Referentenentwurf

des Bundesministeriums des Innern

Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

A. Problem und Ziel

Quer durch alle Branchen ist die Hälfte der deutschen Unternehmen schon heute vom Internet abhängig. Mit dem Grad der wirtschaftlichen Interaktion und Integration wächst auch die Abhängigkeit:

- zwischen den einzelnen Branchen,
- vom Funktionieren der eigenen IT-Systeme,
- aber auch von einem verfügbaren und sicheren Cyberraum insgesamt.

Mit der Abhängigkeit steigen die Risiken: IT-Ausfälle stellen eine reale Gefahr dar. Angriffe nehmen stetig zu und treffen Unternehmen quer durch alle Branchen.
Die vorgesehenen Neuregelungen dienen dazu, den Schutz der Integrität und Authentizität datenverarbeitender Systeme zu verbessern und der gestiegenen Bedrohungslage anzupassen.

Besondere Bedeutung kommt den kritischen Infrastrukturen zu, die für das Funktionieren unseres Gemeinwesens von überragender Bedeutung sind. Der Schutz ihrer IT-Systeme und der für den Infrastrukturbetrieb nötigen Netze hat höchste Priorität.

Das Niveau der IT-Sicherheit der kritischen Infrastrukturen bietet derzeit ein uneinheitliches Bild. 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. In manchen Infrastrukturbereichen existieren ausgeprägte gesetzliche Vorgaben auch zur IT-Sicherheit, in anderen Bereichen fehlen solche gänzlich. Auf Grund des hohen Grades der Vernetzung auch untereinander und der daraus resultierenden Interdependenzen ist dieser Zustand nicht hinnehmbar.

Die Zusammenarbeit zwischen Staat und den Betreibern kritischer Infrastrukturen muss verbessert werden und ein Mindestniveau an IT-Sicherheit bei den Betreibern gewährleistet sein.

Aufgrund der dezentralen und vernetzten Struktur des Internet als zentralem Kommunikationsmedium, kann IT-Sicherheit nur durch eine gemeinsame Verantwortungswahrnehmung aller Beteiligten gewährleistet werden. Um dies zu ermöglichen, kommt den Betreibern und Anbietern der zugrundeliegenden Kommunikationsinfrastruktur bei deren Schutz eine besondere Rolle zu.

B. Lösung

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 Bundesamt für Sicherheit in der Informationstechnik (BSI) erhebliche IT-Sicherheitsvorfälle zu melden. Die dadurch beim BSI zusammenlaufenden Informationen werden dort gesammelt und ausgewertet und die so gewonnenen Erkenntnisse den Betreibern kritischer Infrastrukturen zur Verfügung gestellt. Die Rolle des BSI zur IT-Sicherheit kritischer Infrastrukturen wird insgesamt gestärkt, indem es die Aufgabe erhält, auf Ersuchen bei der Sicherung der Informationstechnik zu beraten und unterstützen.

Die Telekommunikations- und Telemediendiensteanbieter, die eine Schlüsselrolle für die Sicherheit des Cyberraums haben, werden stärker als bisher hierfür in die Verantwortung genommen und dazu verpflichtet, IT-Sicherheit nach dem Stand der Technik nicht nur wie bisher zum Vertraulichkeitsschutz und zum Schutz personenbezogener Daten, sondern auch zum Schutz von Telekommunikations- und Datenverarbeitungssystemen gegen unerlaubte Zugriffe zu gewährleisten, um die Widerstandsfähigkeit der Kommunikationsinfrastruktur insgesamt zu verbessern und die Verfügbarkeit, Integrität und Authentizität datenverarbeitender Systeme und der dort vorgehaltenen Daten zu sichern.

Die Telekommunikationsanbieter sollen überdies bekannte IT-Sicherheitsvorfälle, die zu einem unerlaubten Zugriff auf 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 für das Rückgrat der Informationsgesellschaft verantwortlichen Anbieter zu einem validen und vollständigen Lagebild der IT-Sicherheit beitragen. Dieses dient seinerseits wiederum als Grundlage für die Information der Nutzer (insbesondere Betreiber kritischer Infrastrukturen) durch

staatliche Stellen und für abgestimmte Reaktionen auf Cybersicherheitsvorfälle. Außerdem sollen Telekommunikationsanbieter betroffene Nutzer über bekannte Störungen durch Schadprogrammen auf ihren datenverarbeitenden Systemen informieren und einfach bedienbare Hilfsmittel für die Erkennung und Beseitigung bereitstellen. Die Unterstützung der Nutzer soll diese in die Lage versetzen, Maßnahmen gegen Schadsoftware auf ihren datenverarbeitenden Systemen zu ergreifen, um damit einen Beitrag zur Verbesserung der IT-Sicherheit der Netze insgesamt zu erbringen.

