Referentenentwurf

des Bundesministeriums des Innern

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

A. Problem und Ziel

Die Nutzung informationstechnischer Systeme und das Internet mit seinen vielfältigen Angeboten durchdringen Staat, Wirtschaft und Gesellschaft in immer größerem Maße. Relevante Aspekte der privaten und öffentlichen Lebensbereiche werden zunehmend ins Netz verlagert, dort behandelt 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. Mit dem Grad der wirtschaftlichen und gesellschaftlichen Interaktion und Integration wachsen aber auch die wirtschaftlichen, gesellschaftlichen und individuellen Abhängigkeiten. Parallel dazu steigt die Bedeutung der Verfügbarkeit und Sicherheit der eigenen IT-Systeme sowie eines verfügbaren und sicheren Cyberraums insgesamt.

Die IT-Sicherheitslage in Deutschland ist weiterhin angespannt. Deutschland ist - auch im internationalen Vergleich - zunehmend Ziel von Cyberangriffen, Cyberspionage und sonstigen Formen der Cyberkriminalität. Wirtschaft, Bürger und auch der Staat selbst sind hiervon gleichermaßen betroffen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) erhält und analysiert - u.a. in dem 2011 gegründeten Cyberabwehrzentrum - kontinuierlich eine Vielzahl von Informationen zur aktuellen Bedrohungssituation im Cyberraum. Die Angriffe erfolgen danach zunehmend zielgerichtet, technologisch ausgereifter und komplexer. Die vielfach international agierenden Angreifer arbeiten immer professioneller und effizienter. Neue Schwachstellen werden immer schneller

ausgenutzt. Dabei geht der Trend vom Angebot einzelner Angriffswerkzeuge hin zu kompletten Angriffsdienstleistungen.

Mit dem Gesetz soll eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland erreicht werden. Die vorgesehenen Neuregelungen dienen dazu, den Schutz der Verfügbarkeit, Integrität und Vertraulichkeit datenverarbeitender Systeme zu verbessern und der gestiegenen Bedrohungslage anzupassen. Ziel des Gesetzes ist eine Verbesserung der IT-Sicherheit bei Unternehmen, ein verstärkter Schutz der Bürgerinnen und Bürger in einem sicheren Netz, der Ausbau der IT-Sicherheit der Bundesverwaltung und in diesem Zusammenhang auch eine Stärkung von BSI und Bundeskriminalamt (BKA).

Besondere Bedeutung kommt im Bereich der IT-Sicherheit von Unternehmen den Infrastrukturen zu, die für das Funktionieren unseres Gemeinwesens von überragender Bedeutung sind. Der Schutz der IT-Systeme Kritischer Infrastrukturen und der für den Infrastrukturbetrieb nötigen Netze hat daher höchste Priorität. Das IT-Sicherheitsniveau bei Kritischen Infrastrukturen ist derzeit sehr unterschiedlich: In manchen Infrastrukturbereichen existieren ausgeprägte gesetzliche Vorgaben auch zur IT-Sicherheit, in anderen Bereichen fehlen solche gänzlich. Manche Bereiche verfügen über ein ausgeprägtes Risikomanagement, 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 auch untereinander und der daraus resultierenden Interdependenzen ist dieser Zustand nicht hinnehmbar. Die Zusammenarbeit zwischen Staat und Betreibern Kritischer Infrastrukturen muss daher verbessert werden und ein Mindestniveau an IT-Sicherheit bei den Betreibern Kritischer Infrastrukturen gewährleistet sein.

Auf Grund der dezentralen und vernetzten Struktur des Internet als zentralem Kommunikationsmedium kann IT-Sicherheit nur durch eine gemeinsame Verantwortungswahrnehmung aller Beteiligten gewährleistet werden. Aus diesem Grund werden in dem Gesetz auch die Betreiber und Anbieter der zugrundeliegenden Kommunikationsinfrastruk-

tur sowie Anbieter entsprechender Mediendienste mit besonderen Sicherungspflichten adressiert.

Parallel dazu trägt das Gesetz dazu bei, BSI und BKA rechtlich so aufzustellen, dass diese der steigenden Cyber-Bedrohungslage zum Schutz der Bürgerinnen und Bürger angemessen begegnen können.

B. Lösung

Defizite im Bereich der IT-Sicherheit sind abzubauen. Insbesondere Betreiber Kritischer Infrastrukturen sind wegen der weitreichenden gesellschaftlichen Folgen eines Ausfalls und ihrer besonderen Verantwortung für das Gemeinwohl zu verpflichten, einen Mindeststandard an IT-Sicherheit einzuhalten und dem BSI IT-Sicherheitsvorfälle zu melden. Die beim BSI zusammenlaufenden Informationen werden dort gesammelt und ausgewertet und die darüber gewonnenen Erkenntnisse den Betreibern Kritischer Infrastrukturen zur Verbesserung des eigenen Schutzes zur Verfügung gestellt. Gleichzeitig wird die Rolle des BSI im Bereich der IT-Sicherheit Kritischer Infrastrukturen gestärkt, indem es die Aufgabe erhält, die Betreiber auf Ersuchen bei der Sicherung der Informationstechnik zu beraten und zu unterstützen.

Um den Schutz der Bürgerinnen und Bürger in einem sicheren Netz zu verbessern, werden die Telekommunikations- und Telemediendiensteanbieter, die eine Schlüsselrolle für die Sicherheit des Cyberraums haben, noch stärker in die Verantwortung genommen. Sie werden verpflichtet, IT-Sicherheit nach dem Stand der Technik nicht nur wie bisher zum Schutz der Vertraulichkeit und zum Schutz personenbezogener Daten, sondern auch zum Schutz von Telekommunikations- und Datenverarbeitungssystemen gegen unerlaubte Zugriffe zu gewährleisten. Damit wird die Widerstandsfähigkeit der Kommunikationsinfrastruktur insgesamt verbessert und die Verfügbarkeit, Integrität und Authentizität datenverarbeitender Systeme und der dort vorgehaltenen Daten gesichert.

Telekommunikationsanbieter sollen zudem IT-Sicherheitsvorfälle, die zu einem unerlaubten Zugriff auf die Systeme der Nutzer oder einer Störung ihrer Verfügbarkeit führen

können, unverzüglich melden. Über die bestehenden Meldeverpflichtungen im Bereich des Datenschutzes und bei erheblichen Beeinträchtigungen grundlegender Telekommunikationsdienste hinaus wird so gewährleistet, dass die Unternehmen, die das Rückgrat unserer Informationsgesellschaft bilden, zu einem validen und vollständigen Lagebild der IT-Sicherheit beitragen. Dieses Lagebild dient seinerseits wiederum als Grundlage für die Information der Nutzer durch staatliche Stellen und für abgestimmte Reaktionen auf Cybersicherheitsvorfälle. Außerdem sollen Telekommunikationsanbieter betroffene Nutzer über bekannte Störungen durch Schadprogramme auf ihren datenverarbeitenden Systemen informieren und ihnen einfach bedienbare Hilfsmittel für die Erkennung und Beseitigung bereitstellen. Die Nutzer sollen dadurch in die Lage versetzt werden, selbst Maßnahmen gegen Schadsoftware auf ihren datenverarbeitenden Systemen zu ergreifen, um damit einen Beitrag zur Verbesserung der IT-Sicherheit der Netze insgesamt zu erbringen. Ebenfalls dem Schutz der Bürgerinnen und Bürger dient die Verpflichtung von Telemediendiensteanbieter zum Angebot sicherer Authentifizierungsverfahren. Außerdem sollen Telekommunikations- und Telemediendiensteanbieter ihre Nutzungsdaten zum Schutz der Kunden und zur Beseitigung von Störungen verwenden dürfen.

Daneben sind die geltenden Zuverlässigkeitsanforderungen zu erhöhen: Die Bundesnetzagentur soll die Befugnis bekommen, bei fehlender Zuverlässigkeit eines Unternehmens den Betrieb der betreffenden Telekommunikationsanlage oder des geschäftsmäßigen Erbringens des betreffenden Telekommunikationsdienstes zu untersagen. Parallel dazu sollen mit Maßnahmen und Produkten der Telekommunikationsüberwachung befasste Unternehmen ausdrücklich in die Investitionskontrolle nach dem Außenwirtschaftsgesetz aufgenommen werden. Dadurch wird den mit der steigenden Bedeutung der Abwicklung und Ausgestaltung des Datenverkehrs für Staat und Bürger ebenfalls häufiger berührten Sicherheitsinteressen der Bundesrepublik Deutschland Rechnung getragen.

Angesichts der quantitativ wie qualitativ zunehmenden Cyberangriffe auf die Regierungsnetze ist zudem die Sicherheit der IT der Bundesverwaltung weiter auszubauen

und die Rolle des BSI bei entsprechenden Vorgaben zu stärken. Auch über den Bereich der Bundesverwaltung hinaus muss das BSI weiter gestärkt und die Rechtslage an seine geänderte Rolle und Bedeutung angepasst werden. In diesem Zusammenhang sind auch die Warnbefugnisse des BSI klarer zu regeln. Die in dem Gesetz vorgesehene jährliche Berichtspflicht soll dazu beitragen, das Bewusstsein aller relevanten Akteure für das Thema IT-Sicherheit weiter zu schärfen. Da eine Vielzahl von erfolgreichen IT-Angriffen bereits durch die Umsetzung von Standardsicherheitsmaßnahmen zu verhindern wäre, leistet ein höherer Grad an Sensibilisierung der Nutzer einen wichtigen Beitrag zur Verbesserung der IT-Sicherheit insgesamt. Die gewachsene Rolle des BSI als internationale Zentralstelle für IT-Sicherheit wird festgeschrieben, der Anteil des BSI an der Erstellung des Sicherheitskatalogs für Telekommunikationsnetzbetreiber ausgebaut.

Begleitend dazu ist die Rolle des BKA im Bereich Cyberkriminalität angesichts der zunehmenden Zahl von IT-Angriffen gegen Bundeseinrichtungen und gegen bundesweite Kritische Infrastrukturen weiter als bisher zu fassen. Die Zuständigkeit des BKA wird für polizeiliche Aufgaben auf dem Gebiet der Strafverfolgung über die bereits bestehende Zuständigkeit für Straftaten nach § 303b des Strafgesetzbuches (Computersabotage) hinaus auf Straftaten nach §§ 202a (Ausspähen von Daten), 202b (Abfangen von Daten), 202c (Vorbereiten des Ausspähens und Abfangens von Daten), 263a (Computerbetrug) und 303a (Datenveränderung) des Strafgesetzbuches ausgedehnt, sofern sich diese gegen die innere oder äußere Sicherheit der Bundesrepublik Deutschland oder sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen richten.

Die Regelungen zu den branchenspezifischen Sicherheitsanforderungen und den Meldungen erheblicher IT-Sicherheitsvorfälle für Betreiber Kritischer Infrastrukturen entsprechen im Grundsatz den Vorschlägen der Kommission für eine Richtlinie des Europäischen Parlaments und des Rates über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union. So enthalten die Art. 14 bis 16 des Richtlinienentwurfs Mindestanforderungen bezüglich der Sicherheit der Netze und Informationssysteme. Die Mitgliedstaaten sollen nach den derzeitigen Entwürfen der EU Marktteilnehmer (bestimmte Telemedienanbieter sowie Betreiber Kritischer Infra-

strukturen in den Bereichen Energie, Verkehr, Banken und Börsen und Gesundheitswesen) und die öffentliche Verwaltung zu Maßnahmen zum Risikomanagement und zur Meldung von Sicherheitsvorfällen an die zuständigen nationalen Behörden verpflichten. Bei den laufenden Verhandlungen zum Richtlinienentwurf werden die Inhalte dieses Gesetzes Leitlinie für die Position der Bundesregierung sein.

