Referentenentwurf

des Bundesministeriums des Innern

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

A. Problem und Ziel

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

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

Mit dem Gesetz soll eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme (IT-Sicherheit) in Deutschland erreicht werden. Die vorgesehenen Neuregelungen dienen dazu, die Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität datenverarbeitender Systeme zu verbessern und die Systeme der IT-Sicherheitslage anzupassen. Ziel des Gesetzes ist die Verbesserung der IT-Sicherheit von Unternehmen, der verstärkte Schutz der Bürgerinnen und Bürger im Internet und in diesem Zusammenhang auch die Stärkung von BSI und Bundeskriminalamt (BKA).

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

B. Lösung

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

Um den Schutz der Bürgerinnen und Bürger zu verbessern, werden die Telekommunikations- und Telemediendiensteanbieter, die eine Schlüsselrolle für die Sicherheit des Cyberraums haben, verpflichtet, IT-Sicherheit nach dem Stand der Technik nicht nur zum Schutz des Fernmeldegeheimnisses und zum Schutz personenbezogener Daten, sondern auch im Hinblick auf die Verfügbarkeit ihrer Telekommunikations- und Datenverarbeitungssysteme zu gewährleisten. Damit wird die

Widerstandsfähigkeit der Kommunikationsinfrastruktur insgesamt verbessert und die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit datenverarbeitender Systeme sowie der dort vorgehaltenen Daten gesichert.

Telekommunikationsanbieter sollen zudem IT-Sicherheitsvorfälle, die zu einem unerlaubten Zugriff auf die Systeme der Nutzerinnen und Nutzer oder einer Beeinträchtigung der Verfügbarkeit führen können, unverzüglich über die Bundesnetzagentur an das BSI melden und betroffene Nutzerinnen und Nutzer über bekannte Störungen informieren, die durch Schadprogramme auf den datenverarbeitenden Systemen der Nutzerinnen und Nutzer hervorgerufen werden. Außerdem ist eine Befugnis für Telemedienanbieter zur Erhebung und Verwendung von Nutzungsdaten im Zusammenhang mit Störungen und Missbrauch der genutzten technischen Einrichtungen zu schaffen. Die Befugnisse der Bundesnetzagentur im Bereich der Aufsicht über die Telekommunikationsanbieter werden ergänzt.

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

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

C. Alternativen

Beibehalten des bisherigen Rechtszustandes.

D. Haushaltsangaben ohne Erfüllungsaufwand

Der Erfüllungsaufwand der Verwaltung ist noch Gegenstand von Erörterungen zwischen den Ressorts.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Betreibern Kritischer Infrastrukturen sowie bestimmten Telekommunikations- und Telemediendiensteanbietern entsteht 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, da relevante Vorfälle von den Betreibern auch ohne die im Gesetz vorgesehene Meldepflicht untersucht, bewältigt und dokumentiert werden müssen. Bürokratiekosten entstehen daher nur durch den Mehraufwand, der zusätzlich zu der erforderlichen systematischen Vorfallsbearbeitung durch den Betreiber anfällt. Weitere Kosten entstehen für die Betreiber durch die Durchführung der vorgesehenen Sicherheitsaudits.

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

E.3 Erfüllungsaufwand für die Verwaltung

Der Erfüllungsaufwand der Verwaltung ist noch Gegenstand von Erörterungen zwischen den Ressorts.

F. Weitere Kosten

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

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

Vom …

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1
Änderung des BSI-Gesetzes

Das BSI-Gesetz in der Fassung der Bekanntmachung vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 3 Absatz 7 des Gesetzes vom 7. August 2013 (BGBl. I S. 3154) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird die Angabe zu § 4 wie folgt gefasst:

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

2. § 1 wird wie folgt gefasst:

   „Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) als Bundesoberbehörde. Das Bundesamt ist zuständig für die Informationssicherheit auf nationaler Ebene. Es untersteht dem Bundesministerium des Innern.“

3. Dem § 2 Absatz 9 wird folgender Absatz 10 angefügt:

„(10) Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die

1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und

2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt. Kommunikationstechnik im Sinne des Absatzes 3 gehört nicht zu den Kritischen Infrastrukturen im Sinne dieses Gesetzes."

4. § 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 Wörter „kritischen Informationsinfrastrukturen" durch die Wörter „Sicherheit in der Informationstechnik Kritischer Infrastrukturen" und der Punkt durch ein Semikolon ersetzt.

   c. Dem Absatz 1 Satz 2 werden folgende Nummern 16 und 17 angefügt:

      „16. Aufgaben als zentrale Stelle im Bereich der Sicherheit in der Informationstechnik im Hinblick auf die Zusammenarbeit mit den zuständigen Stellen im Ausland.

      17. Aufgaben nach den §§ 8a und 8b als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen."

   d. Folgender Absatz 3 wird angefügt:

„Das Bundesamt kann Betreiber Kritischer Infrastrukturen auf deren Ersuchen bei der Sicherung ihrer Informationstechnik beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen."

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

„§ 4

Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes".

6. § 7 Absatz 1 wird wie folgt geändert:

a. Satz 1 wird wie folgt neu gefasst:

„Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 kann das Bundesamt

1. die folgenden Warnungen an die Öffentlichkeit oder an die betroffenen Kreise richten:

a) Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten,

b) Warnungen vor Schadprogrammen,

c) Warnungen im Falle eines Verlustes von oder eines unerlaubten Zugriffs auf Daten.

2. Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen."

b. Nach Satz 1 wird folgender Satz 2 eingefügt:

„Das Bundesamt kann zur Wahrnehmung der Aufgaben nach Satz 1 Dritte einbeziehen, wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist."

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

„§ 7a

Untersuchung der Sicherheit in der Informationstechnik

„(1) Das Bundesamt darf zur Erfüllung seiner Aufgaben auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte, Systeme und Dienste untersuchen. Es darf sich hierbei der Unterstützung Dritter bedienen.

(2) Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Förderung der IT-Sicherheit genutzt werden.

(3) Das Bundesamt darf seine Bewertung der Sicherheit der untersuchten informationstechnischen Produkte, Systeme und Dienste weitergeben und veröffentlichen. § 7 Absatz 1 Satz 3 und 4 ist entsprechend anzuwenden.“

8. Nach § 8 werden die folgenden §§ 8a bis 8d eingefügt:

„§ 8a

Sicherheit in der Informationstechnik Kritischer Infrastrukturen

(1) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen ihrer 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 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 zur Gewährleistung der Anforderungen nach Absatz 1 vorschlagen. Das Bundesamt stellt im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sowie im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde auf Antrag fest, ob diese geeignet sind, die Anforderungen nach Absatz 1 zu gewährleisten.

(3) Die Betreiber Kritischer Infrastrukturen haben mindestens alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1 auf geeignete Weise nachzuweisen. Der Nachweis kann durch Sicherheitsaudits, Prüfungen oder Zertifizierungen erfolgen. Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Bei Sicherheitsmängeln kann das Bundesamt die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und, soweit erforderlich, im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.

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

(1) Das Bundesamt ist die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit in der Informationstechnik.

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

3. das Lagebild bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen kontinuierlich zu aktualisieren 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 unverzüglich zu unterrichten.

(3) Die Betreiber Kritischer Infrastrukturen haben dem Bundesamt binnen sechs Monaten nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 eine Kontaktstelle als zuständigen Empfangspunkt im Rahmen der Kommunikationsstrukturen nach § 3 Absatz 1 Satz 2 Nummer 15 zu nennen. Die Betreiber haben sicherzustellen, dass sie hierüber jederzeit erreichbar sind. Das Bundesamt übermittelt die Informationen nach Absatz 2 Nummer 4 an diese Kontaktstelle.

(4) Betreiber Kritischer Infrastrukturen haben bedeutende Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der von ihnen betriebenen Kritischen Infrastrukturen führen können, über die Kontaktstelle unverzüglich an das Bundesamt zu melden. Die Meldung muss Angaben zu der Störung sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und zur Branche des Betreibers enthalten. Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Kritischen Infrastruktur geführt hat.

(5) Zusätzlich zu den Kontaktstellen nach Absatz 3 können Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, eine gemeinsame Ansprechstelle benennen. Wurde eine solche benannt, erfolgt der Informationsaustausch zwischen den Kontaktstellen und dem Bundesamt nach

Absatz 2 Nummer 4 und nach Absatz 4 Satz 1 über die gemeinsame Ansprechstelle.

§ 8c

Anwendungsbereich

(1) Die §§ 8a und 8b finden keine Anwendung auf 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).

(2) § 8a findet keine Anwendung auf Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen sowie auf Betreiber von Telematikinfrastrukturen nach § 291a des Sozialgesetzbuchs Fünftes Buch. Entsprechendes gilt für Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes, Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes für den Geltungsbereich der Genehmigung sowie sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften vergleichbare oder weitergehende Anforderungen im Sinne von § 8a erfüllen müssen.

