler Dienste, d.h. Aufbau von Fachexpertise für Funktionsweise und Architektur der jeweiligen digitalen Dienste, zur Auswertung von in der Meldestelle eingehenden Informationen, zum Fortschreiben des Lagebildes und zur Vorhersage der potentiellen Auswirkungen einer Meldung oder Störung auf die betroffene Kritische Infrastruktur oder ihre Branche: 51 Stellen
- Erweiterung der Befugnisse des BSI zur Kontrolle der Umsetzung angemessener technischer und organisatorischer Vorkehrungen zur Vermeidung von Störungen der relevanten IT-Systeme von kritischen Infrastrukturen (KRITIS): 20 Stellen
- Ausdehnung der BSI-Meldepflichten auf alle Energienetze: 21,5 Stellen
- Ausbau der operativen grenzüberschreitende Zusammenarbeit und des Informationsaustauschs über grenzüberschreitende IT-Störungen, Berichtspflichten gegenüber der Kommission, Bestimmung der Kritischen Infrastrukturen mit grenzübergreifendem Versorgungsgebiet sowie fachliche Unterstützung zur Koordinierung und Angleichung von Vorgaben auf europäischer Ebene: 9,5 Stellen
- Bearbeitung von Ordnungswidrigkeiten als zuständige Verwaltungsbehörde: 10 Stellen
- Unterstützung der Länder über eine koordinierende Geschäftsstelle: 6,5 Stellen

Beim BMI entsteht ein Erfüllungsaufwand von insgesamt 4 Planstellen mit Personalkosten in Höhe von jährlich rund 420.000 EUR zur Wahrnehmung der gestiegenen Anforderungen an die Fachaufsicht über das BSI sowie zur Mitwirkung an drei neuen EU-Gremien (NIS-Expertengruppe, NIS-Committe, NIS-Kooperationsgruppe).

Verwaltung Länder (Kommunen)

Den Ländern und Kommunen kann Erfüllungsaufwand durch die Anpassung der Aufsichtsbefugnisse des BSI und die Ausweitung von Registrierungs- und Meldepflichten gegenüber Anbietern Digitaler Dienste entstehen, zu denen auch Anbieter der öffentlichen Hand zählen können. Der den Ländern und Kommunen entstehende Erfüllungsaufwand ist nach Aussage des Ressorts derzeit nicht bezifferbar, da die Zahl möglicherweise betroffener öffentlicher Anbieter Digitaler Dienste nicht bekannt ist. Angesichts verschiedener Ausnahmetatbestände geht das Ressort von wenigen Betroffen und damit von insgesamt geringfügigen Auswirkungen auf die Länder aus. Konkrete Aufwandsschätzungen, die andere Annahmen zulassen, wurden von Seiten der Länder nicht vorgelegt.

II.2 Rechts- und Verwaltungsvereinfachung

Neben der Regulierung durch EU- und Bundesrecht werden Standards und Anforderungen der IT-Sicherheit maßgeblich durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) bestimmt. D.h. auf untergesetzlicher Ebene werden technische Richtlinien, Leitfäden und Orientierungshilfen entwickelt, die die allgemeinen rechtlichen Vorgaben auskleiden und ihre praktische Umsetzung definieren. Aus Sicht des NKR besteht die Gefahr, dass durch diese untergesetzlich regulierten Anforderungen und Maßnahmen der IT-Sicherheit Aufwände bei Wirtschaft und Verwaltung hervorgerufen werden, die unter Umständen nicht mehr verhältnismäßig sind und bei der Erfüllungsaufwandsabschätzung nicht ausreichend berücksichtigt werden. Der NKR hält es für erforderlich, dass BMI und BSI auch auf untergesetzlicher Ebene eine aufwandsbewusste Alternativenabwägung durchführen, um unnötige und unverhältnismäßige Folgekosten zu vermeiden.

II.3 Umsetzung von EU-Recht

Der Gesetzentwurf dient der Umsetzung der EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-RL). Dem NKR liegen keine Anhaltspunkte dafür vor, dass mit dem Vorhaben über die Umsetzung der NIS-RL hinaus weitere Regelungen mit Auswirkungen auf den Erfüllungsaufwand getroffen werden sollen (1:1-Umsetzung).

II.4 ‚One in one Out'-Regel

Aufgrund der 1:1-Umsetzung von EU-Recht stellt der jährliche Erfüllungsaufwand der Wirtschaft in diesem Regelungsvorhaben kein „In" im Sinne der ‚One in one out'-Regel der Bundesregierung dar.

II.5 Evaluierung

Das Regelungsvorhaben wird anhand der Konzeption zur Evaluierung neuer Regelungsvorhaben gemäß des Arbeitsprogramms bessere Rechtsetzung der Bundesregierung spätestens fünf Jahre nach Inkrafttreten evaluiert. Normenkontrollrat und BMI stimmen darin überein, dass die Evaluierung dieses Regelungsvorhabens zusammen mit der Evaluierung des IT-Sicherheitsgesetzes durchgeführt werden sollte. Der Normenkontrollrat hält es für erforderlich, dabei insbesondere zu prüfen, ob die rechtlichen und untergesetzlichen Maßnahmen in angemessen Verhältnis zum gewonnen Grad an IT-Sicherheit stehen.

III. Zusammenfassung

Das Ressort hat die Auswirkungen auf den Erfüllungsaufwand insgesamt nachvollziehbar dargestellt. Der Nationale Normenkontrollrat erhebt im Rahmen seines gesetzlichen Auftrags keine Einwände gegen die Darstellung der Gesetzesfolgen in dem vorliegenden Regelungsentwurf.

Der Normenkontrollrat gibt zu bedenken, dass dem BSI bereits durch das IT-Sicherheitsgesetz 220 Stellen zugewiesen wurden, die nun noch einmal um 181,5 Stellen aufgestockt werden. Da es sich im Wesentlichen um denselben Aufgabenraum handelt, regt der Normenkontrollrat an, noch stärker zu prüfen, wie die Aufgabenwahrnehmung so gestaltet werden kann, dass Synergieeffekte erschlossen und der Personalaufwuchs gedämpft werden können.

Neben der Regulierung durch EU- und Bundesrecht, werden Standards und Anforderungen der IT-Sicherheit maßgeblich durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) auf untergesetzlicher Ebene bestimmt. Der Normenkontrollrat hält es bezogen auf das gesamte Politikfeld IT-Sicherheit für erforderlich, dass BMI und BSI auch auf untergesetzlicher Ebene eine aufwandsbewusste Alternativenabwägung durchführen und auch untergesetzliche Maßnahmen bei der Evaluierung dieses Politikfeldes berücksichtigen, um unnötige und unverhältnismäßige Folgekosten zu vermeiden.

Der Normenkontrollrat sieht in der engen Einbeziehung der betroffenen Unternehmen und Verwaltungen bei der Ausgestaltung gesetzlicher, vor allem aber untergesetzlicher Bestimmungen eine besondere Chance, zu praktikableren Lösungen zu kommen, die gleichermaßen wirksam und effizient sind. Analog zu den positiven Erfahren, die zuletzt mit dem „Runden Tisch rechtskonforme E-Akte“ erzielt werden konnten, sollten BMI und BSI auch in anderen Bereichen der IT-Sicherheit Dialogformen mit den Betroffenen finden, die dabei helfen, bei der Definition technischer Richtlinien oder sonstiger untergesetzlicher Vorgaben ein hohes Maß an IT-Sicherheit zu gewährleisten ohne unverhältnismäßigen Aufwand zu verursachen.

Dr. Ludewig	Prof. Kuhlmann
Vorsitzender	Berichterstatterin