C. Alternativen

Beibehalten des bisherigen Rechtszustandes.

D. Haushaltsangaben ohne Erfüllungsaufwand

Über die Finanzierung des Mehrbedarfs an Sach- und Personalmitteln wird im Rahmen der Aufstellung des Haushalts entschieden.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Für die Wirtschaft entsteht bei Betreibern Kritischer Infrastrukturen sowie bestimmten Telekommunikations- und Telemediendiensteanbietern Erfüllungsaufwand für die Einhaltung eines Mindestniveaus an IT-Sicherheit und die Einrichtung und Aufrechterhaltung entsprechender Meldewege. Dies wird faktisch aber nur dort zu Mehrkosten führen, wo bislang noch kein hinreichendes Niveau an IT-Sicherheit bzw. keine entsprechenden Meldewege etabliert sind. Für diejenigen betroffenen Wirtschaftsteilnehmer, bei denen dies bereits ganz oder teilweise der Fall ist, entstehen insoweit keine gesonderten Kosten. Zusätzliche Kosten entstehen für die Betreiber Kritischer Infrastrukturen durch die Durchführung der vorgesehenen Sicherheitsaudits.

Die konkrete Berechnung und Darstellung des Erfüllungsaufwands kann erst mit Erlass der Rechtsverordnung nach § 10 BSI-Gesetz auf der Grundlage des im Zweiten Teils der Begründung zu Nummer 9 dargestellten Verfahrens erfolgen, da erst durch die Rechtsverordnung der Adressatenkreis der entsprechenden Verpflichtungen hinreichend konkret eingegrenzt wird.

E.3 Erfüllungsaufwand für die Verwaltung

Die neu geschaffenen Befugnisse und Aufgaben des Bundesamts für Sicherheit in der Informationstechnik sind mit einem entsprechenden Vollzugsaufwand verbunden. Für die Erfüllung der im Gesetz vorgesehenen Aufgaben besteht beim BSI ein zusätzlicher Aufwand von insgesamt 133 zusätzlichen Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 8.897 T€ sowie zusätzlichen Sachkosten in Höhe von jährlich rund 5.000 T€.

Die neuen Mitwirkungsaufgaben für das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) führen dort zu einem zusätzlichen Bedarf von 9 Planstellen/Stellen mit jährlichen Personal– und Sachkosten in Höhe von 681 T€ für die Aufgaben nach § 8a Absatz 2 und 3, § 8b Absatz 2 Nummer 2 und § 10 BSI-Gesetz.

In den Fachabteilungen des BKA entsteht durch die Erweiterung der originären Ermittlungszuständigkeit ein Ressourcenaufwand von 79 zusätzlichen Planstellen / Stellen mit jährlichen Personalkosten in Höhe von rund 5.385 T€ sowie zusätzlichen Sachmitteln in Höhe von einmalig 630 T€ im ersten Jahr.

In den Fachabteilungen des Bundesamtes für Verfassungsschutz (BfV) entsteht durch die Zuständigkeit gemäß dem neuen § 8b Absatz 2 Nummer 2 BSI-Gesetz ein zusätzlicher Ressourcenbedarf von 55 Planstellen / Stellen mit Personal und Sachkosten in Höhe von 4.496 T€ für das Jahr 2015 sowie jeweils ein Haushaltsmittelbedarf in Höhe von 4.170 T€ für die Folgejahre.

F. Weitere Kosten

Keine.

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

Vom …

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1
Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik

Das BSI-Gesetz vom 14. August 2009 (BGBl. I, S. 2821) wird wie folgt geändert:

1. § 1 wird wie folgt gefasst:

   „Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik als nationale Informationssicherheitsbehörde. Es untersteht als Bundesoberbehörde dem Bundesministerium des Innern."

2. Dem § 2 Absatz 9 werden folgende Absätze 10 und 11 angefügt:

   „(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind die durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmten Einrichtungen, Anlagen oder Teile davon in den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind und durch deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe oder erhebliche Störungen der öffentlichen Si-

cherheit eintreten würden. Kommunikationstechnik im Sinne des Absatzes 3 Satz 1 und 2 gehört nicht zu den Kritischen Infrastrukturen im Sinne dieses Gesetzes.

(11) Betreiber Kritischer Infrastrukturen im Sinne dieses Gesetzes sind alle Unternehmen, die Kritische Infrastrukturen betreiben, mit Ausnahme solcher Unternehmen, die 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) sind. Ein Unternehmen, das sich darauf beruft, Kleinstunternehmen im Sinne der vorgenannten Empfehlung der Kommission zu sein, hat dem Bundesamt auf dessen Verlangen das Vorliegen der dafür erforderlichen Voraussetzungen auf geeignete Weise nachzuweisen."

3. § 3 wird wie folgt geändert:

   a. In Absatz 1 Satz 2 Nummer 2 werden die Wörter „andere Stellen" durch das Wort „Dritte" ersetzt.

   b. In Absatz 1 Satz 2 Nummer 15 werden die Worte „kritischen Informationsinfrastrukturen" durch die Worte „der Sicherheit der Informationstechnik Kritischer Infrastrukturen" und der Punkt durch ein Semikolon ersetzt.

   c. In Absatz 1 Satz 2 wird folgende Nummer 16 angefügt:

      „Zentrale Stelle im Bereich der Sicherheit in der Informationstechnik bei der Zusammenarbeit mit den zuständigen Stellen im Ausland."

   d. Folgender Absatz 3 wird angefügt:

      „Das Bundesamt nimmt als zentrale Stelle für die Sicherheit der Informationstechnik Kritischer Infrastrukturen die Aufgaben nach §§ 8a und 8b wahr. Das Bundesamt kann Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen."

4. Die Überschrift von § 4 wird wie folgt gefasst:

   „Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes“.

5. § 7 Absatz 1 wird wie folgt geändert:

   a. In Satz 1 werden nach dem Wort „Schadprogrammen“ die Worte „und im Falle des unberechtigten Abflusses von Daten“ eingefügt.

   b. Nach Satz 1 wird folgender Satz 2 eingefügt:

      „Das Bundesamt kann sich bei der Wahrnehmung der Aufgaben nach Satz 1 der Einschaltung Dritter bedienen, wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist.“

   c. Die bisherigen Sätze 2 und 3 werden die Sätze 3 und 4.

6. Nach § 7 wird folgender § 7a eingefügt:

   „§ 7a

   Untersuchung der IT-Sicherheit

   „(1) Das Bundesamt darf zur Wahrnehmung seiner Aufgaben nach § 3 Absatz 1 Nummer 1 und § 3 Absatz 3 informationstechnische Produkte, Systeme und Dienste untersuchen. Es darf sich dazu aller geeigneten technischen Mittel sowie der Unterstützung Dritter bedienen.

   (2) Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Förderung der IT-Sicherheit genutzt werden. Das Bundesamt darf seine Bewertung der Sicherheit der untersuchten Produkte, Systeme und Dienste weitergeben und veröffentlichen. § 7 Absatz 1 Satz 2 und 3 ist entsprechend anzuwenden.“

7. § 8 Absatz 1 wird wie folgt geändert:

a. § 8 Absatz 1 Satz 1 wie folgt gefasst:

„Das Bundesamt legt verbindliche Mindeststandards für die Sicherheit der Informationstechnik des Bundes fest und berät die Bundesbehörden auf Ersuchen bei der Umsetzung und Einhaltung dieser Mindeststandards."

b. § 8 Absatz 1 Sätze 2 bis 4 werden wie folgt gefasst und ein neuer Satz 5 angefügt:

„Das Bundesministerium des Innern erlässt im Benehmen mit dem Rat der IT-Beauftragten der Ressorts die nach Satz 1 festgelegten Anforderungen als allgemeine Verwaltungsvorschriften. Das Bundesamt kann eine Überprüfung der Einhaltung der nach Satz 1 festgelegten Anforderungen in der Einrichtung durchführen. Diese ist verpflichtet, das Bundesamt und seine Beauftragten hierbei zu unterstützen. Vom Bundesamt festgestellte Mängel bei der Umsetzung dieser Anforderungen sind innerhalb einer vom Bundesamt festgelegten angemessenen Frist zu beheben."

c. Der bisherige Satz 3 wird gestrichen.

d. Der bisherige Satz 4 wird Satz 6.

8. Nach § 8 werden folgende §§ 8a, 8b und 8c eingefügt:

„§ 8a

Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, binnen zwei Jahren nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen und sonstige Maßnahmen zum Schutz derjenigen informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei ist der Stand der Technik zu berücksichtigen. Organisatorische und technische Vorkehrungen und sonstige Maßnahmen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu

den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastruktur steht.

(2) Betreiber Kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards vorschlagen. Das Bundesamt erkennt die branchenspezifischen Sicherheitsstandards im Benehmen mit den zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe auf Antrag an, wenn diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten. Die vom Bundesamt anerkannten branchenspezifischen Sicherheitsstandards konkretisieren die organisatorischen und technischen Vorkehrungen und sonstigen Maßnahmen nach Absatz 1.

(3) Zur Überprüfung der organisatorischen und technischen Vorkehrungen und sonstigen Maßnahmen nach Absatz 1 haben die Betreiber Kritischer Infrastrukturen mindestens alle zwei Jahre die Erfüllung der Anforderungen auf geeignete Weise nachzuweisen. Hierfür übermitteln sie dem Bundesamt mindestens alle zwei Jahre eine Aufstellung der zu diesem Zweck durchgeführten Sicherheitsaudits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Das Bundesamt kann bei Sicherheitsmängeln eine Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse verlangen. Bei Sicherheitsmängeln kann das Bundesamt deren unverzügliche Beseitigung verlangen.

(4) Auf Betreiber Kritischer Infrastrukturen finden die Absätze 1 bis 3 keine Anwendung, soweit diese ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen. Die Vorschriften des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 1 des Gesetzes vom 3. Mai 2012 (BGBl. I S. 958), bleiben unberührt. Satz 1 gilt für Betreiber Kritischer Infrastrukturen, für die aus oder auf Grund von sonstigen Rechtsvorschriften des Bundes vergleichbare oder weitergehende Anforderungen im Sinne der Absätze 1 bis 3 bestehen, entsprechend.

§ 8b
Zentrale Meldestelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Das Bundesamt ist die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit der informationstechnischen Systeme, Komponenten oder Prozesse nach § 8a Absatz 1 Satz 1.

(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe

1. die für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik wesentlichen Informationen, insbesondere zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweise, zu sammeln und auszuwerten,

2. in Zusammenarbeit mit den zuständigen Bundesbehörden die potentiellen Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen zu analysieren,

3. das Lagebild bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen kontinuierlich fortzuschreiben und

4. die Betreiber Kritischer Infrastrukturen, die zuständigen Aufsichtsbehörden sowie die sonst zuständigen Bundesbehörden über sie betreffende Informationen nach den Nummern 1 bis 3 und die in Erfahrung gebrachten Zusammenhänge zu unterrichten.

(3) Um bei Beeinträchtigungen der informationstechnischen Systeme, Komponenten oder Prozesse Kritischer Infrastrukturen eine unverzügliche Information betroffener Betreiber Kritischer Infrastrukturen zu gewährleisten, sind dem Bundesamt binnen sechs Monaten nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 für den Aufbau der Kommunikationsstrukturen nach § 3 Absatz 1 Nummer 15 Warn- und Alarmierungskontakte zu benennen. Der Betreiber hat sicherzustellen, dass er hierüber jederzeit erreichbar ist. Die Unterrichtung durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt dorthin.