(3) § 8b Absätze 3 bis 5 finden keine Anwendung auf Betreiber Kritischer Infrastrukturen, soweit sie ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen sowie auf Betreiber von Telematikinfrastrukturen nach § 291a des Sozialgesetzbuchs Fünftes Buch. Entsprechendes gilt für Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes sowie sonstige Betreiber Kritischer Infrastrukturen, die auf Grund von Rechtsvorschriften vergleichbare oder weitergehende Anforderungen im Sinne von § 8b Absätze 3 bis 5 erfüllen müssen.

§ 8d

Auskunftsverlangen

(1) Das Bundesamt kann auf Antrag Auskunft zu den im Rahmen von § 8a Absatz 2 und 3 erhaltenen Informationen sowie zu den Meldungen nach § 8b Absatz 4 erteilen, wenn keine schutzwürdigen Interessen des betroffenen Betreibers Kritischer Infrastrukturen dem entgegenstehen und durch die Auskunft keine Beeinträchtigung des Verfahrens oder sonstiger wesentlicher Sicherheitsinteressen zu erwarten ist.

(2) Zugang zu den Akten des Bundesamtes in Angelegenheiten nach § 8a und § 8b wird nur Verfahrensbeteiligten gewährt."

9. § 10 wird wie folgt geändert:

a. Dem Wortlaut wird folgender Absatz 1 vorangestellt:

„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 anhand der in den jeweiligen Sektoren erbrachten Dienstleistungen durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, ab welchem Schwellenwert welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt."

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

c. In Absatz 2 werden nach dem Wort „Rechtsverordnung" die Wörter „, die nicht der Zustimmung des Bundesrates bedarf," eingefügt.

d. In Absatz 3 Satz 2 werden nach dem Wort „Rechtsverordnung“ die Wörter „, die nicht der Zustimmung des Bundesrates bedarf,“ eingefügt.

10. Nach § 12 wird folgender § 13 eingefügt:

„§ 13

Berichtspflichten

(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 in 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 Telemediengesetz 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, § 8 Absatz 1, § 9 und § 10 Absatz 1 haben, soweit dies technisch möglich und zumutbar ist, für geschäftsmäßig in der Regel gegen Entgelt angebotene Telemedien durch technische und organisatorische Vorkehrungen sicherzustellen, dass kein unerlaubter Zugriff auf ihre Telekommunikations- und Datenverarbeitungssysteme möglich ist und diese gegen Verletzungen des Schutzes personenbezogener Daten und Störungen, auch soweit sie durch äußere Angriffe bedingt sind, gesichert sind. Vorkehrungen nach Satz 1 müssen den Stand der Technik berücksichtigen.“

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 und Beseitigen von Störungen sowie von Missbrauch seiner für Zwecke seines Telemedienangebotes genutzten technischen Einrichtungen erheben und verwenden. Eine Verwendung der Daten für andere Zwecke ist unzulässig. Störungen im Sinne des Satz 1 sind nur solche Einwirkungen auf die technischen Einrichtungen, bei denen eine Beeinträchtigung für die Verfügbarkeit, Vertraulichkeit oder Integrität der informationsverarbeitenden Systeme des Diensteanbieters selbst oder der Nutzerinnen und Nutzer des

Telemedienangebotes droht. Werden die Nutzungsdaten für diesen Zweck nicht mehr benötigt, sind diese unverzüglich, spätestens aber nach 6 Monaten zu löschen. Der betroffene Nutzer ist über die Erhebung und Verwendung der Nutzungsdaten zu unterrichten."

3. In § 16 Absatz 2 Nr. 3 wird nach der Angabe „§ 13 Abs. 4 Satz 1 Nr. 1 bis 4 oder 5" die Angabe „oder Abs. 7 Satz 1" eingefügt.

Artikel 3
Änderung des Telekommunikationsgesetzes

Das Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 22 des Gesetzes vom 25. Juli 2014 (BGBl. I S. 1266) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird die Angabe zu § 109a wie folgt gefasst:

   „§ 109a Daten- und Informationssicherheit“.

2. § 100 Absatz 1 wird wie folgt gefasst:

   „(1) Soweit erforderlich, darf der Diensteanbieter die Bestandsdaten und Verkehrsdaten der Teilnehmer und Nutzer erheben und verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder zu beseitigen. Dies gilt auch für Störungen, die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können.“

3. § 109 wird wie folgt geändert:

   a. Nach Absatz 2 wird nach Satz 2 folgender Satz eingefügt:

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

   b. Absatz 5 wird wie folgt gefasst:

   „(5) Wer ein öffentliches Telekommunikationsnetz betreibt oder öffentlich zugängliche Telekommunikationsdienste erbringt, hat der Bundesnetzagentur unverzüglich Beeinträchtigungen von Telekommunikationsnetzen und -diensten mitzuteilen, die zu beträchtlichen Sicherheitsverletzungen einschließlich

Störungen, die zu einer Einschränkung der Verfügbarkeit der über diese Netze erbrachten Dienste oder einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können. Für den Inhalt der Mitteilung an die Bundesnetzagentur gilt § 8b Absatz 4 Satz 2 des BSI-Gesetzes entsprechend. Kommt es zu einer Sicherheitsverletzung im Sinne von Satz 1, die beträchtliche Auswirkungen auf den Betrieb der Telekommunikationsnetze oder das Erbringen von Telekommunikationsdiensten hat, kann die Bundesnetzagentur einen detaillierten Bericht über die Sicherheitsverletzung und die ergriffenen Abhilfemaßnahmen verlangen. Soweit es sich um Sicherheitsverletzungen handelt, die die Informationstechnik betreffen können, leitet die Bundesnetzagentur die eingegangenen Meldungen sowie Informationen zu den ergriffenen Abhilfemaßnahmen unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik weiter. 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 unterrichten 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 Europäischen 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."

c. Absatz 6 Satz 1 wird wie folgt geändert:

aa) Das Wort „Benehmen" wird durch das Wort „Einvernehmen" ersetzt.

bb) Vor den Wörtern „dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit" werden die Wörter „im Benehmen mit" eingefügt.

d. Nach Absatz 7 wird folgender Absatz 8 eingefügt:

„Über aufgedeckte Mängel bei der Erfüllung der maßgeblichen Sicherheitsanforderungen in der Informationstechnik sowie die in diesem Zusammenhang von der Bundesnetzagentur geforderten Abhilfemaßnahmen unterrichtet die Bundesnetzagentur unverzüglich das Bundesamt für Sicherheit in der Informationstechnik."

4. § 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 dem Diensteanbieter Störungen bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen, so hat er die Nutzer, soweit ihm diese bereits bekannt sind, unverzüglich darüber zu benachrichtigen. Soweit technisch möglich und zumutbar, hat er die Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Störungen erkennen und beseitigen können."

c. Der bisherige Absatz 4 wird Absatz 5.

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

„Dies gilt auch dann, wenn der Verpflichtete aufgrund seiner organisatorischen Struktur oder aus rechtlichen Gründen nicht die Gewähr zur Einhaltung der Verpflichtungen des Teils 7 bietet."

Artikel 4
Änderung des Energiewirtschaftsgesetzes

Das Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 6 des Gesetzes vom 21. Juli 2014 (BGBl. I S. 1066) geändert worden ist, wird wie folgt geändert:

1. § 11 wird wie folgt geändert:

a. Absatz 1a wird wie folgt geändert:

aa. In Satz 1 werden nach dem Wort „Datenverarbeitungssysteme“ die Wörter „die der Netzsteuerung dienen“ durch die Wörter „die für einen sicheren Netzbetrieb notwendig sind“ ersetzt.

bb. In Satz 2 wird nach dem Wort „hierzu“ das Wort „grundsätzlich“ eingefügt.

cc. Nach Satz 2 werden folgende Sätze 3 bis 5 eingefügt:

> „Soweit der Bereich der Sicherheit in der Informationstechnik betroffen ist, ist ein Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik herzustellen. Der Katalog der Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Anforderungen. § 8a Absatz 3 des BSI-Gesetzes gilt entsprechend.“

dd. Die bisherigen Sätze 3 bis 5 werden die Sätze 6 bis 8.

ee. In Satz 6 werden die Wörter „wird vermutet“ durch die Wörter „liegt vor“ ersetzt.

ff. Satz 8 wird wie folgt neu gefasst:

> „Zu diesem Zwecke kann die Regulierungsbehörde nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation treffen.“

b. Nach Absatz 1a werden folgende Absätze 1b und 1c eingefügt:

„(1b) Betreiber von Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik als Kritische Infrastruktur bestimmt wurden und an ein Energieversorgungsnetz angeschlossen sind, haben binnen zwei Jahren nach Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik einen angemessenen Schutz gegen Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme, die für einen sicheren Anlagenbetrieb notwendig sind, zu gewährleisten. Die Bundesnetzagentur erstellt hierzu im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik einen Katalog von Sicherheitsanforderungen und veröffentlicht diesen. Soweit die Sicherheitsanforderungen den Bereich der Sicherheit in der Informationstechnik betreffen, ist ein Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik herzustellen. Der Katalog von Sicherheitsanforderungen enthält auch Regelungen zur regelmäßigen Überprüfung der Erfüllung der Anforderungen. Ein angemessener Schutz des Betriebs von Energieanlangen liegt vor, wenn dieser Katalog eingehalten und dies vom Betreiber dokumentiert worden ist. Die Einhaltung kann von der Bundesnetzagentur überprüft werden. Zu diesem Zwecke kann die Regulierungsbehörde nähere Bestimmungen zu Format, Inhalt und Gestaltung der Dokumentation treffen.