Die vorgesehene jährliche Berichtspflicht des Bundesamtes für Sicherheit in der Informationstechnik soll dazu beitragen, dass das Bewusstsein aller relevanten Akteure für das Thema IT-Sicherheit insgesamt weiter geschärft wird. In Anbetracht der Tatsache, dass eine Vielzahl von erfolgreichen IT-Angriffen bei Einsatz von Standardwerkzeugen zu verhindern gewesen wären, würde ein höherer Grad an Sensibilisierung der Nutzer einen wichtigen Beitrag zur Verbesserung der IT-Sicherheit insgesamt erbringen. Angesichts der Zunahme der IT-Angriffe gegen Bundeseinrichtungen und gegen bundesweite kritische Infrastrukturen 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, sofern sich diese gegen die innere oder äußere Sicherheit der Bundesrepublik Deutschland oder sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen richten.

C. Alternativen

Beibehalten des bisherigen Rechtszustandes.

D. Haushaltsangaben ohne Erfüllungsaufwand

Für die Länder entsteht kein Erfüllungsaufwand.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Die Einhaltung eines Mindestniveaus an IT-Sicherheit wird bei denjenigen Betreibern kritischer Infrastrukturen einschließlich Telekommunikationsdiensteanbietern und Telemediendiensteanbietern zu Mehraufwendungen führen, welche bisher kein hinreichendes Niveau etabliert haben. Für diejenigen, die bereits heute auf Grund regulativer Vorgaben oder auf freiwilliger Basis dieses Niveau einhalten, entstehen insoweit keine gesonderten Kosten. Zusätzliche Kosten entstehen für die Betreiber kritischer Infrastrukturen durch die Durchführung der vorgegebenen Sicherheitsaudits.

Der Entwurf führt 6 neue Informationspflichten im Sinne des Gesetzes zur Einsetzung eines Nationalen Normenkontrollrates (NKR-Gesetz) für Unternehmen ein. Die Verbände der betroffenen Unternehmen werden im Rahmen der Verbändebeteiligung gebeten, zu erwartende jährliche Fallzahlen und eine Kostenschätzung zu übermitteln.

E.3 Erfüllungsaufwand der Verwaltung

Die neu geschaffenen Befugnisse und Aufgaben des Bundesamts für Sicherheit in der Informationstechnik sind mit einem entsprechenden Vollzugsaufwand verbunden. Für die Konzeptphase nach Verabschiedung des Gesetzes wird das Bundesamt für die Sicherheit in der Informationstechnik (BSI) 23 Planstellen/Stellen benötigen. Dieser Bedarf wird in der Einstiegs/Einführungsphase um weitere 36 zusätzliche Planstellen/Stellen anwachsen und in der Wirkphase einen Bedarf von nochmals weiteren 40 Planstellen/Stellen erzeugen. Für die Erfüllung der im Gesetz vorgesehenen Aufgaben besteht beim BSI ein zusätzlicher Aufwand von insgesamt 99 zusätzlichen Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 6.653 T€ sowie zusätzlichen Sachkosten in Höhe von jährlich rund 6.210 T€.
Die neuen Mitwirkungsaufgaben für das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) führt dort zu einem zusätzlichen Bedarf von 2 Stellen mit jährlichen Personal – und Sachkosten in Höhe von 147 T€ für die Aufgaben nach § 8b Abs. 2 Ziffer 2 und Bedarf an Personal – und Sachkosten für zeitlich befristete Verträge (gerundet 13 Personenjahre) in Höhe von insgesamt 911 T€ für Aufgaben nach § 10 Abs.1.

In den Fachabteilungen des Bundeskriminalamts (BKA) entsteht durch die Erweiterung der originären Ermittlungszuständigkeit ein Ressourcenaufwand von 105 zusätzlichen Planstellen / Stellen mit jährlichen Personalkosten in Höhe von rund 6,1 Mio € sowie zusätzlichem Sachmitteln in Höhe von 680 T € im ersten Jahr.

Mehrbedarf an Sach- und Personalmitteln soll finanziell und stellenmäßig im jeweiligen Einzelplan ausgeglichen werden.

