IT II 1-17002/41#7

Referat ITII1 Stand: 7. Dezember 2016

Referentenentwurf

des Bundesministeriums des Innern

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; 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 soll (Artikel 1 Absatz 1 der Richtlinie (EU) 2016/1148). Die Richtlinie ist gemäß Artikel 25 Absatz 1 bis zum 9. Mai 2018 in nationales Recht umzusetzen. Gemäß Artikel 5 Absatz 1 der Richtlinie ermitteln die Mitgliedstaaten bis zum 9. November 2018 für jeden in Anhang II genannten Sektor und Teilsektor die Betreiber wesentlicher Dienste mit einer Niederlassung in ihrem Hoheitsgebiet.

B. Lösung

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 Gesetzes über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (AtG), des Gesetzes über die Elektrizitäts- und Gasversorgung (EnWG) und des Fünften Buchs Sozialgesetzbuch – Gesetzliche Krankenversicherung (SGB V)) umgesetzt.

Zur Umsetzung der Vorgaben der Richtlinie (EU) 2016/1148 werden die Befugnisse des BSI zur Überprüfung der Einhaltung der technischen und organisatorischen Sicherheitsanforderungen und die Nachweispflicht der Betreiber nach § 8a BSIG und die Regelungen in § 8b BSIG um Vorgaben für das Verfahren bei grenzüberschreitenden 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 wird. 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 die Bußgeldvorschriften in § 15 entsprechend angepasst.

Die in Art. 5 der Richtlinie (EU) 2016/1148 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 Art. 16 der Richtlinie (EU) 2016/1148 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 Richtlinie (EU) 2016/1148 bisher unterschreiten.

Zusätzlich werden mit dem Gesetzentwurf erforderliche Klarstellungen, Bereinigungen und Anpassungen zu 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 Telematik sowie für sonstige Betreiber Kritischer Infrastrukturen entsteht ein Erfüllungsaufwand von maximal 3,5 Millionen Euro.

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

Für das Meldeverfahren kann der Adressatenkreis 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 nicht mehr als rund 1.100 Unternehmen betroffen sein werden. Unter der Annahme, dass pro Betreiber und Jahr eine Meldung eines schweren Sicherheitsvorfalls erfolgt, und unter Ansatz einer Kostenschätzung von 660 Euro pro Meldung ergeben sich Gesamtkosten für die Meldepflicht digitaler Dienste in Höhe von rund 700.000 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 der Gesellschaft für Telematik zu einem Erfüllungsaufwand von etwa 200.000 Euro führen.

Davon Bürokratiekosten:

Einzig die Meldepflicht digitaler Dienste stellt eine Informationspflicht dar, wodurch die Bürokratiekosten um rund 700.000 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

Beim BSI entsteht für die Erfüllung der im Gesetz vorgesehenen Aufgaben ein Erfüllungsaufwand von insgesamt 164,5 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 12,493 Millionen Euro sowie Sachkosten in Höhe von einmalig rund 2,0 Millionen Euro und jährlich von rund 1,0 Millionen Euro.

Erfüllungsaufwand für die Länder und Kommunen entsteht nicht.

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

F. Weitere Kosten

Keine.

Referenten-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 Absatz 9 wird wie folgt gefasst:

„(9) Digitale Dienste im Sinne dieses Gesetzes sind Dienste im Sinne des Artikel 1 Nummer 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), die von einer juristischen Person angeboten werden, und die

1. es Verbrauchern und/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 18.6.2013, S. 63) ermöglichen, Online-Kaufverträge oder Online-Dienstleistungsverträge mit Unternehmern entweder auf der Website des

[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).

Online-Marktplatzes oder auf der Website eines Unternehmers, die von dem Online-Marktplatz 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, und die daraufhin Links anzeigen, über die Informationen im Zusammenhang mit dem angeforderten Inhalt gefunden werden können (Online-Suchmaschinen);

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

Dienste, die zum Schutz grundlegender staatlicher Funktionen eingerichtet worden sind oder für diese genutzt werden, sind vom Anwendungsbereich der Vorschriften für digitale Dienste ausgenommen.“

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

a) Nach Nummer 13 wird eine neue Nummer 13a eingeführt:

„13a. Unterstützung der zuständigen Stellen der Länder in Fragen der Abwehr von Gefahren für die Sicherheit in der Informationstechnik auf deren Ersuchen;“

b) Nummer 17 wird wie folgt geändert:

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

c) Folgende Nummern 18 und 19 werden angefügt:

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

19. Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von Identifizierungsverfahren und die Bewertung, Prüfung und Zertifizierung dieser Verfahren."

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

„§ 5a

Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen

(1) Im Falle einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Stelle des Bundes oder eines Betreibers einer Kritischen Infrastruktur kann das Bundesamt auf deren Ersuchen die Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind, wenn es sich um einen herausgehobenen Fall handelt. Soweit das Bundesamt entsprechende Maßnahmen 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. Diese Daten sind unverzüglich zu löschen, sobald sie für die Wiederherstellung der Sicherheit oder Funktionsfähigkeit der informationstechnischen Systeme nicht mehr benötigt werden. Etwas anderes gilt nur, wenn die Daten in Fällen des Absatzes 4 an Strafverfolgungs- oder Verfassungsschutzbehörden oder den Bundesnachrichtendienst zur Erfüllung von deren gesetzlichen Aufgaben weitergegeben worden sind. In diesen Fällen darf das Bundesamt die Daten bis zur Beendigung der Unterstützung dieser Behörden weiterverarbeiten. Eine Nutzung zu anderen Zwecken ist in

diesen Fällen unzulässig. § 5 Absatz 7 ist entsprechend anzuwenden. Im Übrigen sind die Regelungen des Bundesdatenschutzgesetzes anzuwenden.

(4) Eine Weitergabe von im Rahmen dieser Vorschrift anfallenden Informationen durch das Bundesamt darf nur mit Einwilligung des Ersuchenden erfolgen, 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 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 umfänglichen Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich ist. Die hierdurch entstehenden Kosten hat der Ersuchende zu tragen. Statt selbst tätig zu werden, kann das Bundesamt die ersuchende Stelle auch auf qualifizierte Dritte verweisen. Das Bundesamt und weitere im Auftrag des Ersuchenden tätige qualifizierte Dritte können sich darüber hinaus bei Maßnahmen nach Absatz 1 mit der Einwilligung des Ersuchenden Daten übermitteln. Hierfür gilt Absatz 3 entsprechend.

(6) Soweit dies zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich ist, kann das Bundesamt vom Hersteller der betroffenen informationstechnischen Systeme die Mitwirkung an der Wiederherstellung der Sicherheit oder Funktionsfähigkeit verlangen.

(7) In begründeten Einzelfällen kann das Bundesamt auch bei anderen als den in Absatz 1 genannten Einrichtungen tätig werden, wenn die sonstigen Voraussetzungen nach dieser Vorschrift vorliegen.