(1c) Betreiber von Energieversorgungsnetzen und Betreiber von Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik als Kritische Infrastruktur bestimmt wurden, haben Beeinträchtigungen von Telekommunikations- und elektronischen Datenverarbeitungssystemen, die zu einer Gefährdung oder Störung der Sicherheit oder Zuverlässigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage führen können oder bereits geführt haben, unverzüglich an das Bundesamt für Sicherheit in der Informationstechnik zu melden. Für den Inhalt der Meldung gilt § 8b Absatz 4 Satz 2 des BSI-Gesetzes entsprechend. Die Meldung muss neben Angaben zum Betreiber auch Angaben

zu dem eingesetzten und betroffenen Telekommunikations- oder elektronischen Datenverarbeitungssystems enthalten. Das Bundesamt für Sicherheit in der Informationstechnik leitet die Meldungen unverzüglich an die Bundesnetzagentur weiter. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben sicherzustellen, dass die unbefugte Offenbarung, der ihnen nach Satz 1 zur Kenntnis gelangten Angaben ausgeschlossen wird. Zugang zu den Akten des Bundesamtes für Sicherheit in der Informationstechnik sowie zu den Akten der Bundesnetzagentur nach dieser Vorschrift wird nicht gewährt."

2. § 59 Absatz 1 Satz 2 wird wie folgt geändert:

a. Nach dem Wort „Erstellung“ werden die Wörter „und Überprüfung“ eingefügt.

b. Nach der Angabe „§ 11 Absatz 1a“ wird die Angabe „Satz 2“ durch die Angabe „und 1b“ ersetzt.

Artikel 5
Änderung des Bundeskriminalamtgesetzes

Das Bundeskriminalamtgesetz vom 7. Juli 1997 (BGBl. I S. 1650), das durch Artikel 3 in Verbindung mit Artikel 9 des Gesetzes vom 20. Juni 2013 (BGBl. I S. 1602) geändert worden ist, wird wie folgt geändert:

In § 4 Absatz 1 Satz 1 Nummer 5 werden 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 (IT-Sicherheit) in Deutschland erreicht werden. Die vorgesehenen Neuregelungen dienen dazu, die Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität datenverarbeitender Systeme zu verbessern und die Systeme der IT-Sicherheitslage anzupassen. Ziel des Gesetzes ist eine Verbesserung der IT-Sicherheit bei Unternehmen, ein verstärkter Schutz der Bürgerinnen und Bürger im Internet und in diesem Zusammenhang auch eine Stärkung von Bundesamt für Sicherheit in der Informationstechnik (BSI) und Bundeskriminalamt (BKA). Der Entwurf sieht für Betreiber Kritischer Infrastrukturen die Pflicht zur Einhaltung eines Mindestniveaus an IT-Sicherheit und zur Meldung erheblicher IT-Sicherheitsvorfälle vor. Im Bereich der Telekommunikationsnetzbetreiber werden Zuverlässigkeitsanforderungen eingeführt. Hinzu kommen weitere Pflichten für Telekommunikations- und Telemediendiensteanbieter zum Schutz der Bürgerinnen und Bürger bei ihren Angeboten und den damit einhergehenden Datenverarbeitungsprozessen.

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], Gesundheit [Artikel 74 Absatz 1 Nummer 19 GG] oder Telekommunikation [Artikel 73 Absatz 1 Nummer 7 GG]) und im Übrigen aus der konkurrierenden Gesetzgebungskompetenz für das Recht

der Wirtschaft (Artikel 74 Absatz 1 Nummer 11 GG). Für die Änderung des 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 Energiewirtschaftsgesetzes (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 Einhaltung eines Mindestniveaus an IT-Sicherheit und die Einrichtung und Aufrechterhaltung entsprechender Meldewege einschließlich der in diesem Zusammenhang erforderlichen Anpassungen in den IT-Infrastrukturen. Da relevante

Vorfälle von den Betreibern auch ohne die im Gesetz vorgesehene Meldepflicht behandelt, bewältigt und dokumentiert werden müssen, fallen als Bürokratiekosten nur die Mehraufwände an, die nicht ohnehin im Rahmen einer systematischen Vorfallsbearbeitung durch den Betreiber entstehen.

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 dargestellten Verfahrens erfolgen, da erst durch die Rechtsverordnung der Adressatenkreis der entsprechenden Verpflichtungen hinreichend konkret eingegrenzt werden kann.

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

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

b. Artikel 1, § 8a Absatz 3 Satz 4: Bei Sicherheitsmängeln kann das BSI eine Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse verlangen.

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

d. Artikel 1, § 8b Absatz 4: Die Betreiber Kritischer Infrastrukturen haben bedeutende Störungen 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 grundsätzlich nicht erforderlich ist. Haben diese Störungen jedoch zu einem Ausfall oder einer Beeinträchtigung der Kritischen Infrastrukturen geführt, ist dies dem BSI unverzüglich unter Nennung des Betreibers zu melden.

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

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

3. Erfüllungsaufwand der Verwaltung

Der Erfüllungsaufwand der Verwaltung ist noch Gegenstand von Erörterungen zwischen den Ressorts.

Für die Länder entsteht kein Erfüllungsaufwand.

IV. Weitere Kosten

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

V. Gleichstellungspolitische 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 BSI-Gesetzes)

Zu Nummer 1 (Änderung der Inhaltsangabe)

Die Änderung der Inhaltsangabe ist eine notwendige Folgeänderung.

Zu Nummer 2 (§ 1 Bundesamt für Sicherheit in der Informationstechnik)

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

Zu Nummer 3 (§ 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 Benennung der relevanten Sektoren folgt im Grundsatz der innerhalb der Bundesregierung abgestimmten Einteilung Kritischer Infrastrukturen. Dazu gehören die Bereiche Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie das Finanz- und Versicherungswesen. Zur Umsetzung der in den §§ 8a und 8b des BSI-Gesetzes getroffenen Vorgaben sind innerhalb dieser Sektoren diejenigen Einrichtungen, Anlagen oder Teile davon zu identifizieren, die 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.

Die weitere Konkretisierung bedarf der sektor- und branchenspezifischen Einbeziehung aller betroffenen Kreise (Verwaltung, Wirtschaft und Wissenschaft). Die jeweils anzulegenden Maßstäbe können nur in einem gemeinsamen Arbeitsprozess mit Vertretern der möglicherweise betroffenen Betreiber Kritischer Infrastrukturen und unter Einbeziehung der Expertise von externen Fachleuten in sachgerechter Weise erarbeitet werden. Hinzu kommt, dass der technische und gesellschaftliche Wandel sowie die im Rahmen der Umsetzung der neuen gesetzlichen Vorgaben gemachten Erfahrungen in den Folgejahren gegebenenfalls Anpassungen erforderlich machen. Die nähere Bestimmung der Kritischen Infrastrukturen ist daher gemäß Satz 2 der auf der Grundlage von § 10 Absatz 1 des BSI-Gesetzes 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 11.

Die Kommunikationstechnik von Regierung, Parlament und öffentlicher Bundesverwaltung ist nach Satz 3 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 sind ebenfalls ausgenommen, da der Bund für sie keine Gesetzgebungskompetenz besitzt. Das gleiche gilt für den Sektor Kultur und Medien, da auch hier die Gesetzgebungskompetenz im gegenständlichen Rahmen überwiegend bei den Ländern liegt.

Zu Nummer 4 (§ 3 Aufgaben des Bundesamtes)

Zu Buchstabe a (Zurverfügungstellung gewonnener Erkenntnisse)

Die Änderung in Absatz 1 Satz 2 Nummer 2 dient der Klarstellung, dass durch das BSI bei der Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen gewonnene Erkenntnisse nicht nur Behörden, sondern auch anderen („Dritten“) zur Verfügung gestellt werden können. Hierdurch soll noch einmal der Mehrwert betont werden, den eine verbreitete Erkenntnisbasis und ein verbessertes

Lagebild des BSI für Wirtschaft und Gesellschaft haben können. Dies gilt insbesondere für die Betreiber Kritischer Infrastrukturen im Sinne des BSI-Gesetzes. Adressat sollen aber auch sonstige Einrichtungen oder Unternehmen sein, die zwar keine Betreiber Kritischer Infrastrukturen im Sinne des BSI-Gesetzes sind, dennoch aber anerkannter Maßen zum Bereich der Kritischen Infrastrukturen im weiteren Sinne gehören oder sonst ein berechtigtes Interesse an den entsprechenden Informationen haben (zum Beispiel Einrichtungen aus dem nicht erfassten Sektor Kultur und Medien oder wissenschaftliche Einrichtungen).