F. Weitere Kosten

Keine.

Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

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. Dem § 2 Absatz 9 wird folgender Absatz 10 angefügt:
   „(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind die in der 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 Sicherheit eintreten würden. Kommunikationstechnik im Sinne des Absatzes 3 Satz 1 und 2 gehört nicht zu den kritischen Infrastrukturen im Sinne dieses Gesetzes."

2. § 3 wird wie folgt geändert:

   a. In § 3 Absatz 1 Satz 2 Nummer 2 werden die Wörter „andere Stellen" durch das Wort „Dritte" ersetzt.

   b. 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."

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

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

4. Nach § 8 werden folgende §§ 8a und 8b eingefügt:

„§ 8a

Sicherheit 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) Stand der Technik im Sinne dieses Gesetzes 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 vergleichbare Verfahren, Einrichtungen und Betriebsweisen heranzuziehen, die mit Erfolg in der Praxis erprobt wurden.

(3) Betreiber kritischer Infrastrukturen und ihre Branchenverbände können branchenspezifische Sicherheitsstandards erarbeiten. Das Bundesamt erkennt die branchenspezifischen Sicherheitsstandards im Benehmen mit den zuständigen Aufsichtsbehörden 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.

(4) Betreiber kritischer Infrastrukturen haben zur Überprüfung der organisatorischen und technischen Vorkehrungen und sonstigen Maßnahmen nach Absatz 1 nach

Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 mindestens alle zwei Jahre Sicherheitsaudits durch anerkannte Auditoren durchzuführen. Sie übermitteln dem Bundesamt mindestens alle zwei Jahre eine Aufstellung der durchgeführten Sicherheitsaudits einschließlich der aufgedeckten Sicherheitsmängel. Das Bundesamt kann bei Sicherheitsmängeln eine Übermittlung der gesamten Ergebnisse des Sicherheitsaudits verlangen. Bei Sicherheitsmängeln kann das Bundesamt deren unverzügliche Beseitigung verlangen.

(5) Soweit aus oder auf Grund von Rechtsvorschriften des Bundes weitergehende Anforderungen an die informationstechnischen Systeme, Komponenten oder Prozesse kritischer Infrastrukturen anzuwenden sind, finden die Absätze 1 bis 4 keine Anwendung.

§ 8b

Zentrale Meldestelle für die Sicherheit in der Informationstechnik für die Betreiber 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 und die zuständigen Aufsichtsbehörden unverzüglich über die sie betreffenden Informationen nach den Nummern 1 bis 3 und die in Erfahrung gebrachten Zusammenhänge zu unterrichten.

(3) Um bei schwerwiegenden Beeinträchtigungen der informationstechnischen Systeme, Komponenten oder Prozesse kritischer Infrastrukturen eine unverzügliche

Information betroffener Betreiber kritischer Infrastrukturen zu gewährleisten, sind dem Bundesamt binnen eines Jahres 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 des Bundesamtes nach Absatz 2 Nummer 4 erfolgt dorthin.

(4) Betreiber kritischer Infrastrukturen haben über die Warn- und Alarmierungskontakte nach Absatz 3 schwerwiegende Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, das heißt Beeinträchtigungen, die Auswirkungen auf die Funktionsfähigkeit der von ihnen betriebenen kritischen Infrastrukturen haben können, unverzüglich an das Bundesamt zu melden.

(5) Soweit aus oder auf Grund von Rechtsvorschriften des Bundes bereits Anforderungen im Sinne der Absätze 3 und 4 bestehen, finden die Absätze 3 und 4 keine Anwendung. Die in den genannten Rechtsvorschriften benannten Meldestellen oder Aufsichtsbehörden haben Meldungen zu erheblichen IT-Sicherheitsvorfällen im Sinne von Absatz 4 unverzüglich an das Bundesamt weiterzuleiten.

5. § 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, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Technologie, dem Bundesministerium der Justiz, dem Bundesministerium der Finanzen, dem Bundesministerium für Arbeit und Soziales, dem Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr, Bau und Stadtentwicklung, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit durch Rechtsverordnung die kritischen Infrastrukturen nach § 2 Absatz 10.“

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

6. 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 2 und 3 ist entsprechend anzuwenden“.