(4) Betreiber Kritischer Infrastrukturen haben über die Warn- und Alarmierungskontakte nach Absatz 3 Satz 1 Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der von ihnen betriebenen Kritischen Infrastruktur führen können, unverzüglich an das Bundesamt zu melden. Die Meldung muss Angaben zu den technischen Rahmenbedingungen, insbesondere der eingesetzten und betroffenen Informationstechnik sowie zur Branche des Betreibers enthalten. Die Nennung des Betreibers ist nicht erforderlich.

(5) Führt eine Beeinträchtigung der informationstechnischen Systeme, Komponenten oder Prozesse zu einem Ausfall oder zu einer Beeinträchtigung der Kritischen Infrastruktur, ist dies unverzüglich durch den Betreiber der Kritischen Infrastruktur über die Warn- und Alarmierungskontakte nach Absatz 3 Satz 1 unter Angabe der Informationen nach Absatz 4 Satz 2 sowie der Nennung des Betreibers an das Bundesamt zu melden.

(6) Zusätzlich zu den Warn- und Alarmierungskontakten nach Absatz 3 Satz 1 können alle oder ein Teil der Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, einen gemeinsamen Ansprechpartner benennen, über den der Informationsaustausch zwischen den Warn- und Alarmierungskontakten und dem Bundesamt nach Absatz 2 Nummer 4 und nach Absatz 4 erfolgt.

(7) Auf Betreiber Kritischer Infrastrukturen finden die Absätze 3 bis 6 keine Anwendung, soweit diese ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen. Die Vorschriften des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 1 des Gesetzes vom 3. Mai 2012 (BGBl. I S. 958), bleiben unberührt. Für Betreiber Kritischer Infrastrukturen, für die aus oder auf Grund von sonstigen Rechtsvorschriften des Bundes vergleichbare oder weitergehende Anforderungen im Sinne der Absätze 3 bis 6 bestehen, gilt Satz 1 entsprechend.

§ 8c

Auskunftsverlangen Dritter

Das Bundesamt kann Dritten Auskunft zu den im Rahmen von § 8a Absatz 2 und 3 anfallenden Informationen sowie zu den Meldungen nach § 8b Absatz 4 und 5 geben, wenn schutzwürdige Interessen der Betreiber Kritischer Infrastrukturen nicht entgegenstehen und durch die Auskunft keine Beeinträchtigung des Verfahrens oder sonstiger wesentlicher Sicherheitsinteressen zu erwarten ist. In den Fällen des § 8a Absatz 3 und des § 8b Absatz 5 ist die Zustimmung des betroffenen Betreibers erforderlich. Zugang zu den Akten des Bundesamtes in Angelegenheiten nach § 8a und § 8b wird nicht gewährt.“

9. § 10 wird wie folgt geändert:

a. Vor Absatz 1 wird folgender neuer Absatz 1 eingefügt:

„Das Bundesministerium des Innern bestimmt nach Anhörung von Vertretern der Wissenschaft, betroffener Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung und Landwirtschaft, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit durch Rechtsverordnung die Kritischen Infrastrukturen nach § 2 Absatz 10. Zugang zu Akten, die diese Verordnung betreffen, wird nicht gewährt.“

b. Die bisherigen Absätze 1 und 2 werden die Absätze 2 und 3.

10. Nach § 12 wird folgender § 13 eingefügt:

„§ 13

Berichtspflicht des Bundesamtes

(1) Das Bundesamt unterrichtet das Bundesministerium des Innern über seine Tätigkeit.

(2) Die Unterrichtung nach Absatz 1 dient auch der Aufklärung der Öffentlichkeit durch das Bundesministerium des Innern über Gefahren für die Sicherheit der Informationstechnik, die mindestens einmal jährlich in einem zusammenfassenden Bericht erfolgt. § 7 Absatz 1 Satz 3 und 4 ist entsprechend anzuwenden.“

Artikel 2

Änderung des Telemediengesetzes

Das Telemediengesetzes vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 31. Mai 2010 (BGBl. I S. 692) geändert worden ist, wird wie folgt geändert:

1. § 13 wird wie folgt geändert:

   a. Nach Absatz 6 wird folgender Absatz 7 eingefügt:

   „(7) Diensteanbieter im Sinne von § 7 Absatz 1 und § 10 Absatz 1 haben, soweit dies technisch möglich und zumutbar ist, für geschäftsmäßig in der Regel gegen Entgelt angebotene Telemedien durch die erforderlichen technischen und organisatorischen Vorkehrungen sicherzustellen, dass ein Zugriff auf die Telekommunikations- und Datenverarbeitungssysteme nur für Berechtigte möglich ist. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen. Bei personalisierten Telemediendiensten ist den Nutzern die Anwendung eines sicheren und dem Schutzbedarf angemessenen Authentifizierungsverfahrens anzubieten."

   b. Der bisherige Absatz 7 wird Absatz 8.

2. Nach § 15 Absatz 8 wird folgender Absatz 9 eingefügt:

   „(9) Soweit erforderlich, darf der Diensteanbieter Nutzungsdaten zum Erkennen, Eingrenzen oder Beseitigen von Störungen seiner für Zwecke seines Telemedienangebotes genutzten technischen Einrichtungen erheben und verwenden. Absatz 8 Satz 2 gilt entsprechend."

Artikel 3
Änderung des Telekommunikationsgesetzes

Das Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 1 des Gesetzes vom 3. Mai 2012 (BGBl. I S. 958) geändert worden ist, wird wie folgt geändert:

1. § 100 Absatz 1 wird wie folgt gefasst:

   „(1) Soweit erforderlich, darf der Diensteanbieter zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen, einschließlich der Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können, die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden.“

2. § 109 Absatz 2 wird wie folgt geändert:

   a. Nach Satz 2 wird folgender Satz 3 eingefügt:

   „Maßnahmen nach Satz 2 müssen den Stand der Technik berücksichtigen.“

   b. Die bisherigen Sätze 3 und 4 werden Sätze 4 und 5.

3. § 109 Absatz 5 wird wie folgt gefasst:

   „Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat Beeinträchtigungen von Telekommunikationsnetzen und -diensten, die zu beträchtlichen Sicherheitsverletzungen einschließlich Störungen der Verfügbarkeit der über diese Netze erbrachten Dienste oder einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können und von denen der Netzbetreiber

oder der Telekommunikationsdiensteanbieter Kenntnis erlangt, der Bundesnetzagentur unverzüglich mitzuteilen. Sofern es bereits zu einer Sicherheitsverletzung im Sinne von Satz 1 gekommen ist, durch die beträchtliche Auswirkungen auf den Betrieb der Telekommunikationsnetze oder das Erbringen von Telekommunikationsdiensten entstehen, kann die Bundesnetzagentur einen detaillierten Bericht über die Sicherheitsverletzung und die ergriffenen Abhilfemaßnahmen verlangen. Soweit es sich um IT-Sicherheitsvorfälle handelt, sind die eingegangenen Meldungen sowie Informationen zu den ergriffenen Abhilfemaßnahmen von der Bundesnetzagentur unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik weiterzuleiten. Erforderlichenfalls unterrichtet die Bundesnetzagentur die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union und die Europäische Agentur für Netz- und Informationssicherheit über die Sicherheitsverletzungen. Die Bundesnetzagentur kann die Öffentlichkeit informieren oder die nach Satz 1 Verpflichteten zu dieser Unterrichtung auffordern, wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung im öffentlichen Interesse liegt. Die Bundesnetzagentur legt der Kommission, der Europäischen Agentur für Netz- und Informationssicherheit und dem Bundesamt für Sicherheit in der Informationstechnik einmal pro Jahr einen zusammenfassenden Bericht über die eingegangenen Mitteilungen und die ergriffenen Abhilfemaßnahmen vor.“

4. § 109 Absatz 6 wird wie folgt geändert:

   Das Wort „Benehmen“ in Satz 1 wird durch „Einvernehmen“ ersetzt. Vor den Worten „dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit“ werden die Worte „im Benehmen mit“ eingefügt.

5. Nach § 109 Absatz 6 wird folgender Absatz 7 eingefügt:

   „Über aufgedeckte Mängel bei der Erfüllung der maßgeblichen IT-Sicherheitsanforderungen sowie die in diesem Zusammenhang von der Bundes-

netzagentur geforderten Abhilfemaßnahmen unterrichtet die Bundesnetzagentur unverzüglich das Bundesamt für Sicherheit in der Informationstechnik."

6. § 109a wird wie folgt geändert:

   a. Die Überschrift wird wie folgt gefasst:

      „§109a
      Daten- und Informationssicherheit".

   b. Nach Absatz 3 wird folgender Absatz 4 eingefügt:
      „(4) Werden Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, sind diese vom Diensteanbieter unverzüglich zu benachrichtigen. Soweit technisch möglich und zumutbar, müssen die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hingewiesen werden, mit deren Hilfe die Nutzer Störungen, die von ihren Datenverarbeitungssystemen ausgehen, erkennen und beseitigen können."

   c. Der bisherige Absatz 4 wird Absatz 5.

7. In § 115 Absatz 3 wird nach Satz 1 folgender Satz 2 eingefügt:

   „Dies gilt auch dann, wenn andere Tatsachen die Annahme rechtfertigen, dass das betroffene Unternehmen nicht die erforderliche Zuverlässigkeit zur Einhaltung der Verpflichtungen des Teils 7 besitzt."

Artikel 4
Änderungen des Außenwirtschaftsgesetzes

In § 5 Absatz 3 wird folgende Nummer 3 angefügt:

„3. mit der Umsetzung technischer oder organisatorischer Maßnahmen nach § 110 des Telekommunikationsgesetzes betraut sind oder die technische Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation herstellen oder vertreiben."

Artikel 5
Änderung des Bundeskriminalamtgesetzes

Das Bundeskriminalamtgesetz vom 7. Juli 1997 (BGBl. I S. 1650), das zuletzt durch Artikel 2 des SIS-II-Gesetzes vom 6. Juni 2009 (BGBl. I S. 1226) geändert worden ist, wird wie folgt geändert:

§ 4 Absatz 1 Satz 1 Nummer 5 wird wie folgt geändert:

a. Die Angabe „§ 303b“ wird durch die Wörter „den §§ 202a, 202b, 202c, 263a, 303a und 303b“ ersetzt,
b. vor dem Wort „sicherheitsempfindliche“ werden die Wörter „Behörden oder Einrichtungen des Bundes oder“ eingefügt.

Artikel 6
Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A: Allgemeiner Teil

I. Zweck und Inhalt des Gesetzes

Mit dem Gesetz soll eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland erreicht werden. Die vorgesehenen Neuregelungen dienen dazu, den Schutz der Verfügbarkeit, Integrität und Authentizität datenverarbeitender Systeme zu verbessern und der gestiegenen Bedrohungslage anzupassen. Ziel des Gesetzes ist eine Verbesserung der IT-Sicherheit bei Unternehmen, ein verstärkter Schutz der Bürgerinnen und Bürger in einem sicheren Netz, der Ausbau der IT-Sicherheit der Bundesverwaltung und in diesem Zusammenhang auch eine Stärkung von Bundesamt für Sicherheit in der Informationstechnik (BSI) und Bundeskriminalamt (BKA). Der Entwurf sieht daher für Betreiber Kritischer Infrastrukturen die Pflicht zur Einhaltung eines Mindestniveaus an IT-Sicherheit und zur Meldung erheblicher IT-Sicherheitsvorfälle vor. Das Außenwirtschaftsrecht wird verschärft und Zuverlässigkeitsanforderungen im Bereich der Telekommunikationsnetzbetreiber eingeführt. Hinzu kommen weitere Pflichten für Telekommunikations- und Telemediendiensteanbieter zum Schutz der Bürgerinnen und Bürger bei ihren Angeboten und der damit einhergehenden Datenverarbeitungsprozesse. Das BSI wird bei der Sicherung der IT des Bundes und in seiner nationalen sowie internationalen Warn-, Beratungs- und Unterstützungsrolle und das BKA in seinen Aufgaben im Bereich der Strafverfolgung weiter gestärkt.

II. Gesetzgebungskompetenz des Bundes

Für die Änderungen des BSI-Gesetzes (Artikel 1), die unmittelbar die Sicherung der Informationstechnik in der Bundesverwaltung betreffen, hat der Bund eine ungeschriebene Gesetzgebungskompetenz kraft Natur der Sache sowie aus Artikel 86 Satz 2 des Grundgesetzes (GG). Für die Regelungen zum Schutz der Informationstechnik Kritischer Infrastrukturen 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] 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 Telemediengesetzes (Artikel 2) ergibt sich die Gesetzgebungskompetenz des Bundes ebenfalls aus 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 der Länder nicht hingenommen werden können. Insbesondere wäre zu befürchten, dass unterschiedliche landesrechtliche Behandlungen gleicher Lebenssachverhalte, z. B. 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 3) können auf die ausschließliche Gesetzgebungskompetenz des Bundes nach Artikel 73 Absatz 1 Nummer 7 GG gestützt werden. Für die Änderung des Außenwirtschaftsgesetzes (Artikel 4) ergibt sich die Gesetzgebungskompetenz des Bundes aus der konkurrierenden Gesetzgebungskompetenz für das Recht der Wirtschaft (Artikel 74 Absatz 1 Nummer 11 GG). Die Änderung des BKA-Gesetzes (Artikel 5) 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

Für die Wirtschaft entsteht bei Betreibern Kritischer Infrastrukturen sowie bestimmten Telekommunikations- und Telemediendiensteanbietern Erfüllungsaufwand für die Ein-

haltung eines Mindestniveaus an IT-Sicherheit und die Einrichtung und Aufrechterhaltung entsprechender Meldewege. Dies wird faktisch aber nur dort zu Mehrkosten führen, wo bislang noch kein hinreichendes Niveau an IT-Sicherheit bzw. keine entsprechenden Meldewege etabliert sind. Für diejenigen betroffenen Wirtschaftsteilnehmer, bei denen dies bereits ganz oder teilweise der Fall ist, entstehen insoweit keine gesonderten Kosten. Zusätzliche Kosten entstehen für die Betreiber Kritischer Infrastrukturen durch die Durchführung der vorgesehenen Sicherheitsaudits.

Die konkrete Berechnung und Darstellung des Erfüllungsaufwands kann erst mit Erlass der Rechtsverordnung nach § 10 BSI-Gesetz auf der Grundlage des im Zweiten Teils der Begründung zu Nummer 9 dargestellten Verfahrens erfolgen, da erst durch die Rechtsverordnung der Adressatenkreis der entsprechenden Verpflichtungen hinreichend konkret eingegrenzt wird.

Für die Wirtschaft fallen außerdem Bürokratiekosten für folgende neue Informationspflichten im Sinne des Gesetzes zur Einsetzung eines Nationalen Normenkontrollrates (NKR-Gesetz) an:

a. Artikel 1, § 8a Absatz 3 Satz 2: Die Betreiber Kritischer Infrastrukturen übermitteln dem BSI regelmäßig eine Aufstellung der zur Überprüfung der organisatorischen und technischen Vorkehrungen und sonstigen Maßnahmen nach § 8a Absatz 3 Satz 1 durchgeführten Sicherheitsaudits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel.

b. Artikel 1, § 8a Absatz 3 Satz 3: Bei Sicherheitsmängeln kann das BSI eine Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse nach § 8a Absatz 3 Satz 1 verlangen.

c. Artikel 1, § 8b Absatz 3 Satz 1: Die Betreiber Kritischer Infrastrukturen haben dem BSI Warn-und Alarmierungskontakte zu benennen, über die sie jederzeit erreichbar sind.

d. Artikel 1, § 8b Absatz 4: Die Betreiber Kritischer Infrastrukturen haben Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die Auswirkungen auf ihre eigene Funktionsfähigkeit haben können, unter Angabe der technischen Rahmenbedingungen unverzüglich an das BSI zu melden, wobei eine Nennung des Betreibers selbst nicht erforderlich ist.

e. Artikel 1, § 8b Absatz 5: Führen Beeinträchtigungen der informationstechnischen Systeme, Komponenten oder Prozesse zu einem Ausfall oder einer Beeinträchtigung der Kritischen Infrastruktur, ist dies dem BSI unverzüglich unter Nennung des Betreibers zu melden.

f. Artikel 3, § 109 Absatz 5 Satz 1: Die Betreiber öffentlicher Telekommunikationsnetze und die Erbringer öffentlich zugänglicher Telekommunikationsdienste haben der Bundesnetzagentur Beeinträchtigungen, die zu einer Störung der Verfügbarkeit oder zu einem unerlaubten Zugriff auf Systeme der Nutzer führen können, unverzüglich mitzuteilen.

g. Artikel 3, § 109a Absatz 4 Satz 2: Die Betreiber öffentlicher Telekommunikationsnetze und die Erbringer öffentlich zugänglicher Telekommunikationsdienste haben ihre Nutzer unverzüglich zu benachrichtigen, wenn Störungen bekannt werden, die von Systemen der Nutzer ausgehen.

Die Verbände der betroffenen Unternehmen werden im Rahmen der Verbändebeteiligung gebeten, zu erwartende jährliche Fallzahlen und zu erwartende Gesamtkosten mitzuteilen.

3. Erfüllungsaufwand der Verwaltung

Die neu geschaffenen Befugnisse und Aufgaben des BSI sind mit einem entsprechenden Vollzugsaufwand verbunden.

Der zusätzliche Personalbedarf des BSI begründet sich neben den erweiterten Verantwortlichkeiten insbesondere darin, dass Informationstechnik in den sieben relevanten KRITIS-Sektoren sehr unterschiedlich eingesetzt ist. Dies betrifft sowohl die genutzten Komponenten, Produkte, Systeme und externen IKT-Dienstleistungen, 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 -Branchen erforderlich. Der geforderte Personalbedarf ermöglicht den Aufbau der notwendigen Fachexpertise und stellt die Basis für Grundlagenberatung und Unterstützung dar, eine systematische, individuelle Einzelberatung aller Kritischen Infrastrukturunternehmen ist hingegen nicht leistbar. Zur Ermittlung des Stands der Technik in einzelnen KRITIS-Branchen als auch für die Anerkennung der von den Branchen erstellten Branchenstandards, ist in hohem Maße Fachkompetenz und Ressourcenaufwand in Bezug auf die jeweiligen KRITIS-Sektoren und -Branchen und den dort genutzten IT-Lösungen erforderlich. Dies gilt ebenfalls für die Identifizierung konkreter Sicherheitsmängel und die Prüfung angeforderter Auditberichte. Auch zum Auswerten von in der Meldestelle eingehender Informationen, dem Fortschreiben des Lagebildes und bei der Vorhersage der potenziellen Auswirkungen einer Meldung bzw. Störung auf die betroffene Kritische Infrastruktur oder ihre Branche, ist spezielles Know-How in Bezug auf die KRITIS-Sektoren und -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.

Für die Erfüllung der im Gesetz vorgesehenen Aufgaben besteht beim BSI damit ein zusätzlicher Aufwand von insgesamt 133 zusätzlichen Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 8.897 T€ sowie Sachkosten in Höhe von jährlich rund 5.000 T€.

Die neuen Mitwirkungsaufgaben für das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) führen dort zu einem zusätzlichen Bedarf von 9 Planstellen/Stellen mit jährlichen Personal- und Sachkosten in Höhe von 681 T€ für die Aufgaben nach § 8a Abs. 2 und 3, § 8b Abs. 2 Ziffer 2 und § 10 BSI-Gesetz.

In den Fachabteilungen des BKA entsteht durch die Erweiterung der originären Ermittlungszuständigkeit ein Ressourcenaufwand von 79 zusätzlichen Planstellen / Stellen mit jährlichen Personalkosten in Höhe von rund 5.385 T€ sowie zusätzlichen Sachmitteln in Höhe von einmalig 630 T€ im ersten Jahr.

In den Fachabteilungen des Bundesamtes für Verfassungsschutz (BfV) entsteht durch die Zuständigkeit gemäß § 8b Abs. 2 Nr. 2 BSI-Gesetz ein zusätzlicher Ressourcenbedarf von 55 Planstellen / Stellen mit Personal und Sachkosten in Höhe von 4.496 T€ für das Jahr 2015 sowie jeweils ein Haushaltsmittelbedarf in Höhe von 4.170 T€ für die Folgejahre.

Für die Länder entsteht kein Erfüllungsaufwand.

IV. Weitere Kosten

Für die Wirtschaft entstehen keine weiteren Kosten.

V. Gleichstellungspolitische Gesetzesfolgenabschätzung

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 soll, 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.

Zweiter Teil: Zu den einzelnen Vorschriften

Zu Artikel 1 (Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik)

Zu Nummer 1 (§ 1 Bundesamt für Sicherheit in der Informationstechnik)

Die neue Fassung des § 1 trägt der geänderten Rolle des BSI Rechnung. Die Aufgaben des BSI neben der Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes haben an Bedeutung gewonnen. Das BSI dient zunehmend Bürgern, Unternehmen, Verwaltungen und der Politik als Ansprechpartner in Fragen der IT-Sicherheit. Auch auf EU-Ebene und 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 des BSI-Gesetzes. Da es bislang noch keine gesetzlich geregelte Allgemeindefinition der Kritischen Infrastrukturen in Deutschland gibt, ist dies notwendig, um die Adressaten der §§ 8a und 8b des BSI-Gesetzes zu bestimmen. Die Auflistung der Sektoren folgt im Grundsatz der innerhalb der Bundesregierung abgestimmten Einteilung Kritischer Infrastrukturen. Zu den vom Regelungsbereich des Gesetzes erfassten Sektoren gehören die Bereiche Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie das Finanz- und Versicherungswesen. Die Kommunikationstechnik von Regierung, Parlament und öffentlicher Bundesverwaltung ist nach Satz 2 von den Kritischen Infrastrukturen im Sinne des BSI-Gesetzes ausgenommen. Als Spezialregelung gelten hier die §§ 4, 5 und 8 des BSI-Gesetzes. Die Verwaltungen der Länder und Kommunen sowie der Sektor Kultur und Medien sind ebenfalls ausgenommen, da der Bund für sie keine Gesetzgebungskompetenz besitzt.

Zur Umsetzung der in den §§ 8a und 8b des BSI-Gesetzes getroffenen Vorgaben sind innerhalb der genannten Sektoren diejenigen Einrichtungen, Anlagen oder Teile davon zu identifizieren, die für das Funktionieren des Gemeinwesens und die Sicherung der Grundbedürfnisse der Bevölkerung von hoher Bedeutung, insoweit besonders schutzwürdig und deswegen als Kritische Infrastrukturen im Sinne des BSI-Gesetzes einzustufen sind. Diese 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 Unternehmen 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 bedingen werden. Die Festlegung der Kritischen Infrastrukturen ist daher im Rahmen der Vorgaben aus § 2 Absatz 10 der auf der Grundlage von § 10 zu erlassenden Rechtsverordnung vorbehalten. Methodisch ist hierbei vorgesehen, die Einteilung der Kritischen Infrastrukturen nach den Kriterien Qualität und Quantität vorzunehmen. Zu Einzelheiten siehe die Ausführungen zu Nummer 9.

Die Regelungen des BSI-Gesetzes finden unter dem Gesichtspunkt der Verhältnismäßigkeit gemäß § 2 Absatz 11 keine Anwendung auf solche Unternehmen, die als sog. 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 Mio. Euro nicht überschreiten. Die entsprechenden Voraussetzungen müssen bei dem Betreiber der betreffenden Kritischen Infrastruktur selbst vorliegen und sind dem BSI auf dessen Verlangen hin auf geeignete Weise zu belegen. 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 solches und die damit einhergehenden Verpflichtungen unberührt.

Zu Nummer 3 (§ 3 Aufgaben des Bundesamtes)

Zu Buchstabe a (Zurverfügungstellung gewonnener Erkenntnisse an Dritte)

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 Betroffenen („Dritten“) zur Verfügung gestellt werden können. Hierdurch soll auch noch einmal der Mehrwert betont werden, den eine verbreitete Erkenntnisbasis und ein verbessertes Lagebild des BSI für Wirtschaft und Gesellschaft haben kann. Dies gilt gerade für die Betreiber Kritischer Infrastrukturen im Sinne des BSI-Gesetzes. Adressat dieser Erkenntnisse sollen aber auch sonstige Unternehmen oder z.B. Betreiber aus dem Sektor Kultur und Medien sein, die zwar mangels Bundeskompetenz nicht von der Definition nach § 2 Absatz 10 erfasst werden können, aber anerkannter Maßen zum Bereich der Kritischen Infrastrukturen gehören.

Zu Buchstabe b

Buchstabe b enthält redaktionelle Anpassungen.

Zu Buchstabe c (Bundesamt als zentrale Stelle im internationalen Bereich)

Die ausdrückliche Festschreibung der Aufgabe als zentrale Stelle im internationalen Bereich der Sicherheit in der Informationstechnik durch Aufnahme der neuen Nummer 16 in Absatz 1 Satz 2 trägt der gewachsenen Rolle des BSI als nationalem und internationalem Ansprechpartner in Fragen der IT- und Cybersicherheit in Deutschland Rechnung.

Zu Buchstabe d (Aufgabe des Bundesamtes im Bereich Sicherheit der Informationstechnik Kritischer Infrastrukturen):

Bei Absatz 3 Satz 1 handelt es sich um eine notwendige Ergänzung der Aufgaben des BSI um die neuen Aufgaben nach §§ 8a, 8b. Absatz 3 Satz 2 ermöglicht es dem BSI hierbei, Betreiber Kritischer Infrastrukturen auf Ersuchen bei der Sicherung ihrer Informationstechnik insbesondere im Hinblick auf die Erfüllung der Anforderungen nach den §§ 8a und 8b zu beraten und zu unterstützen. Das BSI hat nach pflichtgemäßem Ermessen zu entscheiden, ob es einem entsprechenden Ersuchen nachkommt.

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.

Zu Nummer 5 (§ 7 Warnungen)

Zu Buchstabe a (Unberechtigter Abfluss von Daten)

Die Aufnahme der Fallgruppe des unberechtigten Abflusses von Daten in Absatz 1 Satz 1 stellt klar, dass das BSI nach § 7 auch in Fällen tätig werden kann, in denen nicht primär die Warnung vor einem Schadprogramm oder einer Sicherheitslücke sondern vielmehr die Bewältigung eines bereits erfolgten unberechtigten Abflusses von Daten im Vordergrund steht.

Zu Buchstabe b (Einschaltung Dritter)

Der neue Absatz 1 Satz 2 ermöglicht es dem BSI unter Datenschutzgesichtspunkten, sich bei der Warnung der (freiwilligen) Mitwirkung Dritter zu bedienen. Oftmals wird das BSI abhandengekommene Daten nicht direkt einem Betroffenen zuordnen oder diesen nicht ohne weiteres informieren können. Im Interesse einer effizienten Warnung der Betroffenen soll sich das BSI daher an Informationsintermediäre wenden können, die an der Identifizierung und Information der Betroffenen auf Grund ihrer Stellung mitwirken können (insbesondere von den Kunden genutzte Provider, Diensteanbieter etc.).

Zu Buchstabe c

Der Änderungsbefehl enthält redaktionelle Anpassungen.

Zu Nummer 6 (§ 7a Untersuchung der IT-Sicherheit)

Absatz 1 des neuen § 7a dient dazu, Rechtssicherheit für Untersuchungen von IT Produkten durch das BSI herzustellen. Die gesetzliche Befugnis geht als Spezialgesetz insbesondere den Verboten des Urhebergesetzes (UrhG) vor und führt dazu, dass die Daten- und Informationsbeschaffung von vornherein nicht mehr als unbefugt im Sinne von § 202a des Strafgesetzbuches (StGB) sowie § 17 des Gesetzes gegen den Unlauteren Wettbewerb (UWG) anzusehen ist.

Absatz 2 soll dem BSI ermöglichen, der zunehmenden Erwartungshaltung der Öffentlichkeit Rechnung zu tragen, dass das BSI als unabhängige Instanz auch die Anwender außerhalb der Bundesverwaltung mit Informationen über die Sicherheit von informationstechnischen Produkten, Systemen oder Diensten versorgt. Durch die Einschränkung der Veröffentlichung auf die Bewertung und den Verweis auf § 7 Absatz 1 Satz 2 und 3 wird den berechtigten Schutzinteressen der Hersteller und Rechteinhaber Rechnung getragen. Da die Hersteller von Schadsoftware kein berechtigtes Schutzinteresse haben, soll die Bewertung im Fall der Schadsoftware auch die übrigen Erkenntnisse umfassen können.

Zu Nummer 7 (§ 8 Vorgaben des Bundesamtes)

Mit der vorgesehenen Änderung soll die Beachtung und Befolgung der Vorgaben des BSI innerhalb der Bundesverwaltung weiter gestärkt werden. Dazu bedürfen Verwaltungsvorschriften des Bundesministeriums des Innern, mit denen die vom BSI festzulegenden Mindeststandards für die Bundesverwaltung verbindlich gemacht werden, nicht mehr der Zustimmung des Rats der IT-Beauftragten. Künftig ist vor Erlass der Verwaltungsvorschriften lediglich das Benehmen mit diesem Gremium herzustellen.

Bei der Festlegung der Mindeststandards sind die betroffenen Sicherheitsbelange und die mit der Umsetzung verbundenen Aufwände sorgfältig gegeneinander abzuwägen. Gegebenenfalls sind entsprechend angemessene Umsetzungsfristen zu gewähren. Im

Interesse der Umsetzbarkeit der Vorgaben berät das BSI die Bundesbehörden auf Ersuchen bei deren Umsetzung und Einhaltung.

Zu Nummer 8 (§ 8a Sicherheit der Informationstechnik Kritischer Infrastrukturen, § 8b Zentrale Meldestelle für die Sicherheit in der Informationstechnik der Betreiber Kritischer Infrastrukturen und § 8c Auskunftsverlangen Dritter)

Zu § 8a (Sicherheit 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 als kritisch eingestuften, Dienstleistungen. Zum Schutz vor IT-Ausfällen und um eine Grundlage für die Aufrechterhaltung der Versorgungssicherheit und der öffentlichen Sicherheit bei IT-Ausfällen zu schaffen, sollen branchenspezifische Mindestanforderungen zum Schutz der kritischen Systeme, Komponenten und Prozesse der Kritischen Infrastrukturen erfüllt werden, auf die die Gesellschaft existentiell angewiesen ist. Hierfür sind organisatorische und technische Vorkehrungen und sonstige Maßnahmen erforderlich. Es handelt sich um eine grundlegende Verpflichtung, die jeder zu beachten hat, der ganz oder teilweise geschäftsmäßig Kritische Infrastrukturen im Sinne des BSI-Gesetzes betreibt oder daran mitwirkt. Besonders kritische Prozesse bedürfen im Einzelfall besonderer Sicherheitsmaßnahmen durch Abschottung. Mit Blick auf die Erwägungen zu der Erforderlichkeit eines nationalen Routings besonders sensibler IT-Bereiche sollten diese Prozesse weder mit dem Internet oder öffentlichen Netzen verbunden, noch von über das Internet angebotenen Diensten abhängig sein.

Die Notwendigkeit, angemessene organisatorische und technische Vorkehrungen und sonstige Maßnahmen zu treffen, besteht auch dann, wenn Unternehmen ihre IT durch Dienstleister betreiben lassen. Auf Grund der weitreichenden gesellschaftlichen Auswirkungen ist dabei der Stand der Technik zu berücksichtigen. Stand der Technik im Sinne von Absatz 1 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 und Vertraulichkeit gesichert erscheinen lässt. Bei der Bestimmung des Standes der Technik sind insbesondere einschlägige internationale, europäische und nationale Normen heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden.

Bei der Frage der Angemessenheit sind bei dem für den Betreiber erforderlichen Aufwand insbesondere die erforderlichen Kosten zu berücksichtigen. Die Mindestanforderungen müssen von den Betreibern in Sicherheits- und Notfallkonzepte gegossen werden, um deren Umsetzung zu dokumentieren. Die Vorgaben orientieren sich an bewährten Maßstäben und sind an die Vorgaben für Diensteanbieter nach dem Telekommunikationsgesetz sowie an die Vorgaben für Betreiber von Energieversorgungsnetzen nach dem Energiewirtschaftsgesetz angelehnt.

Absatz 2 ermöglicht in Branchen, wo dies 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 Unternehmen und Verbände branchenintern zusammenfinden und für die jeweilige Branche einheitliche Sicherheitsstandards erarbeiten. Der UP KRITIS stellt als etablierte Kooperationsplattform zwischen Betreibern und Staat bereits entsprechende Strukturen zur Verfügung. Dabei ist darauf zu achten, dass eine Kompatibilität zu Selbstregulierungen im Bereich des Datenschutzes besteht. 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 den zuständigen Bundes- und Aufsichtsbehörden erfolgen, um die Vereinbarkeit und Koordinierung mit anderen Belangen der Sicherheitsvorsorge zu gewährleisten.

Die vom BSI im Benehmen mit der jeweils zuständigen Aufsichtsbehörde und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) anerkannten branchenin-

ternen Standards konkretisieren die Verpflichtungen nach Absatz 1 für die Branche und können vor diesem Hintergrund nur dann anerkannt werden, wenn sie geeignet sind, die Mindestanforderungen nach Absatz 1 zu gewährleisten und insbesondere dem Stand der Technik entsprechen. Soweit keine branchenspezifischen Standards erarbeitet wurden, gilt die allgemeine Regelung aus Absatz 1. Auch dann, wenn branchenspezifische Sicherheitsstandards erarbeitet wurden, steht es dem einzelnen Betreiber frei, eigene dem Stand der Technik entsprechende Maßnahmen umzusetzen.

Der Nachweis der Sicherheitsaudits, -prüfungen oder -zertifizierungen nach Absatz 3 dient der Kontrolle und Überprüfung der erforderlichen Maßnahmen nach Absatz 1. Nur so kann sichergestellt werden, dass durch die getroffenen Maßnahmen robuste Grundlagen geschaffen wurden und ein angemessenes Sicherheitsniveau zum Schutz der für das Gemeinwesen kritischen Prozesse eingehalten wird. Die Ausgestaltung der Sicherheitsaudits, -prüfungen und Zertifizierungen soll nicht im Detail gesetzlich vorgegeben werden, da diese von den jeweils erarbeiteten branchenspezifischen Mindeststandards, den in den Branchen vorhandenen technischen Gegebenheiten und gegebenenfalls 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, ein Information Security Management (Sicherheitsorganisation, IT-Risikomanagement, etc.) betreibt, kritische Cyber-Assets identifiziert hat und managt, Maßnahmen zur Angriffsprävention und –erkennung betreibt und ein Business Continuity Management (BCM) implementiert hat und darüber hinaus die branchenspezifischen Besonderheiten (z.B. verankert durch den jeweiligen branchenspezifischen Sicherheitsstandard, sofern ein solcher erstellt und anerkannt wurde) umsetzt.

Die Sicherheitsaudits, -prüfungen oder Zertifizierungen sollten 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 anerkannt im Sinne des Gesetzes, wenn er seine Qualifikation zur Überprüfung der Einhaltung der Mindest-

standards gegenüber dem BSI formal glaubhaft machen kann. Denkbar ist z.B. die Anknüpfung an Zertifizierungen, die für die fachlich-technische Prüfung im jeweiligen Sektor angeboten werden (z.B. zertifizierte Prüfer für bestimmte ISO-Normen, o.ä.).

Der Nachweis nach Absatz 3 soll - nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 - nach wesentlichen Änderungen im Unternehmen, spätestens jedoch im Abstand von zwei Jahren erbracht werden. Eine Kontrolle der Einhaltung der Erfordernisse nach Absatz 1 kann zudem über etablierte Prüfmechanismen erfolgen. So prüfen Wirtschaftsprüfer bereits jetzt die im Rahmen der Jahresabschlussprüfung rechnungsrelevanten IT-Systeme.

Absatz 4 Sätze 1 und 2 stellen sicher, dass Unternehmen, die bereits der Regulierung durch die Bundesnetzagentur nach dem Telekommunikationsgesetz unterfallen, keinen zusätzlichen Verpflichtungen aus den Absätzen 1 bis 3 unterliegen. Satz 3 macht deutlich, dass auch sonst vergleichbare oder weitergehende Vorgaben in Spezialgesetzen möglich sind und bestehende Rechtsvorschriften mit vergleichbaren oder weitergehenden Anforderungen nicht berührt werden. Rechtsvorschriften sind vergleichbar, wenn sie mindestens das Sicherheitsniveau nach den Absätzen 1 bis 3 gewährleisten. Weitergehend sind insbesondere solche Anforderungen, die einen strengeren materiellen Standard als den Stand der Technik vorsehen. Durch die Regelung wird die Gefahr einer Doppelregulierung für die betreffenden Unternehmen ausgeschlossen.

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

§ 8b regelt die Funktion des BSI als zentrale Meldestelle für die Sicherheit in der Informationstechnik für Betreiber Kritischer Infrastrukturen und dient der umfassenden Information aller Akteure über die aktuelle Cybergefährdungslage. Diese ist Voraussetzung für die nationale Handlungsfähigkeit und Grundlage für eine bundesweit abgestimmte Reaktion. Die im Rahmen von § 8b übermittelten Informationen sind üblicherweise rein technischer Natur und haben keinen Personenbezug. Sollte im Einzelfall ein Personen-

bezug gegeben sein, richtet sich die Übermittlungsbefugnis nach den allgemeinen datenschutzrechtlichen Regelungen oder gegebenenfalls spezialgesetzlichen Regelungen. Für die nach § 8b erhaltenen Informationen gilt dementsprechend auch der allgemeine Grundsatz der Datensparsamkeit.

Im Einzelnen:

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

Absatz 2 regelt die Aufgaben des BSI zu diesem Zweck. Als zentrale Meldestelle sammelt das BSI alle bei ihm eingehenden Meldungen, erstellt und aktualisiert unter Einbeziehung seiner sonstigen Erkenntnisse ein Lagebild und stellt seine Informationen, soweit Quellen- und Geheimschutz dies zulassen, in angemessener Form, zum Beispiel konsolidiert, sanitarisiert oder als Rohdatenmaterial Dritten zur Verfügung. Die Öffentlichkeit wird nur dann benachrichtigt, wenn das öffentliche Interesse dies erfordert.

Absatz 3 stellt durch eine Anbindung der Betreiber Kritischer Infrastrukturen an die Warn- und Alarmierungsmechanismen nach § 3 Absatz 1 Nummer 15 sicher, dass ein schneller Informationsfluss gewährleistet ist und bei schwerwiegenden Beeinträchtigungen andere betroffene Kritische Infrastrukturen sowie das Lagezentrum des BSI unverzüglich informiert werden.

Absatz 4 regelt die Verpflichtung von Betreibern Kritischer Infrastrukturen, dem BSI unverzüglich Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu melden. Dazu zählen insbesondere Sicherheitslücken, Schadprogramme und erfolgte, versuchte oder erfolgreich abgewehrte Angriffe auf die Sicherheit in der Informationstechnik sowie außergewöhnliche und unerwartete technische Defekte mit IT-Bezug (z.B. nach Softwareupdates oder Ausfall der Serverkühlung). Beeinträchtigungen sind dann meldepflichtig, wenn sie die Funktionsfähigkeit des Unternehmens bzw. der von diesem betriebenen Kritischen Infrastrukturen bedrohen können. Die Mel-

dungen sind notwendig, um eine möglichst umfassende und frühzeitige Warnung möglicherweise ebenfalls betroffener weiterer Unternehmen zu gewährleisten und darüber hinaus fundierte Aussagen zur IT-Sicherheitslage in Deutschland treffen zu können. Die Nennung des Betreibers ist für solche Meldefälle nicht erforderlich, sondern kann auch pseudonymisiert erfolgen. Hierdurch wird der besonderen Sensibilität entsprechender Meldungen im Hinblick auf die wirtschaftlichen Auswirkungen eines möglichen Bekanntwerdens solcher Vorfälle Rechnung getragen. Auf die Nennung des Betreibers wird daher dort verzichtet, wo die Meldung primär der Beratung und Warnung möglicher ebenfalls betroffener Kreise und der Erfassung der Cyberbedrohungslage dient. Gleichzeitig sollte auf Grund der nur pseudonymisierten Meldepflicht bei der Frage, ob ein Meldefall vorliegt oder nicht, von den meldepflichtigen Unternehmen ein möglichst niedrige Schwelle angelegt werden („im Zweifel Meldung“). Dadurch reduziert sich für die Unternehmen der entsprechende Ermittlungsaufwand.

Absatz 5 regelt die Meldepflicht für Beeinträchtigungen der informationstechnischen Systeme, Komponenten oder Prozesse, die konkret zu einem Ausfall oder zu einer Beeinträchtigung der Kritischen Infrastruktur führen. Diese sind - anders als die Fälle nach Absatz 4 unter Nennung des Betreibers an das BSI zu melden, da im konkreten Schadensfall eine schnelle Krisenreaktion erfolgen muss - insbesondere um ähnliche Vorfälle bei anderen Betreibern noch abwenden zu können. Hierzu muss das BSI sofort auf den Meldenden zugehen können, um die dafür benötigten Informationen zu erhalten. Aufgrund der Zeitkritikalität und der unmittelbaren Gefährdung der Versorgungssicherheit kann das Interesse der Meldenden, anonym zu bleiben, nicht in gleicher Weise berücksichtigt werden, wie bei den schadensferneren Vorfällen nach Absatz 4

Das BSI erstellt unter Einbeziehung der Betreiber Kritischer Infrastrukturen und der Aufsichtsbehörden einen Kriterienkatalog für meldungsrelevante Sicherheitsvorfälle nach den Absätzen 4 und 5.

Absatz 6 eröffnet klarstellend die Möglichkeit für alle oder einen Teil der Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, zu den Warn- und Alarmie-

rungskontakten nach Absatz 3 einen gemeinsamen einheitlichen Ansprechpartner zu benennen, über den der Informationsaustausch zwischen den Warn- und Alarmierungskontakten und dem BSI nach Absatz 2 Nummer 4 und nach Absatz 4 erfolgen soll. Hierfür können bestehende Strukturen, beispielsweise über die Aufsichtsbehörden oder die eingerichteten Single Points of Contact (SPOCs) des UP KRITIS, genutzt und erweitert werden. Um die Sicherheit sensibler Daten zu gewährleisten, kann das BSI im Hinblick auf § 3 Absatz 1 Nummer 15 vorgeben, über welche Wege und Verfahren die Meldungen erfolgen sollen. Aus der Wirtschaft wurde bereits vorgetragen, dass ein solches Meldeverfahren wie folgt ausgestaltet werden könnte: Es beginnt mit der verschlüsselten Versendung der Meldung des betroffenen Unternehmens an den gemeinsamen einheitlichen Ansprechpartner. Diesem ist die Identität des Meldenden bekannt, aber durch die Verschlüsselung kann er den Inhalt der Meldung von Dritten nicht einsehen. In einem nächsten Schritt entfernt der gemeinsame einheitliche Ansprechpartner die Unternehmensidentität und fügt eine Pseudoidentität etwa im Sinne eines Kennzeichens ein. Danach erfolgt der Versand der weiterhin verschlüsselten Meldung an das BSI, das mithilfe eines entsprechenden Schlüssels Zugriff auf den Meldeinhalt erlangt. Eine potentiell notwendige Kommunikation zwischen den Teilnehmern erfolgt auf dem umgekehrten Wege und damit ebenfalls über den gemeinsamen einheitlichen Ansprechpartner. Der ganze Übermittlungsprozess muss vom Ablauf nachvollziehbar und auch auditierbar sein.

Im konkreten Schadensfall nach Absatz 5 erfolgen die Meldungen hingegen auf Grund der besonderen Dringlichkeit der Informationen direkt über die Warn- und Alarmierungskontakte nach Absatz 3 an das BSI.

Absatz 7 Sätze 1 und 2 stellen sicher, dass Unternehmen, die bereits spezifischen Meldepflichten nach § 109 des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 1 des Gesetzes vom 3. Mai 2012 (BGBl. I S. 958), unterfallen, keinen zusätzlichen Verpflichtungen aus den Absätzen 3 bis 6 unterliegen. Satz 3 macht deutlich, dass auch sonst vergleichbare oder weitergehende Vorgaben in Spezialgesetzen möglich sind und bestehende Rechtsvorschriften mit vergleichbaren

oder weitergehenden Meldepflichten nicht berührt werden. Damit wird die Gefahr einer Doppelregulierung und paralleler Meldewege für die betreffenden Unternehmen ausgeschlossen. Jedenfalls müssen solche Vorschriften aber vorsehen, dass entsprechende Meldungen an eine andere Meldestelle oder die zuständige Aufsichtsbehörde durch diese unverzüglich an das BSI weitergeleitet werden. Dadurch wird insbesondere sichergestellt, dass das BSI seine Aufgaben nach Absatz 2 wahrnehmen kann.