Zu Buchstabe b (IT-Sicherheit Kritischer Infrastrukturen)
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 trägt der gewachsenen Rolle des BSI als nationalem und internationalem Ansprechpartner in Fragen der IT- und Cybersicherheit in Deutschland Rechnung. Die Bezugnahme auf die Sicherheit in der Informationstechnik nach § 2 Absatz 2 des BSI-Gesetzes stellt dabei klar, dass die Zuständigkeiten anderer international im Bereich Cybersicherheit aktiver Ministerien und Bundesbehörden (zum Beispiel das Auswärtiges Amt, das Bundesministerium der Verteidigung, das Bundesamt für Verfassungsschutz oder der Bundesnachrichtendienst) unberührt bleiben.

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

Zu Buchstabe d (Aufgaben des Bundesamtes im Bereich der Sicherheit in der Informationstechnik Kritischer Infrastrukturen)
Absatz 3 ermöglicht es dem BSI, Betreiber Kritischer Infrastrukturen auf Ersuchen bei der Sicherung ihrer Informationstechnik, insbesondere im Hinblick auf die Erfüllung der Anforderungen nach den §§ 8a und 8b des BSI-Gesetzes, zu beraten und zu

unterstützen. Das BSI hat nach pflichtgemäßem Ermessen zu entscheiden, ob es einem entsprechenden Ersuchen des Betreibers einer Kritischen Infrastruktur nachkommt.

Zu Nummer 5 (§ 4 Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes)

Die Änderung der Überschrift dient klarstellend der Abgrenzung zur neuen Aufgabe des BSI nach § 8b des BSI-Gesetzes.

Zu Nummer 6 (§ 7 Warnungen)

Zu Buchstabe a (Warnbefugnis)

Die Neufassung von Absatz 1 Satz 1 strukturiert die bereits bestehenden Befugnisse des BSI neu und ergänzt diese um die Befugnis zu Warnungen im Falle eines Verlustes von oder eines unerlaubten Zugriffs auf Daten (Nummer 1 Buchstabe c). Hierdurch wird klargestellt, 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 Abflusses von Daten im Vordergrund steht.

Zu Buchstabe b (Einbeziehung Dritter)

Satz 2 ermöglicht es dem BSI (auch zur Klarstellung unter Datenschutzgesichtspunkten), bei Warnungen auch Dritte einzubeziehen, sofern dies für eine wirksame und rechtzeitige Warnung erforderlich ist. Oftmals wird das BSI abhandengekommene Daten nicht direkt einem Betroffenen zuordnen oder diesen nicht ohne weiteres selbst unterrichten können. Im Interesse einer effizienten Warnung der Betroffenen kann sich das BSI daher an sog. Informationsintermediäre mit der Bitte um Unterstützung wenden, die beispielsweise auf Grund der bei ihnen vorhandenen weitergehenden Informationen oder aus technischen Gründen in der Lage sind, an einer möglichst schnellen Unterrichtung der Betroffenen mitzuwirken.
Informationsintermediäre in diesem Sinne sind insbesondere die von den Kundinnen und Kunden genutzten Provider und Diensteanbieter.

Zu Nummer 7 (§ 7a Untersuchung der Sicherheit in der Informationstechnik)

Absatz 1 dient dazu, Rechtssicherheit für umfassende Untersuchungen von IT-Produkten (z.B. mittels Reverse-Engineering), -Systemen und -Diensten durch das BSI herzustellen. Die gesetzliche Befugnis geht als Spezialgesetz insbesondere den Verboten des Urheberrechtsgesetzes (UrhG) vor und führt dazu, dass die Daten- und Informationsbeschaffung über den Aufbau und die Funktionsweise der Untersuchungsgegenstände nicht als unbefugt im Sinne von § 202a des Strafgesetzbuches (StGB) bzw. § 17 des Gesetzes gegen den Unlauteren Wettbewerb (UWG) anzusehen ist. Auf dem Markt bereitgestellte Untersuchungsgegenstände sind solche, die für einen Erwerb durch das BSI verfügbar sind bzw. vom BSI beschafft werden können. Dies umfasst auch solche Untersuchungsgegenstände, die vom Hersteller bzw. Anbieter angekündigt wurden, aber noch nicht allgemein zum Einsatz kommen. Die Formulierung ist angelehnt an eine entsprechende Formulierung im Produktsicherheitsgesetz. Untersuchungsrechte des BSI bei Herstellern, Anbietern und sonstigen Einrichtungen werden durch Absatz 1 nicht begründet.

Bei der Auswahl der Dritten, die vom BSI mit der Untersuchung beauftragt werden können, hat das BSI die schutzwürdigen Interessen des Herstellers bzw. Anbieters zu berücksichtigen. Hierzu gehört auch die Verpflichtung des Dritten zur Wahrung einer entsprechenden Vertraulichkeit. Die Beauftragung eines direkten Konkurrenten des Herstellers bzw. Anbieters ist in diesem Zusammenhang ausgeschlossen.

Absatz 2 enthält eine Zweckbindung für die aus der Untersuchung nach Absatz 1 gewonnenen Erkenntnisse.

Absatz 3 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 aktuellen 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 3 und 4 wird den berechtigten Schutzinteressen der Hersteller und Rechteinhaber Rechnung getragen. Da Hersteller von Schadsoftware kein berechtigtes

Schutzinteresse haben, soll die Bewertung im Fall von Schadsoftware auch die übrigen Erkenntnisse umfassen können.

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

Zu § 8a (Sicherheit in der Informationstechnik Kritischer Infrastrukturen)

Zweck von Absatz 1 ist der ordnungsgemäße Betrieb Kritischer Infrastrukturen im Sinne des BSI-Gesetzes und die fortlaufende Verfügbarkeit der jeweils angebotenen, in der Rechtsverordnung nach § 10 als kritisch eingestuften Dienstleistungen. Zur Vermeidung von Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse (siehe hierzu § 2 Absatz 2 des BSI-Gesetzes), die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind, sollen branchenspezifische Mindestanforderungen an die IT-Sicherheit zum Schutz der Kritischen Infrastrukturen nach § 2 Absatz 10 des BSI-Gesetzes erfüllt werden. Durch die Erfassung nicht nur der informationstechnischen Systeme, sondern auch der informationstechnischen Komponenten, die darin oder in sonstigen Systemen Verwendung finden, sowie der informationstechnischen Prozesse, also der Vorgänge der Informationsverarbeitung, wird sichergestellt, dass die Betreiber Kritischer Infrastrukturen überall dort Absicherungsmaßnahmen ergreifen müssen, wo Informationstechnik Einfluss auf die Erbringung ihrer kritischen Dienstleistungen hat. Hierfür sind angemessene organisatorische und technische Vorkehrungen zu treffen, zu denen auch infrastrukturelle und personelle Maßnahmen gehören können. Besonders kritische Prozesse bedürfen im Einzelfall besonderer Sicherheitsmaßnahmen durch Abschottung. Mit Blick auf die Erwägungen zu der Erforderlichkeit eines nationalen Routings besonders sensibler IT-Bereiche sollten diese Prozesse etwa weder mit dem Internet oder öffentlichen Netzen verbunden, noch von über das Internet angebotenen Diensten abhängig sein. Das Erfordernis, angemessene organisatorische und technische Vorkehrungen zu treffen, besteht auch dann, wenn der Betreiber seine IT durch einen externen Dienstleister betreiben lässt.

Auf Grund der weitreichenden gesellschaftlichen Auswirkungen ist bei den technischen und organisatorischen Vorkehrungen der Stand der Technik zu berücksichtigen. Stand der Technik in diesem Sinne ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Schutz der Funktionsfähigkeit von informationstechnischen Systemen, Komponenten oder Prozessen gegen Beeinträchtigungen der Verfügbarkeit, Integrität 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. Die Verpflichtung zur Berücksichtigung des Stands der Technik schließt die Möglichkeit zum Einsatz solcher Vorkehrungen nicht aus, die einen ebenso effektiven Schutz wie die anerkannten Vorkehrungen nach dem Stand der Technik bieten.

Bei der Frage der Angemessenheit ist der bei dem Betreiber erforderliche Aufwand, insbesondere die von ihm aufzuwendenden Kosten zu berücksichtigen. Die Mindestanforderungen müssen von den Betreibern in Sicherheits- und Notfallkonzepten niedergelegt werden, um deren Umsetzung zu dokumentieren.

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 Betreiber Kritischer Infrastrukturen 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. Auch die branchenspezifischen Sicherheitsstandards müssen regelmäßig dem sich weiterentwickelnden Stand der Technik angepasst werden.

Die Bewertung und Anerkennung der vorgetragenen Standards soll im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe sowie im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde erfolgen, um die Vereinbarkeit und Koordinierung mit anderen Belangen der Sicherheitsvorsorge zu gewährleisten. Die Differenzierung zwischen einem „Einvernehmen“ mit der zuständigen Aufsichtsbehörde des Bundes und einem „Benehmen“ mit der sonst zuständigen Aufsichtsbehörde berücksichtigt die Rechtsprechung des Bundesverfassungsgerichts, wonach Mitentscheidungsbefugnisse der einen föderalen Ebene bei Entscheidungen der anderen föderalen Ebene mit dem Grundgesetz nicht zu vereinbaren sind („Verbot der Mischverwaltung“). Unabhängig davon soll auch über das Benehmenserfordernis sichergestellt werden, dass die fachliche Expertise der sonstigen Aufsichtsbehörden einbezogen wird.

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

Der Nachweis durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nach Absatz 3 dient der Kontrolle und Überprüfung der getroffenen Maßnahmen nach Absatz 1. Nur so kann sichergestellt werden, dass von dem Betreiber ein angemessenes Sicherheitsniveau zum Schutz seiner Kritischen Infrastrukturen eingehalten wird. Die Ausgestaltung der Sicherheitsaudits, Prüfungen und Zertifizierungen soll nicht im Detail gesetzlich vorgegeben werden, da diese von den gegebenenfalls erarbeiteten branchenspezifischen Mindeststandards, den in den Branchen vorhandenen technischen Gegebenheiten und bereits bestehenden Auditierungs- und Zertifizierungssystemen abhängt. Generell soll geprüft werden, ob der Betreiber die für seine Branche und Technologie geeigneten und wirksamen Maßnahmen und Empfehlungen befolgt, ein Information Security Management (Sicherheitsorganisation, IT-Risikomanagement, etc.) betreibt, kritische Cyber-Assets identifiziert hat und managt, Maßnahmen zur Angriffsprävention und -erkennung betreibt, ein Business Continuity Management (BCM) implementiert hat und darüber hinaus die branchenspezifischen

Besonderheiten (z.B. verankert durch den jeweiligen branchenspezifischen Sicherheitsstandard, sofern ein solcher erstellt und anerkannt wurde) umsetzt.

Die Sicherheitsaudits, Prüfungen oder Zertifizierungen sollen von dazu nachweislich qualifizierten Prüfern bzw. Zertifizierern durchgeführt werden. Bei Zertifizierungen nach internationalen, europäischen oder nationalen Standards kann auf die bestehenden Zertifizierungsstrukturen zurückgegriffen werden. Ein Auditor gilt als qualifiziert, wenn er seine Qualifikation zur Überprüfung der Einhaltung der Mindeststandards gegenüber dem BSI formal glaubhaft machen kann. Denkbar ist in diesem Zusammenhang etwa die Anknüpfung an Zertifizierungen, die für die fachlich-technische Prüfung im jeweiligen Sektor angeboten werden (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 heute u.a. auch die im Rahmen der Jahresabschlussprüfung die für die Rechnungslegung relevanten IT-Systeme.

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

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

§ 8b regelt die Meldungen an das BSI als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen. Die entsprechenden Meldungen sind Voraussetzung für die nationale Handlungsfähigkeit und Grundlage für bundesweit abgestimmte Reaktionen. 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 auch sonstigen 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. Als zentrale Meldestelle sammelt das BSI alle eingehenden Meldungen, erstellt und aktualisiert - unter Einbeziehung seiner sonstigen Erkenntnisse - ein Lagebild und stellt seine Informationen den Betreibern Kritischer Infrastrukturen, den zuständigen Aufsichtsbehörden sowie den sonst zuständigen Behörden in angemessener Form (zum Beispiel konsolidiert, sanitarisiert oder als Rohdatenmaterial) zur Verfügung, soweit Quellen- und Geheimschutz sowie insbesondere die schutzwürdigen Interessen der Betreiber Kritischer Infrastrukturen dies zulassen. Die Betreiber leisten also durch die ihnen obliegende Meldepflicht einen eigenen Beitrag und bekommen dafür, da sie auch von den Meldungen der anderen Betreiber an das BSI und der Bewertung dieser Meldungen durch das BSI profitieren, im Gegenzug ein Mehrfaches an Informationen und Know-how zurück.

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

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

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

Die Störungen sind dann meldepflichtig, wenn sie bedeutend sind. Eine bedeutende Störung liegt vor, wenn die Funktionsfähigkeit des Betreibers oder die von diesem betriebene Kritische Infrastruktur bedroht sind.

Entsprechende Meldungen an das BSI - auch im Vorfeld konkreter Schadenseintritte - sind notwendig, um eine möglichst umfassende und frühzeitige Warnung möglicherweise ebenfalls betroffener Betreiber Kritischer Infrastrukturen zu gewährleisten und darüber hinaus fundierte Aussagen zur IT-Sicherheitslage in Deutschland treffen zu können.

Die namentliche 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 entsprechender Vorfälle Rechnung getragen. Auf die Nennung des Betreibers wird dementsprechend 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 im konkreten Fall eine meldepflichtige

Störung vorliegt oder nicht, im Rahmen der gesetzlichen Vorgaben von den meldepflichtigen Betreibern eine möglichst niedrige Schwelle angelegt werden („im Zweifel Meldung“). Dadurch reduziert sich für die Betreiber der entsprechende Ermittlungsaufwand.

Etwas anderes gilt für bedeutende Störungen der informationstechnischen Systeme, Komponenten oder Prozesse, die bereits konkret zu einem Ausfall oder einer Beeinträchtigung der Kritischen Infrastruktur geführt haben. Diese sind unter Nennung des Betreibers an das BSI zu melden, da im konkreten Schadensfall regelmäßig eine schnelle Krisenreaktion erfolgen muss - insbesondere um ähnliche Vorfälle bei anderen Betreibern noch abwenden zu können. Hierzu muss das BSI gegebenenfalls auch sofort auf den Meldenden zugehen können, um die dafür benötigten Informationen zu erhalten. Aufgrund der Zeitkritikalität und der unmittelbaren Gefährdung der Versorgungssicherheit kann das Interesse der Meldenden, anonym zu bleiben, in diesen Fällen nicht in gleicher Weise berücksichtigt werden wie bei den schadensferneren Vorfällen.

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

Absatz 5 eröffnet klarstellend die Möglichkeit für Betreiber Kritischer Infrastrukturen, die dem gleichen Sektor angehören, ergänzend zu den Kontaktstellen nach Absatz 3 Satz 1 eine gemeinsame Ansprechstelle zu benennen, über die der Informationsaustausch zwischen den Kontaktstellen und dem BSI nach Absatz 2 Nummer 4 und Absatz 4 Satz 1 erfolgen soll. Hierfür können bestehende Strukturen, beispielsweise über die ansonsten im Bereich der Sicherheitsvorsorge zuständigen Aufsichtsbehörden oder die eingerichteten Single Points of Contact (SPOCs) des UP KRITIS, genutzt und erweitert werden. Aus der Wirtschaft wurde vorgetragen, dass ein solches Meldeverfahren wie folgt ausgestaltet werden könnte: Es beginnt mit der verschlüsselten Versendung der

Meldung des betroffenen Betreibers an die gemeinsame Ansprechstelle. Der gemeinsamen Ansprechstelle ist die Identität des Meldenden bekannt, aber durch die Verschlüsselung kann er den Inhalt der Meldung nicht einsehen. In einem nächsten Schritt entfernt die gemeinsame Ansprechstelle die Identität des Betreibers 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 Weg und damit ebenfalls über die gemeinsame Ansprechstelle. Der gesamte Übermittlungsprozess muss vom Ablauf her nachvollziehbar und auch auditierbar sein.

Im konkreten Schadensfall, also in den Fällen nach Absatz 4 Satz 4, erfolgen die Meldungen an das BSI auf Grund der besonderen Dringlichkeit der Informationen direkt über die von den Betreibern benannten Kontaktstellen nach Absatz 3.

Zu § 8c (Anwendungsbereich)

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

Nach § 8c Absatz 1 finden die §§ 8a und 8b des BSI-Gesetzes unter dem Gesichtspunkt der Verhältnismäßigkeit jedoch 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.

Absatz 2 nimmt Unternehmen, die ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, vom Anwendungsbereich des § 8a des BSI-Gesetzes aus. Grund hierfür ist, dass diese mit § 109 des Telekommunikationsgesetzes bereits einer § 8a des BSI-Gesetzes gleichwertigen Regelung unterfallen. Entsprechendes gilt für Betreiber von Energieversorgungsnetzen und Energieanlagen im Sinne des Energiewirtschaftsgesetzes. Eine gleichwertige Regelung enthält auch das Atomgesetz einschließlich der darauf beruhenden Rechtsverordnungen sowie des untergesetzlichen Regelwerks für Genehmigungsinhaber nach § 7 Absatz 1 des Atomgesetzes. Aufgrund der Genehmigungsvoraussetzung des § 7 Absatz 2 Nummer 5 des Atomgesetzes in Verbindung mit den konkretisierenden Regelungen sowie der Aufsicht nach § 19 des Atomgesetzes sind hier ebenfalls gleichwertige Regelungen vorhanden. Im Falle einer Kollision zwischen den Zielen der nuklearen Sicherheit und Sicherung kerntechnischer Anlagen einerseits und der Versorgungssicherheit andererseits ist die nukleare Sicherheit und Sicherung kerntechnischer Anlagen in der Abwägung vorrangig zu berücksichtigen. Ergänzend wird klargestellt, dass - zur Vermeidung unnötiger Doppelregulierungen - auch sonst vergleichbare oder weitergehende Vorgaben in oder auf Grund von Spezialgesetzen nicht berührt werden. Die Regelung normiert insoweit einen allgemeinen Vorrang speziellerer Anforderungen und nimmt damit insbesondere den Fall in den Blick, dass nach Inkrafttreten des Gesetzes in anderen Regelungsbereichen mit § 8a des BSI-Gesetzes bzw. den spezialgesetzlich normierten Regelungsbereichen vergleichbare Regelungen getroffen werden.

Absatz 3 nimmt Unternehmen, die ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, vom

Anwendungsbereich der Absätze 3 bis 5 von § 8b des BSI-Gesetzes aus. Grund hierfür ist, dass diese mit § 109 Absatz 5 des Telekommunikationsgesetzes (neu) einer § 8b Absatz 3 bis 5 des BSI-Gesetzes gleichwertigen Regelung unterfallen. Das gleiche gilt für Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes. Der Meldepflicht unterfallen auch Genehmigungsinhaber nach § 7 Absatz des Atomgesetzes. Ergänzend wird - entsprechend Absatz 2 - klargestellt, dass - zur Vermeidung unnötiger Doppelregulierungen - auch sonst vergleichbare oder weitergehende Vorgaben in oder auf Grund von Spezialgesetzen nicht berührt werden. Die Regelung normiert insoweit einen allgemeinen Vorrang speziellerer Anforderungen und nimmt damit insbesondere den Fall in den Blick, dass nach Inkrafttreten des Gesetzes in anderen Regelungsbereichen mit § 8b des BSI-Gesetzes bzw. den spezialgesetzlich normierten Regelungsbereichen vergleichbare Regelungen getroffen werden.

Zu § 8d (Auskunftsverlangen)

§ 8d regelt abschließend die Auskunft zu Informationen, die im Rahmen von § 8a Absatz 2 und 3 an das BSI übersandt wurden, sowie zu den Meldefällen nach § 8b Absatz 4 unter Berücksichtigung des besonderen schutzwürdigen Interesses der meldepflichtigen Betreiber Kritischer Infrastrukturen an einer vertraulichen Behandlung der von ihnen gemeldeten Informationen. Dies gilt insbesondere in den Fällen der §§ 8a Absatz 3, 8b Absatz 4 Satz 3. Aber auch in den Fällen des § 8b Absatz 4 Satz 1 sind Konstellationen denkbar, bei denen die Auskunft 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 Akten des BSI in Angelegenheiten nach den §§ 8a und 8b des BSI-Gesetzes wird nur Verfahrensbeteiligten gewährt. Bei den Informationen, die das BSI im Rahmen dieser Aufgabe sammelt und analysiert (etwa im Zusammenhang mit der

Erstellung des Lagebildes), handelt es sich um hochsensible, kumulierte sicherheitskritische Informationen, die einem besonders hohen Schutzbedürfnis unterliegen. Die hohe Sicherheitsempfindlichkeit dieser Informationen und deren Risikopotential schließen eine Zugänglichkeit von vornherein aus.

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

Zu Buchstabe a (Kriterien zur Bestimmung der Kritischen Infrastrukturen)

§ 10 Absatz 1 ermächtigt das Bundesministerium des Innern, in Konkretisierung der systemischen Definition Kritischer Infrastrukturen nach § 2 Absatz 10 des BSI-Gesetzes - 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) im Rahmen der Erstellung einer Rechtsverordnung.

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

Unter der Kategorie Qualität wird näher erfasst, welche Dienstleistungen innerhalb der genannten Sektoren in dem Sinne kritisch sind, dass sie von hoher Bedeutung für das Funktionieren des Gemeinwesens sind und durch ihren Ausfall oder ihre Beeinträchtigung nachhaltig wirkende Versorgungsengpässe oder erhebliche 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 könnten jedenfalls sein:

1. SEKTOR ENERGIE
   - Stromversorgung (Branche: Elektrizität)
   - Versorgung mit Erdgas (Branche: Gas)
   - Versorgung mit Mineralöl (Branche: Mineralöl)

2. SEKTOR INFORMATIONSTECHNIK UND TELEKOMMUNIKATION
   - Sprach- und Datenkommunikation (Branchen: Telekommunikation, Informationstechnik)
   - Verarbeitung und Speicherung von Daten (Branche: Informationstechnik)

3. SEKTOR TRANSPORT UND VERKEHR
   - Transport von Gütern (Branchen: Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik)
   - Transport von Personen im Nahbereich (Branchen: Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik)
   - Transport von Personen im Fernbereich (Branchen: Luftfahrt, Seeschifffahrt, Binnenschifffahrt, Schienenverkehr, Straßenverkehr, Logistik)

4. SEKTOR GESUNDHEIT
   - Medizinische Versorgung (Branchen: Medizinische Versorgung, Labore)

- Versorgung mit Arzneimitteln und Medizinprodukten (Branchen: Medizinische Versorgung, Labore, Arzneimittel und Impfstoffe)

5. SEKTOR WASSER

- Trinkwasserversorgung (Branche: Öffentliche Wasserversorgung)
- Abwasserbeseitigung (Branche: Öffentliche Abwasserbeseitigung)

6. SEKTOR ERNÄHRUNG

- Versorgung mit Lebensmitteln (Branchen: Ernährungswirtschaft, Lebensmittelhandel)

7. SEKTOR FINANZ- UND VERSICHERUNGSWESEN

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

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

Zu Buchstabe b (Folgeänderung)

Buchstabe b enthält eine notwendige Folgeänderung.

Zu Buchstaben c und d (Fehlende Zustimmungsbedürftigkeit)

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

Zu Nummer 10 (§ 13 Berichtspflichten)

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

Die gesetzliche Etablierung einer Berichtspflicht und die vorgesehene Veröffentlichung eines Jahresberichts nach Absatz 2 dienen der Sensibilisierung der Öffentlichkeit für das Thema IT-Sicherheit. Da eine Vielzahl von Cyberangriffen bereits durch Basismaßnahmen abgewehrt werden könnte, spielt die Aufklärung und Sensibilisierung der Öffentlichkeit eine zentrale Rolle für die Erhöhung der IT-Sicherheit in Deutschland.

Zu Artikel 2 (Änderung des Telemediengesetzes)

Zu Nummer 1 (§ 13 Pflichten des Diensteanbieters)

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

Wegen der zunehmenden Verbreitung von Schadsoftware über Telemediendienste werden die bestehenden Pflichten für Telemediendiensteanbieter im Sinne von § 7 Absatz 1, § 8 Absatz 1, § 9 und § 10 Absatz 1 des Telemediengesetzes, die ihre Telemedien geschäftsmäßig und in der Regel gegen Entgelt anbieten, um technische und organisatorische Schutzmaßnahmen zur Gewährleistung von IT-Sicherheit der für Dritte angebotenen Inhalte ergänzt. Adressiert werden damit Contentprovider, die eigene Inhalte publizieren, Network-Provider, die fremde Informationen in einem Kommunikationsnetz übermitteln, Access-Provider, die den Zugang zur Nutzung vermitteln, sowie Hostprovider, die fremde Informationen für Nutzerinnen und Nutzer speichern. Daneben wird über § 9 auch das sog. Caching, also die zeitlich begrenzte Zwischenspeicherung fremder Informationen zur beschleunigten Übermittlung, erfasst.

Geschäftsmäßig ist ein Angebot dann, wenn es auf einer nachhaltigen Tätigkeit beruht, es sich also um eine planmäßige und dauerhafte Tätigkeit handelt. Weitere Voraussetzung ist, dass es sich um einen Dienst handelt, der „in der Regel gegen Entgelt“ angeboten wird. Hierfür gelten die allgemeinen Grundsätze, so dass von einer Entgeltlichkeit grundsätzlich auch bei werbefinanzierten Webseiten auszugehen ist, sofern hierüber entsprechende Einnahmen erzielt werden. Das nicht-kommerzielle Angebot von Telemedien durch Private und Idealvereine wird demgegenüber nicht erfasst.

Die betreffenden Diensteanbieter haben durch technische und organisatorische Vorkehrungen, die den Stand der Technik berücksichtigen, sicherzustellen, dass kein unerlaubter Zugriff auf ihre Telekommunikations- und Datenverarbeitungssysteme möglich ist und diese gegen Verletzungen des Schutzes personenbezogener Daten und Störungen (vgl. hierzu § 15 Absatz 9 Satz 3) gesichert sind. Voraussetzung ist, dass die entsprechenden Vorkehrungen für den konkreten Diensteanbieter technisch möglich und zumutbar sind. Durch das Kriterium der Zumutbarkeit wird sichergestellt, dass von

dem Diensteanbieter nur solche Vorkehrungen zu treffen sind, die in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck stehen. Dies ermöglicht eine flexible Anpassung der jeweiligen Anforderungen im Einzelfall.

Hiermit soll u.a. 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.

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

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

Zu Nummer 2 (§ 15 Nutzungsdaten)

Die Regelung ermächtigt die Anbieter von Telemedien, Nutzungsdaten auch zum [Erkennen,] Eingrenzen oder Beseitigen von Störungen sowie von einem Missbrauch ihrer für Zwecke ihres Dienstes genutzten technischen Einrichtungen zu erheben und zu

verwenden. Eine Verwendung der Daten für andere Zwecke ist gemäß Satz 2 unzulässig.

Satz 3 definiert den Begriff der Störungen im Sinne des Telemediengesetzes. Störungen sind danach nur solche Einwirkungen auf die technischen Einrichtungen, bei denen eine Beeinträchtigung für die Verfügbarkeit, Vertraulichkeit oder Integrität der informationsverarbeitenden Systeme des Diensteanbieters selbst oder der Nutzerinnen und Nutzer des Telemedienangebotes droht. 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.

Ziel der Regelung ist es, Diensteanbietern die Möglichkeit zu geben, eine Infektion der von ihnen angebotenen Telemedien mit Schadprogrammen abwehren zu können. IT-Sicherheitskonzepte sehen in der Praxis eine gestufte Absicherung vor. Das bedeutet, dass nicht nur auf dem Webserver selbst Absicherungsmaßnahmen ergriffen werden, sondern dem Server z.B. auch ein sog. Intrusion-Detection-System vorgeschaltet wird, um ein versuchtes Eindringen in den Server rechtzeitig zu bemerken und dieses gegebenenfalls auch automatisch verhindern zu können.

Hier bestand bislang eine Lücke im Bereich der Erlaubnistatbestände des Telemediengesetzes, beispielsweise um Angriffe (Denial of Service, Schadprogramme, Veränderung ihrer Werbeangebote von außerhalb) abwehren zu können. Dabei ist auch eine Weiterentwicklung der Angriffsmethoden zu berücksichtigen.

Gerade bei Telemedienangeboten beziehen sich Cyberangriffe oftmals auf einen Missbrauch der dem Telemedienangebot zugrundeliegenden Technik. Insbesondere das Einbrechen in Server und der anschließende Diebstahl z.B. von Kundendaten, wie in der Vergangenheit immer häufiger geschehen, wäre unter dem Begriff der "Störung" nicht mehr subsumierbar. Das Gesetz trägt dem durch eine Erweiterung um die Fallgruppe des Missbrauchs Rechnung.

Zur Durchführung von Angriffen werden neuerdings verstärkt auch manipulierte Webseiten genutzt. Für die Anbieter von Telemediendiensten bedeutet dies, dass sich auch die zu verfolgenden IT-Sicherheitsziele verändert haben. Die Anbieter müssen ihre Systeme nicht nur zum Selbstschutz gegen Manipulationen, Hacking oder Verfügbarkeitsangriffen schützen, sondern ihre Systeme auch gegen solche Angriffe härten, die ihre Systeme nur als Zwischenstation für Angriffe auf die Nutzerinnen und Nutzer der Dienste oder Dritte missbrauchen.

Der Anbieter muss auf Anforderung der für den Datenschutz zuständigen Stellen nachweisen können, dass er die nach diesem Absatz erhobenen Daten tatsächlich nur für die in Satz 1 genannten Zwecke erhebt und verwendet. Ein entsprechender Nachweis kann beispielsweise durch ein Datenschutzkonzept erbracht werden, aus dem hervorgeht, welche technischen und organisatorischen Maßnahmen ergriffen werden, um eine Verwendung zu anderen Zwecken auszuschließen.

Die Sätze 4 und 5 entsprechen den in Absatz 8 Sätze 2 und 3 getroffenen Regelungen.

Zu Nummer 3 (§ 16 Bußgeldvorschriften)

Die Aufnahme eines Verstoßes gegen die in § 13 Absatz 7 Satz 1 geregelte Pflicht des Diensteanbieters zum Einsatz technischer und organisatorischer Schutzmaßnahmen zur Gewährleistung von IT-Sicherheit der für Dritte angebotenen Inhalte in die Bußgeldvorschriften des § 16 Absatz 2 Nr. 3 entspricht der Bußgeldbewährung eines Verstoßes gegen die weiteren in § 13 Absatz 4 geregelten Pflichten des Diensteanbieters. Bußgeldbewährt ist damit auch der Einsatz technischer und organisatorischer Maßnahmen durch den Diensteanbieter, die nicht den Stand der Technik berücksichtigen.

Zu Artikel 3 (Änderung des Telekommunikationsgesetzes)

Zu Nummer 1 (Änderung der Inhaltsangabe)

Nummer 1 enthält eine notwendige Folgeänderung.

Zu Nummer 2 (§ 100 Absatz 1 Störungen von Telekommunikationsanlagen und Missbrauch von Telekommunikationsdiensten)

Die Änderung dient der Klarstellung, dass 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 3 (§ 109 Technische Schutzmaßnahmen)

Zu Buchstabe a (Berücksichtigung des Stands der Technik)

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

Auf Grund der hohen Bedeutung für die Kommunikation des Einzelnen und die dadurch bedingte Verletzlichkeit der Gesellschaft insgesamt, müssen auch zum Schutz gegen unerlaubte Zugriffe auf die Telekommunikations- und Datenverarbeitungssysteme Maßnahmen getroffen werden, die den Stand der Technik berücksichtigen. Angriffe auf die Systeme erfolgen zunehmend auf höchstem technischen Niveau unter Ausnutzung öffentlich noch nicht bekannter Lücken in der Sicherheitsarchitektur von Hardware- und Software-Produkten. Durch diese Angriffe werden die Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität datenverarbeitender Systeme bedroht. Mit der

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

Zu Buchstabe b (Meldepflichten)

Die bestehenden Meldepflichten werden um die Verpflichtung ergänzt, bekannt gewordene Vorfälle zu melden, die zu erheblichen Sicherheitsverletzungen von datenverarbeitenden Systemen der Endnutzer führen können. Über die bestehenden Meldeverpflichtungen im Bereich des Datenschutzes hinaus 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. 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 in diesem Stadium allerdings noch nicht gegen die Verfügbarkeit der Netze insgesamt, sondern die Funktionsfähigkeit und Verlässlichkeit der IT einzelner Nutzerinnen und Nutzer richtet und ggf. spätere schwerwiegende Folgen nach sich zieht.

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

Die bei der Bundesnetzagentur 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 Buchstabe c (Erstellung eines Sicherheitskataloges)

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 („Einvernehmen“ statt „Benehmen“) wird diesem Erfordernis Rechnung getragen.

Zu Buchstabe d (Übermittlung der Auditergebnisse an das BSI)

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

Zu Nummer 4 (§ 109a Daten- und Informationssicherheit)

Zu Buchstabe a (Änderung der Überschrift)

Buchstabe a enthält eine redaktionelle Folgeänderung und trägt dem erweiterten Regelungsbereich Rechnung.

Zu Buchstabe b (Information der Nutzerinnen und Nutzer)

Die Neuregelung soll die Information der Nutzerinnen und Nutzer über Verletzungen der IT-Sicherheit gewährleisten, die von einem von ihnen betriebenen datenverarbeitenden System ausgehen. Derzeit wird eine entsprechende Information der Nutzerinnen und Nutzer bei den einzelnen Providern uneinheitlich gehandhabt. Die Information soll Nutzerinnen und Nutzer in die Lage versetzen, selbst Maßnahmen gegen die auf ihren Systemen vorhandene Schadsoftware zu ergreifen. Durch den Einschub „soweit ihm diese bereits bekannt sind“, wird klargestellt, dass Verkehrsdaten zur Ermittlung der Nutzerinnen und Nutzer nur im Rahmen von § 100 Absatz 1 erhoben werden dürfen.

Hierfür ist Voraussetzung, dass die Nutzerinnen und Nutzer über angemessene Werkzeuge verfügen, um entsprechende Schutzmaßnahmen ergreifen zu können. Ergänzend zur Informationspflicht werden die Anbieter von Telekommunikationsdiensten für die Öffentlichkeit deshalb verpflichtet, die Nutzerinnen und Nutzer auf einfach bedienbare Sicherheitswerkzeuge hinzuweisen, die sowohl vorbeugend als auch zur

Beseitigung von Störungen im Falle einer bereits erfolgten Infizierung des Datenverarbeitungssystems mit Schadsoftware eingesetzt werden können. Nicht erforderlich ist insoweit eine individuelle Untersuchung der Technik oder eine individuelle Beratung durch den Anbieter. Die Informations- und Hinweispflicht kann beispielsweise über eine entsprechende Umleitung der betroffenen Nutzerinnen und Nutzer auf eine Hinweisseite realisiert werden, sofern die tatsächlich betroffenen Nutzerinnen und Nutzer und nicht nur die Kundinnen und Kunden des Anbieters erreicht werden sollen. Soweit dies technisch nicht möglich ist, werden die Anbieter nur ihre Kundinnen und Kunden informieren und auf Hilfsmittel hinweisen können, da die Endnutzerinnen bzw. Endnutzer für sie in der Regel nicht ermittelbar sein werden. Auf die Barrierefreiheit der angebotenen Sicherheitswerkzeuge ist besonders zu achten.

Zu Nummer 5 (§ 115 Absatz 3 Satz 2 Zuverlässigkeit)

Die Regelung ergänzt die Befugnisse der Bundesnetzagentur nach den Absätzen 1 bis 3 dahingehend, dass auch die fehlende Gewähr eines mit sicherheitskritischen Aufgaben betrauten Unternehmens zur Einhaltung der Verpflichtungen nach Teil 7 zu einer vollständigen oder teilweisen Untersagung des Betriebs der betreffenden Telekommunikationsanlage oder des geschäftsmäßigen Erbringens des betreffenden Telekommunikationsdienstes berechtigt. Dies kann dann Fall sein, wenn die organisatorische Struktur eines Unternehmens oder die für ein Unternehmen geltenden Rechtsvorschriften die Annahme rechtfertigen, dass mit der Dienstleistungserbringung Angriffe auf die Vertraulichkeit, Integrität und Verfügbarkeit der übertragenen Kommunikation verbunden sind.

Werden die Dienste von dem Verpflichteten einem zur Erfüllung seiner Verpflichtungen beauftragten Dritten (etwa im Rahmen eines Outsourcings) übertragen, ist sicherzustellen, dass auch der Dritte die entsprechenden Anforderungen an die Gewähr zur Einhaltung der Verpflichtungen nach Teil 7 bietet.

Zu Artikel 4 (Änderung des Energiewirtschaftsgesetzes)

Zu Nummer 1 (§ 11 Betrieb von Energieversorgungsnetzen)

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

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

Zu Buchstabe bb (Folgeänderung)
Folgeänderung zur Änderung unter Buchstabe c.

Zu Buchstabe cc (Katalog der Sicherheitsanforderungen)
Soweit der Bereich der Sicherheit in der Informationstechnik betroffen ist, ist - abweichend von dem ansonsten bei der Erstellung des Sicherheitskataloges geltenden Benehmenserfordernis - ein Einvernehmen mit dem BSI herzustellen. Dadurch wird die Berücksichtigung der fachlichen Expertise des BSI in Fragen der Sicherheit in der Informationstechnik gewährleistet.

Der Sicherheitskatalog der Bundesnetzagentur nach Satz 2 enthält Vorschriften zu Zertifizierungen und regelmäßigen Überprüfungen der Schutzmaßnahmen in den Unternehmen. Entsprechend § 8a Absatz 3 des BSI-Gesetzes sind die Überprüfungen mindestens alle zwei Jahre durchzuführen. Nach Satz 4 ist die Regulierungsbehörde verpflichtet, die Überprüfungen von den Betreibern zu fordern. Die Änderung trägt dem in § 8a des BSI-Gesetzes etablierten Schutzniveau Rechnung und verhindert, dass der Sicherheitskatalog der Bundesnetzagentur hinter dieses Schutzniveau zurückfällt.

Zu Buchstabe dd (Folgeänderung)
Buchstabe d. enthält eine notwendige Folgeänderung.

Zu Buchstabe ee (Bedeutung des Sicherheitskataloges)

Bislang wird ein angemessener Schutz der Telekommunikations- und Datenverarbeitungssysteme vermutet, wenn die Netzbetreiber die Anforderungen des Sicherheitskataloges erfüllen. Soweit ein Betreiber nachweisen kann, dass seine Maßnahmen einen ebenfalls angemessenen Schutz gewähren, kann er von dem Sicherheitskatalog abweichen. Mit der Formulierung „liegt zumindest dann vor“ bekommen die Vorgaben des Sicherheitskataloges ein noch größeres Gewicht. Ein angemessener Schutz der Telekommunikations- und Datenverarbeitungssysteme liegt immer dann vor, wenn die Anforderungen des Sicherheitskataloges erfüllt sind. Damit bleibt grundsätzlich kein Spielraum mehr für die Betreiber, andere aus ihrer Sicht angemessene Schutzmaßnahmen zu erarbeiten. Der Sicherheitskatalog der Bundesnetzagentur stellt einen Mindeststandard dar, der von den Betreibern einzuhalten ist.

Zu Buchstabe ff (Konzentration auf der Fachebene)

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

Zu Buchstabe b (Sicherheitskatalog und Meldepflicht)

Mit Absatz 1b wird eine neue Vorschrift eingefügt, mit der die Betreiber von Energieanlagen, die als Kritische Infrastruktur bestimmt wurden, adressiert werden. Die Aufnahme von Schutzstandards für Energieanlagen, die gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, ist notwendig, um einen umfassenden Schutz für den Netzbetrieb sicherstellen zu können. Energieanlagen, die mit dem öffentlichen Versorgungsnetz verbunden sind, sollen verpflichtet sein, dort, wo eine Gefährdung für den Netzbetrieb möglich ist, ebenfalls Sicherheitsmaßnahmen zu ergreifen. Aufgrund der technischen Nähe ist es notwendig und sinnvoll, dass die Sicherheitsstandards für Netzbetreiber und für die betroffenen Energieanlagen aufeinander abgestimmt sind. Aus diesem Grund wird die Bundesnetzagentur als für die Sicherheitsstandards des Netzbetriebs zuständige Behörde beauftragt, auch die Sicherheitsstandards für die Energieanlagen zu erarbeiten und deren Einhaltung zu überwachen. Absatz 1b entspricht insoweit Absatz 1a.

Mit Absatz 1c wird für Betreiber Kritischer Infrastrukturen eine Meldepflicht an das BSI eingeführt. Gemäß § 8b Absatz 1 des BSI-Gesetzes ist das BSI die zentrale Meldestelle für Betreiber Kritischer Infrastrukturen in Angelegenheiten der Sicherheit der informationstechnischen Systeme, Komponenten oder Prozesse. Die Einrichtung einer solchen zentralen Stelle ist sinnvoll, um Wissen und Erfahrungen bestmöglich zu bündeln. Damit Sicherheitsprobleme aus dem Energiesektor ebenfalls in dieses „Kompetenzzentrum“ einfließen können, sieht Absatz 1c vor, dass Beeinträchtigungen von Telekommunikations- und elektronischen Datenverarbeitungssystemen, die zu einer Gefährdung oder Störung der Sicherheit oder Zuverlässigkeit des Energieversorgungsnetzes oder der betreffenden Energieanlage führen können oder bereits geführt haben, unverzüglich an das BSI zu melden sind. Entsprechende Meldungen an das BSI - auch im Vorfeld konkreter Schadenseintritte - sind notwendig, um eine möglichst umfassende und frühzeitige Warnung möglicherweise ebenfalls betroffener Betreiber Kritischer Infrastrukturen zu gewährleisten und darüber hinaus fundierte Aussagen zur IT-Sicherheitslage in Deutschland treffen zu können. Umgekehrt ist das BSI nach § 8b Absatz 2 des BSI-Gesetzes verpflichtet, auch die Betreiber von Netzen oder Energieanlagen im Sinne von Absatz 1a und 1b über Sicherheitsvorfälle zu informieren. Das besondere Interesse der Meldeverpflichteten an einer vertraulichen Behandlung der von ihnen gemeldeten Informationen wird berücksichtigt. Die hochsensiblen sicherheitskritischen Informationen unterliegen einem besonderen Schutzbedürfnis.

Zu Nummer 2 (§ 59 Absatz 1 Organisation)

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

Zu Artikel 5 (Änderung des Bundeskriminalamtgesetzes)

Zusätzlich zu den Fällen, in denen sich die Straftat nach § 303b StGB (Computersabotage) 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 einer entsprechenden Straftat gegen Bundeseinrichtungen gegeben ist. Bisher liegt die Zuständigkeit für die polizeilichen Aufgaben der Strafverfolgung in der Regel bei den Ländern, wobei die örtliche Zuständigkeit abhängig davon ist, 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.