„(8) Im Falle von Anlagen oder Tätigkeiten, die einer Genehmigung nach dem Atomgesetz bedürfen, ist in Fällen der Absätze 1, 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.“

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

5) § 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) Nach Satz 3 wird folgender Satz eingefügt:

„Das Bundesamt kann die Vorlage der Dokumentation, die der Überprüfung zugrunde gelegt wurde, verlangen.“

cc) Der neue Satz 5 wird wie folgt gefasst:

„Das Bundesamt 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 die Einhaltung der Anforderungen nach Absatz 1 überprüfen; es kann sich bei der Durchführung der Aufsicht einer qualifizierten Stelle bedienen. Der Betreiber hat dem Bundesamt und den in seinem Auftrag handelnden Personen zu diesem Zweck das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstige Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren. Er trägt die Kosten dieser Überprüfung, sofern das aufsichtsrechtliche Tätigwerden des Bundesamts auf Grund von Anhaltspunkten erfolgte, die berechtigte

Zweifel an der ordnungsgemäßen Einhaltung der Anforderungen nach Absatz 1 begründen.“

c) Der bisherige Absatz 4 wird Absatz 5.

6) § 8b Absatz 2 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 in einem anderen Mitgliedstaat der Europäischen Union über nach Absatz 4 oder vergleichbare Regelungen gemeldete erhebliche Störungen, die Auswirkungen in dem jeweiligen 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

1. Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer erheblichen Beeinträchtigung 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 führen können,

über die Kontaktstelle unverzüglich an das Bundesamt zu melden.“

bb) In Satz 2 werden nach den Wörtern „Angaben zu der Störung“ ein Komma und die Wörter „möglichen grenzübergreifenden

Auswirkungen“ eingefügt und die Wörter „Branche des Betreibers“ durch die Wörter „erbrachten kritischen Dienstleistung sowie die Auswirkungen der Störung auf diese“ ersetzt.

7) 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 im Rahmen der Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen, zu bewältigen. Die Anbieter haben Maßnahmen zu treffen, um den Auswirkungen von Sicherheitsvorfällen auf innerhalb der Europäischen Union erbrachte digitale Dienste vorzubeugen beziehungsweise diese so gering wie möglich zu halten, damit die Verfügbarkeit dieser Dienste gewährleistet wird. Maßnahmen zur Bewältigung von Risiken für die Sicherheit der Netz- und Informationssysteme nach Satz 1 müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist, und dabei folgende Faktoren berücksichtigen:

(a) Sicherheit der Systeme und Anlagen,

(b) Bewältigung von Sicherheitsvorfällen,

(c) Betriebskontinuitätsmanagement

(d) Überwachung, Überprüfung und Erprobung,

(e) Einhaltung der internationalen Normen.

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

(2) 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:

(a) die Zahl der von dem Sicherheitsvorfall betroffenen Nutzer, insbesondere der Nutzer, die den Dienst für die Bereitstellung ihrer eigenen Dienste benötigen;

(b) Dauer des Sicherheitsvorfalls;

(c) geografische Ausbreitung in Bezug auf das von dem Sicherheitsvorfall betroffene Gebiet;

(d) Ausmaß der Unterbrechung der Bereitstellung des Dienstes;

(e) Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten.

Die Pflicht zur Meldung eines Sicherheitsvorfalls entfällt, wenn der Anbieter digitaler Dienste nicht hinreichend Zugang zu den Informationen hat, die benötigt werden, um die Auswirkung eines Sicherheitsvorfalls gemessen an den Parametern gemäß Satz 2 zu bewerten. Für den Inhalt der Meldungen gilt § 8b Absatz 3 entsprechend, soweit nicht durch Durchführungsakte der Kommission nach Artikel 16 Absatz 9 der Richtlinie (EU) 2016/1148 etwas anderes bestimmt ist. Das Bundesamt hat die zuständige Behörde in einem anderen Mitgliedstaat der Europäischen Union über nach Satz 1 gemeldete Sicherheitsvorfälle, die Auswirkungen in diesem Mitgliedstaat haben, zu unterrichten.

(3) Bei Vorliegen von Nachweisen, dass ein Anbieter digitaler Dienste die in Absatz 1 in Verbindung mit den Durchführungsrechtsakten der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 und die in Absatz 2 in Verbindung mit den Durchführungsrechtsakten der Kommission nach Artikel 16 Absatz 9 der Richtlinie (EU) 2016/1148 niedergelegten Anforderungen nicht einhält, kann das Bundesamt von den Anbietern digitaler Dienste verlangen

1. die Übermittlung der zur Beurteilung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen, einschließlich der nachweislichen Sicherheitsmaßnahmen;

2. bei jedem Fall von Nichteinhaltung der in den Absätzen 1 und 2 niedergelegten Anforderungen Abhilfe zu schaffen.

Als Nachweise gelten auch Feststellungen, die dem Bundesamt von zuständigen Behörden in einem anderen Mitgliedstaat der Europäischen Union vorgelegt werden. Hat ein Anbieter digitaler Dienste seine Hauptniederlassung oder einen Vertreter oder Netz- und Informationssysteme in einem anderen Mitgliedstaat der Europäischen Union, arbeitet das Bundesamt bei der Erfüllung der Aufgaben nach Satz 1 mit der zuständigen Behörde dieses Mitgliedstaates zusammen. Die Zusammenarbeit kann auch den Informationsaustausch zwischen den zuständigen Behörden und das Ersuchen umfassen, die in Satz 1 Nummer 2 genannten Maßnahmen zu ergreifen."

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

a) In Absatz 1 Satz 2 werden nach der Angabe „Absatz 4" die Wörter "des Anhangs" eingefügt.

b) In Absatz 2 werden in Nummer 2 die Wörter „, soweit sie den Regelungen des § 11 des Energiewirtschaftsgesetzes unterliegen," angefügt.

c) Absatz 3 wird wie folgt geändert:

aa) Die Wörter „Absatz 3 bis 5" werden jeweils ersetzt durch die Angabe „Absatz 4".

bb) In Nummer 2 werden vor dem Wort „Energiewirtschaftsgesetzes" die Wörter „§ 11 des" eingefügt.

d) Folgender Absatz 4 wird angefügt:

„(4) § 8c Absatz 1 und 2 gilt nicht für Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG der Kommission. § 8c Absatz 2 gilt nicht für Anbieter, die ihren Hauptsitz in einem anderen Mitgliedstaat der Europäischen Union haben oder, soweit sie nicht in einem Mitgliedstaat der Europäischen Union niedergelassen sind, einen

Vertreter in einem anderem Mitgliedstaat der Europäischen Union benannt haben, in dem die digitalen Dienste ebenfalls angeboten werden. Für Anbieter nach Satz 2 gilt § 8c Absatz 3 nur, soweit diese in der Bundesrepublik Deutschland Netz- und Informationssysteme betreiben, die sie im Rahmen der Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen."

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

a) In Absatz 1 Satz 1 werden nach den Wörtern „§ 8a Absatz 2 und 3" und den Wörtern „§ 8b Absatz 4" jeweils die Wörter „und § 8c Absatz 3" und nach den Wörtern „Kritischer Infrastrukturen" die Wörter „oder des Anbieters digitaler Dienste" eingefügt

b) In Absatz 2 werden die Wörter „und 8b" durch „bis 8c" ersetzt.

c) Folgender Absatz 3 wird angefügt:

„(3) Für Betreiber nach § 8d Absatz 2 und 3 gelten die Absätze 1 und 2 entsprechend."

10) In § 10 werden folgende Absätze 4 und 5 angefügt:

„(4) Soweit die Durchführungsrechtsakte der Kommission nach Artikel 16 Absatz 8 und 9 der Richtlinie (EU) 2016/1148 keine abschließenden Bestimmungen über die für Anbieter digitaler Dienste nach § 8c Absatz 1 Satz 3 geltenden Sicherheitsanforderungen und die Parameter zur Festlegung erheblicher Auswirkungen von Sicherheitsvorfällen sowie Form und Verfahren der Meldungen nach § 8c Absatz 2 Satz 2 und 4 enthalten, werden diese vom Bundesministerium des Innern durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, bestimmt.

(5) Das Bundesministerium des Innern kann durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, das Nähere zur Feststellung der Erheblichkeit von Beeinträchtigungen der Funktionsfähigkeit Kritischer Infrastrukturen nach § 8b Absatz 4, die auf Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme beruhen, bestimmen."

11) In § 11 wird nach der Angabe „durch § 5“ die Angabe „und § 5a“ eingefügt.

12) In § 13 werden folgende Absätze 3 bis 5 angefügt:

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

1. die nationalen Maßnahmen zur Ermittlung der Betreiber wesentlicher Dienste;

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

3. eine zahlenmäßige Aufstellung der Betreiber wesentlicher Dienste, 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.

Informationen, die zu einer Identifizierung einzelner Betreiber führen können, sind von einer Übermittlung ausgeschlossen.

(4) Sobald bekannt wird, dass eine Einrichtung oder Anlage oder Teile davon nach § 2 Absatz 10 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 unter Wahrung der Vertraulichkeit der Meldungen nach § 8b und § 8c bis zum 9. August 2018 und danach jährlich an die Kooperationsgruppe nach Artikel 11 der Richtlinie (EU) 2016/1148 einen zusammenfassenden Bericht zu den die in Anhang II der Richtlinie (EU)

2016/1148 genannten Sektoren oder digitale Dienste betreffenden Meldungen, einschließlich der Zahl der Meldungen und der Art der gemeldeten Sicherheitsvorfälle sowie der ergriffenen Maßnahmen. Informationen, die zu einer Identifizierung einzelner Betreiber führen können, sind von einer Übermittlung ausgeschlossen.“

13)§ 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 4 wird der Punkt durch ein Komma ersetzt.

cc) Folgende Nummern 5 bis 7 werden angefügt:

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

6. entgegen § 8c Absatz 2 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vornimmt, oder

7. einer vollziehbaren Anordnung nach § 8c Absatz 3

a) Nummer 1 oder

b) Nummer 2

zuwiderhandelt.“

b) Dem Absatz 2 wird folgender Satz 2 angefügt:

„In den Fällen des Absatz 1 Nummern 5 bis 7 wird die Ordnungswidrigkeit nur geahndet, wenn der Anbieter 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 denselben digitalen Dienste anbietet.“

14)Nach § 14 wird folgender § 15 angefügt;

„§ 15

Übergangsvorschriften

(1) Die Anbieter digitaler Dienste betreffenden Vorschriften 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

§ 95 des Energiewirtschaftsgesetzes vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 1 des Gesetzes vom 26. Juli 2016 (BGBl. I S. 1786) geändert worden ist, wird wie folgt geändert:

1) 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,“

2) Dem Absatz 5 wird folgender Satz 2 angefügt:

„In den Fällen des Absatzes 1 Nummer 2b ist das Bundesamt für Sicherheit in der Informationstechnik Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten.“

Artikel 4
Änderung des SGB V

Das Fünfte Buch Sozialgesetzbuch – Gesetzliche Krankenversicherung – (Artikel 1 des Gesetzes vom 20. Dezember 1988, BGBl. I S. 2477, 2482), das zuletzt durch Artikel 1a des Gesetzes vom 31. Juli 2016 (BGBl. I S. 1937) 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 Zulassungen und Bestätigungen nach Absatz 1a bis 1c und 1e einschließlich der zugrunde gelegten Nachweise, eine Aufstellung der nach Absatz 6 und 7 getroffenen Maßnahmen einschließlich der festgestellten Sicherheitsmängel und Ergebnisse und sonstige für die Bewertung der Sicherheit der Telematikinfrastruktur sowie der zugelassenen Dienste und bestätigten Anwendungen erforderlichen Informationen vor. Im Anschluss an die Bewertung der in Satz 1 genannten Informationen kann das Bundesamt für Sicherheit in der Informationstechnik der Gesellschaft für Telematik verbindliche Anweisungen zur Abhilfe der festgestellten Sicherheitsmängel erteilen. Die Gesellschaft für Telematik ist befugt, Betreibern von zugelassenen Diensten und bestätigten Anwendungen nach Absatz 1a bis 1c und 1e, verbindliche Anweisungen zur Abhilfe festgestellter Sicherheitsmängel zu erteilen. Die Gesellschaft für Telematik trägt die Kosten der Überprüfung, sofern das aufsichtsrechtliche Tätigwerden

des Bundesamts für Sicherheit in der Informationstechnik auf Grund von Anhaltspunkten erfolgte, die berechtigte Zweifel an der Sicherheit der Telematikinfrastruktur begründen. Die Betreiber von zugelassenen Diensten und bestätigten Anwendungen nach Absatz 1a bis 1c und 1e tragen die Kosten der Überprüfung, sofern das aufsichtsrechtliche Tätigwerden des Bundesamts für Sicherheit in der Informationstechnik auf Grund von Anhaltspunkten erfolgte, die berechtigte Zweifel an der Sicherheit der zugelassenen Dienste und bestätigten Anwendungen begründen."

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 Nummer 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
Inkrafttreten

(1) Dieses Gesetz tritt am Tag nach seiner 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-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 soll (Artikel 1 Absatz 1 der Richtlinie (EU) 2016/1148). 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 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 vorrangigen Spezialgesetze (des Gesetzes über die friedliche Verwendung der Kernenergie und den Schutz gegen ihre Gefahren (AtG), des Gesetzes über die Elektrizitäts- und Gasversorgung (EnWG) und des Fünften Buchs Sozialgesetzbuch – Gesetzliche Krankenversicherung (SGB V)) umgesetzt.

Zur Umsetzung der Vorgaben der Richtlinie (EU) 2016/1148 werden die Befugnisse des BSI zur Überprüfung der Einhaltung der technischen und organisatorischen Sicherheitsanforderungen und die Nachweispflicht der Betreiber nach § 8a BSIG und die Regelungen in § 8b BSIG um Vorgaben für das Verfahren bei grenzüberschreitenden Vorfällen angepasst. 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 die Bußgeldvorschriften in § 15 entsprechend angepasst.

Die in Art. 5 der Richtlinie (EU) 2016/1148 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 Art. 16 der Richtlinie (EU) 2016/1148 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 Richtlinie (EU) 2016/1148 bisher unterschreiten.

Zusätzlich werden mit dem Gesetzentwurf erforderliche Klarstellungen, Bereinigungen und Anpassungen zu 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 oder 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) und des Telemediengesetzes (Artikel 4) ergibt sich ergänzend 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 Berechtigung des Bundes zur Inanspruchnahme dieser 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 Telekommunikationsanbietern, der Gesellschaft für Telematik, sonstigen Betreibern Kritischer Infrastrukturen sowie Anbietern digitaler Dienste:

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.

Der Gesellschaft für Telematik 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.

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.

Ergänzende Prüfungen sind nicht als Regelfall, sondern lediglich im Einzelfall auf Stichprobenbasis bzw. bei begründetem Anlass durchzuführen. Unter der Annahme, dass das zuständige Bundesamt für Sicherheit in der Informationstechnik 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 35.000 € kostet, wird der Gesamtaufwand auf maximal 3,5 Millionen € abgeschätzt.

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.

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 wird von ca. 1.100 Anbietern mit mehr als 50 Mitarbeitern beziehungsweise einer Bilanzsumme, die 10 Millionen Euro überschreitet, ausgegangen, die ihren Sitz in Deutschland haben. 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 auch umgesetzt werden. Die Umsetzung der Vorgaben der Richtlinie (EU) 2016/1148 sollte danach keine größeren Kosten nach sich ziehen.

Der jährliche Erfüllungsaufwand für das Meldeverfahren ergibt sich 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. Es wird geschätzt, dass von den Regelungen für digitale Dienste in Deutschland nicht mehr als rund 1.100 Unternehmen betroffen sein werden. Unter der Annahme, dass pro Betreiber und Jahr eine Meldung eines schweren Sicherheitsvorfalls erfolgt und unter Ansatz einer Kostenschätzung von 660 Euro pro Meldung ergeben sich so Gesamtkosten für die Meldepflicht digitaler Dienste in Höhe von rund 700.000 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 der Gesellschaft für Telematik 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. Hierfür werden Kosten von nicht mehr als 660 Euro pro Kontaktstelle, also insgesamt etwa 200.000 Euro abgeschätzt.

3. Erfüllungsaufwand der Verwaltung

Beim BSI entsteht für die Erfüllung der im Gesetz vorgesehenen Aufgaben ein Aufwand von insgesamt 164,5 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 12,493 Millionen Euro sowie Sachkosten in Höhe von einmalig rund 2,0 Millionen Euro und jährlich von rund 1,0 Millionen Euro.

Der Personalbedarf des BSI begründet sich zum einen dadurch, dass durch die Umsetzung der Richtlinie (EU) 2016/1148 Aufsichtsbefugnisse des BSI über die Betreiber Kritischer Infrastrukturen ausgeweitet und neue Aufgaben und Verfahren eingeführt werden. Dies betrifft insbesondere die Einführung von

Mindestanforderungen und Meldepflichten für Anbieter digitaler Dienste, die mit der Durchführung einer entsprechenden nationalen Aufsicht und Sanktionierung durch das BSI verbunden sind. Darüber hinaus werden die Aufsichtsbefugnisse des BSI über die Betreiber Kritischer Infrastrukturen durch die von der Richtlinie (EU) 2016/1148 verpflichtend vorgesehene Möglichkeit einer ex-ante-Kontrolle erweitert und Verfahren der grenzüberschreitenden Zusammenarbeit mit anderen Mitgliedstaaten sowie Berichtspflichten gegenüber der Kommission eingeführt.

Dadurch ergibt sich auch die Notwendigkeit zur Ausweitung der Grundlagenarbeit und Fachkompetenz im BSI, die bisher vordringlich auf die Sicherheit der Informationstechnik des Bundes und der Betreiber Kritischer Infrastrukturen fokussiert war. Die Überprüfung der Anbieter von digitalen Diensten und die Zusammenarbeit mit den zuständigen Stellen der anderen Mitgliedstaaten, der Kommission und weiteren Agenturen der Europäischen Union (namentlich ENISA) in diesem Bereich müssen sich an der IKT-Sicherheit zur Gewährleistung der zu erbringenden Dienstleistung ausrichten. Hierzu sind umfangreiche Kenntnisse über die Funktionsweise und Architektur der jeweiligen digitalen Dienste erforderlich. Auch zum Auswerten von in der Meldestelle eingehenden Informationen, zum Fortschreiben des Lagebildes und zur Vorhersage der potentiellen Auswirkungen einer Meldung bzw. Störung auf die betroffene Kritische Infrastruktur oder ihre Branche ist spezielles Wissen in Bezug auf die jeweiligen digitalen Dienste zwingend erforderlich. Der geforderte Personalbedarf ermöglicht den Aufbau der notwendigen Fachexpertise als Grundlage für die geforderte Bewertung, Unterstützung und Zusammenarbeit.

Die Aufgaben als zentrale Meldestelle für die Sicherheit in der Informationstechnik werden im Hinblick auf die Zusammenarbeit mit den zuständigen Stellen im Ausland durch die verstärkte Zusammenarbeit bei Sicherheitsvorfällen mit grenzüberschreitendem Bezug ausgeweitet. Des Weiteren ist der zusätzliche Personalaufwand durch die Bearbeitung von Ordnungswidrigkeiten als zuständige Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten nach den § 14 Absatz 2 BSIG, § 46 Absatz 3 Nummer 3 AtG, §95 Absatz 5 Satz 2 EnWG und § 307 Absatz 4 SGB V sowie durch zusätzliche Berichtspflichten gegenüber der Kommission insbesondere im Zusammenhang mit

der Feststellung der Betreiber Kritischer Infrastrukturen und gegenüber der NIS-Kooperationsgruppe begründet.

Erfüllungsaufwand für die Länder und Kommunen entsteht nicht.

[BNetzA, BMUB und BMG]

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

IV. Weitere Kosten

Keine.

V. Gleichstellungspolitische Relevanz

Die Regelungen sind inhaltlich geschlechtsneutral und damit ohne Gleichstellungsrelevanz. § 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 − 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 Gesetzesentwurf ist mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen vereinbar. Er 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.

IX. Befristung und Evaluierung

Eine Befristung ist nicht vorgesehen, da der Gesetzesentwurf der Umsetzung der Richtlinie (EU) 2016/1148 dient, die unbefristet gilt. Der Gesetzesentwurf sieht eine Evaluierung anhand der Konzeption zur Evaluierung neuer Regelungsvorhaben gemäß dem Arbeitsprogramm bessere Rechtsetzung der Bundesregierung vom 28. März 2012, Ziffer II. 3., fünf Jahre nach Inkrafttreten vor.

B. Besonderer Teil

Zu Artikel 1 (Änderung des BSI-Gesetzes)

Zu Nummer 1 (Änderung des § 2 BSIG)

Die ursprünglich in § 2 Absatz 9 enthaltene Definition des Begriffs „Datenverkehr“ war entbehrlich, da dieser Begriff in dem Gesetz nicht weiter verwendet wird. Die Einfügung eines neuen Absatzes 9 dient der Umsetzung der Richtlinie (EU) 2016/1148. Mit den Änderungen wird der Katalog in § 2 um eine neue Definition zu digitalen Diensten gemäß Artikel 4 Nummer 5 und 6 sowie Nummer 17 bis 19 der Richtlinie (EU) 2016/1148 ergänzt. Gleichzeitig wird der Anwendungsbereich der für diese geltenden Vorgaben gemäß Artikel 18 der Richtlinie (EU) 2016/1148 auf Anbieter eingegrenzt, die einen der konkret genannten Dienste innerhalb der Europäischen Union zur Nutzung bereitstellen. In diesem Fall sind die für digitale Dienste geltenden Vorgaben unabhängig davon anwendbar, ob der Anbieter in einem der Mitgliedstaaten der Europäischen Union niedergelassen ist oder nicht. Dienste, die von einer natürlichen Person oder Kleinstunternehmen und 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 Richtlinie (EU) 2016/1148 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 Richtlinie (EU) 2016/1148 niedergelegten Mindestanforderungen und Meldepflichten gelten nach Artikel 1 Absatz 3 der Richtlinie (EU) 2016/1148 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.

Mit Satz 2 wird klargestellt, dass Dienste, die zum Schutz grundlegender staatlicher Funktionen eingerichtet worden sind oder für diese genutzt werden, vom Anwendungsbereich der besonderen Vorschriften für digitale Dienste ausgenommen werden. Zu diesen Diensten zählen zum Beispiel für die Nutzung durch die Bundesverwaltung eingerichtete Cloud-Dienste (sogenannte „Bundescloud“). Die Regelung ist auf Art. 1 Absatz 6 der Richtlinie (EU) 2016/1148 gestützt, nach der Maßnahmen zum Schutz ihrer grundlegenden staatlichen Funktionen, insbesondere Maßnahmen zum Schutz der nationalen Sicherheit, einschließlich Maßnahmen zum Schutz von Informationen, deren Preisgabe nach Erachten der Mitgliedstaaten ihren wesentlichen Sicherheitsinteressen widerspricht, und 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 Absatz 1 Satz 2 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 lediglich eine Beratung oder Warnung in Fragen der Sicherheit in der Informationstechnik vorgesehen. Eine Unterstützung durch das Bundesamt 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.

Die Änderung in Nummer 17 dient der Umsetzung der Richtlinie (EU) 2016/1148. Mit der Änderung werden die Aufgaben als zentrale Stelle für die Sicherheit in der Informationstechnik auf digitale Dienste nach § 2 BSIG erweitert.

Mit der Ergänzung in Nummer 18 werden Maßnahmen mittels sogenannter Mobile Incident Response Teams, mit denen das Bundesamt andere Stellen bei der Wiederherstellung ihrer IT-Systeme nach Cyber-Angriffen unterstützen soll, in den Aufgabenkatalog des BSI-Gesetzes aufgenommen. 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 BSI-Gesetz). Die Unterstützung von Stellen des Bundes und von Betreibern Kritischer Infrastrukturen ist hierin bereits enthalten. Da der Einsatz von Mobile Incident Response Teams aber nach § 5a Absatz 1 BSI-Gesetz geregelt und in Ausnahmefällen auch anderen Einrichtungen zu Gute kommen soll, wird die Aufgabe insgesamt noch einmal ausdrücklich festgeschrieben.

Mit der Ergänzung in Nummer 19 wird die Zuständigkeit des BSI für die Bewertung von Verfahren unter dem Gesichtspunkt der Informationssicherheit gesetzlich klargestellt. Sicherheitstechnisch relevante Verfahren, insbesondere Identifizierungsverfahren, bedürfen einer abschließenden Bewertung unter dem Gesichtspunkt der Informationssicherheit. Das BSI ist kraft seines gesetzlichen Auftrags innerhalb der Bundesverwaltung für diesen Bereich zuständig, da der Gesetzgeber mit der Bündelung der Fachkompetenz des Bundes im Bereich der Informationssicherheit beim BSI (§ 1 Satz 2 BSIG) gerade das Ziel verfolgt hat, eine einheitliche Bewertung für sicherheitstechnisch relevante Verfahren und Maßnahmen zu erzielen. Darüber hinaus verfügt das BSI als einzige Behörde innerhalb der Bundesverwaltung über die technische Kompetenz, die für eine abschließende Bewertung solcher Verfahren erforderlich ist. Die neu eingefügte Nr. 19 stellt daher sicher, dass dieses gesetzgeberische Ziel bestmöglich erreicht wird.

Zu Nummer 3 (neuer § 5a Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen)

Die Richtlinie (EU) 2016/1148 sieht in Kapitel II in Verbindung mit Anhang 1 zur Richtlinie vor, dass die Mitgliedstaaten 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 Vorfällen und Risiken gewährleisten (s. Erwägungsgrund 34).

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

Zwar kann das Bundesamt im Rahmen seiner ihm in § 3 BSI-Gesetz zugewiesenen Aufgaben (vergleiche insbesondere § 3 Absatz 1 Satz 2 Nummer 1 und § 3 Absatz 3 BSI-Gesetz), auf Einwilligungsbasis und nach allgemeinem Datenschutzrecht bereits jetzt von Cyber-Attacken betroffene Stellen des Bundes oder 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 Netzwerkverkehr 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 Bundesamt mit MIRTs künftig verstärkt auch operative Unterstützung bei der Bewältigung von Vorfällen bei Stellen des Bundes und Betreibern Kritischer Infrastrukturen leisten können. Voraussetzung ist, dass es sich um einen herausgehobenen Fall handelt. Dabei wird das Bundesamt nur auf Ersuchen tätig, da die MIRTs primär der Unterstützung der betroffenen Einrichtung dienen. Dieser soll 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 erfassten Betroffenen, wird der Einsatz der MIRTs des Bundesamtes nicht gebührenpflichtig sein. Hierdurch wird gewährleistet, dass von einem Hilfeersuchen nicht aus Kostengründen abgesehen wird. Zur Klarstellung wird entsprechend 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 von kommerziellen IT-Dienstleistern 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 Bundesamt erfolgen. Insbesondere forensische Arbeiten werden indes häufig im Bundesamt selbst erfolgen.

Die Möglichkeit eines Einsatzes der MIRTs des Bundesamtes entbindet die um Unterstützung ersuchenden Einrichtungen 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 Bundesamtes zum Tätigwerden nicht besteht. Hieraus folgt, dass ein Ersuchender keinen Anspruch auf ein Tätigwerden des Bundesamtes hat, sondern dem Bundesamt ein Ermessensspielraum zusteht.

Die vom Bundesamt 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 Gefährdungen (z.B. den Kontrollservern des Angreifers oder 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. Dies ist insbesondere dann zu bejahen, 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. Im Falle des Einsatzes eines Verschlüsselungstrojaners kann es zum Beispiel sein, dass der erste Angriff noch als außergewöhnlich einzustufen ist, dies aber für spätere Fälle nicht mehr gilt, da 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, 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 Bundesamt 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. Dies kann nur mittels umfassender Analyse der Log- und Kommunikationsdaten aufgeklärt und die Bereinigung der infizierten Systeme dadurch 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 für Maßnahmen der Strafverfolgung, der Spionageabwehr, des Sabotageschutzes oder der nachrichtendienstlichen Aufklärung genutzt werden sollen. 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 BSI-Gesetz vorgesehene hohe Datenschutzniveau wird auf § 5a BSI-Gesetz übertragen. Im Übrigen gelten zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten die Vorgaben des Bundesdatenschutzgesetzes. Für die Unterstützungsleistungen des Bundesamtes stellt § 5a eine Sondernorm dar, die sonstigen Regelungen vorgeht.

Nach Absatz 4 dürfen anfallenden Informationen durch das Bundesamt 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 übermittelt werden. Diese Regelung dient dem Schutz der Interessen der unterstützten Einrichtung. Sofern die bei der Analyse und Wiederherstellung der Sicherheit oder Funktionsfähigkeit der informationstechnischen Systeme erarbeiteten Ergebnisse und Fakten bekannt würden, könnten Angreifer daraus wertvolle Informationen für neue Angriffe auf die Sicherheit dieser Systeme erhalten. Außerdem setzt die Einschaltung des Bundesamtes 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 übernommen. In diesem Zusammenhang begründen Angriffe, die eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informatorischen 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 ausgeschlossen wird. Soweit das Bundesamt 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 bezieht sich die Regelung im neuen § 5a Absatz 5 auch explizit nicht nur auf Dritte, die IT-Sicherheitsdienstleistungen anbieten, sondern generell auf qualifizierte Dritte. Dies trägt der Tatsache Rechnung, dass 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 Bundesamt 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 BSI-Gesetz 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 BSI-Gesetz sieht § 5a Absatz 6 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, sofern von der ersuchenden Stelle Soft- oder Hardware eingesetzt wird, deren Supportzeitraum bereits abgelaufen ist und der Hersteller das Ende des Supportzeitraumes rechtzeitig angekündigt hat. Die ersuchende Einrichtung hat dem Hersteller die entstandenen Kosten in diesem Fall zu ersetzen. Seine Mitwirkungspflicht bleibt davon unberührt.

In Absatz 7 wird dem Bundesamt 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 Absatz 1) ein vergleichbares öffentliches Interesse an der Behebung des Vorfalls besteht, auch wenn die betroffene Einrichtung nicht zu dem Adressatenkreis des Absatz 1 zählt. Zwar soll der Einsatz der MIRTs primär auf diese beschränkt bleiben. Dem Bundesamt 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 Gefahrenpotenzial (z.B. chemische 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 Falle 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 in der Atomgesetzgebung sowie der damit verbundenen Gewährleistung der nuklearen Sicherheit und Sicherung von kerntechnischen Anlagen zu berücksichtigen. Daher ist insbesondere in Fällen der Absätze 1, 5 und 7 vor Tätigwerden des Bundesamtes das Benehmen mit den zuständigen atomrechtlichen Aufsichtsbehörden des Bundes und der Länder herzustellen, da unmittelbare Auswirkungen auf Sicherungsmaßnahmen nach Atomgesetz möglich sind. Hierdurch soll eine gegenseitige Beeinflussung von jeweils in unterschiedlichen Rechtsgebieten zuständigen Behörden vermieden werden und gleichzeitig ein effektiver und zeitnaher Einsatz der MIRTs erreicht werden. Wegen des besonders hohen Bedrohungs- bzw. Schadenspotentials haben zudem die Vorgaben aufgrund des Atomgesetzes Vorrang.“

Zu Nummer 4 (Änderung des § 7a BSIG)

Im Rahmen der Analyse und Wiederherstellung der Sicherheit 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 klargestellt.

Zu Nummer 5 (Änderung des § 8a BSIG)

Die Änderungen in Absatz 3 und der neu eingefügte Absatz 4 dienen der Umsetzung von Artikel 15 der Richtlinie (EU) 2016/1148. Nach Artikel 15 Absatz 2 der Richtlinie (EU) 2016/1148 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 Buchst. b) der Richtlinie (EU) 2016/1148 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 zu treffenden Sicherheitsmaßnahmen nur überprüfen, soweit diese konkrete Mängel anzeigen. Nach Artikel 15 der Richtlinie (EU) 2016/1148 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 dem neuen Satz 4 wird die Nachweispflicht der Betreiber 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 aus Absatz 1 hinreichend belegt werden kann, sollen ihr 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 eine Befugnis für das BSI zum Betreten der Einrichtungen des Betreibers 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 Richtlinie (EU) 2016/1148. Die Einräumung eines Betretungsrechts unter Wahrung der grundrechtlichen Anforderungen sowie der Verhältnismäßigkeit dient der Umsetzung des Auftrags an die Mitgliedstaaten aus Artikel 15 der Richtlinie (EU) 2016/1148, eine effektive Kontrolle der Einhaltung der Anforderungen aus Artikel 14 der Richtlinie (EU) 2016/1148 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 anerkannte Stellen, soweit sie über die notwendige Expertise und Neutralität verfügen, sein. 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 6 (Änderung des § 8b BSIG)

Die Einfügung eines neuen Buchstaben d) in Absatz 2 Nummer 4 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. Zuständige Behörden in einem anderen Mitgliedstaat der Europäischen Union sind die zentralen Anlaufstellen im Bereich der Netz- und Informationssicherheit, die nach Art. 8 Absatz 3 der Richtlinie (EU) 2016/1148 jeder Mitgliedstaat der Europäischen Union zu benennen hat und die nach Art. 8 Absatz 4 der Richtlinie (EU) 2016/1148 als Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit dienen. Gemäß Art. 8 Absatz 7 der Richtlinie (EU) 2016/1148 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 BSI-KritisV betreiben.

Die Änderung in Absatz 4 Satz 1 dient der Umsetzung von Art. 14 Absatz 3 und 4 der Richtlinie (EU) 2016/1148. 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 Absatz 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 Richtlinie (EU) 2016/1148 angepasst, nach deren Artikel 14 die Meldepflicht an Auswirkungen auf einzelne Dienste anknüpft, und die in § 10 Absatz 1 bereits entsprechend angelegte Systematik zur Bestimmung Kritischer Infrastrukturen abgebildet, die innerhalb der jeweiligen Sektoren nicht zwischen Branchen, sondern kritischen Dienstleistungen unterscheidet. Gleichzeitig wird der zu meldende Inhalt auf die bereits zum Zeitpunkt der Meldung jeweils bekannten Auswirkungen auf die Dienstleistungserbringung bezogen. Die weiteren Änderungen in Absatz 4 Satz 2 dienen der Umsetzung des Artikels 14 Absatz 3 der Richtlinie (EU) 2016/1148. Darin ist vorgesehen, dass Meldungen der Betreiber die Informationen enthalten müssen, die es der zuständigen Behörde ermöglichen, zu bestimmen, ob ein Sicherheitsvorfall grenzüberschreitende erhebliche Auswirkungen hat. Das Bundesamt wird so in die Lage versetzt, seiner Verpflichtung zur Unterrichtung der zuständigen Behörden in einem anderen Mitgliedstaat der Europäischen Union nach Absatz 2 Nummer d) nachzukommen. Betreiber sollten bei den Angaben der zu erheblichen Auswirkungen in einem anderen Mitgliedstaat insbesondere die in Artikel 14 Absatz 3 der Richtlinie (EU) 2016/1148 genannten Parameter berücksichtigen.

Zu Nummer 7 (Einfügen eines neuen § 8c BSIG)

Der neu eingefügte § 8c dient der Umsetzung der Vorgaben der Richtlinie (EU) 2016/1148 an Anbieter digitaler Dienste und der damit verbundenen Aufsicht durch das Bundesamt für Sicherheit in der Informationstechnik. Mit Absatz 1 werden die Vorgaben des Artikels 16 Absätze 1 und 2 der Richtlinie (EU) 2016/1148 umgesetzt.

Mit Absatz 2 werden die Vorgaben des Artikels 16 Absätze 3 und 4 der Richtlinie (EU) 2016/1148 umgesetzt, mit denen eine Pflicht zur Meldung von Sicherheitsvorfällen, die erhebliche Auswirkungen auf die Bereitstellung eines digitalen Dienstes haben, eingeführt wird. Satz 2 und Satz 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 Art. 16 Absatz 8 und 9 der Richtlinie (EU) 2016/1148 durch Durchführungsrechtsakte der Kommission näher bestimmt werden. Mit Satz 5 wird die Verpflichtung aus Art. 16 Absatz 6 der Richtlinie (EU) 2016/1148 umgesetzt. Danach sind zuständige Behörden in einem anderen Mitgliedstaat der Europäischen Union über gemeldete Sicherheitsvorfälle zu unterrichten, soweit diese Auswirkungen in diesem Mitgliedstaat haben. Zuständige Behörden in einem anderen Mitgliedstaat der Europäischen Union sind die zentralen Anlaufstellen im Bereich der Netz- und Informationssicherheit, die nach Art. 8 Absatz 3 der Richtlinie (EU) 2016/1148 jeder Mitgliedstaat der Europäischen Union zu benennen hat und die nach Art. 8 Absatz 4 der Richtlinie (EU) 2016/1148 als Verbindungsstelle zur Gewährleistung der grenzüberschreitenden Zusammenarbeit dienen. Gemäß Art. 8 Absatz 7 der Richtlinie (EU) 2016/1148 veröffentlicht die Kommission eine Liste der benannten zentralen Anlaufstellen. Absatz 3 beinhaltet die in Artikel 17 Richtlinie (EU) 2016/1148 vorgesehene Befugnis zu Aufsichts- und Kontrollmaßnahmen, soweit Anbieter digitaler Dienste den in Absätzen 1 und 2 vorgesehenen Pflichten nachweislich nicht oder nur unzureichend nachgekommen sind. Als Nachweise gelten auch Feststellungen, die dem Bundesamt für Sicherheit in der Informationstechnik von zuständigen Behörden in einem anderen Mitgliedstaat der Europäischen Union vorgelegt werden. Auf diese Weise wird eine angemessene Kontrolle und Aufsicht für die Fälle sichergestellt, in denen Ort der Hauptniederlassung und 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 8 (Änderung und Neunummerierung des § 8c BSIG)

Mit den Änderungen in Absatz 1 wird ein redaktionelles Versehen bei dem Verweis auf die Empfehlung 2003/361/EC der Kommission korrigiert.

Mit der Ergänzung des Absatz 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 Richtlinie (EU) 2016/1148. Bisher müssen Kontaktstellen nicht von den in § 8d (neu) Absatz 3 Nummern 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 Richtlinie (EU) 2016/1148 geforderten Informationen der Betreiber zu ermöglichen 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 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 den Anbieter bereits an die zuständige Behörde in einem anderen Mitgliedstaat der Europäischen Union erfolgen, weil sie dort ihren Hauptsitz oder, 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. 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 die Vertretung des Diensteanbieters anzuknüpfen; bei Anbietern aus Drittstaaten im Übrigen, wenn ein digitaler Dienst im Inland angeboten wird.

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

Mit den Änderungen in Absatz 1 wird der Anwendungsbereich der zu Kritischen Infrastrukturen bestehenden Spezialregelung im Sinne von § 1 Absatz 3 des Informationsfreiheitsgesetzes auf Anbieter digitaler Dienste nach § 8c ausgeweitet, um dem Schutz der insbesondere im Meldeverfahren zu übermittelnden hochsensiblen Informationen hinreichend Rechnung zu tragen. Hiermit werden zugleich die Regelungen zur Wahrung der Vertraulichkeit der von den Betreibern und Anbietern gemeldeten Informationen in Artikel 16 Absatz 7 der Richtlinie (EU) 2016/1148 umgesetzt.

Für den Bereich der Kritischen Infrastrukturen bestehen entsprechende Vorgaben in Art. 14 Absatz 6 der Richtlinie (EU) 2016/1148. Mit dem neu eingefügten Absatz 3 wird klargestellt, dass die Vertraulichkeitsregelungen auch für die Betreiber gelten, die spezialgesetzlich geregelten Pflichten unterliegen.

Zu Nummer 10 (Änderung des § 10 BSIG)

Mit dem neuen Absatz 4 wird die Ermächtigung zum Erlass einer Rechtsverordnung geschaffen, soweit dies für die Umsetzung der Durchführungsrechtsakte der Kommission nach Art. 16 Absatz 8 und 9 der Richtlinie (EU) 2016/1148 erforderlich ist. Dies gilt nur, 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.

Mit dem neuen Absatz 5 wird eine Ermächtigung zum Erlass einer Rechtsverordnung geschaffen, mit der das Bundesministerium des Innern die Voraussetzungen für eine Meldepflicht nach § 8b Absatz 4 Satz 1 weiter konkretisieren und im Hinblick auf die Erheblichkeit der Beeinträchtigung der Funktionsfähigkeit einer Kritischen Infrastrukturen die Kriterien gemäß Art. 14 Absatz 4 der Richtlinie (EU) 2016/1148

berücksichtigen kann. Leitlinien nach Artikel 14 Absatz 7 der Richtlinie (EU) 2016/1148 sollen beim Erlass einer solchen Rechtsverordnung berücksichtigt werden.

Zu Nummer 11 (Änderung des § 11 BSIG)

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

Zu Nummer 12 (Neue § 13 Absatz 3 bis 5 BSIG)

Die neu eingefügten Absätze 3 und 4 dienen der Umsetzung von Artikel 5 der Richtlinie (EU) 2016/1148.

Mit dem neuen Absatz 3 werden die Berichtspflichten an die Kommission im nationalen Recht festgeschrieben. Die in Absatz 3 Nummern 1 bis 3 genannten Informationen sind der Kommission gemäß Artikel 5 Absatz 7 der Richtlinie (EU) 2016/1148 bis zum 9. November 2018 und danach alle zwei Jahre zu übermitteln, damit diese die Umsetzung der Richtlinie, bewerten kann, insbesondere, ob die Mitgliedstaaten bei der Ermittlung der Betreiber 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 Richtlinie (EU) 2016/1148 genannten Sektoren, soweit dies nicht zu einer Identifizierbarkeit einzelner Betreiber, Einrichtungen oder Anlagen führt. Die Übermittlung von Listen einzelner Betreiber, Einrichtungen oder Anlagen, die als Kritische Infrastrukturen eingestuft sind, ist ausgeschlossen. Soweit die Kommission technische Leitlinien nach Art. 5 Absatz 7 der Richtlinie (EU) 2016/1148 erlässt, um zur Bereitstellung vergleichbarer Informationen beizutragen, sind diese nach Maßgabe der Art. 1 Absatz 5 und 6 der Richtlinie (EU) 2016/1148 zu berücksichtigen.

Mit Absatz 4 werden die Vorgaben des Artikel 5 Absatz 4 der Richtlinie (EU) 2016/1148 umgesetzt, der eine gegenseitige Konsultationspflicht der Mitgliedstaaten 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 Sorge dafür getragen, 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 Richtlinie (EU) 2016/1148, mit dem die Mitgliedstaaten verpflichtet werden, der mit Artikel 11 der Richtlinie (EU) 2016/1148 einzurichtenden Kooperationsgruppe der Mitgliedstaaten bis zum 9. August 2018 und dann jährlich zu den eingegangenen Meldungen nach Art. 14 und 16 der Richtlinie (EU) 2016/1148 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 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.

Zu Nummer 13 (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 Richtlinie (EU) 2016/1148 um, nach denen die Mitgliedstaaten 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, soweit 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 14 (neuer § 15 BSIG)

Mit der Vorschrift wird eine Übergangsregelung zur Anwendbarkeit der die Anbieter digitaler Dienste betreffenden Vorschriften getroffen. Bezüglich der für diese geltenden Mindestanforderungen und Meldepflichten, der hierzu durchzuführenden Aufsicht und der Sanktionierung von Verstößen sieht die Richtlinie (EU) 2016/1148 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 Art. 16 bis 18 der Richtlinie (EU) 2016/1148 dienenden § 8c, § § 10 Absatz 4 (Verordnungsermächtigung) und 14 (Sanktionen) sind daher entsprechend der in Artikel 25 der Richtlinie (EU) 2016/1148 vorgesehenen Umsetzungsfrist erst ab dem 10. Mai 2018 anwendbar.

Zu Artikel 2 (Änderung des Atomgesetzes)

Genehmigungsinhaber nach den §§ 6, 7 und 9, die Anlagen, die die Versorgungssicherheit betreffen und damit der NIS-RL unterliegen, werden bereits vom EnWG und dortigen Sanktionen erfasst werden. Regelung soll dazu dienen, Betreiber, die lediglich nach AtG Pflichten unterliegen und NICHT Kritis nach KRITISV sind, von einer Übermittlung bei grenzüberschreitenden Vorfällen auszunehmen. Insoweit sollte BMUB zugestimmt werden (Soweit danach keine Aspekte der Versorgungssicherheit betroffen, unterliegen Betreiber auch nicht der NIS-RL).

Zu Artikel 3 (Änderung des § 95 Energiewirtschaftsgesetzes)

Betreiber von Energieversorgungsnetzen und Energieanlagen im Sinne des Energiewirtschaftsgesetzes unterliegen bereits nach den Vorgaben des § 11 EnWG zu §§ 8a und 8b BSIG vergleichbaren Anforderungen, die den Vorgaben des Artikel 14 Absatz 1 bis 3 der Richtlinie (EU) 2016/1148 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 Einrichtungen, Anlagen oder Teilen davon, die in der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes 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.

Im EnWG waren bisher allerdings keine Sanktionen bei Verstößen gegen die Einhaltung von Mindestanforderungen oder die Meldepflicht nach § 11 Absatz 1a bis 1c EnWG vorgesehen. Die Änderungen in Absatz 1 Nummer 2a und 2b dienen der Ausweitung der Bußgeldvorschriften auf die gemäß § 11 Absatz 1a und 1b zur Einhaltung von Sicherheitsanforderungen und Meldepflichten verpflichteten Betreiber und setzen insofern die Vorgaben des Art. 21 der Richtlinie (EU) 2016/1148 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 § 291b SGB-V)

Die Gesellschaft für Telematik 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 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 Artikel 14 Absatz 1 bis 3 der Richtlinie (EU) 2016/1148 erfüllen. § 291b Absatz 1 SGB V enthält an die Gesellschaft für Telematik gerichtete technische und

funktionale Vorgaben, einschließlich der 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 Absatz 1b bis 1e sind die weiteren Rahmenbedingungen für den Betrieb und Nutzung der Telematikinfrastruktur geregelt, mit denen der Sicherstellungsauftrag der Gesellschaft für Telematik für 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, 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 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 hat.

Die Gesellschaft für Telematik 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 Richtlinie (EU) 2016/1148 entspricht. Nach Art. 15 Absatz 1 und 2 der Richtlinie (EU) 2016/1148 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 4 erfüllt. Für diesen Fall sieht die Richtlinie (EU) 2016/1148 vor, dass neben den Ergebnissen der Überprüfung durch einen qualifizierten Prüfer auch die diesen zugrunde gelegten Nachweise verlangt werden können. Artikel 15 Absatz 3 der Richtlinie (EU) 2016/1148 sieht vor, dass die

zuständige Behörde den Betreibern verbindliche Anweisungen zur Abhilfe der festgestellten Mängel erteilen kann. Absatz 8 Satz 1 bezieht sich ausschließlich auf sicherheitsrelevante Informationen.

Im Rahmen ihres Sicherstellungsauftrags für den Betrieb und die Nutzung der Telematikinfrastruktur verfügt die Gesellschaft für Telematik 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 Absatz 6 und Absatz 7 genannten Befugnissen zu Maßnahmen zur Gefahrenabwehr und Überwachung auch die nähere Ausgestaltung der Zulassungsverfahren [BMG bitte prüfen, ob Entzug der Zulassung nicht jeweils ausdrücklich geregelt werden sollte]. Die Gesellschaft für Telematik 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 Gesellschaft für Telematik allerdings lediglich in Abstimmung mit dem BSI. In Abstimmung im Sinne der Vorschriften bedeutet dabei, dass über ein Stellungnahmerecht hinaus ein Diskussionsprozess mit dem Ziel einer einvernehmlichen Lösung stattfindet. Die Einigung mit dem Bundesamt für Sicherheit in der Informationstechnik stellt den Regelfall dar. Im Falle einer Entscheidung gegen die Auffassung des Bundesamtes für Sicherheit in der Informationstechnik durch die Gesellschaft für Telematik ist dies gesondert und nachvollziehbar zu dokumentieren und zu begründen. Mit dem neuen Absatz 8 wird ergänzend sichergestellt, dass das Bundesamt für Sicherheit in der Informationstechnik in diesen Fällen die Entscheidung prüfen und entsprechend den Vorgaben in Art. 15 Absatz 3 der

Richtlinie (EU) 2016/1148 verbindliche Anweisungen zur Abhilfe der festgestellten Mängel erteilen kann.

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 Richtlinie (EU) 2016/1148 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 4 wird das Bundesamt für Sicherheit in der Informationstechnik, 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.

Zu Artikel 5 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten des Gesetzes.Das Gesetz soll 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.