Artikel 2

Änderung des Bundeskriminalamtgesetzes

§ 4 Absatz 1 Satz 1 Nummer 5 des Bundeskriminalamtgesetzes vom 7. Juli 1997 (BGBl. I S. 1650), das zuletzt durch Artikel 3 des Gesetzes vom 21. Juli 2012 (BGBl. I S. 1566) geändert worden ist, wird wie folgt geändert:

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

Artikel 3

Änderung des Telemediengesetzes

§ 13 des 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. Nach Absatz 6 wird folgender Absatz 7 eingefügt:

„Diensteanbieter haben für geschäftsmäßig in der Regel gegen Entgelt angebotene Telemedien technische Vorkehrungen oder sonstige Maßnahmen zum Schutz von Telekommunikations- und Datenverarbeitungssystemen gegen uner-

laubten Zugriff zu treffen, soweit dies technisch möglich und zumutbar ist. Dabei ist der Stand der Technik zu berücksichtigen.“

2. Der bisherige Absatz 7 wird Absatz 8.

Artikel 4
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. §109 Abs.2 wird wie folgt geändert:

Nach Satz 4 wird folgender Satz 5 eingefügt:

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

2. § 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:

„Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat Beeinträchtigungen von Telekommunikationsnetzen und -diensten, die zu einer Störung der Verfügbarkeit der über diese Netze erbrachten Dienste oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssystemen der Nutzer oder Teilnehmer führen können und von denen der Netzbetreiber oder der Telekommunikationsdiensteanbieter Kenntnis erlangt, der Bundesnetzagentur unverzüglich mitzuteilen. Die Bundesnetzagentur unterrichtet das Bundesamt für Sicherheit in der Informationstechnik. Werden Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, sind diese vom Diensteanbieter unverzüglich zu benachrichtigen. Soweit technisch möglich und zumutbar, müs-

sen 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.

Artikel 5

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A: Allgemeiner Teil

I. Zweck und Inhalt des Gesetzes

Der Entwurf sieht für Betreiber kritischer Infrastrukturen einschließlich Telekommunikationsdiensteanbietern und Telemediendiensteanbietern die Pflicht zur Einhaltung eines Mindestniveaus an IT-Sicherheit vor. Für Betreiber kritischer Infrastrukturen einschließlich der Telekommunikationsdiensteanbieter ist außerdem die Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle vorgesehen. Spiegelbildlich zu diesen Verpflichtungen wird das BSI in seiner Beratungs- und Unterstützungsrolle für die Verpflichteten 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 GG. Für die Regelungen zum Schutz der Informationstechnik kritischer Infrastrukturen folgt die Gesetzgebungskompetenz des Bundes teilweise aus speziellen Kompetenztiteln (Luftverkehr [Art. 73 Absatz 1 Nummer 6 GG], Eisenbahnen [Art. 73 Absatz1 Nummer 6a, Art. 74 Absatz 1 Nummer 23 GG], Schifffahrt [Art. 74 Absatz 1 Nummer 21 GG] oder Telekommunikation [Art. 73 Absatz 1 Nummer 7 GG] und ansonsten aus der konkurrierenden Gesetzgebungskompetenz für das Recht der Wirtschaft (Art. 74 Absatz 1 Nummer 11 GG). Für die Änderung des Telemediengesetzes (Artikel 3) ergibt sich die Gesetzgebungskompetenz des Bundes ebenfalls aus Art. 74 Absatz 1 Nummer 11). Die Berechtigung des Bundes zur Inanspruchnahme dieser Gesetzgebungskompetenz ergibt sich aus Artikel 72 Absatz 2 Grundgesetz. 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 Änderung des BKA-Gesetzes (Artikel 2) beruht auf der Gesetzgebungskompetenz nach Art. 73 Absatz 1 Nummer 10 GG. Die Änderungen im Telekommunikationsgesetz (Artikel 4) können auf die ausschließliche Gesetzgebungskompetenz des Bundes nach Artikel 73 Absatz 1 Nummer 7 GG gestützt werden.

III. Erfüllungsaufwand

1. Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

2. Erfüllungsaufwand für die Wirtschaft

Die Einhaltung eines Mindestniveaus an IT-Sicherheit wird bei denjenigen Betreibern kritischer Infrastrukturen einschließlich Telekommunikationsdiensteanbietern und Telemediendiensteanbietern zu Mehraufwendungen führen, welche bisher kein hinreichendes Niveau etabliert haben. Für diejenigen, die bereits heute auf Grund regulativer Vorgaben oder auf freiwilliger Basis dieses Niveau einhalten, entstehen insoweit keine gesonderten Kosten. Zusätzliche Kosten entstehen für die Betreiber kritischer Infrastrukturen durch die Durchführung der vorgegebenen Sicherheitsaudits.
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 Bundesamt für Sicherheit in der Informationstechnik regelmäßig eine Aufstellung der zur Überprüfung der technischen Vorkehrungen und sonstigen Maßnahmen nach § 8a Absatz 3 Satz 1 durchgeführten Sicherheitsaudits.
b. Artikel 1, § 8a Absatz 3 Satz 3: Auf Verlangen des Bundesamtes haben die Betreiber die Ergebnisse der Sicherheitsaudits nach § 8a Absatz 3 Satz 1 zu übermitteln.
c. Artikel 1, § 8b Absatz 3 Satz 1: Die Betreiber kritischer Infrastrukturen haben dem Bundesamt für Sicherheit in der Informationstechnik Warn-und Alarmierungskontakte zu benennen, über welche 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, unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik zu melden.
e. Artikel 3, § 109a Absatz 4 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.
f. 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 Bundesamts für Sicherheit in der Informationstechnik sind mit einem entsprechenden Vollzugsaufwand verbunden.
Für die Konzeptphase nach Verabschiedung des Gesetzes wird das Bundesamt für die Sicherheit in der Informationstechnik (BSI) 23 Planstellen/Stellen benötigen. Dieser Bedarf wird in der Einstiegs/Einführungsphase um weitere 36 zusätzliche Planstellen/Stellen anwachsen und in der Wirkphase einen Bedarf von weiteren 40 Planstellen/Stellen erzeugen. 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 Identifizie-

rung 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.

In der Konzeptphase sind vor allem konzeptionelle und methodische Aufbauarbeiten zu leisten, die in der Einstiegsphase exemplarisch mit besonders geeigneten kritischen Branchen oder Unternehmen beispielhaft umgesetzt, getestet und verfeinert werden. In der Wirkphase entsteht der zusätzliche Stellenbedarf durch die Erweiterung auf den Kreis aller identifizierten Betreiber kritischer Infrastrukturen und durch die Wahrnehmung aller damit zusammenhängenden Aufgaben einschließlich der Beratungs- und Unterstützungsleistung vor Ort sowie des 24/7-Betriebs des Lagezentrums.
Für die Erfüllung der im Gesetz vorgesehenen Aufgaben besteht beim BSI damit ein zusätzlicher Aufwand von insgesamt 99 zusätzlichen Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 6.653 T€ sowie Sachkosten in Höhe von jährlich rund 6.210 T€..

Die neuen Mitwirkungsaufgaben für das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) führt dort zu einem zusätzlichen Bedarf von 2 Stellen mit jährlichen Personal – und Sachkosten in Höhe von 147 T€ für die Aufgaben nach § 8b Abs. 2 Ziffer 2 und Bedarf an Personal – und Sachkosten für zeitlich befristete Verträge (gerundet 13 Personenjahre) in Höhe von insgesamt 911 T€ für Aufgaben nach § 10 Abs.1.

In den Fachabteilungen des Bundeskriminalamts (BKA) entsteht durch die Erweiterung der originären Ermittlungszuständigkeit ein Ressourcenaufwand von 105 zusätzlichen Planstellen / Stellen mit jährlichen Personalkosten in Höhe von rund 6,1 Mio € sowie zusätzlichem Sachmitteln in Höhe von 680 T € im ersten Jahr.

Mehrbedarf an Sach- und Personalmitteln soll finanziell und stellenmäßig im jeweiligen Einzelplan ausgeglichen werden.

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 berücksichtigen insoweit § 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.

VI. Nachhaltigkeit

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

Zweiter Teil: Zu den einzelnen Vorschriften

Zu Artikel 1 (Änderung des BSI-Gesetzes)

Zu Nummer 1 (§ 2 Begriffsbestimmungen)

In § 2 Absatz 10 Satz 1 wird der Begriff der kritischen Infrastrukturen im Sinne des BSI-Gesetzes definiert. Eine Definition der kritischen Infrastrukturen ist notwendig, um die Adressaten der §§ 8a und 8b zu bestimmen. Die Auflistung der Sektoren folgt der in der Bundesregierung abgestimmten Einteilung kritischer Infrastrukturen. Zu den vom Regelungsbereich erfassten Sektoren gehören die Bereiche Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen. Kommunikationstechnik von Regierung, Parlament und öffentliche Bundesverwaltung sind nach Satz 2 von den kritischen Infrastrukturen im Sinne des BSI-Gesetzes ausgenommen, da für sie als Spezialregelung §§ 4 und 8 gilt. Die Verwaltungen der Länder und Kommunen sind ebenfalls ausgenommen, da der Bund für sie keine Gesetzgebungskompetenz besitzt.