Zu § 8c (Auskunftsverlangen Dritter)

§ 8c regelt abschließend die Auskunft zu Informationen, die im Rahmen von § 8a Absatz 4 an das BSI übersandt wurden, sowie zu den Meldefällen nach § 8b Absätze 4 und 5 unter Berücksichtigung des besonderen wirtschaftlichen Interesses der meldepflichtigen Betreiber Kritischer Infrastrukturen an einer vertraulichen Behandlung der von ihnen gemeldeten Informationen. Dies gilt insbesondere in den Fällen der §§ 8a Absatz 4, 8b Absatz 5. Aber auch in den Fällen des § 8a Absatz 4 sind Konstellationen denkbar, bei denen die Auskunft an einen Dritten die 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. Die Regelung dient insoweit auch der Sicherung der Meldeverfahren an das BSI, was ebenfalls in die Abwägung bei der Bearbeitung eines Auskunftsbegehrens miteinzubeziehen ist.

Ein Zugang zu den Akten des BSI, die dessen Aufgabe als zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der informationstechnischen Systeme betreffen, wird nicht gewährt. Bei den Informationen, die das BSI im Rahmen dieser Aufgabe sammelt, analysiert und erstellt (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.

Zu Nummer 9 (§ 10 Ermächtigung zum Erlass von Rechtsverordnungen)

§ 10 Absatz 1 ermächtigt das Bundesministerium des Innern, in Konkretisierung der systemischen Definition Kritischer Infrastrukturen nach § 2 Absatz 10 - im Einvernehmen mit den genannten Bundesministerien - die Kriterien zur Bestimmung derjenigen Einrichtungen, Anlagen oder Teile von solchen festzulegen, die als Kritische Infrastruktur im Sinne des BSI-Gesetzes einzuordnen sind. Diese Konkretisierung im Detail bedarf der sektor- und branchenspezifischen Einbeziehung aller betroffenen Kreise (Verwaltung, Wirtschaft und Wissenschaft). Aus diesem Grund ist die genaue Festlegung von Kategorien betroffener Einrichtungen, Anlagen oder Teile von solchen einer Rechtsverordnung vorbehalten.

In die Rechtsverordnung bzw. Anhängen zu der Rechtsverordnung sollen in abstrakter Form die als Kritische Infrastrukturen einzuordnenden Einrichtungen, Anlagen oder Teile davon aufgenommen werden. Methodisch ist dabei 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 dass durch ihren Ausfall oder ihre Beeinträchtigung nachhaltig wirkende Versorgungsengpässe oder erhebliche Störungen der öffentlichen 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 können jedenfalls sein:

1. SEKTOR ENERGIE
    - Stromversorgung (Branche: Elektrizität)
    - Versorgung mit Erdgas (Branche: Gas)
    - Versorgung mit Kraftstoff (Branche: Mineralöl)
    - Versorgung mit Heizöl (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 und Kartenzahlung (Branchen: Banken, Finanzdienstleister)
- Bargeldversorgung (Branche: Banken)
- Kreditvergabe (Branche: Banken, Finanzdienstleister)
- Geld- und Devisenhandel (Branche: Börsen)
- Wertpapier- und Derivatshandel (Branche: Börsen)
- Versicherungsleistungen (Branche: Versicherungen)

Ausgehend von einer solchen - in der Rechtsverordnung vorzunehmenden - Einteilung soll die Kategorie Quantität den Versorgungsgrad der jeweiligen Einrichtungen, Anlagen oder Teile 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 einer solchen eine kritische

Dienstleistung mit einem Versorgungsgrad über dem entsprechenden Schwellenwert erbringen und sie damit die Verpflichtung nach den §§ 8a, 8b trifft.

Ein Zugang zu Akten, die diese Verordnung betreffen, insbesondere im Zusammenhang mit der Entstehung der Verordnung, wird gemäß Absatz 1 Satz 2 nicht gewährt. Bei den Informationen, die hierbei gesammelt und analysiert werden, handelt es sich um hochsensible sicherheitskritische Informationen, die einem besonders hohen Schutzbedürfnis unterliegen. Die hohe Sicherheitsempfindlichkeit dieser Informationen und deren Risikopotential schließen eine Zugänglichkeit von vornherein aus.

Zu Nummer 10 (§ 13 Berichtspflicht des Bundesamtes)

Die gesetzliche Etablierung einer Berichtspflicht und die vorgesehene Veröffentlichung eines Jahresberichts dienen der Sensibilisierung der Öffentlichkeit für das Thema IT-Sicherheit. Da eine Vielzahl von erfolgreichen Cyberangriffen durch Basismaßnahmen zu verhindern wäre, spielt die Aufklärung und Sensibilisierung der Öffentlichkeit eine zentrale Rolle für die Erhöhung der IT-Sicherheit in Deutschland.

Zu Artikel 2 (Änderung des Telemediengesetzes)

Zu Nummer 1 (§ 13 Pflichten des Diensteanbieters)

Zu Buchstabe a. und b.:

Zu Satz 1 und 2:

Wegen der zunehmenden Verbreitung von Schadsoftware über Telemediendienste werden die bestehenden Anbieterpflichten für Telemediendiensteanbieter nach § 7 Absatz 1 und § 10 Absatz des Telemediengesetzes um technische Schutzmaßnahmen zur Gewährleistung von IT-Sicherheit der für Dritte angebotenen Inhalte ergänzt. Adressiert werden damit die sogenannten Contentprovider, die eigene Inhalte publizieren, sowie die sog. Hostprovider, die fremde Informationen für Nutzer speichern.

Ein Zugriff von anderen als den hierzu Berechtigten (Telemediendiensteanbieter und Nutzer) ist zu verhindern, um Angreifern eine Kompromittierung des Systems unmöglich zu machen. Hiermit soll insbesondere einer der Hauptverbreitungswege von Schadsoftware, das unbemerkte Herunterladen allein durch das Aufrufen bzw. Nutzen einer dafür von Angreifern präparierten Webseite (sog. Drive-by-downloads) eingedämmt werden. Bereits durch eine regelmäßige Aktualisierung der für das Telemedienangebot verwendeten Software (Einspielen von Sicherheitspatches) seitens der Webseitenbetreiber könnten zahlreiche dieser Angriffe vermieden werden. Kompromittierungen können zudem auch durch Inhalte erfolgen, auf die der Diensteanbieter keinen unmittelbaren technischen Einfluss hat (z.B. über kompromittierte Werbebanner, die auf der Webseite eingebunden sind). Dagegen sind organisatorische Vorkehrungen zu treffen - zum Beispiel die vertragliche Verpflichtung der Werbedienstleister, denen Werbefläche eingeräumt wird, zu notwendigen Schutzmaßnahmen. Damit wird ein Beitrag zur Verbesserung der IT-Sicherheit insgesamt geleistet.

Die Bandbreite der erfassten Diensteanbieter vom Kleingewerbetreibenden bis zum Informationsintermediär ist groß. Das nicht-kommerzielle Angebot von Telemedien durch Private und Idealvereine wird nicht erfasst. Erforderlich sind Maßnahmen, wenn ihr Auf-

wand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Geeignete Maßnahmen in diesem Sinne sind u.a. die regelmäßige Aktualisierung der für das Telemedienangebot verwendeten Software sowie das Einspielen von Sicherheitspatches. Der Verweis auf die Erforderlichkeit ermöglicht eine flexible Anpassung der jeweiligen Anforderungen im Einzelfall.

Zu Satz 3

Bürgerinnen und Bürger sind zunehmend im Netz aktiv. Gleichzeitig entstehen in sprunghaft wachsender Anzahl attraktive Geschäftsangebote im Internet. Auch die Erledigung von Geschäften, die die Grundbedürfnisse der Menschen betreffen, wird zunehmend ins Netz verlagert. Da es hierbei häufig (zumeist unter Zugriffsschutz) zur Verarbeitung teils auch sensibler personenbezogener Daten (oftmals auch in Verbindung mit Geschäften, die den privaten Lebensbereich betreffen) und zu finanziellen Transaktionen kommt, gewinnen sichere Authentifizierungsverfahren zunehmend an Bedeutung. Das Schutzniveau dieser Verfahren ist aber uneinheitlich und orientiert sich oftmals nicht an der Sensibilität der zu behandelten Daten. Anbieter von geschäftsmäßig in der Regel gegen Entgelt angebotenen Telemedien werden daher verpflichtet, hinreichend sichere Authentifizierungsverfahren anzubieten. Authentifizierungsverfahren nach den entsprechenden aktuellen und veröffentlichten Technischen Richtlinien des BSI sind dabei jedenfalls als dem Stand der Technik gemäß hinreichend sicher anzusehen.

Das Merkmal „dem Schutzbedarf angemessen“ gibt dem Telemediendiensteanbieter die Möglichkeit, bei dem sicheren Authentifizierungsverfahren je nach Sensibilität und Umfang der verarbeiteten Daten ein unterschiedlich angepasstes Schutzniveau anzulegen. Es ist darauf zu achten, dass die Verfahren für die Kunden nachvollziehbar und handhabbar gestaltet werden. Durch die Mindestvorgabe, sichere Authentifizierungsvorhaben zumindest als eine von mehreren Alternativen anzubieten, kann den Bürgerinnen und Bürger an diesem gut wahrnehmbaren Punkt der Nutzung des Telemediendienstes zudem selbst die Entscheidung überlassen werden, welches Schutzniveau sie für ihre Daten anstreben.

Zu Nummer 2 (§ 15 Nutzungsdaten)

Die Regelung ermächtigt die Diensteanbieter, Nutzungsdaten zum Erkennen, Eingrenzen oder Beseitigen von Störungen seiner für Zwecke seines Dienstes genutzten technischen Einrichtungen zu erheben und zu verwenden. Diensteanbieter müssen die Möglichkeit haben, eine Infektion der von ihnen angebotenen Telemedien mit Schadprogrammen zu erkennen, um entsprechende Schutzmaßnahmen ergreifen zu können. Hier bestand bislang eine Lücke im Bereich der Erlaubnistatbestände des Telemediengesetzes, denn auch die Telemedienanbieter brauchen eine entsprechende Ermächtigung, beispielsweise um Angriffe (Denial of Service, Schadprogramme, Veränderung ihrer Werbeangebote von außerhalb) abwehren zu können. Zur Erkennung und Abwehr bestimmter Angriffe gegen Webseiten und andere Telemedien ist die Erhebung und kurzfristige Speicherung und Auswertung der Nutzungsdaten erforderlich. Diese soll durch den neuen § 15 Absatz 9 TMG, der sich an § 100 Absatz 1 TKG anlehnt, geschaffen werden. Dabei ist auch eine Weiterentwicklung der Angriffsmethoden zu berücksichtigen.

Zur Durchführung von Angriffen werden neuerdings verstärkt auch manipulierte Webseiten genutzt. Für die Anbieter von (Telemedien-) Diensten im Internet bedeutet dies, dass sich die zu verfolgenden IT-Sicherheitsziele im Internet verändert haben. Sie müssen ihre Systeme nicht nur zum Selbstschutz gegen Manipulationen, Hacking oder Verfügbarkeitsangriffen schützen, sondern sie müssen heute ihre Systeme auch gegen Angriffe härten, die diese Systeme nur als Zwischenstation für Angriffe auf die Nutzer der Dienste oder Dritte missbrauchen. Technische Einrichtungen im Sinne dieser Vorschrift sind alle Einrichtungen des Diensteanbieters, die dieser benötigt, um sein Telemedienangebot zur Verfügung zu stellen. Insbesondere ist das der Datenspeicher (Server), auf dem das Telemedienangebot zum Abruf bereitgehalten wird. Der Begriff der Störung ist umfassend zu verstehen als jede vom Diensteanbieter nicht gewollte Veränderung der von ihm für sein Telemedienangebot genutzten technischen Einrichtungen, also beispielsweise auch eine Veränderung, welche die technischen Einrichtung selbst nur als Zwischenstation nutzt, um die Nutzer des Telemedienangebots anzugreifen.

Zu Artikel 3 (Änderung des Telekommunikationsgesetzes)

Zu Nummer 1 (§ 100 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten)

Die Änderung dient der Klarstellung, dass Diensteanbieter Bestands- und Verkehrsdaten auch zum Erkennen und Beseitigen von Schadprogrammen und entsprechender Infrastruktur, insbesondere Botnetze, zum Beispiel durch Prüfungen des Netzwerkverkehrs, der Verwendung von sogenannten Honeypots (Fallen für Schadprogramme im Netz) oder Spamtraps (Blockieren der Versendung von Schadprogrammen) verwenden dürfen.

Zu Nummer 2 (§ 109 Absatz 2 Technische Schutzmaßnahmen)

Die gesetzlichen Vorgaben zu technischen Schutzmaßnahmen enthalten nach derzeitiger Rechtslage erhöhte Anforderungen nur für Maßnahmen zum Vertraulichkeitsschutz (Fernmeldegeheimnis) und den Schutz personenbezogener Daten, welche den „Stand der Technik“ berücksichtigen müssen. Zur Gewährleistung der IT-Sicherheit werden im Übrigen auch weiterhin nur „angemessene technische Vorkehrungen und Maßnahmen“ verlangt, wobei die Angemessenheit einzelner Maßnahmen nur unbestimmt definiert ist und insbesondere auch von allgemeinen Wirtschaftlichkeitserwägungen abhängig gemacht werden kann.

Auf Grund der hohen Bedeutung für die Kommunikation des Einzelnen und die dadurch bedingte Verletzlichkeit der Gesellschaft insgesamt, müssen - zum Schutz gegen unerlaubte Zugriffe auf die Telekommunikations- und Datenverarbeitungssysteme - Maßnahmen getroffen werden, die den Stand der Technik berücksichtigen. Angriffe auf die Netze erfolgen zunehmend auf höchstem technischem Niveau unter Ausnutzung öffentlich noch nicht bekannter Lücken in der Sicherheitsarchitektur von Hardware- und Software-Produkten. Durch diese Angriffe werden die Verfügbarkeit, Integrität und Authentizität datenverarbeitender Systeme bedroht. Mit der durch den neuen Satz 3 aufgenommenen Änderung werden entsprechende Mindestanforderungen für den Schutz gegen unerlaubte Zugriffe und die Auswirkungen von Sicherheitsverletzungen aufgestellt.

Adressiert sind Betreiber von Telekommunikationsnetzen und Anbieter von Telekommunikationsdiensten, die der Öffentlichkeit zugänglich sind.

Zu Nummer 3 (§ 109 Absatz 5 Meldepflichten)

Die bestehenden Meldepflichten werden durch die vorgeschlagene Regelung um die Verpflichtung ergänzt, bekannt gewordene Vorfälle zu melden, die zu erheblichen Sicherheitsverletzungen von datenverarbeitenden Systemen der Endnutzer führen können. Ziel ist es, bereits in diesem Vorfeldbereich eine Verbesserung des Lagebildes zur IT-Sicherheit zu erreichen. Verletzungen der IT-Sicherheit (z.B. Manipulationen der Internet-Infrastruktur und Missbrauch einzelner Server oder Anschlüsse, etwa zum Errichten und Betreiben eines Botnetzes) bergen ein großes Gefahrenpotential, das sich allerdings in diesem Stadium (noch) nicht gegen die Verfügbarkeit der Netze insgesamt, sondern die Funktionsfähigkeit und Verlässlichkeit der IT einzelner Nutzer richtet und ggf. spätere schwerwiegende Folgen nach sich zieht.

Bislang besteht eine solche Meldepflicht nur für tatsächlich aufgetretene Störungen und nur, sofern die durch Sicherheitsverletzungen verursachten Auswirkungen auf den Betrieb der TK-Netze oder das Erbringen von TK-Diensten beträchtlich sind.

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

Zu Nummer 4 (§ 109 Absatz 6 Erstellung des Sicherheitskatalogs)

Die zunehmende Nutzung normaler 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 wird diesem Erfordernis Rechnung getragen.

Zu Nummer 5 (§ 109 Absatz 7 Übermittlung der Auditergebnisse an das BSI)

Über die im Rahmen von Audits aufgedeckten IT-Sicherheitsmängel sowie die in diesem Zusammenhang von der Bundesnetzagentur geforderten Abhilfemaßnahmen ist das BSI von der Bundesnetzagentur unverzüglich zu unterrichten.

Zu Nummer 6 (§ 109a Daten- und Informationssicherheit)

Die Neuregelung soll die Information des Nutzers über Verletzungen der IT-Sicherheit gewährleisten, die von einem durch ihn betriebenen datenverarbeitenden System ausgehen. Derzeit wird eine entsprechende Information des Nutzers bei den einzelnen Providern uneinheitlich gehandhabt. Die Information soll Nutzer in die Lage versetzen, selbst Maßnahmen gegen Schadsoftware zu ergreifen. Hierfür ist weiter Voraussetzung, dass der Nutzer über angemessene Werkzeuge verfügen kann, um diese Schutzmaßnahmen zu ergreifen. Ergänzend zur Informationspflicht werden Anbieter von Telekommunikationsdiensten für die Öffentlichkeit deshalb verpflichtet, auf einfach bedienbare Sicherheitswerkzeuge hinzuweisen, die sowohl vorbeugend als auch zur Beseitigung von Störungen im Falle einer Infizierung des Datenverarbeitungssystems des Nutzers mit Schadsoftware genutzt werden können. Nicht erforderlich sind insoweit eine individuelle Untersuchung der Technik oder eine individuelle Beratung des Kunden. Die Informations- und Hinweispflicht kann dabei beispielsweise über Umleitung der betroffenen Nutzer auf eine Hinweisseite realisiert werden, um tatsächlich die betroffenen Nutzer und nicht nur die Vertragspartner der Anbieter zu erreichen. Soweit dies technisch nicht möglich ist, werden die Anbieter nur ihre Kunden informieren und auf Hilfsmittel hinweisen können, da der Endnutzer für sie in der Regel nicht ermittelbar sein wird.

Zu Nummer 7 (§ 115 Absatz 3 Satz 2 Zuverlässigkeit):

Die Regelung stellt im Hinblick auf die Befugnisse der Bundesnetzagentur nach den Abs. 1 bis 3 klar, dass auch die fehlende Zuverlässigkeit eines mit sicherheitskritischen Aufgaben betrauten Unternehmens zu Anordnungen und Maßnahmen bis hin zu einer vollständigen oder teilweisen Untersagung des Betriebs der betreffenden Telekommunikationsanlage oder des geschäftsmäßigen Erbringens des betreffenden Telekommuni-

kationsdienstes berechtigt, soweit dies für die ordnungsgemäße Erfüllung der Pflichten des 7. Teils erforderlich ist. Werden die Dienste von dem Verpflichteten einem zur Erfüllung seiner Verpflichtungen beauftragten Dritten (etwa im Rahmen eines Outsourcings) übertragen, ist auch sicherzustellen, dass diese Dritten die entsprechenden Anforderungen an die Zuverlässigkeit erfüllen.

Zu Artikel 4 (Änderung des Außenwirtschaftsgesetzes)

Mit Aufnahme von mit der Umsetzung technischer und organisatorischer Maßnahmen nach § 110 TKG betrauten Unternehmen sowie von Herstellern von technischen Einrichtungen zur Umsetzung gesetzlich vorgesehener Maßnahmen zur Überwachung der Telekommunikation i.S.d. § 110 Absatz 4 TKG in § 5 Absatz 3 wird der zentralen Bedeutung der sicheren und vertraulichen Abwicklung dieser Maßnahmen für die Sicherheitsinteressen der Bundesrepublik Deutschland Rechnung getragen.

Die Regelung bezieht sich auf den Teilbereich von Netzwerk-Dienstleistungen, die im Zusammenhang mit der Umsetzung staatlicher TKÜ-Maßnahmen stehen, die an dem Telekommunikationsnetz aufsetzen und vom Netzbetreiber durchgeführt werden müssen und für die ein herausgehobenes Sicherheitsinteresse besteht. Ergänzend werden auch die Hersteller bzw. wegen der starken technischen Bezüge der Vertrieb der hierfür erforderlichen Einrichtungen erfasst. Grund ist, dass Angriffe, die auf das Ausspähen und die Manipulation bzw. Unterdrückung von TKÜ-Maßnahmen gerichtet sind, potentiell sowohl über die für staatliche TKÜ-Maßnahmen eingesetzten technischen Einrichtungen als auch über hierzu (i.d.R. ergänzend) notwendige Tätigkeiten durchgeführt werden können.

Die besondere Bedeutung der Gewährleistung einer ordnungsgemäßen und vertraulichen Durchführung dieser Maßnahmen für den Erhalt wesentlicher Sicherheitsinteressen der Bundesrepublik Deutschland wird bereits dadurch deutlich, dass die einschlägigen Befugnisnormen an hohe Hürden geknüpft sind. Entsprechende Maßnahmen können von staatlichen Stellen u.a. zur Abwehr von drohenden Gefahren für die freiheitliche demokratische Grundordnung oder den Bestand oder die Sicherheit des Bundes oder eines Landes einschließlich der Sicherheit der in der Bundesrepublik Deutschland stationierten Truppen der nichtdeutschen Vertragsstaaten des Nordatlantikvertrags sowie zur Abwehr von Gefahren für den Bestand und die Sicherheit der Bundesrepublik Deutschland, anderer Staaten oder internationaler Organisationen sowie der Verfolgung schwerer Straftaten mit Bezug zur inneren und äußeren Sicherheit durchgeführt werden müssen.

Gleichzeitig ist die sichere und vertrauliche Durchführung dieser Maßnahmen in hohem Maße von der Vertrauenswürdigkeit der hierfür eingesetzten Systeme und Prozesse abhängig. Eine auf Missbrauch angelegte Manipulation staatlicher TKÜ-Maßnahmen, die an dem Telekommunikationsnetz aufsetzen und von dem Netzbetreiber durchgeführt werden müssen (Ausspähen und Manipulation der Maßnahmen), kann durch technisch-organisatorische Prüfungen und Sicherheitsmaßnahmen allein nicht zuverlässig ausgeschlossen werden. Für diesen besonders sicherheitskritischen Bereich ist daher die Zuverlässigkeit des Herstellers bzw. Dienstleisters für die Gewährleistung wesentlicher Sicherheitsinteressen der Bundesrepublik Deutschland wesentlich. Wird diese Vertrauenswürdigkeit beeinträchtigt, können daraus gravierende und nachteilige Folgen entstehen, da ein kurzfristiges Auswechseln von entsprechenden Diensten bzw. Produkten im Allgemeinen nicht möglich ist. Zudem muss auch für die Zukunft sichergestellt werden, dass es in Deutschland langfristig Unternehmen gibt, die über entsprechende Kapazitäten und technologische Fähigkeiten verfügen.

Zu Artikel 5 (Änderung des Bundeskriminalamtgesetzes)

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 StGB (Computersabotage) hinaus auf Straftaten nach §§ 202a, 202b, 202c, 263a und 303a StGB ausgedehnt. Zusätzlich zu den Fällen, in denen sich die genannten Straftaten gegen die innere oder äußere Sicherheit der Bundesrepublik Deutschland oder 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.

Zu Artikel 6 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten.