Bundesrat **Drucksache 643/14**

29.12.14

In - Fz - K - R - U - Wi

Gesetzentwurf
der Bundesregierung

Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

A. Problem und Ziel

Die Nutzung informationstechnischer Systeme (IT-Systeme) und des Internets mit seinen vielfältigen Angeboten durchdringen Staat, Wirtschaft und Gesellschaft in immer größerem Maße. Bedeutende Teilbereiche des privaten und öffentlichen Lebens werden zunehmend ins Netz verlagert oder von diesem beeinflusst. Quer durch alle Branchen ist schon heute mehr als die Hälfte aller Unternehmen in Deutschland vom Internet abhängig. Mit der digitalen Durchdringung der Gesellschaft entstehen in nahezu allen Lebensbereichen neue Potentiale, Freiräume und Synergien. Gleichzeitig wächst die Abhängigkeit von IT-Systemen im wirtschaftlichen, gesellschaftlichen und individuellen Bereich und damit die Bedeutung der Verfügbarkeit und Sicherheit der IT-Systeme sowie des Cyberraums insgesamt.

Die IT-Sicherheitslage in Deutschland ist weiterhin angespannt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erhält und analysiert − u.a. im CERT-Bund, dem IT-Lagezentrum sowie in besonderen Einzelfällen auch in dem 2011 gegründeten Cyberabwehrzentrum − kontinuierlich eine Vielzahl von Informationen zur aktuellen Bedrohungssituation im Cyberraum. Die Angriffe erfolgen zunehmend zielgerichtet und sind technologisch immer ausgereifter und komplexer.

Mit dem Gesetz soll eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme (IT-Sicherheit) in Deutschland erreicht werden. Die vorgesehenen Neuregelungen dienen dazu, den Schutz der Systeme im Hinblick auf die Schutzgüter der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit und

---

Fristablauf: 09.02.15

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

Authentizität) zu verbessern, um den aktuellen und zukünftigen Gefährdungen der IT-Sicherheit wirksam begegnen zu können. Ziel des Gesetzes ist die Verbesserung der IT-Sicherheit von Unternehmen, der verstärkte Schutz der Bürgerinnen und Bürger im Internet und in diesem Zusammenhang auch die Stärkung von BSI und Bundeskriminalamt (BKA).

Besondere Bedeutung kommt im Bereich der IT-Sicherheit denjenigen Infrastrukturen zu, die für das Funktionieren unseres Gemeinwesens zentral sind. Der Schutz der IT-Systeme von solchen Kritischen Infrastrukturen und der für den Infrastrukturbetrieb nötigen Netze ist daher von größter Wichtigkeit. Das IT-Sicherheitsniveau bei Kritischen Infrastrukturen ist derzeit sehr unterschiedlich: In manchen Infrastrukturbereichen existieren detaillierte gesetzliche Vorgaben auch zur IT-Sicherheit, in anderen Bereichen fehlen solche vollständig. Manche Bereiche verfügen über ein ausgeprägtes Risikomanagement und übergreifende Sicherheitskonzepte, führen Audits durch, beteiligen sich am Informationsaustausch und an Übungen. In anderen Bereichen sind diese Maßnahmen noch nicht oder nur rudimentär entwickelt. Auf Grund des hohen Grades der Vernetzung und der daraus resultierenden Interdependenzen zwischen den unterschiedlichen Bereichen Kritischer Infrastrukturen ist dieser Zustand nicht hinnehmbar.

B. Lösung

Defizite im Bereich der IT-Sicherheit sind abzubauen. Insbesondere Betreiber Kritischer Infrastrukturen sind wegen der weitreichenden gesellschaftlichen Folgen, die ein Ausfall oder eine Beeinträchtigung ihrer Infrastrukturen nach sich ziehen kann, und ihrer insoweit besonderen Verantwortung für das Gemeinwohl zu verpflichten, ein Mindestniveau an IT-Sicherheit einzuhalten und dem BSI IT-Sicherheitsvorfälle zu melden. Die beim BSI zusammenlaufenden Informationen werden ausgewertet und den Betreibern Kritischer Infrastrukturen zur Verbesserung des Schutzes ihrer Infrastrukturen schnellstmöglich zur Verfügung gestellt. Die Betreiber leisten insoweit durch die Meldepflicht einen eigenen Beitrag zur IT-Sicherheit und bekommen dafür, da sie auch von den Meldungen der anderen Betreiber und der Auswertung dieser Meldungen durch das BSI profitieren, im Gegenzug ein Mehrfaches an Informationen und Know-how zurück. Gleichzeitig wird die Beratungsfunktion des BSI in diesem Bereich gestärkt.

Um den Schutz der Bürgerinnen und Bürger zu verbessern, werden die Telekommunikationsanbieter, die eine Schlüsselrolle für die Sicherheit des Cyberraums haben, verpflichtet, IT-Sicherheit nach dem Stand der Technik nicht nur zum Schutz des Fernmeldegeheimnisses und zum Schutz personen-

bezogener Daten, sondern auch im Hinblick auf die Verfügbarkeit ihrer Telekommunikations- und Datenverarbeitungssysteme zu gewährleisten. Die Umsetzung der zugrunde liegenden IT-Sicherheitskonzepte in den Unternehmen wird von der Bundesnetzagentur regelmäßig überprüft. Damit wird die Widerstandsfähigkeit der Kommunikationsinfrastruktur insgesamt verbessert und die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit datenverarbeitender Systeme sowie der dort vorgehaltenen Daten gesichert. Mittelbar steigt so auch die Verantwortung der Hersteller zum Angebot entsprechender Produkte.

Telekommunikationsanbieter sollen zudem IT-Sicherheitsvorfälle, die zu einem unerlaubten Zugriff auf die Systeme der Nutzerinnen und Nutzer oder einer Beeinträchtigung der Verfügbarkeit führen können, unverzüglich über die Bundesnetzagentur an das BSI melden und betroffene Nutzerinnen und Nutzer über bekannte Störungen informieren, die durch Schadprogramme auf den datenverarbeitenden Systemen der Nutzerinnen und Nutzer hervorgerufen werden.

Da eine Vielzahl von IT-Angriffen bereits durch die Umsetzung von Standard-sicherheitsmaßnahmen abgewehrt werden könnte, leistet eine verstärkte Sensibilisierung der Nutzerinnen und Nutzer durch die im Gesetz vorgesehene Aufklärung der Öffentlichkeit durch einen jährlichen Bericht einen wichtigen Beitrag zur Verbesserung der IT-Sicherheit. Die gewachsene Rolle des BSI als nationale zentrale Stelle für IT-Sicherheit gegenüber ausländischen Staaten wird festgeschrieben, der Anteil des BSI an der Erstellung des Sicherheitskatalogs für Telekommunikationsnetzbetreiber ausgebaut. Begleitend dazu wird das BKA im Bereich Cyberkriminalität angesichts der zunehmenden Zahl von IT-Angriffen gegen Bundeseinrichtungen und gegen bundesweite Kritische Infrastrukturen in seinen Rechten gestärkt.

Die Regelungen für Betreiber Kritischer Infrastrukturen, die branchenspezifische Sicherheitsanforderungen sowie die Meldepflicht erheblicher IT-Sicherheitsvorfälle betreffen, entsprechen im Grundsatz dem Vorschlag der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union.

C. Alternativen

Beibehalten des bisherigen Rechtszustandes.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Hinsichtlich des Erfüllungsaufwands für die Wirtschaft ist zu unterscheiden zwischen Genehmigungsinhabern nach dem Atomgesetz, Betreibern von Energieversorgungsnetzen und Energieanlagen, bestimmten Telekommunikationsanbietern, sonstigen Betreibern Kritischer Infrastrukturen sowie bestimmten Telemediendiensteanbietern:

Betreibern Kritischer Infrastrukturen entsteht Erfüllungsaufwand für

- die Einhaltung eines Mindestniveaus an IT-Sicherheit,
- den Nachweis der Erfüllung durch Sicherheitsaudits,
- die Einrichtung und Aufrechterhaltung von Verfahren für die Meldung erheblicher IT-Sicherheitsvorfälle an das BSI sowie
- das Betreiben einer Kontaktstelle.

Genehmigungsinhabern nach dem Atomgesetz entsteht Erfüllungsaufwand für

- die Einrichtung von Verfahren für die Meldung von IT-Sicherheitsvorfällen an das BSI.

Betreibern von Energieversorgungsnetzen und Energieanlagen, die als Kritische Infrastruktur im Sinne des BSI-Gesetzes eingestuft wurden, entsteht Erfüllungsaufwand für

- die Einrichtung von Verfahren für die Meldung von IT-Sicherheitsvorfällen an das BSI .

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

- für die Einhaltung zusätzlicher IT-Sicherheitsanforderungen sowie
- die Überprüfung der Einhaltung dieser Sicherheitsanforderungen.

Telemediendiensteanbietern entsteht Erfüllungsaufwand für

- die Sicherung ihrer technischen Einrichtungen durch Maßnahmen nach dem Stand der Technik.

Betreibern öffentlicher Telekommunikationsnetze und öffentlich zugänglicher Telekommunikationsdienste entsteht Erfüllungsaufwand für

- die Sicherung ihrer technischen Einrichtungen durch Maßnahmen nach dem Stand der Technik,
- die Aufrechterhaltung und Erweiterung von Verfahren für die Meldung von IT-Sicherheitsvorfällen an die Bundesnetzagentur sowie
- die Benachrichtigung der Nutzerinnen und Nutzer, wenn erkannt wird, dass von deren Datenverarbeitungssystemen Störungen ausgehen.

Die Verpflichtung zur Einhaltung eines Mindestniveaus an IT-Sicherheit wird dort zu Mehrkosten führen, wo kein hinreichendes IT-Sicherheitsniveau vorhanden ist. Der entstehende Aufwand hängt einerseits vom erforderlichen Sicherheitsniveau und andererseits vom jeweiligen Status quo des Normadressaten ab. Der hierfür anfallende Aufwand kann im Voraus nicht quantifiziert werden. Entsprechendes gilt für den durch die Überprüfung der Einhaltung dieses Sicherheitsniveaus entstehenden Aufwand für Sicherheitsaudits. Der Aufwand und damit die Kosten für eine Zertifizierung oder für ein Audit hängen stark von dem gewählten Zertifizierungsverfahren sowie von den jeweiligen Gegebenheiten im Unternehmen ab. Auch dieser Aufwand kann daher im Voraus nicht quantifiziert werden. Auch die Verpflichtung zum Betreiben einer Kontaktstelle wird dort zu einem Mehraufwand führen, wo noch keine entsprechende Kontaktstelle vorhanden ist. Die Kosten hierfür hängen von der konkreten Ausgestaltung der Erreichbarkeit durch den Betreiber der Kritischen Infrastruktur ab. Kostensenkend kann sich insoweit die Einrichtung einer gemeinsamen übergeordneten Ansprechstelle auswirken.

Der jährliche Erfüllungsaufwand der Wirtschaft 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.

Die konkrete Berechnung der Gesamtkosten kann erst mit Erlass der Rechtsverordnung nach § 10 des BSI-Gesetzes auf der Grundlage des im Zweiten Teils der Begründung dargestellten Verfahrens erfolgen, da erst durch die Rechtsverordnung der Adressatenkreis der entsprechenden Verpflichtungen hinreichend konkret eingegrenzt und eine entsprechende Zahl meldepflichtiger Betreiber Kritischer Infrastrukturen benannt werden kann.

Nach aktuellen Schätzungen wird die Zahl der meldepflichtigen Betreiber Kritischer Infrastrukturen bei maximal 2.000 Betreibern liegen. Weiterhin wird geschätzt, dass pro Betreiber maximal sieben Meldungen von IT-Sicherheitsvorfällen pro Jahr erfolgen. Da relevante IT-Sicherheitsvorfälle von den Betreibern auch ohne die im Gesetz vorgesehene Meldepflicht untersucht, bewältigt und dokumentiert werden müssen, fällt bei den Bürokratiekosten nur insoweit ein Mehraufwand an, als die Bearbeitung über die ohnehin im Rahmen einer systematischen Bearbeitung relevanten Vorfälle hinausgeht. Auf Grund von Angaben aus der Wirtschaft auf der Grundlage von Berechnungen nach dem Standardkostenmodell werden die Kosten für die Bearbeitung einer Meldung derzeit mit 660 Euro pro Meldung (11 Stunden Zeitaufwand bei einem Stundensatz von 60 Euro) beziffert. Zum Teil werden solche Vorfälle schon heute dem BSI gemeldet.

Legt man den Berechnungen eine Anzahl von 2.000 Betreibern Kritischer Infrastrukturen zugrunde, die jeweils sieben IT-Sicherheitsvorfälle pro Jahr melden, für deren Bearbeitung jeweils ein zusätzlicher Aufwand von 660 Euro pro Meldung entsteht, so entsteht den Betreibern Kritischer Infrastrukturen für die Erfüllung der Meldepflicht ein jährlicher Erfüllungsaufwand von insgesamt 9,24 Millionen Euro.

Hinzu kommt der Erfüllungsaufwand für die Betreiber öffentlicher Telekommunikationsnetze und öffentlich zugänglicher Telekommunikationsdienste für die Aufrechterhaltung und Erweiterung von Verfahren für die Meldung von IT-Sicherheitsvorfällen an die Bundesnetzagentur. Da es in diesem Bereich bereits ein etabliertes Verfahren zur Meldung von IT-Sicherheitsvorfällen an die Bundesnetzagentur gibt, das durch das Gesetz lediglich erweitert wird, lässt sich der hierdurch entstehende Mehraufwand nicht quantifizieren. Auf Grund von Angaben aus der Wirtschaft werden die Kosten für die Bearbeitung einer Meldung derzeit auch für diesen Bereich mit 660 Euro pro Meldung (11 Stunden Zeitaufwand bei einem Stundensatz von 60 Euro) beziffert. Von entsprechenden Kosten je Meldung wird auch für die Genehmigungsinhaber nach dem Atomgesetz ausgegangen.

E.3 Erfüllungsaufwand für die Verwaltung

Schon heute werden den zuständigen Behörden IT-Sicherheitsvorfälle gemeldet.

Beim BSI entsteht für die Erfüllung der im Gesetz vorgesehenen Aufgabe − in Abhängigkeit von der Zahl der Betreiber Kritischer Infrastrukturen und der Anzahl der eingehenden Meldungen − ein Aufwand von insgesamt zwischen 115 bis zu maximal 216,5 Planstellen/Stellen mit Personalkosten in Höhe von jährlich zwischen rund 8,95 und bis zu maximal 15,867 Millionen Euro sowie Sachkosten in Höhe von einmalig rund 5 bis 7 Millionen Euro.

Beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) führen die neuen Mitwirkungsaufgaben zu einem Bedarf von zwischen 9 und bis zu maximal 13 Planstellen/Stellen mit jährlichen Personalkosten zwischen 711 000 und bis zu maximal 1,011 Millionen Euro.

Bei der Bundesnetzagentur (BNetzA) führen die neuen Aufgaben zu einem Bedarf von bis zu maximal 28 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von rund bis zu maximal 3,202 Millionen Euro. Des Weiteren entstehen Kosten für Sachmittel in Höhe von einmalig 150 000 Euro im ersten Jahr für die Aufgaben nach § 109 Absatz 4 Satz 7 und 8 sowie Absatz 5 des Telekommunikations-gesetzes.

In den Fachabteilungen des BKA entsteht ein Ressourcenaufwand von zwischen 48 und bis zu maximal 78 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von jährlich zwischen rund 3,226 und bis zu maximal 5,310 Millionen Euro. Des Weiteren entstehen Kosten für Sachmittel in Höhe von jährlich bis zu maximal 630 000 Euro.

In den Fachabteilungen des Bundesamtes für Verfassungsschutz (BfV) entsteht durch die Zuständigkeit gemäß § 8b Absatz 2 Nummer 4 des BSI-Gesetzes ein Bedarf von zwischen 26,5 und maximal 48,5 Planstellen/Stellen mit Personalkosten in Höhe von jährlich zwischen 1,836 und maximal 3,253 Millionen Euro. Des Weiteren entstehen Kosten für Sachmittel in Höhe von maximal 610 000 Euro jährlich.

In den Fachabteilungen des Bundesnachrichtendienstes (BND) entsteht durch die Zuständigkeit gemäß § 8b Absatz 2 Nummer 4 des BSI-Gesetzes im Zusammenhang mit der Prüfung ausländischer Datenstrecken auf Schadsoftware-Signaturen und Rückverfolgung von Schadsoftware im Ausland ein Bedarf von maximal 30 Planstellen/Stellen mit Personalkosten in Höhe von jährlich maximal

2,153 Millionen Euro. Des Weiteren ein jährlicher Bedarf an Sachkosten in Höhe von maximal 688 000 Euro.

In der Fachabteilung des für die nukleare Sicherheit und die Sicherung zuständigen Bundesministeriums für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMUB) führen die neuen Mitwirkungspflichten für das zentrale IT-Meldesystem an das BSI nach § 44b des Atomgesetzes (neu) und bei der Erarbeitung der Sicherheitsanforderungen für Energieanlagen nach § 11 Absatz 1b des Energiewirtschaftsgesetzes zu einem Bedarf von bis zu maximal 4 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von maximal rund 240 000 Euro.

Bei der Bundesbeauftragten für Datenschutz und Informationsfreiheit entsteht ein Bedarf von zwischen 2,4 und bis zu maximal 7 Planstellen/Stellen.

Im Ressort des Bundesministeriums für Arbeit und Soziales wird für das Bundesversicherungsamt vor Erlass der Rechtsverordnung nach § 10 Absatz 1 des BSI-Gesetzes noch nicht quantifizierbarer Aufwand im Hinblick auf die Rechtsaufsicht als zuständige Aufsichtsbehörde über die bundesunmittelbaren Träger der Sozialversicherung er-wartet. Das Gleiche gilt für die fachlichen Aufsichtsbehörden (Bundesamt für Güterverkehr, Eisenbahn-Bundesamt, Luftfahrt-Bundesamt, Bundesaufsichtsamt für Flugsicherung, Generaldirektion Wasserstraßen und Schifffahrt, Bundesamt für Seeschifffahrt und Hydrografie) im Ressort des Bundesministeriums für Verkehr und Digitale Infrastruktur im Hinblick auf den Sektor Transport und Verkehr.

Darüber hinaus können Verträge des Bundes mit Dritten, die Kommunikationstechnik im Auftrag des Bundes betreiben sollen und hierzu Leistungen von Unternehmen in Anspruch nehmen, die dem Gesetz unterliegen, zu Ausgaben führen, die aus heutiger Sicht noch nicht bezifferbar sind.

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

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

F. Weitere Kosten

Infolge der von den Betreibern Kritischer Infrastrukturen umzusetzenden Maßnahmen entstehen geringe, aber noch nicht quantifizierbare Kosten für die fallweise Anpassung der IT-Verfahren, die von den Bundesbehörden bereitgestellt werden.

Begründung
A. Allgemeiner Teil

I. Zweck und Inhalt des Gesetzes

Mit dem Gesetz soll eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme (IT-Sicherheit) in Deutschland erreicht werden. Die vorgesehenen Neuregelungen dienen dazu, den Schutz der Systeme im Hinblick auf die Schutzgüter der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität) zu verbessern und die Systeme der IT-Sicherheitslage anzupassen. Ziel des Gesetzes ist eine Verbesserung der IT-Sicherheit bei Unternehmen, ein verstärkter Schutz der Bürgerinnen und Bürger im Internet und in diesem Zusammenhang auch eine Stärkung des Bundesamts für Sicherheit in der Informationstechnik (BSI) und des Bundeskriminalamts (BKA).

Der Entwurf sieht für Betreiber Kritischer Infrastrukturen zum einen die Pflicht zur Einhaltung eines Mindestniveaus an IT-Sicherheit und zum anderen die Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle vor. Zum Schutz der Bürgerinnen und Bürger kommen weitere Pflichten für Telekommunikations- und Telemediendiensteanbieter bei ihren Angeboten und den damit einhergehenden Datenverarbeitungsprozessen hinzu.

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 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 konkurrierenden 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 aus der konkurrierenden Gesetzgebungskompetenz für das Recht der Wirtschaft (Artikel 74 Absatz 1 Nummer 11 GG). Die Berechtigung des Bundes zur Inanspruchnahme dieser Gesetzgebungskompetenz ergibt sich 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.

Die Änderungen im Telekommunikationsgesetz (Artikel 5) können auf die ausschließliche Gesetzgebungskompetenz des Bundes nach Artikel 73 Absatz 1 Nummer 7 GG gestützt werden. Der Bund hat darüber hinaus die ausschließliche Gesetzgebungskompetenz nach Artikel 73 Absatz 1 Nummer 8 GG für die Rechtsverhältnisse der im Dienst des Bundes und der bundesunmittelbaren Körperschaften des öffentlichen Rechts stehenden Personen (Artikel 6). Die Änderung des BKA-Gesetzes (Artikel 7) beruht auf der Gesetzgebungskompetenz nach Artikel 73 Absatz 1 Nummer 10 GG.

III. Erfüllungsaufwand

1. Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

2. Erfüllungsaufwand für die Wirtschaft

Hinsichtlich des Erfüllungsaufwands für die Wirtschaft ist zu unterscheiden zwischen Genehmigungsinhabern nach dem Atomgesetz, Betreibern von Energieversorgungsnetzen und Energieanlagen, bestimmten Telekommunikationsanbietern, sonstigen Betreibern Kritischer Infrastrukturen sowie bestimmten Telemediendiensteanbietern:

Betreibern Kritischer Infrastrukturen entsteht Erfüllungsaufwand für

- die Einhaltung eines Mindestniveaus an IT-Sicherheit,
- den Nachweis der Erfüllung durch Sicherheitsaudits,
- die Einrichtung und Aufrechterhaltung von Verfahren für die Meldung erheblicher IT-Sicherheitsvorfälle an das BSI sowie
- das Betreiben einer Kontaktstelle.

Genehmigungsinhabern nach dem Atomgesetz entsteht Erfüllungsaufwand für

- die Einrichtung von Verfahren für die Meldung von IT-Sicherheitsvorfällen an das BSI.

Betreibern von Energieversorgungsnetzen und Energieanlagen, die als Kritische Infrastruktur im Sinne des BSI-Gesetzes eingestuft wurden, entsteht Erfüllungsaufwand für

- die Einrichtung von Verfahren für die Meldung von IT-Sicherheitsvorfällen an das BSI.

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

- für die Einhaltung zusätzlicher IT-Sicherheitsanforderungen sowie
- die Überprüfung der Einhaltung dieser Sicherheitsanforderungen.

Telemediendiensteanbietern entsteht Erfüllungsaufwand für

- die Sicherung ihrer technischen Einrichtungen durch Maßnahmen nach dem Stand der Technik.

Betreibern öffentlicher Telekommunikationsnetze und öffentlich zugänglicher Telekommunikationsdienste entsteht Erfüllungsaufwand für

- die Sicherung ihrer technischen Einrichtungen durch Maßnahmen nach dem Stand der Technik,
- die Aufrechterhaltung und Erweiterung von Verfahren für die Meldung von IT-Sicherheitsvorfällen an die Bundesnetzagentur sowie
- die Benachrichtigung der Nutzerinnen und Nutzer, wenn erkannt wird, dass von deren Datenverarbeitungssystemen Störungen ausgehen.

Die Verpflichtung zur Einhaltung eines Mindestniveaus an IT-Sicherheit wird dort zu Mehrkosten führen, wo kein hinreichendes IT-Sicherheitsniveau vorhanden ist. Der entstehende Aufwand hängt einerseits vom erforderlichen Sicherheitsniveau und andererseits vom jeweiligen Status quo des Normadressaten ab. Der hierfür anfallende Aufwand kann im Voraus nicht quantifiziert werden. Entsprechendes gilt für den durch die Überprüfung der Einhaltung dieses Sicherheitsniveaus entstehenden Aufwand für Sicherheitsaudits. Der Aufwand und damit die Kosten für eine Zertifizierung oder für ein Audit hängen stark von dem gewählten Zertifizierungsverfahren sowie von den jeweiligen Gegebenheiten im Unternehmen ab. Auch dieser Aufwand kann daher im Voraus

nicht quantifiziert werden. Auch die Verpflichtung zum Betreiben einer Kontaktstelle wird dort zu einem Mehraufwand führen, wo noch keine entsprechende Kontaktstelle vorhanden ist. Die Kosten hierfür hängen von der konkreten Ausgestaltung der Erreichbarkeit durch den Betreiber der Kritischen Infrastruktur ab. Kostensenkend kann sich insoweit die Einrichtung einer gemeinsamen übergeordneten Ansprechstelle auswirken.

Der jährliche Erfüllungsaufwand der Wirtschaft 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.

Die konkrete Berechnung der Gesamtkosten kann erst mit Erlass der Rechtsverordnung nach § 10 des BSI-Gesetzes auf der Grundlage des im Zweiten Teils der Begründung dargestellten Verfahrens erfolgen, da erst durch die Rechtsverordnung der Adressatenkreis der entsprechenden Verpflichtungen hinreichend konkret eingegrenzt und eine entsprechende Zahl meldepflichtiger Betreiber Kritischer Infrastrukturen benannt werden kann.

Nach aktuellen Schätzungen wird die Zahl der meldepflichtigen Betreiber Kritischer Infrastrukturen bei maximal 2.000 Betreibern liegen. Weiterhin wird geschätzt, dass pro Betreiber maximal sieben Meldungen von IT-Sicherheitsvorfällen pro Jahr erfolgen. Da relevante IT-Sicherheitsvorfälle von den Betreibern auch ohne die im Gesetz vorgesehene Meldepflicht untersucht, bewältigt und dokumentiert werden müssen, fällt bei den Bürokratiekosten nur insoweit ein Mehraufwand an, als die Bearbeitung über die ohnehin im Rahmen einer systematischen Bearbeitung relevanten Vorfälle hinausgeht. Auf Grund von Angaben aus der Wirtschaft auf der Grundlage von Berechnungen nach dem Standardkostenmodell werden die Kosten für die Bearbeitung einer Meldung derzeit mit 660 Euro pro Meldung (11 Stunden Zeitaufwand bei einem Stundensatz von 60 Euro) beziffert. Zum Teil werden solche Vorfälle schon heute dem BSI gemeldet.

Legt man den Berechnungen eine Anzahl von 2.000 Betreibern Kritischer Infrastrukturen zugrunde, die jeweils sieben IT-Sicherheitsvorfälle pro Jahr melden, für deren Bearbeitung jeweils ein zusätzlicher Aufwand von 660 Euro pro Meldung entsteht, so entsteht den Betreibern Kritischer Infrastrukturen für die Erfüllung der Meldepflicht ein jährlicher Erfüllungsaufwand von insgesamt 9,24 Millionen Euro.

Hinzu kommt der Erfüllungsaufwand für die Betreiber öffentlicher Telekommunikationsnetze und öffentlich zugänglicher Telekommunikationsdienste für die Aufrechterhaltung und Erweiterung von Verfahren für die Meldung von IT-Sicherheitsvorfällen an die Bundesnetzagentur. Da es in diesem Bereich bereits ein etabliertes Verfahren zur Meldung von IT-Sicherheitsvorfällen an die Bundesnetzagentur gibt, das durch das Gesetz lediglich erweitert wird, lässt sich der hierdurch entstehende Mehraufwand nicht seriös quantifizieren. Auf Grund von Angaben aus der Wirtschaft werden die Kosten für die Bearbeitung einer Meldung derzeit auch für diesen Bereich mit 660 Euro pro Meldung (11 Stunden Zeitaufwand bei einem Stundensatz von 60 Euro) beziffert. Von entsprechenden Kosten je Meldung wird auch für die Genehmigungsinhaber nach dem Atomgesetz ausgegangen.

3. Erfüllungsaufwand der Verwaltung

Schon heute werden den zuständigen Behörden IT-Sicherheitsvorfälle gemeldet.

Beim BSI entsteht für die Erfüllung der im Gesetz vorgesehenen Aufgaben − in Abhängigkeit von der Zahl der Betreiber Kritischer Infrastrukturen und der Anzahl der eingehenden Meldungen − ein Aufwand von insgesamt zwischen 115 bis zu maximal 216,5 Planstellen/Stellen mit Personalkosten in Höhe von jährlich zwischen rund 8,95 und bis zu maximal 15,867 Millionen Euro sowie Sachkosten in Höhe von einmalig rund 5 bis 7 Millionen Euro.

Der Personalbedarf des BSI begründet sich neben den erweiterten Verantwortlichkeiten insbesondere dadurch, dass Informationstechnik in den sieben relevanten KRITIS-Sektoren (KRITIS: Kritische Infrastrukturen) sehr unterschiedlich eingesetzt wird. Dies betrifft sowohl die genutzten Komponenten, Produkte, Systeme und externen IKT-Dienstleistungen (IKT: Informations- und Kommunikationstechnik) als auch die eingesetzte IT zur Sicherung der Funktionsfähigkeit der kritischen Prozesse selbst. Weiterhin ist zu berücksichtigen, dass im Vergleich zur klassischen Informationstechnik die Besonderheiten der sektorspezifischen Rahmenbedingungen für kritische Prozesse individuell betrachtet werden müssen. Dadurch ergibt sich auch die Notwendigkeit zur deutlichen Ausweitung der Grundlagenarbeit und Fachkompetenz im BSI, die bisher vordringlich auf die Sicherheit der Informationstechnik des Bundes fokussiert war. Die Beratung der KRITIS-Betreiber muss sich an der IKT-Sicherheit zur Gewährleistung der zu erbringenden Dienstleistung ausrichten. Hierzu sind umfangreiche Kenntnisse über die Funktionsweise und informationstechnische Abstützung der kritischen Prozesse der jeweiligen KRITIS-Sektoren und KRITIS-Branchen erforderlich. Der geforderte Personalbedarf

ermöglicht den Aufbau der notwendigen Fachexpertise und stellt die Basis für Grundlagenberatung und Unterstützung dar. Eine systematische, individuelle Einzelberatung für alle Betreiber Kritischer Infrastrukturen ist hingegen nicht möglich. Zur Ermittlung des Stands der Technik in den einzelnen KRITIS-Branchen und für die Anerkennung der von den Branchen erstellten Branchenstandards ist in hohem Maße Fachkompetenz und Ressourcenaufwand erforderlich. Dies gilt ebenfalls für die Identifizierung konkreter Sicherheitsmängel und für die Prüfung angeforderter Auditberichte. Auch zum Auswerten von in der Meldestelle eingehender Informationen, zum Fortschreiben des Lagebildes und bei der Vorhersage der potentiellen Auswirkungen einer Meldung bzw. Störung auf die betroffene Kritische Infrastruktur oder ihre Branche ist spezielles Know-how in Bezug auf die jeweiligen KRITIS-Sektoren und KRITIS-Branchen zwingend erforderlich. Darüber hinaus erfordert die Wahrnehmung der Aufgabe als zentrale Meldestelle für die Sicherheit in der Informationstechnik für die Betreiber Kritischer Infrastrukturen den Ausbau des BSI-Lagezentrums auf einen 24/7-Betrieb. Im Rahmen der neuen Aufgaben des BSI soll es auch zu weiteren Einnahmen von Gebühren kommen.

Beim Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) führen die neuen Mitwirkungsaufgaben zu einem Bedarf von zwischen 9 und bis zu maximal 13 Planstellen/Stellen mit jährlichen Personalkosten zwischen 711 000 und bis zu maximal 1,011 Millionen Euro.

Bei der Bundesnetzagentur (BNetzA) führen die neuen Aufgaben zu einem Bedarf von bis zu maximal 28 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von rund bis zu maximal 3,202 Millionen Euro. Des Weiteren entstehen Kosten für Sachmittel in Höhe von einmalig 150 000 Euro im ersten Jahr für die Aufgaben nach § 109 Absatz 4 Satz 7 und 8 sowie Absatz 5 des Telekommunikationsgesetzes.

In den Fachabteilungen des BKA entsteht ein Ressourcenaufwand von zwischen 48 und bis zu maximal 78 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von jährlich zwischen rund 3,226 und bis zu maximal 5,310 Millionen Euro. Des Weiteren entstehen Kosten für Sachmittel in Höhe von jährlich bis zu maximal 630 000 Euro.

In den Fachabteilungen des Bundesamtes für Verfassungsschutz (BfV) entsteht durch die Zuständigkeit gemäß § 8b Absatz 2 Nummer 4 des BSI-Gesetzes ein Bedarf von zwischen 26,5 und maximal 48,5 Planstellen/Stellen mit Personalkosten in Höhe von jährlich zwischen 1,836 und maximal 3,253 Millionen Euro. Des Weiteren entstehen Kosten für Sachmittel in Höhe von maximal 610 000 Euro jährlich.

In den Fachabteilungen des Bundesnachrichtendienstes (BND) entsteht durch die Zuständigkeit gemäß § 8b Absatz 2 Nummer 4 des BSI-Gesetzes im Zusammenhang mit der Prüfung ausländischer Datenstrecken auf Schadsoftware-Signaturen und Rückverfolgung von Schadsoftware im Ausland ein Bedarf von maximal 30 Planstellen/Stellen mit Personalkosten in Höhe von jährlich maximal 2,153 Millionen Euro. Des Weiteren ein jährlicher Bedarf an Sachkosten in Höhe von maximal 688 000 Euro.

In der Fachabteilung des für die nukleare Sicherheit und die Sicherung zuständigen Bundesministeriums für Umwelt, Naturschutz, Bau und Reaktorsicherheit (BMUB) führen die neuen Mitwirkungspflichten für das zentrale IT-Meldesystem an das BSI nach § 44b des Atomgesetzes (neu) und bei der Erarbeitung der Sicherheitsanforderungen für Energieanlagen nach § 11 Absatz 1b des Energiewirtschaftsgesetzes zu einem Bedarf von bis zu maximal 4 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von maximal rund 240 000 Euro.

Bei der Bundesbeauftragten für Datenschutz und Informationsfreiheit entsteht ein Bedarf von zwischen 2,4 und bis zu maximal 7 Planstellen/Stellen.

Im Ressort des Bundesministeriums für Arbeit und Soziales wird für das Bundesversicherungsamt vor Erlass der Rechtsverordnung nach § 10 Absatz 1 des BSI-Gesetzes noch nicht quantifizierbarer Aufwand im Hinblick auf die Rechtsaufsicht als zuständige Aufsichtsbehörde über die bundesunmittelbaren Träger der Sozialversicherung erwartet. Das Gleiche gilt für die fachlichen Aufsichtsbehörden (Bundesamt für Güterverkehr, Eisenbahn-Bundesamt, Luftfahrt-Bundesamt, Bundesaufsichtsamt für Flugsicherung, Generaldirektion Wasserstraßen und Schifffahrt, Bundesamt für Seeschifffahrt und Hydrografie) im Ressort des Bundesministeriums für Verkehr und Digitale Infrastruktur im Hinblick auf den Sektor Transport und Verkehr.

Darüber hinaus können Verträge des Bundes mit Dritten, die Kommunikationstechnik im Auftrag des Bundes betreiben sollen und hierzu Leistungen von Unternehmen in Anspruch nehmen, die dem Gesetz unterliegen, zu Ausgaben führen, die aus heutiger Sicht noch nicht bezifferbar sind.

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

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

IV. Weitere Kosten

Geringe, aber noch nicht quantifizierbare Kosten für die fallweise Anpassung der von Bundesbehörden bereitgestellten IT-Verfahren infolge der von den Betreibern Kritischer Infrastrukturen umzusetzenden Maßnahmen.

V. Gleichstellungspolitische Relevanz

Die Regelungen sind inhaltlich geschlechtsneutral und damit ohne Gleichstellungsrelevanz. Die Stärkung der IT-Sicherheit betrifft sowohl mittelbar wie unmittelbar Frauen wie Männer gleichermaßen. § 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 mit der Anhebung der Sicherheitsstandards in der deutschen IT-Sicherheitsarchitektur, die zunehmend alle Gesellschaftsbereiche durchdringt, 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.

B. Besonderer Teil

Zu Artikel 1 (Änderung des BSI-Gesetzes)

Zu Nummer 1 (§ 1 Bundesamt für Sicherheit in der Informationstechnik)
Die neue Fassung von § 1 trägt der geänderten Rolle des BSI Rechnung. Die Aufgaben des BSI neben der Abwehr von Gefahren für die Sicherheit in der Informationstechnik des Bundes haben an Bedeutung gewonnen. Das BSI dient zunehmend Bürgerinnen und Bürgern, Unternehmen, Verwaltungen und der Politik als Ansprechpartner in Fragen der IT-Sicherheit. Auch auf EU-Ebene sowie international ist das BSI verstärkt der nationale Ansprechpartner in Fragen der IT- und Cybersicherheit in Deutschland. Die Entwicklung des BSI hin zur nationalen Informationssicherheitsbehörde wird mit der Änderung des § 1 nachvollzogen.

Zu Nummer 2 (§ 2 Begriffsbestimmungen)
§ 2 Absatz 10 Satz 1 definiert den Begriff der Kritischen Infrastrukturen im Sinne der Regelungen des BSI-Gesetzes. Da es bislang noch keine gesetzlich geregelte Definition der Kritischen Infrastrukturen in Deutschland gibt, ist die Begriffsbestimmung notwendig, um die Adressaten der §§ 8a und 8b des BSI-Gesetzes zu bestimmen.

Die Definition folgt im Grundsatz der innerhalb der Bundesregierung abgestimmten Einteilung Kritischer Infrastrukturen. Dazu gehören die Bereiche Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie das Finanz- und Versicherungswesen. Zur Umsetzung der in den §§ 8a und 8b des BSI-Gesetzes getroffenen Vorgaben sind innerhalb dieser Sektoren diejenigen Einrichtungen, Anlagen oder Teile davon zu identifizieren, die als Kritische Infrastrukturen im Sinne des BSI-Gesetzes einzustufen sind, weil sie für das Funktionieren des Gemeinwesens und die Sicherung der Grundbedürfnisse der Bevölkerung von hoher Bedeutung sind und deshalb besonders schutzwürdig sind.

Die weitere Konkretisierung bedarf der sektor- und branchenspezifischen Einbeziehung aller betroffenen Kreise (Verwaltung, Wirtschaft und Wissenschaft). Die jeweils anzulegenden Maßstäbe können nur in einem gemeinsamen Arbeitsprozess mit Vertretern der möglicherweise betroffenen Betreiber Kritischer Infrastrukturen und unter Einbeziehung der Expertise von externen Fachleuten in sachgerechter Weise erarbeitet werden. Hinzu kommt, dass der technische und gesellschaftliche Wandel sowie die im Rahmen der

Umsetzung der neuen gesetzlichen Vorgaben gemachten Erfahrungen in den Folgejahren gegebenenfalls Anpassungen erforderlich machen. Die nähere Bestimmung der Kritischen Infrastrukturen ist daher gemäß Satz 2 einer Rechtsverordnung vorbehalten. Diese ist auf der Grundlage von § 10 Absatz 1 des BSI-Gesetzes zu erlassen. Hierbei ist vorgesehen, die Einteilung der Kritischen Infrastrukturen nach den Kriterien Qualität und Quantität vorzunehmen. Zu Einzelheiten siehe die Ausführungen zu § 10 Absatz 1 des BSI-Gesetzes.

Nicht zu den vom BSI-Gesetz adressierten Kritischen Infrastrukturen gehören die Verwaltung von Regierung und Parlament sowie die öffentliche Bundesverwaltung und die von ihr eingesetzte Technik (einschließlich der Technik, die im Auftrag der Bundesverwaltung betrieben wird). Als Spezialregelung gelten hier unter anderem die §§ 4, 5 und 8 des BSI-Gesetzes. Entsprechendes gilt für die Verwaltungen der Länder und Kommunen, für die der Bund keine Gesetzgebungskompetenz besitzt. Das Gleiche gilt für den Sektor Kultur und Medien, da auch hier die Gesetzgebungskompetenz überwiegend bei den Ländern liegt.

Zu Nummer 3 (§ 3 Aufgaben des Bundesamtes)

Zu Buchstabe a (Änderungen der Aufgaben in Absatz 1 Satz 2)
Zu Doppelbuchstabe aa (Zurverfügungstellung gewonnener Erkenntnisse)
Die Änderung in Absatz 1 Satz 2 Nummer 2 dient der Klarstellung, dass durch das BSI bei der Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen gewonnene Erkenntnisse nicht nur Behörden, sondern auch anderen („Dritten“) zur Verfügung gestellt werden können, soweit dies zur Wahrung der Sicherheitsinteressen erforderlich ist. Hierdurch wird noch einmal der Mehrwert unterstrichen, den eine verbreitete Erkenntnisbasis und ein verbessertes Lagebild des BSI für Wirtschaft und Gesellschaft haben können. Dritte in diesem Sinne sind insbesondere auch die Betreiber Kritischer Infrastrukturen im Sinne des BSI-Gesetzes. Adressat sollen aber auch sonstige Einrichtungen oder Unternehmen sein, die zwar keine Betreiber Kritischer Infrastrukturen im Sinne des BSI-Gesetzes sind, dennoch aber anerkanntermaßen zum Bereich der Kritischen Infrastrukturen im weiteren Sinne gehören oder sonst ein berechtigtes Sicherheitsinteresse an den entsprechenden Informationen haben (zum Beispiel Einrichtungen aus dem nicht erfassten Sektor Kultur und Medien oder wissenschaftliche Einrichtungen).

Zu Doppelbuchstabe bb (IT-Sicherheit Kritischer Infrastrukturen)
Buchstabe b enthält redaktionelle Anpassungen.

Zu Doppelbuchstabe cc (Bundesamt als zentrale Stelle im internationalen Bereich)
Die ausdrückliche Festschreibung der Aufgabe als zentrale Stelle im Bereich der Sicherheit in der Informationstechnik im Hinblick auf die Zusammenarbeit mit den zuständigen Stellen im Ausland durch Aufnahme der neuen Nummer 16 trägt der gewachsenen Rolle des BSI als nationalem und internationalem Ansprechpartner in Fragen der IT- und Cybersicherheit in Deutschland Rechnung. Besondere Zuständigkeiten anderer Stellen im Bereich der Cybersicherheit (zum Beispiel des Auswärtiges Amtes, des Bundesministeriums der Verteidigung, des Bundesamtes für Verfassungsschutz oder des Bundesnachrichtendienstes) bleiben unberührt.

Bei Nummer 17 handelt es sich um eine notwendige Ergänzung um die vom BSI mit diesem Gesetz neu übernommene Aufgabe als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen, die in den §§ 8a bis 8c des BSI-Gesetzes konkretisiert wird.

Zu Buchstabe b (Aufgaben des Bundesamtes im Bereich der Sicherheit in der Informationstechnik Kritischer Infrastrukturen)
Absatz 3 ermöglicht es dem BSI, Betreiber Kritischer Infrastrukturen auf Ersuchen bei der Sicherung ihrer Informationstechnik, insbesondere im Hinblick auf die Erfüllung der Anforderungen nach den §§ 8a und 8b des BSI-Gesetzes, zu beraten und zu unterstützen. Dies soll (ebenso wie Feststellungen nach § 8a Absatz 2 Satz 2 des BSI-Gesetzes) als individuell zurechenbare öffentliche Leistung in der nach § 10 Absatz 3 des BSI-Gesetzes (neu) zu erlassenden Rechtsverordnung erfasst werden. Das BSI entscheidet nach pflichtgemäßem Ermessen, ob es einem entsprechenden Ersuchen des Betreibers einer Kritischen Infrastruktur nachkommt. In diesem Zusammenhang kann das BSI den Betreiber auch an einen qualifizierten Sicherheitsdienstleister verweisen.

Zu Nummer 4 (§ 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes)
Die Änderung der Überschrift dient klarstellend der Abgrenzung zur neuen Aufgabe des BSI nach § 8b des BSI-Gesetzes.

Zu Nummer 5 (§ 7 Absatz 1 Warnungen)
Die Neufassung von Absatz 1 Satz 1 strukturiert die bereits bestehenden Befugnisse des BSI neu und ergänzt diese um die Befugnis zu Warnungen bei Datenverlust oder bei einem unerlaubten Zugriff auf Daten (Nummer 1 Buchstabe c). Hierdurch wird klargestellt, dass das BSI nach § 7 auch in Fällen tätig werden kann, in denen nicht die Warnung vor einem Schadprogramm oder einer Sicherheitslücke im Vordergrund steht, sondern vielmehr die Bewältigung eines bereits erfolgten Verlustes von oder Zugriffs auf Daten. Zur Schadenseingrenzung wird das BSI im Regelfall frühzeitig eine Warnung aussprechen und die Bürgerinnen und Bürger informieren, es sei denn, dieses Vorgehen würde zu erheblichen Sicherheitsrisiken führen.

Satz 2 ermöglicht es dem BSI, auch zur Klarstellung unter Datenschutzgesichtspunkten, bei Warnungen Dritte als Informationsintermediäre einzubeziehen, sofern dies für eine wirksame und rechtzeitige Warnung erforderlich ist, insbesondere um Betroffene schnellstmöglich zu erreichen. Satz 2 eröffnet aber nicht die Möglichkeit, zusätzliche Daten bei den Dritten zu erheben. Informationsintermediäre sind insbesondere die von den Kundinnen und Kunden genutzten Provider und Diensteanbieter.

Oftmals wird das BSI abhandengekommene Daten nicht direkt einem Betroffenen zuordnen oder diesen nicht ohne weiteres selbst unterrichten können. Im Interesse einer effizienten Warnung der Betroffenen kann sich das BSI daher an sog. Informationsintermediäre mit der Bitte um Unterstützung wenden. Die Informationsintermediäre sind beispielsweise auf Grund der bei ihnen vorhandenen weiter gehenden Informationen oder aus technischen Gründen in der Lage, an einer möglichst schnellen Unterrichtung der Betroffenen mitzuwirken.

Zu Nummer 6 (§ 7a Untersuchung der Sicherheit in der Informationstechnik)
Absatz 1 dient dazu, Rechtssicherheit für umfassende Untersuchungen von IT-Produkten (zum Beispiel mittels Reverse-Engineering) und IT-Systemen durch das BSI zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14 und 17 des BSI-Gesetzes herzustellen. Die gesetzliche Befugnis führt dazu, dass die Beschaffung von Daten und Informationen über den Aufbau und die Funktionsweise der Untersuchungsgegenstände durch das BSI nicht als unbefugt im Sinne von § 202a des Strafgesetzbuches (StGB) bzw. § 17 ff. des Gesetzes gegen den unlauteren Wettbewerb (UWG) anzusehen ist. Eine Strafbarkeit nach den §§ 17 ff. UWG würde im Übrigen ein Handeln zu

Zwecken des Wettbewerbs oder aus Eigennutz bzw. Schadenszufügungsabsicht voraussetzen.

Auf dem Markt bereitgestellte bzw. zur Bereitstellung auf dem Markt vorgesehene Untersuchungsgegenstände sind solche, die für einen Erwerb durch das BSI verfügbar sind. Die Formulierung „auf dem Markt bereitgestellte Produkte“ ist angelehnt an eine entsprechende Formulierung im Produktsicherheitsgesetz. Durch die Formulierung „zur Bereitstellung auf dem Markt vorgesehene“ Untersuchungsgegenstände wird klargestellt, dass die Untersuchungsbefugnis auch solche Produkte und Systeme erfasst, die zwar vom Hersteller bereits angekündigt wurden, aber noch nicht allgemein am Markt verfügbar sind.

Untersuchungsrechte des BSI bei Herstellern, Anbietern und sonstigen Einrichtungen werden durch Absatz 1 nicht begründet.

Bei der Auswahl der Dritten, die vom BSI nach Absatz 1 Satz 2 mit der Untersuchung beauftragt werden können, hat das BSI die schutzwürdigen Interessen des Herstellers zu berücksichtigen. Hierzu gehört auch, dass das BSI den beauftragten Dritten zur Wahrung einer entsprechenden Vertraulichkeit verpflichtet. Die Beauftragung eines direkten Konkurrenten des Herstellers ist in diesem Zusammenhang ausgeschlossen.

Absatz 2 enthält eine Zweckbindung für die aus der Untersuchung nach Absatz 1 gewonnenen Erkenntnisse. Soweit erforderlich, ist zudem eine Weitergabe und Veröffentlichung dieser Erkenntnisse durch das BSI zulässig. In diesem Fall ist dem Hersteller zuvor die Gelegenheit zu einer Stellungnahme einzuräumen. Wenn der Hersteller in diesem Rahmen − etwa bei einer festgestellten Sicherheitslücke − selbst an die Öffentlichkeit geht oder sonst Abhilfe schafft, ist eine zusätzliche Veröffentlichung der Erkenntnisse durch das BSI nicht erforderlich. Bei den Erkenntnissen nach diesem Absatz handelt es sich nicht um personenbezogene Daten.

Zu Nummer 7 (§ 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen, § 8b Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen, § 8c Anwendungsbereich und § 8d Auskunftsverlangen)

Zu § 8a (Sicherheit in der Informationstechnik Kritischer Infrastrukturen)
Zweck von Absatz 1 ist der ordnungsgemäße Betrieb Kritischer Infrastrukturen im Sinne des BSI-Gesetzes und die fortlaufende Verfügbarkeit der jeweils angebotenen, in der Rechtsverordnung nach § 10 Absatz 1 des BSI-Gesetzes als kritisch eingestuften Dienstleistungen. Zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse (siehe § 2 Absatz 2 des BSI-Gesetzes), die für die Funktionsfähigkeit der Kritischen Infrastrukturen maßgeblich sind, sollen branchenspezifische Mindestanforderungen an die IT-Sicherheit zum Schutz der Kritischen Infrastrukturen nach § 2 Absatz 10 des BSI-Gesetzes erfüllt werden. Dies umfasst auch Maßnahmen zur Detektion und Behebung von Störungen.

Durch die Erfassung nicht nur der informationstechnischen Systeme, sondern auch der informationstechnischen Komponenten, die darin oder in sonstigen Systemen Verwendung finden, sowie durch die Erfassung der informationstechnischen Prozesse, also der Vorgänge der Informationsverarbeitung, wird sichergestellt, dass die Betreiber Kritischer Infrastrukturen überall dort Absicherungsmaßnahmen ergreifen müssen, wo Informationstechnik Einfluss auf die Erbringung ihrer kritischen Dienstleistungen hat. Hierfür sind angemessene organisatorische und technische Vorkehrungen zu treffen, zu denen auch infrastrukturelle und personelle Maßnahmen gehören können. Besonders kritische Prozesse bedürfen im Einzelfall besonderer Sicherheitsmaßnahmen durch Abschottung. Diese Prozesse sollten weder mit dem Internet oder öffentlichen Netzen verbunden noch von über das Internet angebotenen Diensten abhängig sein. Das Erfordernis, angemessene organisatorische und technische Vorkehrungen zu treffen, besteht auch dann, wenn der Betreiber der Kritischen Infrastruktur seine IT durch einen externen Dienstleister betreiben lässt.

Auf Grund der weitreichenden gesellschaftlichen Auswirkungen ist bei den technischen und organisatorischen Vorkehrungen der Stand der Technik zu berücksichtigen. Stand der Technik in diesem Sinne ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten

oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden. Die Verpflichtung zur Berücksichtigung des Stands der Technik schließt die Möglichkeit zum Einsatz solcher Vorkehrungen nicht aus, die einen ebenso effektiven Schutz wie die anerkannten Vorkehrungen nach dem Stand der Technik bieten.

Bei der Frage der Angemessenheit ist der bei dem Betreiber erforderliche Aufwand, insbesondere die von ihm aufzuwendenden Kosten, zu berücksichtigen. Um die Umsetzung der Mindestanforderungen zu dokumentieren, ist es sachgerecht, dass diese von den Betreibern in entsprechende Sicherheits- und Notfallkonzepte aufgenommen werden.

Absatz 2 ermöglicht in Branchen, in denen es fachlich sinnvoll ist, die Erarbeitung branchenspezifischer Sicherheitsstandards und verankert damit den kooperativen Ansatz, wie er in der Nationalen Strategie zum Schutz Kritischer Infrastrukturen festgeschrieben wurde und im UP KRITIS und seinen Branchenarbeitskreisen realisiert wird. Ziel ist es, dass sich Betreiber Kritischer Infrastrukturen branchenintern zusammenfinden und branchenspezifische Sicherheitsstandards erarbeiten. Der UP KRITIS stellt dabei als etablierte Kooperationsplattform zwischen Betreibern und Staat bereits entsprechende Strukturen zur Verfügung. Darüber hinaus bietet das Deutsche Institut für Normung e. V. − als nationale Normungsorganisation und Mitglied der europäischen und internationalen Normungsorganisationen sowie als Kooperationsplattform zwischen Staat und Betreibern von Informations- und Sicherheitswirtschaft − entsprechende Strukturen und bewährte Prozesse. Auch die branchenspezifischen Sicherheitsstandards müssen regelmäßig dem sich weiterentwickelnden Stand der Technik angepasst werden.

Die Bewertung und Anerkennung der vorgetragenen Standards soll im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sowie im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde erfolgen, um die Vereinbarkeit und Koordinierung mit anderen Belangen der Sicherheitsvorsorge zu gewährleisten. Die Differenzierung zwischen einem „Einvernehmen“ mit der zuständigen Aufsichtsbehörde des Bundes und einem „Benehmen“ mit der sonst zuständigen Aufsichtsbehörde berücksichtigt die Rechtspre-

chung des Bundesverfassungsgerichts, wonach Mitentscheidungsbefugnisse der einen föderalen Ebene bei Entscheidungen der anderen föderalen Ebene mit dem Grundgesetz nicht zu vereinbaren sind („Verbot der Mischverwaltung“). Unabhängig davon soll aber über das Benehmenserfordernis sichergestellt werden, dass die fachliche Expertise der sonstigen Aufsichtsbehörden einbezogen wird.

Auch dann, wenn branchenspezifische Sicherheitsstandards erarbeitet wurden, steht es dem einzelnen Betreiber frei, abweichend davon auch eigene den Stand der Technik berücksichtigende Maßnahmen umzusetzen.

Der Nachweis durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nach Absatz 3 dient der Kontrolle und Überprüfung der von den Betreibern nach Absatz 1 getroffenen Maßnahmen und damit der Einhaltung eines angemessenen Sicherheitsniveaus durch die Betreiber. Die Ausgestaltung der Sicherheitsaudits, Prüfungen und Zertifizierungen soll nicht im Detail gesetzlich vorgegeben werden, da die Ausgestaltung von den gegebenenfalls erarbeiteten branchenspezifischen Sicherheitsstandards, den in den Branchen vorhandenen technischen Gegebenheiten und bereits bestehenden Auditierungs- und Zertifizierungssystemen abhängt. Generell soll geprüft werden, ob der Betreiber die für seine Branche und Technologie geeigneten und wirksamen Maßnahmen und Empfehlungen befolgt, etwa ein Information Security Management (Sicherheitsorganisation, IT-Risikomanagement etc.) betreibt, kritische Cyber-Assets identifiziert hat und managt, Maßnahmen zur Angriffsprävention und -erkennung betreibt, ein Business Continuity Management (BCM) implementiert hat und darüber hinaus die branchenspezifischen Besonderheiten (zum Beispiel den jeweiligen branchenspezifischen Sicherheitsstandard, sofern ein solcher erstellt und anerkannt wurde) umsetzt.

Die Sicherheitsaudits, Prüfungen oder Zertifizierungen sollen von dazu nachweislich qualifizierten Prüfern bzw. Zertifizierern durchgeführt werden. Bei Zertifizierungen nach internationalen, europäischen oder nationalen Standards kann auf die bestehenden Zertifizierungsstrukturen zurückgegriffen werden. Ein Auditor gilt als qualifiziert, wenn er seine Qualifikation zur Überprüfung der Einhaltung der Sicherheitsstandards gegenüber dem BSI auf Verlangen formal glaubhaft machen kann. Denkbar ist in diesem Zusammenhang etwa die Anknüpfung an Zertifizierungen, die für die fachlich-technische Prüfung im jeweiligen Sektor angeboten werden (zum Beispiel zertifizierte Prüfer für bestimmte ISO-Normen oder Ähnliches). Eine Kontrolle der Einhaltung der Erfordernisse nach Absatz 1 kann zudem über etablierte Prüfmechanismen erfolgen. So prüfen Wirt-

schaftsprüfer bereits heute unter anderem im Rahmen der Jahresabschlussprüfung die für die Rechnungslegung relevanten IT-Systeme.

Bei Sicherheitsmängeln kann das BSI im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse verlangen und, soweit erforderlich, die Beseitigung der Sicherheitsmängel verlangen. Auch insoweit wird vom BSI im gesetzlich zulässigen Rahmen die fachliche Expertise der zuständigen Aufsichtsbehörden einbezogen (siehe hierzu die Begründung zu Absatz 2).

Zu § 8b (Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen)

§ 8b regelt die Meldungen an das BSI als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen. Die entsprechenden Meldungen sind Voraussetzung für die nationale Handlungsfähigkeit und Grundlage für bundesweit abgestimmte Reaktionen. Im Einzelnen:

Absatz 1 beschreibt die Aufgabe des BSI als zentraler Meldestelle für die Sicherheit in der Informationstechnik für Betreiber Kritischer Infrastrukturen.

Absatz 2 regelt die weiteren Aufgaben des BSI in diesem Zusammenhang. Das BSI sammelt alle eingehenden Meldungen und erstellt und aktualisiert − unter Einbeziehung seiner sonstigen Erkenntnisse − ein Lagebild. Des Weiteren stellt das BSI den Betreibern Kritischer Infrastrukturen, den zuständigen Aufsichtsbehörden und den sonst zuständigen Behörden des Bundes sowie den zuständigen Aufsichtsbehörden der Länder oder die zu diesem Zweck dem BSI von den Ländern benannten Behörden in angemessener Form (zum Beispiel konsolidiert, sanitarisiert oder als Rohdatenmaterial) die sie betreffenden bzw. die zur Erfüllung ihrer bestehenden Aufgaben erforderlichen Informationen zur Verfügung, soweit Quellen- und Geheimschutz sowie insbesondere die schutzwürdigen Interessen der Betreiber Kritischer Infrastrukturen dem nicht entgegenstehen. Die Betreiber leisten insoweit durch die Meldungen einen eigenen Beitrag und bekommen dafür, da sie auch von den Meldungen der anderen Betreiber an das BSI und der Bewertung dieser Meldungen durch das BSI profitieren, im Gegenzug ein Mehrfaches an Informationen und Know-how zurück.

Die Öffentlichkeit wird benachrichtigt, wenn das öffentliche Interesse dies erfordert. Auch hier dürfen insbesondere die schutzwürdigen Interessen der Betreiber Kritischer Infrastrukturen nicht entgegenstehen.

Absatz 3 stellt durch eine Anbindung der Betreiber Kritischer Infrastrukturen an die Warn- und Alarmierungsmechanismen nach § 3 Absatz 1 Nummer 15 sicher, dass bei erheblichen Störungen der informationstechnischen Systeme, Komponenten oder Prozesse Kritischer Infrastrukturen, die für die Verfügbarkeit der betriebenen Kritischen Infrastrukturen maßgeblich sind, ein schneller Informationsfluss gewährleistet ist und dass das Lagezentrum des BSI sowie andere Betreiber Kritischer Infrastrukturen unverzüglich informiert werden.

Absatz 4 regelt die Verpflichtung von Betreibern Kritischer Infrastrukturen, dem BSI unverzüglich erhebliche Störungen, die die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse betreffen, zu melden. Der Begriff der „Störung“ ist dabei entsprechend der höchstrichterlichen Rechtsprechung zu § 100 Absatz 1 des Telekommunikationsgesetzes funktional zu verstehen. Eine Störung im Sinne des BSI-Gesetzes liegt daher vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken. Dazu zählen insbesondere Fälle von Sicherheitslücken, Schadprogrammen und erfolgten, versuchten oder erfolgreich abgewehrten Angriffen auf die Sicherheit in der Informationstechnik sowie außergewöhnliche und unerwartete technische Defekte mit IT-Bezug (zum Beispiel nach Softwareupdates oder ein Ausfall der Serverkühlung).

Die Störungen sind dann meldepflichtig, wenn sie erheblich sind. Eine solche Störung liegt vor, wenn durch sie die Funktionsfähigkeit der erbrachten kritischen Dienstleistung bedroht ist. Nicht meldepflichtig sind Störungen, die zu keiner Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastrukturen führen können. Erheblich sind insbesondere solche IT-Störungen, die nicht bereits automatisiert oder mit wenig Aufwand mithilfe der nach § 8a als Stand der Technik beschriebenen Maßnahmen abgewehrt werden können. Dies ist beispielsweise der Fall bei neuartigen oder außergewöhnlichen IT-Vorfällen, bei gezielten Angriffen, für neue Modi Operandi sowie für unerwartete Vorkommnisse. Insbesondere gilt dies aber auch für Vorfälle, die nur mit deutlich erhöhtem Ressourcenaufwand bewältigt werden können (erhöhter Koordinierungsaufwand, Hinzuziehen zusätzlicher Experten, Nutzung einer besonderen Aufbauorganisation, Einberu-

fung eines Krisenstabs). IT-Störungen sind hingegen nicht erheblich, wenn es sich um tagtäglich vorkommende Ereignisse (Spam, übliche Schadsoftware, die standardmäßig im Virenscanner abgefangen wird, Hardwareausfälle im üblichen Rahmen) handelt und die mit den nach Stand der Technik nach § 8a des BSI-Gesetzes zu ergreifenden Maßnahmen ohne nennenswerte Probleme bewältigt werden.

Entsprechende Meldungen an das BSI − auch im Vorfeld konkreter Schadenseintritte − sind notwendig, um eine möglichst umfassende und frühzeitige Warnung möglicherweise ebenfalls betroffener Betreiber Kritischer Infrastrukturen zu gewährleisten und darüber hinaus fundierte Aussagen zur IT-Sicherheitslage in Deutschland treffen zu können. Im Sinne einer schnellen Information und Warnung potentiell betroffener Kreise ist es erforderlich, dass die Meldung stufenweise erfolgt. In einem ersten Schritt meldet der Betreiber schnellstmöglich die ihm ohne großen Rechercheaufwand zur Verfügung stehenden Informationen. Der Betreiber ergänzt die initiale Meldung dann nachträglich, im weiteren Verlauf der Vorfallsbearbeitung, um weitere, neu hinzukommende relevante Informationen.

Soweit die Störung nicht zu einem tatsächlichen Ausfall oder einer Beeinträchtigung führt, ist die namentliche Nennung des Betreibers nicht erforderlich. Die Meldung kann in diesem Fall pseudonymisiert erfolgen. Hierdurch wird der besonderen Sensibilität der Meldungen im Hinblick auf die wirtschaftlichen Auswirkungen eines möglichen Bekanntwerdens entsprechender Vorfälle Rechnung getragen. Auf die Nennung des Betreibers wird dementsprechend in den Fällen verzichtet, in denen die Meldung primär der Beratung und Warnung möglicher ebenfalls betroffener Kreise und der Erfassung der Cyberbedrohungslage dient. Gleichzeitig ermöglicht die Pseudonymisierung dem BSI, Rückfragen an den Meldenden zu stellen, ohne dass dessen Klarname dafür erforderlich ist.

Eine Nennung des Namens des Betreibers ist hingegen erforderlich bei bedeutenden Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse, die bereits konkret zu einem Ausfall oder einer Beeinträchtigung der Kritischen Infrastruktur geführt haben. Denn im konkreten Schadensfall muss regelmäßig eine schnelle Krisenreaktion erfolgen, insbesondere um ähnliche Vorfälle bei anderen Betreibern noch abwenden zu können. Hierzu muss das BSI gegebenenfalls auch sofort auf den Meldenden zugehen können, um die dafür benötigten Informationen zu erhalten. Aufgrund der gebotenen Eile und der unmittelbaren Gefährdung der Versorgungssicherheit kann das Interesse der Meldenden,

anonym zu bleiben, in diesen Fällen nicht in gleicher Weise berücksichtigt werden wie bei den Fällen, bei denen es noch nicht zu einem konkreten Schadenseintritt gekommen ist.

Zur weiteren Konkretisierung der Meldepflicht wird das BSI − unter Einbeziehung der Betreiber Kritischer Infrastrukturen und der ansonsten im Bereich der Sicherheitsvorsorge zuständigen Aufsichtsbehörden − Kriterien für meldungsrelevante Sicherheitsvorfälle aufstellen und entsprechend der jeweils aktuellen IT-Sicherheitslage weiterentwickeln.

Absatz 5 eröffnet klarstellend die Möglichkeit für Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, ergänzend zu den Kontaktstellen nach Absatz 3 Satz 1 eine gemeinsame Ansprechstelle zu benennen, über die der Informationsaustausch zwischen den Kontaktstellen und dem BSI in der Regel erfolgen soll. Hierfür können bestehende Strukturen, beispielsweise über die ansonsten im Bereich der Sicherheitsvorsorge zuständigen Aufsichtsbehörden oder die eingerichteten Single Points of Contact (SPOCs) des UP KRITIS, genutzt und erweitert werden. Der gesamte Übermittlungsprozess muss vom Ablauf her nachvollziehbar und auch auditierbar sein.

Die im Rahmen von § 8b übermittelten Informationen sind üblicherweise rein technischer Natur. Sollte im Einzelfall doch ein Personenbezug gegeben sein, stellt Absatz 6 klar, dass personenbezogene Daten nur zu den in § 8b vorgesehenen Zwecken ausgewertet werden dürfen und die allgemeinen datenschutzrechtlichen Regelungen gelten. Für die nach § 8b erhaltenen Informationen gilt dementsprechend auch der allgemeine Grundsatz der Datensparsamkeit aus § 3a des Bundesdatenschutzgesetzes. Ergänzt wird dieses Datenschutzregime durch den Verweis auf § 5 Absatz 7 Satz 3 bis 8 des BSI-Gesetzes.

Zu § 8c (Anwendungsbereich)

Die Anwendung der §§ 8a und 8b des BSI-Gesetzes ist unabhängig von der Organisationsform des Betreibers Kritischer Infrastrukturen, so dass beispielsweise auch Einrichtungen des Bundes, die nicht Kommunikationstechnik im Sinne von § 2 Absatz 3 des BSI-Gesetzes sind, dem Anwendungsbereich unterfallen.

Nach Absatz 1 finden die §§ 8a und 8b des BSI-Gesetzes unter dem Gesichtspunkt der Verhältnismäßigkeit jedoch keine Anwendung auf solche Unternehmen, die als soge-

nannte Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (ABl. L 124 vom 20.5.2003, S. 36) Kritische Infrastrukturen betreiben. Kleinstunternehmen sind gemäß dieser Empfehlung Unternehmen, die weniger als 10 Personen beschäftigen und deren Jahresumsätze bzw. Jahresbilanzen 2 Millionen Euro nicht überschreiten. Die Ausnahme gilt auch für Unternehmen im Sinne von Artikel 3 Absatz 4 der Empfehlung, das heißt für Unternehmen, die an und für sich Kleinstunternehmen im Sinne der Empfehlung sind, von dieser aber ausgenommen wurden, weil 25 % oder mehr ihres Kapitals oder ihrer Stimmrechte direkt oder indirekt von einem oder mehreren öffentlichen Stellen oder Körperschaften des öffentlichen Rechts einzeln oder gemeinsam kontrolliert werden. Die entsprechenden Voraussetzungen müssen bei dem Betreiber der betreffenden Kritischen Infrastruktur selbst vorliegen und sind dem BSI auf dessen Verlangen hin auf geeignete Weise nachzuweisen. Dies kann beispielsweise durch die Vorlage einer Selbsterklärung des Unternehmens mit entsprechenden Nachweisen erfolgen. Organisatorische Maßnahmen des Betreibers, die zu einer (teilweisen) Auslagerung der Verantwortung für einzelne Bereiche der Kritischen Infrastrukturen führen, lassen die Verantwortung des Betreibers für die Kritische Infrastruktur als solche und die damit einhergehenden Verpflichtungen unberührt.

Absatz 2 nimmt Betreiber Kritischer Infrastrukturen, die ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen (Ziffer 1), vom Anwendungsbereich des § 8a des BSI-Gesetzes aus. Grund hierfür ist, dass diese Betreiber mit § 109 des Telekommunikationsgesetzes (neu) bereits einer § 8a des BSI-Gesetzes gleichwertigen Regelung unterfallen. Entsprechendes gilt für Betreiber von Energieversorgungsnetzen und Energieanlagen im Sinne des Energiewirtschaftsgesetzes (Ziffer 2). Eine gleichwertige Regelung enthält auch das Atomgesetz einschließlich der darauf beruhenden Rechtsverordnungen sowie des untergesetzlichen Regelwerks für Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes hinsichtlich der nuklearen Sicherheit (Ziffer 3). Aufgrund der Genehmigungsvoraussetzung des § 7 Absatz 2 Nummer 5 des Atomgesetzes in Verbindung mit den konkretisierenden Regelungen sowie der Aufsicht nach § 19 des Atomgesetzes sind hier ebenfalls gleichwertige Regelungen hinsichtlich der nuklearen Sicherheit vorhanden. Im Falle einer Kollision zwischen den Zielen der nuklearen Sicherheit und Sicherung kerntechnischer Anlagen einerseits und der Versorgungssicherheit andererseits ist die nukleare Sicherheit und Sicherung kerntechnischer Anlagen in der Abwägung vorrangig zu berücksichtigen.

Ziffer 4 normiert einen allgemeinen Vorrang speziellerer Anforderungen und nimmt damit insbesondere den Fall in den Blick, dass nach Inkrafttreten des Gesetzes in anderen Regelungsbereichen mit § 8a des BSI-Gesetzes vergleichbare oder weitergehende Regelungen getroffen werden. So sollen zum Beispiel für die Telematikinfrastruktur im Gesundheitswesen künftig dem § 8a des BSI-Gesetzes vergleichbare Anforderungen gelten.

Absatz 3 nimmt Betreiber Kritischer Infrastrukturen, die ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen (Ziffer 1), vom Anwendungsbereich der Absätze 3 bis 5 von § 8b des BSI-Gesetzes aus. Grund hierfür ist, dass diese Betreiber mit § 109 Absatz 5 des Telekommunikationsgesetzes (neu) einer § 8b Absatz 3 bis 5 des BSI-Gesetzes gleichwertigen Regelung unterfallen. Das Gleiche gilt für Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes (Ziffer 2). Einer spezialgesetzlichen Meldepflicht unterfallen gemäß der neu geschaffenen Regelung des § 44b des Atomgesetzes auch Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes. Diese sind daher ebenfalls auszunehmen (Ziffer 3).

Ziffer 4 normiert einen allgemeinen Vorrang speziellerer Anforderungen und nimmt damit insbesondere den Fall in den Blick, dass nach Inkrafttreten des Gesetzes in anderen Regelungsbereichen mit § 8b des BSI-Gesetzes vergleichbare oder weitergehende Regelungen getroffen werden. So sollen zum Beispiel für die Telematikinfrastruktur im Gesundheitswesen künftig dem § 8b des BSI-Gesetzes vergleichbare Anforderungen gelten.

Zu § 8d (Auskunftsverlangen)

§ 8d regelt als Spezialregelung im Sinne von § 1 Absatz 3 des Informationsfreiheitsgesetzes abschließend die Auskunft an nicht am Meldeverfahren beteiligte Personen oder an nichtöffentliche Institutionen (Dritte) zu Informationen, die im Rahmen von § 8a Absatz 2 und 3 an das BSI übersandt wurden, sowie zu den Meldungen nach § 8b Absatz 4 des BSI-Gesetzes unter Berücksichtigung des besonderen schutzwürdigen Interesses der meldepflichtigen Betreiber Kritischer Infrastrukturen an einer vertraulichen Behandlung der von ihnen gemeldeten Informationen sowie wesentlicher Sicherheitsinteressen.

Auskunft kann demnach nur dann erteilt werden, wenn keine schutzwürdigen Interessen des betroffenen Betreibers Kritischer Infrastrukturen dem entgegenstehen und durch die Auskunft keine Beeinträchtigung wesentlicher Sicherheitsinteressen zu erwarten ist. Dies gilt insbesondere in den Fällen der §§ 8a Absatz 3, 8b Absatz 4 Satz 3 des BSI-Gesetzes. Aber auch in den Fällen des § 8b Absatz 4 Satz 1 des BSI-Gesetzes sind Konstellationen denkbar, bei denen eine Auskunftserteilung die schutzwürdigen wirtschaftlichen Interessen einer ganzen Branche oder auch einzelner Betreiber erheblich beeinträchtigen kann, etwa dann, wenn eine entsprechende Zuordnung auch ohne Nennung des Betreibers möglich ist oder nahe zu liegen scheint. Zugang zu personenbezogenen Daten wird generell nicht gewährt. Für die Weitergabe von Informationen an Betreiber Kritischer Infrastrukturen als am Meldeverfahren Beteiligte gilt § 8b Absatz 2 Nummer 4 des BSI-Gesetzes.

Diese Spezialregelung ist erforderlich, da die Ausnahmevorschriften der §§ 3ff. des Informationsfreiheitsgesetzes die besondere Interessenlage eines Meldeverfahrens für Betreiber Kritischer Infrastrukturen nicht hinreichend berücksichtigen. Denn für die Funktionsfähigkeit eines solchen Meldeverfahrens ist der Schutz der übermittelten hochsensiblen Informationen von entscheidender Bedeutung. Dem öffentlichen Interesse an einem effektiven Schutz der Verfügbarkeit der Kritischen Infrastrukturen ist Vorrang einzuräumen, da sie von hoher Bedeutung für das Funktionieren des Gemeinwesens sind und durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden. Zudem ist der besonderen Sensibilität der im Rahmen von § 8b des BSI-Gesetzes ausgetauschten Informationen sowohl für die meldepflichtigen Betreiber Kritischer Infrastrukturen wie auch für die Gesellschaft Rechnung zu tragen. Wesentliche Sicherheitsinteressen können einer Auskunftserteilung auch dann entgegenstehen, wenn durch eine Veröffentlichung von Erkenntnissen das Vertrauen der Betreiber Kritischer Infrastrukturen in die Vertraulichkeit des Meldeverfahrens erschüttert und hierdurch die Effizienz des Meldeverfahrens insgesamt gefährdet würde.

Ein Zugang zu Akten des BSI in Angelegenheiten nach den §§ 8a und 8b des BSI-Gesetzes wird gemäß Absatz 2 ausschließlich Verfahrensbeteiligten gewährt. Bei den Informationen, die das BSI im Rahmen dieser Aufgabe sammelt und analysiert (etwa im Zusammenhang mit der Erstellung des Lagebildes), handelt es sich um hochsensible, kumulierte sicherheitskritische Informationen, die einem besonders hohen Schutzbedürfnis unterliegen. Die hohe Sicherheitsempfindlichkeit dieser Informationen und deren

Risikopotential schließen eine Zugänglichkeit von vornherein aus. Die Akteneinsicht der Verfahrensbeteiligten erfolgt nach Maßgabe des § 29 des Verwaltungsverfahrensgesetzes.

Zu Nummer 8 (§ 10 Ermächtigung zum Erlass von Rechtsverordnungen)
Zu Buchstabe a (Kriterien zur Bestimmung der Kritischen Infrastrukturen)

§ 10 Absatz 1 ermächtigt das Bundesministerium des Innern, in Konkretisierung der systemischen Definition Kritischer Infrastrukturen nach § 2 Absatz 10 des BSI-Gesetzes − nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit den genannten Bundesministerien − die Kriterien zur Bestimmung derjenigen Einrichtungen, Anlagen oder Teile davon festzulegen, die als Kritische Infrastruktur im Sinne des BSI-Gesetzes einzuordnen sind.

In die Rechtsverordnung bzw. in die Anhänge zu der Rechtsverordnung sollen in abstrakter Form die als Kritische Infrastrukturen einzuordnenden Einrichtungen, Anlagen oder Teile davon benannt werden. Methodisch ist vorgesehen, eine Konkretisierung nach den Kategorien Qualität und Quantität vorzunehmen. Bei der Festlegung der betroffenen Kritischen Infrastrukturen wird die Frage zu beantworten sein, ob erstens mittels der jeweiligen Einrichtungen, Anlagen oder Teile davon eine für die Gesellschaft kritische Dienstleistung erbracht wird (Qualität) und zweitens ein Ausfall oder eine Beeinträchtigung wesentliche Folgen für wichtige Schutzgüter und die Funktionsfähigkeit des Gemeinwesens hätte (Quantität):

Unter der Kategorie Qualität wird näher erfasst, welche Dienstleistungen innerhalb der genannten Sektoren in dem Sinne kritisch sind, dass sie von hoher Bedeutung für das Funktionieren des Gemeinwesens sind und durch ihren Ausfall oder ihre Beeinträchtigung nachhaltig wirkende Versorgungsengpässe oder erhebliche Gefährdungen für die öffentliche Sicherheit eintreten würden. Die Kategorie Qualität sollte sich hierbei insbesondere auf die Sicherheit von Leib, Leben, Gesundheit und Eigentum der Teile der Bevölkerung beziehen, die von einem Ausfall unmittelbar oder mittelbar beeinträchtigt wären. Sie dient der Prüfung, ob ein bestimmter Teil einer Branche überhaupt kritisch ist. Eine Spezifizierung des Qualitätskriteriums soll anhand einer abstrakten Darstellung von solchen kritischen Dienstleistungen erfolgen, die für die Gewährleistung der genannten Werte notwendig sind.

Solche kritischen Dienstleistungen könnten jedenfalls sein:

1. SEKTOR ENERGIE
   - Stromversorgung (Branche: Elektrizität)
   - Versorgung mit Erdgas (Branche: Gas)
   - Versorgung mit Mineralöl (Branche: Mineralöl)
2. SEKTOR INFORMATIONSTECHNIK UND TELEKOMMUNIKATION
   - Sprach- und Datenkommunikation (Branchen: Telekommunikation, Informationstechnik)
   - Verarbeitung und Speicherung von Daten (Branche: Informationstechnik)
3. SEKTOR TRANSPORT UND VERKEHR
   - Transport von Gütern (Branchen: Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik)
   - Transport von Personen im Nahbereich (Branchen: Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik)
   - Transport von Personen im Fernbereich (Branchen: Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik)
4. SEKTOR GESUNDHEIT
   - medizinische Versorgung (Branchen: medizinische Versorgung, Labore)
   - Versorgung mit Arzneimitteln und Medizinprodukten (Branchen: medizinische Versorgung, Labore, Arzneimittel und Impfstoffe)
5. SEKTOR WASSER
   - Trinkwasserversorgung (Branche: öffentliche Wasserversorgung)
   - Abwasserbeseitigung (Branche: öffentliche Abwasserbeseitigung)
6. SEKTOR ERNÄHRUNG
   - Versorgung mit Lebensmitteln (Branchen: Ernährungswirtschaft, Lebensmittelhandel)

7. SEKTOR FINANZ- UND VERSICHERUNGSWESEN

- Zahlungsverkehr Zahlungsdienstleistungen durch Überweisung, Zahlungskarten und E-Geld (Branchen: Banken, Finanzdienstleister)
- Bargeldversorgung (Branche: Banken)
- Kreditvergabe (Branche: Banken, Finanzdienstleister)
- Geld- und Devisenhandel (Branche: Börsen, Banken, Zahlungsdienstleister)
- Wertpapier- und Derivatehandel (Branche: Börsen, Banken, Zahlungsdienstleister)
- Versicherungsleistungen (Branche: Versicherungen)

Ausgehend von einer solchen in der Rechtsverordnung abschließend vorzunehmenden Einteilung soll die Kategorie Quantität den Versorgungsgrad der jeweiligen Einrichtungen, Anlagen oder Teile davon erfassen. Zu untersuchen ist in diesem Zusammenhang, ob die Auswirkungen eines Ausfalls bzw. einer Beeinträchtigung der jeweiligen Einrichtungen, Anlagen oder Teile davon für die Versorgung einer entsprechend großen Zahl an Personen (Schwellenwert) mit einer kritischen Dienstleistung unmittelbar oder mittelbar wesentlich sind, das heißt aus gesamtgesellschaftlicher Sicht eine stark negative Wirkung hätten. Zur konkreten Ausfüllung dieses Kriteriums sollen unter Einbeziehung von Verwaltung, Wirtschaft und Wissenschaft möglichst spezifische Schwellenwerte gebildet und in die Rechtsverordnung aufgenommen werden. Die jeweils maßgeblichen Schwellenwerte können dabei pro Sektor/Branche bzw. Dienstleistung variieren.

Mögliche Adressaten können so anhand der Rechtsverordnung feststellen, ob sie mit einer entsprechenden Anlage, Einrichtung oder eines Teils davon eine kritische Dienstleistung mit einem Versorgungsgrad über dem entsprechenden Schwellenwert erbringen und ob sie damit den Verpflichtungen nach den §§ 8a, 8b des BSI-Gesetzes unterliegen.

Zu den Buchstaben b und c (Zustimmungsbedürftigkeit)

Die Buchstaben c und d betreffen redaktionelle Klarstellungen in den bereits bestehenden Verordnungsermächtigungen des BSI-Gesetzes.

Zu Nummer 9 (§ 13 Berichtspflichten)

Über die Berichtspflicht nach Absatz 1 wird sichergestellt, dass das Bundesministerium des Innern als zuständige Aufsichtsbehörde vom BSI über dessen laufende Tätigkeit unterrichtet wird. Relevante Informationen können so unter anderemauch in die regelmäßigen Sitzungen des Nationalen Cyber-Sicherheitsrates einfließen.

Die gesetzliche Verankerung einer Berichtspflicht und die vorgesehene Veröffentlichung eines Jahresberichts nach Absatz 2 dienen der Sensibilisierung der Öffentlichkeit für das Thema IT-Sicherheit. Der Bericht ergänzt die bestehenden fachlichen Informationsangebote des BSI und trägt als Beitrag der Bundesregierung zur Diskussion im politischen Raum bei. Da eine Vielzahl von Cyberangriffen bereits durch Basismaßnahmen abgewehrt werden könnte, spielt die Aufklärung und Sensibilisierung der Öffentlichkeit eine zentrale Rolle für die Erhöhung der IT-Sicherheit in Deutschland.

Zu Artikel 2 (Änderung des Atomgesetzes)

Die Regelung in § 44b ordnet für alle Genehmigungsinhaber von kerntechnischen Anlagen bzw. Tätigkeiten nach den §§ 6, 7 und 9 des Atomgesetzes bei Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einer Gefährdung oder Störung der nuklearen Sicherheit und Sicherung führen können oder bereits geführt haben, eine unverzügliche Meldepflicht an das BSI als zentraler Meldestelle in Angelegenheiten der Sicherheit der informationstechnischen Systeme, Komponenten oder Prozesse gemäß § 8b Absatz 1 des BSI-Gesetzes an.

Die dem BSI in § 8b Absatz 2 BSI-Gesetz eröffneten Aufgaben und Befugnisse sollen auch für Meldungen der Genehmigungsinhaber nach den §§ 6, 7 und 9 des Atomgesetzes gelten.

Die beim BSI eingegangenen Meldungen leitet das Bundesamt unverzüglich an die für die nukleare Sicherheit zuständigen Genehmigungs- und Aufsichtsbehörden der Länder und an das für die nukleare Sicherheit und den Strahlenschutz zuständige Bundesministerium weiter. § 8b Absätze 1, 2 und 6 des BSI-Gesetzes gelten hierbei entsprechend.

Zu Artikel 3 (Änderung des Energiewirtschaftsgesetzes)

Zu Nummer 1 (§ 11 Betrieb von Energieversorgungsnetzen)
Zu Buchstabe a (Redaktionelle Klarstellungen und Konkretisierungen)
Mit den Änderungen in Absatz 1a sollen in der Praxis aufgetretene Unklarheiten beseitigt und das Schutzniveau konkretisiert werden.

Zu Doppelbuchstabe aa (Schutz der Telekommunikations- und Datenverarbeitungssysteme)
Die Formulierung „die der Netzsteuerung dienen“ in Satz 1 hat in der Vergangenheit zu Diskussionen darüber geführt, wie weit die Verpflichtung reicht. Die nunmehr gewählte Formulierung stellt klar, dass die Telekommunikationssysteme und Datenverarbeitungssysteme der Netzbetreiber so zu schützen sind, dass ein sicherer Netzbetrieb garantiert ist.

Zu Doppelbuchstabe bb (Katalog der Sicherheitsanforderungen)
§ 11 Absatz 1a wurde mit der EnWG-Novelle 2011 in das Energiewirtschaftsgesetz aufgenommen. Ein erster Entwurf des Sicherheitskataloges der Bundesnetzagentur wurde erarbeitet und wird derzeit mit der Branche erörtert. Der vorgelegte Sicherheitskatalog enthält Vorschriften zu Zertifizierungen und regelmäßigen Überprüfungen der Schutzmaßnahmen in den Unternehmen. Mit dem nun ergänzten Satz 3 ist die Regulierungsbehörde verpflichtet, die Überprüfungen von den Betreibern zu fordern. Die Änderung trägt dem in § 8a Absatz 3 des BSI-Gesetzes etablierten Schutzniveau Rechnung und verhindert, dass der Sicherheitskatalog der Bundesnetzagentur hinter diesem Schutzniveau zurückfallen könnte. Für den vorgelegten Sicherheitskatalog hat dies keine praktischen Folgen, da dieser bereits entsprechende Anforderungen vorsieht.

Zu Doppelbuchstabe cc (Bedeutung des Sicherheitskataloges)
Bislang wird ein angemessener Schutz der Telekommunikations- und Datenverarbeitungssysteme vermutet, wenn die Netzbetreiber die Anforderungen des Sicherheitskataloges erfüllen. Soweit ein Betreiber nachweisen kann, dass seine Maßnahmen einen ebenfalls angemessenen Schutz gewähren, kann er von dem Sicherheitskatalog abweichen. Mit der Formulierung „liegt vor“ bekommen die Vorgaben des Sicherheitskataloges ein noch größeres Gewicht. Ein angemessener Schutz der Telekommunikations- und Datenverarbeitungssysteme liegt demnach nur dann vor, wenn die Anforderungen des Sicherheitskataloges erfüllt sind. Damit bleibt grundsätzlich kein Spielraum mehr für

die Betreiber, andere aus ihrer Sicht angemessene Schutzmaßnahmen zu erarbeiten. Der Sicherheitskatalog der Bundesnetzagentur stellt einen Mindeststandard dar, der von den Betreibern einzuhalten ist.

Zu Doppelbuchstabe dd (Konzentration auf der Fachebene)
Von der Festlegungskompetenz wurde bislang kein Gebrauch gemacht. Vielmehr wird der Inhalt und Anwendungsbereich des Sicherheitskataloges weiter ausgedehnt. Es ist sachgerecht, das gesamte Verfahren von der Erstellung des Sicherheitskataloges bis zur Überprüfung seiner Einhaltung bei der Fachabteilung zu bündeln.

Zu Buchstabe b (Sicherheitskatalog und Meldepflicht)
Mit Absatz 1b wird eine neue Vorschrift eingefügt, die sich an die Betreiber von Energieanlagen, die als Kritische Infrastruktur bestimmt wurden, richtet. Die Aufnahme von Schutzstandards für Energieanlagen, die in der Rechtsverordnung nach § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, ist notwendig, um einen umfassenden Schutz für den Netzbetrieb sicherstellen zu können. Energieanlagen, die mit dem öffentlichen Versorgungsnetz verbunden sind, werden verpflichtet, dort, wo eine Gefährdung für den Netzbetrieb möglich ist, ebenfalls Sicherheitsmaßnahmen zu ergreifen. Aufgrund der technischen Nähe ist es notwendig und sinnvoll, dass die Sicherheitsstandards für Netzbetreiber und für die betroffenen Energieanlagen aufeinander abgestimmt sind. Aus diesem Grund wird die Bundesnetzagentur als für die Sicherheitsstandards des Netzbetriebs zuständige Behörde beauftragt, auch die Sicherheitsstandards für die Energieanlagen zu erarbeiten und deren Einhaltung zu überwachen. Absatz 1b entspricht insoweit Absatz 1a. Darüber hinaus wird klargestellt, dass Vorgaben auf Grund des Atomgesetzes für Telekommunikations- und elektronische Datenverarbeitungssysteme von Anlagen nach § 7 Absatz 1 des Atomgesetzes Vorrang haben.

Mit Absatz 1c wird für Betreiber von Einrichtungen, Anlagen oder Teilen davon, die in der Rechtsverordnung nach gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur eingestuft wurden, eine Meldepflicht an das BSI eingeführt. Gemäß § 8b Absatz 1 des BSI-Gesetzes ist das BSI die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit der informationstechnischen Systeme, Komponenten oder Prozesse. Die Einrichtung einer solchen zentralen Stelle ist sinnvoll, um Wissen und Erfahrungen bestmöglich zu bündeln. Damit Sicherheitsprobleme aus dem Energiesektor ebenfalls in dieses „Kompetenzzentrum“ einfließen können, sieht Absatz 1c vor, dass erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und

Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage führen können oder bereits geführt haben, unverzüglich an das BSI zu melden sind. Die Anforderungen an den Inhalt der Meldung entsprechen denen aus der allgemeinen Meldepflicht für die Betreiber Kritischer Infrastrukturen nach § 8b Absatz 4 Satz 2 des BSI-Gesetzes. Entsprechende Meldungen an das BSI − auch im Vorfeld konkreter Schadenseintritte − sind notwendig, um eine möglichst umfassende und frühzeitige Warnung möglicherweise ebenfalls betroffener Betreiber Kritischer Infrastrukturen zu gewährleisten und darüber hinaus fundierte Aussagen zur IT-Sicherheitslage in Deutschland treffen zu können. Umgekehrt ist das BSI nach § 8b Absatz 2 Nummer 4 des BSI-Gesetzes verpflichtet, auch die Betreiber von Netzen oder Energieanlagen im Sinne von Absatz 1a und 1b über Sicherheitsvorfälle zu informieren. Das besondere Interesse der Meldeverpflichteten an einer vertraulichen Behandlung der von ihnen gemeldeten Informationen wird berücksichtigt. Die hochsensiblen sicherheitskritischen Informationen unterliegen einem besonderen Schutzbedürfnis.

Zu den Nummern 2 bis 4 (Änderung von Übergangsvorschriften)

Die Übergangsvorschriften aus § 21e Absatz 5 und § 21f Absatz 2 sollen den fließenden Übergang hin zum BSI-konformen Intelligenten Messsystem ermöglichen. Zwar wurden seit der EnWG-Novelle 2011 die erforderlichen Schutzprofile und Technischen Richtlinien des BSI zügig fortentwickelt, allerdings sind zertifizierte Messsysteme, wie sie § 21e Absatz 4 des Energiewirtschaftsgesetzes fordert, Anfang 2015 voraussichtlich noch nicht am Markt verfügbar. Nichtsdestoweniger sollen insbesondere in Pilotprojekten bereits Messsysteme eingesetzt und getestet werden können, die zwar über einen hohen technischen Standard verfügen, jedoch noch nicht BSI-zertifiziert sind. Diese Pilotprojekte sind für das künftige Zusammenspiel aller Akteure im intelligenten Energienetz von großer Bedeutung. Dies erfordert eine Verlängerung der bestehenden Übergangsvorschriften und dient letztendlich dem reibungslosen Ablauf des technischen Übergangs.

Durch die Neufassung wird außerdem stärker herausgestellt, dass Rechtsverordnungen nach § 21i Absatz 1 Nummer 11 des Energiewirtschaftsgesetzes den maßgeblichen Zeitpunkt bestimmen oder differenziert ausgestalten können, ab dem der Einsatz nicht BSI-konformer Messsysteme nicht mehr zugelassen wird. Diese Flexibilität ist erforderlich, um auf unterschiedliche Entwicklungsstände verschiedenster technischer Modullösungen (zum Beispiel Modul zum Steuern unterbrechbarer Verbrauchsein-

richtungen, Modul zum Steuern von EE-Anlagen etc.) wie auch auf die in Pilotprojekten gemachten Erfahrungen reagieren zu können. Sie ist auch nötig, um einen Gleichklang mit möglichen nach § 21i Absatz 1 Nummer 8 des Energiewirtschaftsgesetzes verordneten Einbauverpflichtungen herzustellen.

Zu Nummer 5 (§ 59 Absatz 1 Organisation)

Es handelt sich um eine Folgeänderung zu den Änderungen in § 11 Absatz 1a des Energiewirtschaftsgesetzes. Mit der Änderung wird klargestellt, dass die Fachabteilung der Bundesnetzagentur für die Erstellung und Überprüfung des Sicherheitskataloges gemäß § 11 Absatz 1a und 1b zuständig ist.

Zu Artikel 4 (Änderung des Telemediengesetzes)

Zu Nummer 1 (§ 13 Pflichten des Diensteanbieters)

Zu Buchstabe a (Schutz der Telekommunikations- und Datenverarbeitungssysteme nach dem Stand der Technik)

Wegen der zunehmenden Verbreitung von Schadsoftware über Telemediendienste werden die bestehenden Pflichten für Telemediendiensteanbieter, die ihre Telemedien geschäftsmäßig anbieten, um technische und organisatorische Maßnahmen zum Schutz vor unerlaubten Zugriffen, der personenbezogenen Daten und vor Störungen ergänzt.

Geschäftsmäßig ist ein Angebot dann, wenn es auf einer nachhaltigen Tätigkeit beruht, es sich also um eine planmäßige und dauerhafte Tätigkeit handelt. Bei einem entgeltlichen Dienst liegt dies regelmäßig vor, so z.B. bei werbefinanzierten Webseiten. Das nicht-kommerzielle Angebot von Telemedien durch Private und Idealvereine wird demgegenüber nicht erfasst.

Die betreffenden Diensteanbieter haben im Rahmen ihrer jeweiligen Verantwortlichkeit durch technische und organisatorische Vorkehrungen, die den Stand der Technik berücksichtigen, sicherzustellen, dass kein unerlaubter Zugriff auf die für ihre Telemedienangebote genutzten technischen Einrichtungen möglich ist und dass diese Einrichtungen gegen Verletzungen des Schutzes personenbezogener Daten und Störungen gesichert sind. Voraussetzung ist, dass die entsprechenden Vorkehrungen für den konkreten Diensteanbieter technisch möglich und wirtschaftlich zumutbar sind. Durch das Kriterium der Zumutbarkeit wird sichergestellt, dass von dem Diensteanbieter nur solche Vorkeh-

rungen zu treffen sind, deren Kosten in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen. Dies ermöglicht eine flexible Anpassung der jeweiligen Anforderungen im Einzelfall.

Ein wesentliches Ziel der Regelung ist es, einen der Hauptverbreitungswege von Schadsoftware einzudämmen: das unbemerkte Herunterladen allein durch das Aufrufen bzw. Nutzen einer dafür von Angreifern präparierten Website (sogenannte Drive-by-Downloads). Bereits durch eine regelmäßige Aktualisierung der für das Telemedienangebot verwendeten Software (Einspielen von Sicherheitspatches) seitens der Websitebetreiber könnten zahlreiche dieser Angriffe vermieden werden. Kompromittierungen können zudem auch durch Inhalte erfolgen, auf die der Diensteanbieter keinen unmittelbaren technischen Einfluss hat (zum Beispiel über kompromittierte Werbebanner, die auf der Webseite eingebunden sind). Dagegen sind organisatorische Vorkehrungen zu treffen. Hierzu zählt beispielsweise, Werbedienstleister, denen Werbefläche eingeräumt wird, vertraglich zu notwendigen Schutzmaßnahmen zu verpflichten. Die entsprechenden Maßnahmen sind im Rahmen der jeweiligen Verantwortlichkeit zu treffen.

Vorkehrungen nach Satz 1 können insbesondere die Anwendung eines als sicher anerkannten Verschlüsselungsverfahrens sowie − bei personalisierten Telemedien − das Angebot eines sicheren und dem jeweiligen Schutzbedarf angemessenen Authentifizierungsverfahrens sein. Je nach Sensibilität und Umfang der verarbeiteten Daten kann das erforderliche Schutzniveau unterschiedlich sein. Authentifizierungsverfahren nach den entsprechenden aktuellen und veröffentlichten Technischen Richtlinien des BSI sind dabei jedenfalls als dem Stand der Technik gemäß hinreichend sicher anzusehen. Auf die Barrierefreiheit der Verfahren ist besonders zu achten.

Zu Buchstabe b (Folgeänderung)
Buchstabe b enthält eine notwendige Folgeänderung.

Zu Nummer 2 (§ 16 Bußgeldvorschriften)
Die Aufnahme eines Verstoßes gegen die in § 13 Absatz 7 Satz 1 Nummer 1 oder Nummer 2 Buchstabe a des Telemediengesetzes geregelte Pflicht des Diensteanbieters zum Einsatz technischer und organisatorischer Schutzmaßnahmen zur Gewährleistung von IT-Sicherheit der für Dritte angebotenen Inhalte in die Bußgeldvorschriften des § 16 Absatz 2 Nummer 3 entspricht der Bußgeldbewehrung eines Verstoßes gegen die weiteren in § 13 Absatz 4 geregelten Pflichten des Diensteanbieters. Bußgeldbewehrt ist

damit auch der Einsatz technischer und organisatorischer Maßnahmen durch den Diensteanbieter, die nicht den Stand der Technik berücksichtigen.

Zu Artikel 5 (Änderung des Telekommunikationsgesetzes)

Zu Nummer 1 (Änderung der Inhaltsangabe)
Nummer 1 enthält eine notwendige Folgeänderung.

Zu Nummer 2 (§ 100 Absatz 1 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten)
Die Änderung dient der Klarstellung, dass ein Diensteanbieter Bestands- und Verkehrsdaten auch zum Erkennen und Beseitigen von Störungen verwenden darf, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. Möglich sind in diesem Zusammenhang beispielsweise Prüfungen des Netzwerkverkehrs, die Verwendung von sogenannten Honeypots (Fallen für Schadprogramme im Netz) oder Spamtraps (Blockieren der Versendung von Schadprogrammen).

Zu Nummer 3 (§ 109 Technische Schutzmaßnahmen)
Zu Buchstabe a (Berücksichtigung des Stands der Technik)
Die gesetzlichen Vorgaben zu technischen Schutzmaßnahmen enthalten nach derzeitiger Rechtslage erhöhte Anforderungen nur für Maßnahmen zum Schutz der Vertraulichkeit (Fernmeldegeheimnis) und für den Schutz personenbezogener Daten. Diese Maßnahmen müssen den Stand der Technik berücksichtigen. Zur Gewährleistung der IT-Sicherheit werden im Übrigen nur „angemessene technische Vorkehrungen und Maßnahmen“ verlangt, wobei die Angemessenheit einzelner Maßnahmen unbestimmt ist und daher insbesondere auch von allgemeinen Wirtschaftlichkeitserwägungen abhängig gemacht werden kann.

Auf Grund der hohen Bedeutung für die Kommunikation des Einzelnen und damit der gesamtgesellschaftlichen Relevanz müssen auch zum Schutz gegen unerlaubte Zugriffe auf die Telekommunikations- und Datenverarbeitungssysteme Maßnahmen getroffen werden, die den Stand der Technik berücksichtigen. Angriffe auf die Systeme erfolgen zunehmend auf höchstem technischen Niveau unter Ausnutzung öffentlich noch nicht bekannter Lücken in der Sicherheitsarchitektur von Hardware- und Softwareprodukten.

Durch diese Angriffe werden die Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität datenverarbeitender Systeme bedroht. Mit der Änderung werden entsprechende Mindestanforderungen für den Schutz gegen unerlaubte Zugriffe und die Auswirkungen von Sicherheitsverletzungen aufgestellt. Sie richten sich an Betreiber von öffentlichen Telekommunikationsnetzen und Anbieter von öffentlichen Telekommunikationsdiensten.

Zu Buchstabe b (Überprüfung der Sicherheitskonzepte)

Die bestehende Regelung im bisherigen Satz 7, wonach die Bundesnetzagentur die Umsetzung des Sicherheitskonzeptes überprüfen kann, wird ersetzt durch eine Verpflichtung zur regelmäßigen Überprüfung der Umsetzung des Sicherheitskonzeptes, die mindestens alle zwei Jahre stattfinden soll. Hierdurch soll erreicht werden, dass die technischen und organisatorischen Maßnahmen jederzeit den Stand der Technik berücksichtigen. Ferner wird den zunehmenden Bedrohungen Rechnung getragen, die dazu führen können, dass mit der Dienstleistungserbringung Angriffe auf die Vertraulichkeit, Integrität und Verfügbarkeit der übertragenen Kommunikation verbunden sind. Bei der Überprüfung kann sich die Bundesnetzagentur der Mittel nach § 115 Absatz 1 und Absatz 2 des Telekommunikationsgesetzes bedienen und mögliche Verstöße gemäß § 115 Absatz 3 des Telekommunikationsgesetzes ahnden.

Zu Buchstabe c (Meldepflichten)

Die bestehenden Meldepflichten gegenüber der Bundesnetzagentur in § 109 Absatz 5 des Telekommunikationsgesetzes werden um die Verpflichtung ergänzt, bekannt gewordene Vorfälle zu melden, die zu beträchtlichen Sicherheitsverletzungen von datenverarbeitenden Systemen der Endnutzer führen können (Nummer 2). Über die bestehenden Meldeverpflichtungen im Bereich des Datenschutzes und bei beträchtlichen Beeinträchtigungen grundlegender Telekommunikationsdienste hinaus wird so gewährleistet, dass die Unternehmen, die das Rückgrat unserer Informationsgesellschaft bilden, ebenfalls zu einem validen und vollständigen Lagebild der IT-Sicherheit beitragen. Ziel ist es, bereits in diesem Vorfeldbereich eine Verbesserung des Lagebildes zur IT-Sicherheit zu erreichen. Verletzungen der IT-Sicherheit (zum Beispiel Manipulationen der Internet-Infrastruktur und Missbrauch einzelner Server oder Anschlüsse, etwa zum Errichten und Betreiben eines Botnetzes) bergen ein großes Gefahrenpotential, das sich in diesem Stadium allerdings noch nicht gegen die Verfügbarkeit der Netze insgesamt, sondern gegen die Funktionsfähigkeit und Verlässlichkeit der IT einzelner Nutzerinnen und Nutzer richtet und gegebenenfalls spätere schwerwiegende Folgen nach sich zieht.

Das Telekommunikationsgesetz sieht eine solche Meldepflicht gegenüber der Bundesnetzagentur bislang nur für tatsächlich aufgetretene Störungen und außerdem nur dann vor, wenn die durch Sicherheitsverletzungen verursachten Auswirkungen auf den Betrieb der Telekommunikationsnetze oder das Erbringen von Telekommunikationsdiensten beträchtlich sind.

Die bei der Bundesnetzagentur hat die bei ihr eingegangenen Meldungen sowie Informationen zu den von dem betreffenden Unternehmen ergriffenen Abhilfemaßnahmen unverzüglich an das BSI weiterzuleiten. Dadurch wird das BSI in die Lage versetzt, seinen Aufgaben nach § 8b Absatz 2 des BSI-Gesetzes nachzukommen.

Zu Buchstabe d (Erstellung eines Sicherheitskataloges)
Die zunehmende Nutzung von Informationstechnik im Rahmen der Telekommunikationstechnik erfordert auch eine normative Stärkung der IT-Sicherheitsbelange bei der Erstellung des Sicherheitskataloges nach Absatz 6. Durch die stärkere Einbeziehung der fachlichen Kompetenz des BSI („Einvernehmen“ statt „Benehmen“) wird diesem Erfordernis Rechnung getragen. Zudem erfolgt eine entsprechende Anpassung für die Bundesbeauftragte bzw. den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit.

Zu Buchstabe e (Übermittlung der Auditergebnisse an das BSI)

Über die im Rahmen von Audits aufgedeckten Mängel bei der Erfüllung der Sicherheitsanforderungen in der Informationstechnik sowie die in diesem Zusammenhang von der Bundesnetzagentur geforderten Abhilfemaßnahmen ist das BSI von der Bundesnetzagentur unverzüglich zu unterrichten.

Zu Nummer 4 (§ 109a Daten- und Informationssicherheit)
Zu Buchstabe a (Änderung der Überschrift)
Buchstabe a enthält eine redaktionelle Folgeänderung und trägt dem erweiterten Regelungsbereich Rechnung.

Zu Buchstabe b (Information der Nutzerinnen und Nutzer)
Die Neuregelung soll die Information der Nutzerinnen und Nutzer über Verletzungen der IT-Sicherheit gewährleisten, die von einem von ihnen betriebenen datenverarbeitenden System ausgehen. Derzeit wird eine entsprechende Information der Nutzerinnen und Nutzer bei den einzelnen Providern uneinheitlich gehandhabt. Die Information soll Nut-

zerinnen und Nutzer in die Lage versetzen, selbst Maßnahmen gegen die auf ihren Systemen vorhandene Schadsoftware zu ergreifen. Hierfür ist Voraussetzung, dass die Nutzerinnen und Nutzer über angemessene Werkzeuge verfügen, um entsprechende Schutzmaßnahmen ergreifen zu können. Ergänzend zur Informationspflicht werden die Anbieter von öffentlichen Telekommunikationsdiensten deshalb verpflichtet, soweit es technisch möglich und zumutbar ist, die Nutzerinnen und Nutzer auf einfach bedienbare Sicherheitswerkzeuge hinzuweisen, die sowohl vorbeugend als auch zur Beseitigung von Störungen bei einer bereits erfolgten Infizierung des Datenverarbeitungssystems mit Schadsoftware eingesetzt werden können.

Nicht erforderlich ist eine individuelle Untersuchung der Technik oder eine individuelle Beratung durch den Anbieter. Soweit eine Benachrichtigung der betroffenen Nutzerinnen und Nutzer innerhalb von wenigen Tagen technisch nicht möglich ist, werden die Anbieter nur ihre Teilnehmerinnen und Teilnehmer informieren und auf Hilfsmittel hinweisen können. Auf die Barrierefreiheit der angebotenen Sicherheitswerkzeuge ist besonders zu achten.

Durch den Einschub „soweit ihm diese bereits bekannt sind“ wird klargestellt, dass zur Ermittlung der Nutzerinnen und Nutzer nur auf solche Verkehrsdaten zugegriffen werden darf, die bereits aufgrund anderer Vorschriften erhoben und gespeichert wurden (etwa im Rahmen von § 100 Absatz 1 des Telekommunikationsgesetzes). Eine Erhebung weiterer Daten ausschließlich zum Zweck der Durchführung einer Benachrichtigung ist nicht zulässig.

Zu Buchstabe c (Folgeänderung)
Buchstabe c enthält eine notwendige Folgeänderung.

Zu Nummer 5 (Änderung der Bußgeldvorschriften)
Nummer 5 enthält eine notwendige Folgeänderung zu der Erweiterung der Meldepflichten in § 109 Absatz 5 des Telekommunikationsgesetzes.

Zu Artikel 6 (Änderung des Bundesbesoldungsgesetzes)

Zu den Nummern 1 und 2 (Anhebung der Besoldungsgruppe)

Mit der Anhebung der Besoldungsgruppe des Präsidenten des BSI auf die Besoldungsstufe B 7 wird der geänderten nationalen wie internationalen Rolle des Bundesamtes für Sicherheit in der Informationstechnik Rechnung getragen. Dem Bundesamt kommt in der Sicherheitsarchitektur der Bundesrepublik Deutschland mit der zunehmenden Digitalisierung aller Gesellschaftsbereiche und der steigenden Cyberbedrohungslage eine immer größere Bedeutung zu. Neben der mit diesem Gesetz einhergehenden Zuständigkeitserweiterung ist bereits nach geltender Rechtslage ein zunehmender Verantwortungs- und Aufgabenzuwachs verbunden. National wie international spielt das Bundesamt bei seinen Ansprechpartnern wie auch in der öffentlichen Wahrnehmung eine immer größere Rolle.

Zu Artikel 7 (Änderung des Bundeskriminalamtgesetzes)

Zu den Nummern 1 und 2 (Zuständigkeitserweiterung)

Durch die Vorschrift wird die Zuständigkeit des Bundeskriminalamts für die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung über die bereits bestehende Zuständigkeit für Straftaten nach § 303b des Strafgesetzbuchs (Computersabotage) hinaus auf Straftaten nach den §§ 202a, 202b, 202c, 263a und 303a des Strafgesetzbuchs ausgedehnt. Zusätzlich zu den Fällen, in denen sich die genannten Straftaten gegen die innere oder äußere Sicherheit der Bundesrepublik Deutschland oder gegen sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen richten, wird geregelt, dass die Zuständigkeit des BKA auch bei derartigen Straftaten gegen Bundeseinrichtungen gegeben ist. Bisher liegt die Zuständigkeit für die polizeilichen Aufgaben der Strafverfolgung in der Regel bei den Ländern, wobei die örtliche Zuständigkeit oftmals dem Zufall überlassen bleibt, abhängig davon, wo der Vorfall zuerst entdeckt wird. Gerade bei Angriffen auf bundesweite Einrichtungen ist eine klare Zuständigkeitsregelung notwendig. Die nachrichtendienstlichen Zuständigkeiten und Befugnisse bleiben unberührt.

Zu Artikel 8 (Weitere Änderung des BSI-Gesetzes)

Die Anpassung ist notwendig, da die schwebende Änderung in Artikel 3 Absatz 7 des Gesetzes zur Strukturreform des Gebührenrechts des Bundes vom 7. August 2013 (BGBl. I S. 3154) so nicht mehr ausführbar ist.

Zu Artikel 9 (Änderung des Gesetzes zur Strukturreform des Gebührenrechts des Bundes)

Siehe die Begründung zu Artikel 8.

Zu Artikel 10 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten des Gesetzes. Zu Satz 2 siehe die Begründung zu Artikel 8.

Das Gesetz soll fünf Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 des BSI-Gesetzes anhand der Konzeption zur Evaluierung neuer Regelungsvorhaben gemäß dem Arbeitsprogramm bessere Rechtsetzung der Bundesregierung vom 28. März 2012, Ziffer II. 3., evaluiert werden.

Anlage

Stellungnahme des Nationalen Normenkontrollrates gem. § 6 Abs. 1 NKRG:
Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (NKR-Nr. 3044)

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

I. Zusammenfassung

Bürgerinnen und Bürger Erfüllungsaufwand:	Keine Auswirkungen
Wirtschaft Jährlicher Erfüllungsaufwand:	Der bezifferbare Mehraufwand beläuft sich auf gut 9 Mio. Euro. Hinzu kommt der Aufwand für die erforderliche Anpassung der IT-Systeme, den Nachweis der Erfüllung der IT-Sicherheitsstandards und den Betrieb der Kontaktstellen.
Verwaltung Jährlicher Erfüllungsaufwand (Personalkosten): Jährlicher Erfüllungsaufwand (Sachkosten): Einmaliger Erfüllungsaufwand:	Maximal 36 Mio. Euro (425 Stellen) 2 Mio. Euro 6 Mio. Euro

Der mit dem Regelungsvorhaben verbundene Erfüllungsaufwand ist wesentlich von der Zahl der Unternehmen abhängig, die diesem Gesetz unterfallen sollen. Die Kriterien, nach welchen die Unternehmen bestimmt werden sollen, sollen jedoch erst zu einem späteren Zeitpunkt in einer Rechtsverordnung geregelt werden. Vor diesem Hintergrund ist die Annahme des Ressorts, dass 2.000 Unternehmen von dem Gesetz betroffen sein werden, mit nicht unerheblichen Unsicherheiten behaftet. Damit sind auch die Angaben zum Erfüllungsaufwand nur eingeschränkt belastbar.

Legt man die oben genannte Zahl der Darstellung zugrunde, hat das Ressort den Aufwand der Wirtschaft, soweit dies ex ante möglich ist, nachvollziehbar dargestellt.

Vor diesem Hintergrund ist ebenfalls der Aufwand auf Seiten der Verwaltung (unter Einbeziehung der vom Ressort zur Verfügung gestellten weiteren Informationen) nachvollziehbar dargestellt. Gleichwohl ist aus Sicht des Nationalen Normenkontrollrats schwer zu beurteilen, inwieweit die ausgewiesenen Personalkapazitäten im Einzelnen tatsächlich erforderlich sind, um den zusätzlichen Aufgaben nachzukommen, die der Entwurf für die Verwaltung beinhaltet.

Auch deshalb begrüßt der Normenkontrollrat, dass das Ressort die Wirkungen des Regelungsvorhabens entsprechend dem Evaluierungsverfahren der Bundesregierung überprüfen wird. Dies soll fünf Jahre nach dem Inkrafttreten der Rechtsverordnung

geschehen, mit welcher die Kriterien für die Bestimmung der betroffenen Unternehmen festgelegt werden sollen.

II. Im Einzelnen

Das Regelungsvorhaben hat den Schutz der IT-Systeme so genannter kritischer Infrastrukturen und weiterer Unternehmen, die für das Gemeinwesen von zentraler Bedeutung sind, zum Ziel. Geschützt werden sollen IT-Infrastrukturen von Unternehmen aus den Sektoren Energie, Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen. Die Kriterien für die Bestimmung der betroffenen Unternehmen sollen in einer Rechtsverordnung festgelegt werden. Auf Seiten der Verwaltung soll das Bundesamt für Sicherheit in der Informationstechnik (BSI) zur zentralen Stelle und Ansprechpartner für IT-Sicherheit in Deutschland ausgebaut werden.

II.1 Erfüllungsaufwand der Wirtschaft

Das Ressort geht bei seiner Darstellung des Erfüllungsaufwands von 2.000 Unternehmen aus, die im Sinne des Regelungsvorhabens als systemrelevant einzustufen sind, das heißt, deren Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit mit sich bringen würden. Diese Annahme fußt auf einer Untersuchung des BSI und des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe. Zu berücksichtigen ist hierbei, dass die Zahl der Unternehmen wesentlich von der noch zu erstellenden Rechtsverordnung abhängt. Daher ist zum jetzigen Zeitpunkt lediglich eine sehr grobe Einschätzung der Zahl der Unternehmen möglich. Aus diesem Grund sind die Darstellungen des Erfüllungsaufwands nur eingeschränkt belastbar.

Das Regelungsvorhaben enthält für die Betreiber kritischer Infrastrukturen im Wesentlichen vier Vorgaben:

II.1.1 Einhaltung von Mindestanforderungen an die IT-Sicherheit

Betreiber kritischer Infrastrukturen sollen verpflichtet werden, spätestens zwei Jahre nach Erlass der oben genannten Rechtsverordnung organisatorische und technische Mindestanforderungen zur Vermeidung von Beeinträchtigungen ihrer informationstechnischen Systeme und Prozesse zu erfüllen, soweit diese für den Betrieb ihrer kritischen Infrastrukturen erforderlich sind.

Die Verpflichtung zur Sicherstellung dieses Mindeststandards an IT-Sicherheit wird dort zu Mehrkosten führen, wo kein hinreichendes IT-Sicherheitsniveau vorhanden ist. Der hierfür anfallende Aufwand ist ex ante nicht seriös bezifferbar, da er einerseits von den jeweiligen Sicherheitsanforderungen und andererseits davon

abhängt, welche Maßnahmen die Unternehmen schon jetzt zur Sicherung ihrer Systeme ergriffen haben.

II.1.2 Meldung erheblicher IT-Sicherheitsvorfälle an das BSI

Ferner sollen Betreiber kritischer Infrastrukturen erhebliche Störungen ihrer informationstechnischen Systeme und Prozesse an das BSI melden, wenn diese Störungen zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastruktur führen können oder bereits geführt haben. Die Meldung soll Angaben zur Störung, zu den betroffenen IT-Systemen, zur vermuteten oder tatsächlichen Ursache etc. enthalten.

Das Ressort geht von sieben relevanten IT-Sicherheitsvorfällen pro Jahr und Unternehmen aus. Ausweislich einer Untersuchung von Seiten der Wirtschaft liegen die Kosten einer Meldung bei 660 Euro (bei rund 11 Stunden Zeitaufwand pro Meldung). Bei Zugrundelegung der oben genannten 2.000 Betreiber kritischer Infrastrukturen ist von einem jährlichen Erfüllungsaufwand von rund 9,2 Mio. Euro auszugehen.

II.1.3 Nachweis der Erfüllung der Mindestanforderungen durch Sicherheitsaudits

Darüber hinaus sollen die Betreiber kritischer Infrastrukturen künftig mindestens alle zwei Jahre nachweisen, dass sie die Mindestanforderungen erfüllen. Dies kann durch Sicherheitsaudits, Zertifizierungen oder auf sonstige geeignete Weise geschehen.

Da dieser Aufwand stark vom gewählten Prüfverfahren und von den Gegebenheiten im Unternehmen abhängig ist, ist dieser Aufwand ex ante kaum seriös quantifizierbar.

II.1.4 Betreiben einer Kontaktstelle

Betreiber kritischer Infrastrukturen sollen gegenüber dem BSI eine Kontaktstelle benennen, über die die Kommunikation zwischen dem BSI und dem Unternehmen abgewickelt werden kann. Diese Kontaktstelle soll jederzeit erreichbar sein.

Die Verpflichtung zum Betreiben einer Kontaktstelle wird dort zu Mehraufwand führen, wo noch keine Stelle existiert, die diese Aufgabe übernehmen kann. Um eventuelle Mehrkosten so gering wie möglich zu halten, ist im Regelungsvorhaben vorgesehen, dass Betreiber kritischer Infrastrukturen eine gemeinsame (übergeordnete) Kontaktstelle betreiben können. Dies dürfte auch die Umsetzung dieser Vorgabe für kleinere Unternehmen erleichtern, sofern solche nach der zu

erlassenden Rechtsverordnung von dem vorliegenden Regelungsentwurf betroffen sind.

II.1.5 Weitere Adressaten aus dem Wirtschaftsbereich

Betreiber öffentlicher Telekommunikationsnetze und öffentlich zugänglicher Telekommunikationsdienste sollen nur von einem Teil der oben genannten Vorgaben betroffen sein:

- Auch diese Betreiber sollen Maßnahmen zur Sicherung ihrer IT-technischen Einrichtungen vornehmen. Sie sollen dem Stand der Technik entsprechen. Die Ausführungen unter II.1.1 gelten entsprechend.
- Ferner sollen sie wie die Betreiber kritischer Infrastrukturen IT-Sicherheitsvorfälle an die Bundesnetzagentur (BNetzA) melden. Dabei ist zu berücksichtigen, dass es in diesem Bereich bereits ein Verfahren zur Meldung von IT-Sicherheitsvorfällen gibt. Danach ist eine Meldung an die BNetzA nur für tatsächlich aufgetretene Störungen und nur dann erforderlich, wenn die durch Sicherheitsverletzungen verursachten Auswirkungen beträchtlich sind. Durch das vorliegende Regelungsvorhaben soll diese Verpflichtung insofern erweitert werden, als die Betreiber künftig auch Vorfälle melden sollen, die zu erheblichen Sicherheitsverletzungen von datenverarbeitenden Systemen der Endnutzer führen können. Insofern ist in diesem Bereich von einer Erhöhung der Zahl der Meldungen auszugehen.

II.2 Erfüllungsaufwand der Verwaltung

Nach Angaben des Ressorts führt das Regelungsvorhaben zu einem erheblichen Mehraufwand auf Seiten der betroffenen Behörden. Der Mehrbedarf liegt bei Zugrundelegung der oben genannten 2.000 Unternehmen bei maximal 425 Stellen (rund 36 Mio. Euro; auch bei den folgenden Angaben handelt es sich jeweils um Maximalwerte). Der Mehrbedarf soll in den jeweiligen Einzelplänen ausgeglichen werden:

- Der Großteil des oben genannten Mehraufwands entfällt mit knapp 220 Stellen (knapp 16 Mio. Euro) auf das BSI. Darüber hinaus ist mit Sachkosten von einmalig rund 6 Mio. Euro zu rechnen.

  Mit dem Regelungsentwurf soll das BSI zur nationalen Informationssicherheitsbehörde ausgebaut werden. Hierfür soll die Grundlagenarbeit im BSI deutlich ausgebaut werden, um insbesondere im Bereich der Beratung von Unternehmen (wie auch von Behörden) die erforderliche Fachkompetenz vorweisen zu können. Diese ist außerdem erforderlich, um konkrete Sicherheitsmängel identifizieren sowie die in den oben genannten

Wirtschaftssektoren jeweils erforderlichen Sicherheitsstandards erarbeiten zu können.

Aus Sicht des Ressorts wird außerdem aus der Auswertung der Meldungen von Seiten der Wirtschaft und der Beratung der Betreiber kritischer Infrastrukturen ein erheblicher Mehraufwand resultieren. Dieser ergibt sich unter anderem daraus, dass Informationstechnik in den sieben Sektoren sehr unterschiedlich eingesetzt wird. Dies betrifft sowohl die genutzten Komponenten, Systeme und externen Dienstleistungen als auch die eingesetzten Systeme zur Sicherung der Funktionsfähigkeit der kritischen Prozesse.

- Ausweislich des Entwurfs ist beim Bundeskriminalamt mit einem Mehraufwand von knapp 80 Stellen (gut 5 Mio. Euro) zu rechnen.

  Mit dem Entwurf soll die Zuständigkeit des Bundeskriminalamts für die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung ausgeweitet werden. So soll die Zuständigkeit künftig auch die Straftatbestände des Ausspähens von Daten, des Abfangens von Daten, des Computerbetrugs etc. umfassen.
- Für das Bundesamt für Verfassungsschutz (BfV) geht der Entwurf von einem Mehraufwand von knapp 50 Stellen (3,3 Mio. Euro) aus.

  Dieser resultiert aus der Auswertung der vom BSI zur Verfügung gestellten Informationen und sich daraus für das BfV ergebenden Handlungserfordernissen.
- Der übrige Stellenmehrbedarf entfällt auf das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, die Bundesnetzagentur, den Bundesnachrichtendienst, das Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit sowie auf die Bundesbeauftragte für Datenschutz und Informationsfreiheit.
- Darüber hinaus dürfte auf Seiten der Aufsichtsbehörden ein gewisser Mehraufwand durch die Auswertung der Berichte des BSI für ihre Zwecke auftreten.

II.3 Evaluation

Das Ressort beabsichtigt, das Regelungsvorhaben fünf Jahre nach Inkrafttreten der Rechtsverordnung zu evaluieren, mit welcher die Kriterien für die Bestimmung der betroffenen Unternehmen festgelegt werden sollen.

Zusammenfassend ist festzustellen, dass die Darstellung des Erfüllungsaufwands mit nicht unerheblichen Unsicherheiten behaftet ist, da der Kreis der Adressaten derzeit nicht hinreichend einschätzbar ist. Damit sind die Angaben zum Erfüllungsaufwand nur

eingeschränkt belastbar. Bei Zugrundelegung der Zahl von 2.000 Unternehmen ist der mit dem Regelungsvorhaben verbundene Aufwand, soweit dies ex ante möglich ist, nachvollziehbar dargestellt.

Hinsichtlich des Aufwands der Verwaltung ist es aus Sicht des Nationalen Normenkontrollrats schwer zu beurteilen, inwieweit die ausgewiesenen Personalkapazitäten im Einzelnen tatsächlich erforderlich sind, um den zusätzlichen Aufgaben nachzukommen, die der Entwurf für die Verwaltung beinhaltet. In diesem Zusammenhang wird bei der Umsetzung besonderes Augenmerk darauf zu legen sein, dass in den verschiedenen Behörden, die von dem Gesetz betroffen sind, dieselben Arbeiten – zum Beispiel die Analyse einer Schadsoftware – nicht mehrfach vorgenommen werden.

Im Hinblick auf die parallel zu diesem Gesetzgebungsverfahren laufenden Verhandlungen über die NIS-Richtlinie gilt es, ein Auseinanderfallen der Regelungen zu vermeiden, da eventuelle spätere Änderungen infolge der Richtlinie zu unnötigem Mehraufwand bei den Adressaten führen würden.

Auch vor dem Hintergrund der Unsicherheiten im Hinblick auf die Folgekosten begrüßt der Normenkontrollrat, dass das Ressort die Wirkungen des Regelungsvorhabens entsprechend dem Evaluierungsverfahren der Bundesregierung überprüfen wird.

Dr. Ludewig	Prof. Kuhlmann
Vorsitzender	Berichterstatterin