Innerhalb der vom Gesetz erfassten Sektoren sind diejenigen Einrichtungen, Anlagen oder Teile davon zu identifizieren, die aus Bundessicht für das Funktionieren des Gemeinwesens und die Sicherung der Grundbedürfnisse der Bevölkerung von hoher Bedeutung und insoweit besonders schutzwürdig sind. Mögliche Kriterien für die Ermittlung dieser Infrastrukturen sind insbesondere der Versorgungsgrad, die Auswirkungen eines Ausfalls bzw. einer Beeinträchtigung auf die Bevölkerung oder auf andere kritische Infrastrukturen, zeitliche Aspekte (Schnelligkeit und Dauer des Ausfalls bzw. der Beeinträchtigung), Marktbeherrschung sowie die Auswirkung auf den Wirtschaftsstandort. Die weitere Konkretisierung ist der Rechtsverordnung nach § 10 vorbehalten.

Zu Nummer 2 (§ 3 Aufgaben des Bundesamtes)

Die Änderung in Absatz 1 dient der Klarstellung, dass Erkenntnisse nicht nur Behörden zur Verfügung gestellt werden können, sondern auch anderen Betroffenen. Adressat dieser Erkenntnisse können dabei insbesondere Betreiber kritischer Infrastrukturen aus dem Sektor Kultur und Medien sein, die mangels Bundeskompetenz nicht von der Definition nach § 2 Absatz 10 erfasst werden können, aber anerkannter Maßen zum Bereich der kritischen Infrastrukturen gehören.

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, Betreiber kritischer

Infrastrukturen auf Ersuchen bei der Sicherung ihrer Informationstechnik insbesondere im Hinblick auf die Erfüllung der Anforderungen nach §§ 8a, 8b zu beraten und zu unterstützen. Ob das BSI einem Ersuchen nachkommt, entscheidet es nach pflichtgemäßem Ermessen.

Zu Nummer 3 (§ 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes)

Die Änderung der Überschrift dient klarstellend der Abgrenzung zur neuen Aufgabe nach § 8b.

Zu Nummer 4 (§ 8a Sicherheit der Informationstechnik kritischer Infrastrukturen, § 8b Zentrale Meldestelle für die Sicherheit in der Informationstechnik für die Betreiber kritischer Infrastrukturen)

Zu § 8a

Zweck von § 8a Absatz 1 ist der ordnungsgemäße Betrieb kritischer Infrastrukturen und die fortlaufende Verfügbarkeit der jeweils angebotenen 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 de kritischen Infrastrukturen erfüllt werden, auf die die Gesellschaft existentiell angewiesen ist. Hierzu 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 betreibt oder daran mitwirkt. Die Notwendigkeit, angemessene organisatorische und technische Vorkehrungen und sonstige Maßnahmen zu treffen, besteht auch dann, wenn Unternehmen ihre IT durch Dienstleister betreiben lassen. 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. Aufgrund der weitreichenden gesellschaftlichen Auswirkungen ist dabei der Stand der Technik zu berücksichtigen. 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 enthält eine Legaldefinition für den Begriff „Stand der Technik“ aus Absatz 1.

Absatz 3 ermöglicht in Branchen, wo dies geeignet und notwendig ist, die Erarbeitung branchenspezifischer Sicherheitsstandards und verankert damit den kooperativen Ansatz. Ziel ist es, dass sich Unternehmen und Verbände branchenintern zusammenfinden und für die jeweilige Branche einheitliche Sicherheitsstandards erarbeiten. Dabei ist darauf zu achten, dass eine Kompatibilität zu Selbstregulierungen im Bereich des Datenschutzes besteht. Die vom BSI im

Benehmen mit der jeweils zuständigen Aufsichtsbehörde anerkannten brancheninternen Standards konkretisieren die Verpflichtungen nach Absatz 1 für die Branche und können von daher nur 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 soweit branchenspezifische Sicherheitsstandards erarbeitet wurden, steht es dem einzelnen Betreiber frei, eigene dem Stand der Technik entsprechende Maßnahmen einzusetzen.

Die Sicherheitsaudits nach Absatz 4 dienen 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 soll nicht im Detail gesetzlich vorgegeben werden, da diese von den jeweils erarbeiteten brancheneinheitlichen Mindeststandards und den in den Branchen vorhandenen technischen Gegebenheiten abhängen wird. Generell soll geprüft werden, ob der Betreiber die für seine Branche und Technologie geeignete und wirksame 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 bzw. den jeweiligen branchenspezifischen Sicherheitsstandard, sofern ein solcher erstellt und anerkannt wurde, umsetzt. Sicherheitsaudits sollten von anerkannten Auditoren und nach wesentlichen Änderungen im Unternehmen, spätestens jedoch im Abstand von zwei Jahren durchgeführt werden. Ein Auditor gilt als anerkannt im Sinne des Gesetzes, wenn er seine Qualifikation zur Überprüfung der Einhaltung der Mindeststandards gegenüber dem Bundesamt für Sicherheit in der Informationstechnik 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.).

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.

Die Regelung in Absatz 5 stellt sicher, dass weitergehende Vorgaben möglich sind und insbesondere bestehende spezialgesetzliche Rechtsvorschriften mit weitergehenden Anforderungen nicht berührt werden. Diese müssen mindestens das Sicherheitsniveau nach § 8a Abs. 1 BSIG gewährleisten. Weitergehend sind dabei insbesondere solche Anforderungen, die einen strengeren materiellen Standard als den Stand der Technik vorsehen.

Zu § 8b

§ 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 Cyber-Gefährdungslage. Diese ist Voraussetzung für die nationale Handlungsfähigkeit und die 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 Personenbezug gegeben sein, richtet sich die Übermittlungsbefugnis nach den allgemeinen datenschutzrechtlichen Regelungen oder gegebenenfalls spezialgesetzlichen Regelungen. Im Einzelnen:

Absatz 2 regelt die Aufgaben des BSI zu diesem Zweck. 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 und das Lagezentrum des Bundesamtes unverzüglich informiert werden. Hierfür können bestehende Strukturen beispielsweise über die Aufsichtsbehörden 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.

Absatz 4 regelt die Verpflichtung von Betreibern kritischer Infrastrukturen, dem BSI unverzüglich schwerwiegende Beeinträchtigungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse insbesondere durch Sicherheitslücken, Schadprogramme und erfolgte, versuchte oder erfolgreich abgewehrte Angriffe auf die Sicherheit in der Informationstechnik zu melden. Beeinträchtigungen sind dann schwerwiegend, wenn sie die Funktionsfähigkeit des Unternehmens bzw. der von diesem betriebenen kritischen Infrastrukturen beeinträchtigen können. Diese Meldungen sind notwendig, um fundierte Aussagen zur IT-Sicherheitslage in Deutschland treffen und frühzeitig Maßnahmen ergreifen zu können. Die Regelung in Absatz 5 stellt sicher, dass weitergehende Vorgaben möglich sind und insbesondere bestehende weitergehende Rechtsvorschriften nicht berührt werden.

Zu Nummer 5 (§ 10 Ermächtigung zum Erlass von Rechtsverordnungen)

Mit § 10 Absatz 1 wird das Bundesministerium des Innern ermächtigt, in Konkretisierung der systemischen Definition kritischer Infrastrukturen nach § 2 Absatz 10 im Einvernehmen mit den

betroffenen Bundesministerien die Kriterien zur Bestimmung derjenigen Einrichtungen, Anlagen oder Teile davon festzulegen, die als kritische Infrastruktur im Sinne des BSI-Gesetzes einzuordnen sind. In einem Anhang zur Rechtsverordnung werden abstrakt die als kritische Infrastrukturen einzuordnenden Einrichtungen, Anlagen oder Teile davon aufgelistet. Als Kriterien für die Einordnung einer Einrichtung, Anlage oder eines Teils davon als kritische Infrastruktur kommen insbesondere der Versorgungsgrad, die Auswirkungen eines Ausfalls bzw. einer Beeinträchtigung auf die Bevölkerung oder auf andere kritische Infrastrukturen, zeitliche Aspekte (Schnelligkeit und Dauer des Ausfalls bzw. der Beeinträchtigung), Marktbeherrschung sowie die Auswirkung auf den Wirtschaftsstandort in Betracht.

Zu Nummer 6 (§ 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 bei Einsatz von Standardwerkzeugen 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 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 3 (Änderung des Telemediengesetzes)

Wegen der zunehmenden Verbreitung von Schadsoftware über Telemediendienste werden die bestehenden Anbieterpflichten für Telemediendiensteanbieter um technische Schutzmaßnahmen zur Gewährleistung von IT-Sicherheit der für Dritte angebotenen Inhalte ergänzt. 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.Die Verpflichtung, Mindestanforderungen zur IT-Sicherheit einzuhalten, dient dazu, die Verbreitung von Schadprogrammen zu reduzieren und damit einen Beitrag zur Verbesserung der IT-Sicherheit insgesamt zu leisten.

Technisch möglich und zumutbar sollte i.d.R. eine regelmäßige Aktualisierung der für das Telemedienangebot verwendeten Software sowie das Einspielen von Sicherheitspatches sein. Die Bandbreite der erfassten Diensteanbieter vom Kleingewerbetreibenden bis zum Informationsintermediär ist groß. Der Verweis auf die Zumutbarkeit ermöglicht jedoch eine flexible Anpassung der Anforderungen (Ausgestaltung ggf. durch die Rspr.). Das rein private (d.h. nicht geschäftsmäßige) Angebot von Telemedien wird von dem Vorschlag nicht erfasst.

Zu Artikel 4 (Änderung des Telekommunikationsgesetzes)

Zu Nummer 1 (§ 109 Technische Schutzmaßnahmen)

Die gesetzlichen Vorgaben zu technischen Schutzmaßnahmen enthalten 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 (§ 109 Absatz 2 Satz 1 und 3 TKG).

Aufgrund der hohen Bedeutung für die Grundversorgung des Einzelnen mit Kommunikation und der dadurch bedingten Verletzlichkeit der Gesellschaft insgesamt, müssen zum Schutz gegen unerlaubte Zugriffe auf die Telekommuniktions – und Datenverarbeitungssysteme Maßnahmen getroffen werden, die den Stand der Technik berücksichtigen. Angriffe auf die Netze erfolgen zunehmend auf höchstem technischen 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 der Netzbetreiber selbst und der Endnutzer bedroht.

Mit der vorgeschlagenen Änderung werden entsprechende Mindestanforderungen für den Schutz gegen unerlaubte Zugriffe und die Auswirkungen von Sicherheitsverletzungen für Nutzer und zusammengeschaltete Netze aufgestellt. Adressiert sind Betreiber von Telekommunikationsnetzen und Anbieter von Telekommunikationsdiensten, die der Öffentlichkeit zugänglich sind.

Zu Nummer 2 (§ 109a Daten- und Informationssicherheit)

Die vorgeschlagene Regelung dient der angemessene Information und Unterstützung der Endkunden (insb. der Verbraucher) bei der Prävention und der Beseitigung von IT-Sicherheitsvorfällen. Die bestehenden Meldepflichten werden durch die vorgeschlagene Regelung um die Verpflichtung ergänzt, bekannt gewordene Vorfälle zu melden, die die IT-Sicherheit von datenverarbeitenden Systemen der Endnutzer gefährden. Ziel ist es, eine Verbesserung des Lagebilds zur IT-Sicherheit zu erreichen. Die geltende Meldeverpflichtung in § 109 Abs. 5 TKG bezieht sich auf schwere Störungen mit beträchtlichen Auswirkungen auf den Betrieb der TK-Netze und grundlegender TK-Dienste in ihrer Gesamtheit. IT-Angriffe mit nicht unmittelbar

schwerwiegenden Folgen werden aber nicht erfasst, da diese nicht die Verfügbarkeit der TK-Netze und grundlegender TK-Dienste in ihrer Gesamtheit beeinträchtigen und auch nicht unmittelbar zu Leistungsminderungen bei einer nennenswerten Zahl von Nutzern führen.

Verletzungen der IT-Sicherheit (z.B. Manipulationen der Internet-Infrastuktur 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 (etwa auch KRITIS) richtet und ggf. spätere schwerwiegende Folgen nach sich zieht.

Die vorgeschlagene Neuregelung soll zudem die Information des Nutzers über Verletzungen der IT-Sicherheit, die von einem von ihm betriebenen datenverarbeitenden System ausgehen, gewährleisten. Derzeit wird eine entsprechende Information des Nutzers bei den einzelnen Providern uneinheitlich gehandhabt. Die Information soll Nutzer in die Lage versetzen, selbst Maßnahmen gegen Malware 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.

Zu Artikel 5 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten.