Deutscher Bundestag **Drucksache 18/5121**

18. Wahlperiode 10.06.2015

Beschlussempfehlung und Bericht

des Innenausschusses (4. Ausschuss)

zu dem Gesetzentwurf der Bundesregierung
– Drucksache 18/4096 –

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

A. Problem

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

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

Mit dem Gesetz soll eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme (IT-Sicherheit) in Deutschland erreicht werden. Die vorgesehenen Neuregelungen dienen dazu, den Schutz der Systeme im Hinblick auf die Schutzgüter der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität) zu verbessern, um den aktuellen und zukünftigen Gefährdungen der IT-Sicherheit wirksam begegnen zu können. Ziel des Gesetzes sind die Verbesserung der IT-Sicherheit von Unternehmen, der verstärkte Schutz der Bürgerinnen und Bürger im Internet und in diesem Zusammenhang auch die Stärkung von BSI und Bundeskriminalamt (BKA).

Besondere Bedeutung kommt im Bereich der IT-Sicherheit denjenigen Infrastrukturen zu, die für das Funktionieren unseres Gemeinwesens zentral sind. Der Schutz der IT-Systeme von solchen Kritischen Infrastrukturen und der für den

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

B. Lösung

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

Um den Schutz der Bürgerinnen und Bürger zu verbessern, werden die Telekommunikationsanbieter, die eine Schlüsselrolle für die Sicherheit des Cyberraums haben, verpflichtet, IT-Sicherheit nach dem Stand der Technik nicht nur zum Schutz des Fernmeldegeheimnisses und zum Schutz personenbezogener Daten, sondern auch im Hinblick auf die Verfügbarkeit ihrer Telekommunikations- und Datenverarbeitungssysteme zu gewährleisten. Die Umsetzung der zugrunde liegenden IT-Sicherheitskonzepte in den Unternehmen wird von der Bundesnetzagentur regelmäßig überprüft. Damit werden die Widerstandsfähigkeit der Kommunikationsinfrastruktur insgesamt verbessert und die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit datenverarbeitender Systeme sowie der dort vorgehaltenen Daten gesichert. Mittelbar steigt so auch die Verantwortung der Hersteller zum Angebot entsprechender Produkte.

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

Da eine Vielzahl von IT-Angriffen bereits durch die Umsetzung von Standardsicherheitsmaßnahmen abgewehrt werden könnte, leistet eine verstärkte Sensibilisierung der Nutzerinnen und Nutzer durch die im Gesetz vorgesehene Aufklärung der Öffentlichkeit durch einen jährlichen Bericht einen wichtigen Beitrag zur Verbesserung der IT-Sicherheit. Die gewachsene Rolle des BSI als nationale zentrale Stelle für IT-Sicherheit gegenüber ausländischen Staaten wird festgeschrieben, der Anteil des BSI an der Erstellung des Sicherheitskatalogs für Telekommunikationsnetzbetreiber ausgebaut. Begleitend dazu wird das BKA im Bereich Cyber-

kriminalität 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.

Annahme des Gesetzentwurfs in geänderter Fassung mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN.

C. Alternativen

Vorlage eines Gesetzentwurfs auf Grundlage des Entschließungsantrags auf Ausschussdrucksache 18(4)327.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

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

Betreibern Kritischer Infrastrukturen entsteht Erfüllungsaufwand für

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

Genehmigungsinhabern nach dem Atomgesetz entsteht Erfüllungsaufwand für

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

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

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

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

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

Telemediendiensteanbietern entsteht Erfüllungsaufwand für

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

Betreibern öffentlicher Telekommunikationsnetze und öffentlich zugänglicher Telekommunikationsdienste entsteht Erfüllungsaufwand für

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

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

Der jährliche Erfüllungsaufwand der Wirtschaft für das Meldeverfahren ergibt sich aus

- der Anzahl der meldepflichtigen Unternehmen,
- der Anzahl der meldepflichtigen Vorfälle pro Jahr und pro Unternehmen sowie
- dem Aufwand pro Meldung.

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

Nach aktuellen Schätzungen wird die Zahl der meldepflichtigen Betreiber Kritischer Infrastrukturen bei maximal 2.000 Betreibern liegen. Weiterhin wird geschätzt, dass pro Betreiber maximal sieben Meldungen von IT-Sicherheitsvorfällen pro Jahr erfolgen. Da relevante IT-Sicherheitsvorfälle von den Betreibern auch ohne die im Gesetz vorgesehene Meldepflicht untersucht, bewältigt und dokumentiert werden müssen, fällt bei den Bürokratiekosten nur insoweit ein Mehr-

aufwand an, als die Bearbeitung über die ohnehin im Rahmen einer systematischen Bearbeitung relevanten Vorfälle hinausgeht. Auf Grund von Angaben aus der Wirtschaft auf der Grundlage von Berechnungen nach dem Standardkostenmodell werden die Kosten für die Bearbeitung einer Meldung derzeit mit 660 Euro pro Meldung (11 Stunden Zeitaufwand bei einem Stundensatz von 60 Euro) beziffert. Zum Teil werden solche Vorfälle schon heute dem BSI gemeldet.

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

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

E.3 Erfüllungsaufwand der Verwaltung

Schon heute werden den zuständigen Behörden IT-Sicherheitsvorfälle gemeldet.

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

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

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

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

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

Weiteren entstehen Kosten für Sachmittel in Höhe von maximal 610 000 Euro jährlich.

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

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

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

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

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

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

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

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.

Beschlussempfehlung

Der Bundestag wolle beschließen,

den Gesetzentwurf auf Drucksache 18/4096 mit folgenden Maßgaben, im Übrigen unverändert, anzunehmen:

1. Artikel 1 wird wie folgt geändert:

a) Nach Nummer 4 wird folgende Nummer 4a eingefügt:

‚4a. § 5 Absatz 1 wird wie folgt geändert:

a) Satz 4 wird wie folgt gefasst:

„Die Bundesbehörden sind verpflichtet, das Bundesamt bei Maßnahmen nach Satz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu behördeninternen Protokolldaten nach Satz 1 Nummer 1 sowie Schnittstellendaten nach Satz 1 Nummer 2 sicherzustellen.“

b) Nach Satz 4 wird folgender Satz eingefügt:

„Protokolldaten der Bundesgerichte dürfen nur in deren Einvernehmen erhoben werden.“ ‘

b) In Nummer 6 wird Absatz 2 wie folgt geändert:

„(2) Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14 und 17 genutzt werden. Das Bundesamt darf seine Erkenntnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung dieser Aufgaben erforderlich ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben.“

c) Nach Nummer 6 wird folgende Nummer 6a eingefügt:

‚6a. § 8 Absatz 1 wird wie folgt gefasst:

„(1) Das Bundesamt erarbeitet Mindeststandards für die Sicherheit der Informationstechnik des Bundes. Das Bundesministerium des Innern kann im Benehmen mit dem IT-Rat diese Mindeststandards ganz oder teilweise als allgemeine Verwaltungsvorschriften für alle Stellen des Bundes erlassen. Das Bundesamt berät die Stellen des Bundes auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards. Für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach diesem Absatz empfehlenden Charakter.“ ‘

d) Nummer 7 wird wie folgt geändert:

aa) § 8a wird wie folgt geändert:

aaa) Absatz 1 Satz 2 wird wie folgt gefasst:

„Dabei soll der Stand der Technik eingehalten werden.“

bbb) Absatz 3 Satz 4 wird wie folgt gefasst:

„Das Bundesamt kann bei Sicherheitsmängeln verlangen:

1. die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und
2. im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel.“

ccc) Nach Absatz 3 wird folgender Absatz 4 eingefügt:

„(4) Das Bundesamt kann zur Ausgestaltung des Verfahrens der Sicherheitsaudits, Prüfungen und Zertifizierungen nach Absatz 3 Anforderungen an die Art und Weise der Durchführung, an die hierüber auszustellenden Nachweise sowie fachliche und organisatorische Anforderungen an die prüfende Stelle nach Anhörung von Vertretern der betroffenen Betreiber und der betroffenen Wirtschaftsverbände festlegen.“

bb) § 8b wird wie folgt geändert:

aaa) Absatz 4 Satz 1 und 2 werden wie folgt gefasst:

„Betreiber Kritischer Infrastrukturen haben erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen

1. führen können oder
2. geführt haben,

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, der Art der betroffenen Einrichtung oder Anlage sowie zur Branche des Betreibers enthalten.“

bbb) Nach Absatz 5 wird folgender Absatz 6 eingefügt:

„(6) Soweit erforderlich kann das Bundesamt vom Hersteller der betroffenen informationstechnischen Produkte und Systeme die Mitwirkung an der Beseitigung oder Vermeidung einer Störung nach Absatz 4 verlangen. Satz 1 gilt für Störungen bei Betreibern und Genehmigungsinhabern im Sinne von § 8c Absatz 3 entsprechend.“

ccc) Der bisherige Absatz 6 wird Absatz 7.

cc) In § 8c Absatz 2 Nummer 4 werden die Wörter „Betreiber Kritischer Infrastrukturen, die“ durch die Wörter „Betreiber Kritischer Infrastrukturen, soweit sie“ ersetzt.

e) In Nummer 8 Buchstabe a wird nach Satz 1 folgender Satz eingefügt:

„Der nach Satz 1 als bedeutend anzusehende Versorgungsgrad ist anhand von branchenspezifischen Schwellenwerten für jede wegen ihrer Bedeutung als kritisch anzusehende Dienstleistung im jeweiligen Sektor zu bestimmen.“

f) Nummer 9 wird wie folgt geändert:

aa) Die Wörter „Folgender § 13 wird“ werden durch die Wörter „Die folgenden §§ 13 und 14 werden“ ersetzt.

bb) Nach § 13 wird folgender § 14 angefügt:

„§ 14

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 8a Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine dort genannte Vorkehrung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig trifft,
2. einer vollziehbaren Anordnung nach § 8a Absatz 3 Satz 4
   a) Nummer 1 oder
   b) Nummer 2

   zuwiderhandelt,
3. entgegen § 8b Absatz 3 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine Kontaktstelle nicht oder nicht rechtzeitig benennt oder
4. entgegen § 8b Absatz 4 Satz 1 Nummer 2 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht.

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 2 Buchstabe b mit einer Geldbuße bis zu hunderttausend Euro, in den übrigen Fällen des Absatzes 1 mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.

(3) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist das Bundesamt.“

2. In Artikel 2 wird in § 44b Satz 2 die Angabe „6“ durch die Angabe „7“ ersetzt.
3. In Artikel 5 Nummer 5 werden die Wörter „eine Beeinträchtigung von Telekommunikationsnetzen oder -diensten, die zu einer beträchtlichen Sicherheitsverletzung führt, nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig mitteilt“ durch die Wörter „eine Mitteilung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht“ ersetzt.
4. Nach Artikel 9 wird folgender Artikel 10 eingefügt:

„Artikel 10

Evaluierung

Artikel 1 Nummern 2, 7 und 8 sind vier Jahre nach Inkrafttreten der Rechtsverordnung nach Artikel 1 Nummer 8 unter Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem Deutschen Bundestag bestellt wird, zu evaluieren.“

5. Der bisherige Artikel 10 wird Artikel 11.

Berlin, den 10. Juni 2015

Der Innenausschuss

Wolfgang Bosbach
Vorsitzender

Clemens Binninger
Berichterstatter

Gerold Reichenbach
Berichterstatter

Martina Renner
Berichterstatterin

Dr. Konstantin von Notz
Berichterstatter

Bericht der Abgeordneten Clemens Binninger, Gerold Reichenbach, Martina Renner und Dr. Konstantin von Notz

A. Allgemeiner Teil

I. Überweisung

Der Gesetzentwurf auf **Drucksache 18/4096** wurde in der 95. Sitzung des Deutschen Bundestages am 20. März 2015 an den Innenausschuss federführend sowie an den Ausschuss für Recht und Verbraucherschutz, den Haushaltsausschuss, den Ausschuss für Wirtschaft und Energie, den Ausschuss für Verkehr und digitale Infrastruktur sowie den Ausschuss Digitale Agenda zur Mitberatung überwiesen. Dem Haushaltsausschuss wurde der Gesetzentwurf auch gemäß § 96 GO-BT überwiesen.

Der Parlamentarische Beirat für nachhaltige Entwicklung beteiligte sich gutachtlich.

II. Stellungnahmen der mitberatenden Ausschüsse

Der **Ausschuss für Recht und Verbraucherschutz** hat in seiner 57. Sitzung am 10. Juni 2015 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN die Annahme des Gesetzentwurfs in der Fassung des Änderungsantrags der Koalitionsfraktionen empfohlen. Zudem hat er mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Oppositionsfraktionen empfohlen, den Entschließungsantrag der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Ausschussdrucksache 18(4)327 abzulehnen.

Der **Haushaltsausschuss** hat in seiner 49. Sitzung am 10. Juni 2015 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN empfohlen, dem Gesetzentwurf zuzustimmen. Seinen Bericht gemäß § 96 GO-BT wird der Haushaltsausschuss gesondert abgeben.

Der **Ausschuss für Wirtschaft und Energie** hat in seiner 41. Sitzung am 10. Juni 2015 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN die Annahme des Gesetzentwurfs in der Fassung des Änderungsantrags der Koalitionsfraktionen empfohlen. Zudem hat er mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Oppositionsfraktionen die Ablehnung des Entschließungsantrages der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Ausschussdrucksache 18(4)327 empfohlen.

Der **Ausschuss für Verkehr und digitale Infrastruktur** hat in seiner 43. Sitzung am 10. Juni 2015 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN empfohlen, den Gesetzentwurf in der Fassung des Änderungsantrags der Koalitionsfraktionen anzunehmen. Zudem hat er die Ablehnung des Entschließungsantrags der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Ausschussdrucksache 18(4)327 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Oppositionsfraktionen empfohlen.

Der **Ausschuss Digitale Agenda** hat in seiner 39. Sitzung am 10. Juni 2015 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN die Annahme des Gesetzentwurfs in der Fassung des Änderungsantrags der Koalitionsfraktionen empfohlen. Zudem hat er mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Oppositionsfraktionen die Ablehnung des Entschließungsantrages der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Ausschussdrucksache 18(4)327 empfohlen.

III. Beratungsverlauf und Beratungsergebnisse im federführenden Ausschuss

Der Innenausschuss hat in seiner 39. Sitzung am 4. März 2015 einvernehmlich beschlossen, eine öffentliche Anhörung zu dem Gesetzentwurf auf Drucksache 18/4096 durchzuführen. Die öffentliche Anhörung, an der sich acht

Sachverständige beteiligt haben, hat der Innenausschuss in seiner 44. Sitzung am 20. April 2015 durchgeführt. Hinsichtlich des Ergebnisses der Anhörung wird auf das Protokoll der 44. Sitzung (Protokoll 18/44) verwiesen. Sowohl bei der Anhörung als auch bei den nachfolgenden Beratungen lagen die Prüfbitte des Parlamentarischen Beirats für nachhaltige Entwicklung auf Ausschussdrucksache 18(4)241 und die Stellungnahme des Bundesministeriums des Innern auf Ausschussdrucksache 18(4)285 vor.

Der **Innenausschuss** hat den Gesetzentwurf auf Drucksache 18/4096 in seiner 49. Sitzung am 10. Juni 2015 abschließend beraten. Er empfiehlt mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN, den Entwurf in der aus der Beschlussempfehlung ersichtlichen Fassung anzunehmen. Die Änderungen entsprechen dem Änderungsantrag auf Ausschussdrucksache 18(4)326, der zuvor von den Fraktionen der CDU/CSU und SPD in den Innenausschuss eingebracht und mit gleichem Abstimmungsergebnis angenommen wurde.

Zuvor wurde der Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN auf Ausschussdrucksache 18(4)327 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN abgelehnt. Der Entschließungsantrag auf Ausschussdrucksache 18(4)327 lautet:

Der Bundestag wolle beschließen:

I. Der Deutsche Bundestag stellt fest,

Die Digitalisierung und Vernetzung von Gesellschaft, Wirtschaft und Staat schreitet weiter voran und damit auch die die Abhängigkeit von IT-Systemen. Zugleich ist nicht erst seit dem durch Edward Snowden bekannt gewordenen Überwachungs- und Abhörskandal westlicher Geheimdienste klar, dass digitale Infrastrukturen auch durch staatliche Behörden bedroht sind. Beinahe täglich erfahren wir von gravierenden Sicherheitslücken in Software und von zahlreichen Hackerangriffen auf private als auch öffentliche IT-Strukturen. Die IT-Sicherheitslage in Deutschland ist weiterhin angespannt, wie der Lagebericht zur IT-Sicherheit des Bundesamts für Sicherheit in der Informationstechnik (BSI) nachweist.

Das gesellschaftliche Vertrauen und das Vertrauen der Wirtschaft in die Integrität der digitalen Infrastruktur sind wesentliche Grundlagen für die digitale Zukunft. Eine Stärkung und Verbesserung der IT-Sicherheit ist aber vor allem auch dringend geboten, um den Menschen – auch vor dem Hintergrund des NSA-Überwachungsskandals - Schutz vor der Verletzung ihrer Grundrechte, insbesondere ihres Grundrechts auf Vertraulichkeit und Integrität der von Ihnen genutzten informationstechnischen Systeme zu bieten.

II. Der Deutsche Bundestag fordert die Bundesregierung auf,

1. einen Gesetzentwurf vorzulegen, der das neu geschaffene IT-Sicherheitsgesetz zurücknimmt und stattdessen weitergehende, insbesondere grundrechts- und rechtsstaatskonforme Regelungen zur IT-Sicherheit enthält,

a. der nicht allein den Schutz Kritischer Infrastrukturen, sondern auch die Schutzpflicht des Grundrechts der Menschen auf Vertraulichkeit und Integrität ihrer informationstechnischen Systeme zum Ziel hat, sowie den grundlegenden datenschutzrechtlichen Anforderungen und dem Fernmeldegeheimnis gerecht wird,

b. dessen Anwendungsbereich auch öffentliche Stellen umfasst,

c. der hinreichend bestimmte und normenklare gesetzliche Regelungen zur Bestimmung der betroffenen Wirtschaftsbereiche und Betreiber sowie des Begriffs der kritischen Infrastruktur enthält,

d. der konkret, eng und unter strenger Beachtung des Grundsatzes der Zweckbindung regelt, von wem und zu welchen Zwecken die im Rahmen der Meldepflichten übermittelten personenbeziehbaren Daten verarbeitet werden dürfen; der Meldepflichten für Sicherheitsvorfälle nicht erst im Falle „erheblichen Störungen“ vorsieht, sondern bereits zu einem Zeitpunkt, in dem noch kein Schaden eingetreten ist“,

e. der Massenspeicherungen von Daten (Bestandsdaten, Verkehrsdaten oder Inhaltsdaten) allein für Zwecke der IT-Sicherheit ausschließt,

f. der positive und wettbewerbsrelevante Anreize für die Wirtschaft setzt, ihre IT-Sicherheitskonzepte stetig und proaktiv fortzuentwickeln und zu pflegen, und hierzu insbesondere zu prüfen, ob ein System der unabhängigen Auditierung und Zertifizierung von Produkten und Verfahren einen effizienteren Ansatz bietet,

g. der sicherstellt, dass die Qualität von IT-Sicherheitskonzepten in Behörden und Unternehmen durch zu auditierende Sicherheitsprüfungen wie zum Beispiel sog. Penetrationstests qualitativ verbessert werden, der ein Verfahren zur unabhängigen Festsetzung von Standards der IT-Sicherheit nach gesetzlich festgelegten Kriterien vorsieht,

h. der für die gesetzlichen Vorgaben für technische Schutzstandards nicht nur den „Stand der Technik „berücksichtigt“, sondern auch Standards, die auf der Basis von Risikoanalysen und konkretisierbaren Gefahrenlagen (Szenarien) ermittelt werden, einhält,

i. der eine Kontrolle der Einhaltung durch ein zumindest für diesen Aufgabenbereich unabhängig gestelltes Bundesamt für Sicherheit in der Informationstechnik (BSI) vorsieht,

j. der klarstellt, dass neu zu regelnde Meldepflichten unbeschadet der in § 42a BDSG und § 109a TKG zum Zwecke des Datenschutzes geregelten Meldepflichten bestehen,

k. der die Vorgaben der höchstrichterlichen Rechtsprechung des Bundesverfassungsgerichts (Urteil vom 02.03.2010 – 1 BvR 256/08, 1 BvR 263/08, 1 BvR 586/08) und des Europäischen Gerichtshofs (Urteil vom 08.04.2014 - C-293/12 und C-594/12) zur Vorratsdatenspeicherung beachtet,

l. der wirksame Sanktionen bei Zuwiderhandlungen, insbesondere gegen gesetzliche Vorgaben für einzuhaltende Sicherheitsstandards vorsieht,

m. der insbesondere im Hinblick auf personenbezogene Daten ausdrücklich regelt, an wen und zu welchen konkreten Zwecken das BSI die durch die Meldungen erlangten Informationen übermitteln darf und unter welchen Voraussetzungen deren Weiterverarbeitung erfolgt,

n. der anlassbezogene Informationspflichten über Verletzungen der IT-Sicherheit gegenüber betroffenen Unternehmen und Öffentlichkeit differenzierend regelt,

o. der die Weitergabe von Erkenntnissen aus dem Lagebild des BSI sowie Erkenntnissen aus der Erweiterung der Aufgaben des BSI zur Untersuchung von informationstechnischer Systeme, normenklar regelt und Erkenntnisse der Öffentlichkeit verpflichtend und unmittelbar zur Verfügung stellt und eine grundsätzliche Pflicht zur unverzüglichen Veröffentlichung von Sicherheitslücken enthält,

p. der die Einbeziehung der Datenschutzbeauftragten des Bundes und der Länder in die Festlegung von Informationssicherheitsstandards und in die vorgesehenen Meldewege mit vorsieht,

q. der, entgegen des im IT-Sicherheitsgesetz vorgesehenen und mangelhaft begründeten Stellenaufbaus bei Nachrichtendiensten, keine Stellenaufwüchse und keine neuen Überwachungsbefugnisse der Nachrichtendienste im Zusammenhang mit der IT-Sicherheit vorsieht, solange die von den Nachrichtendiensten dabei zu verwendenden Methoden und Instrumente, somit auch die dadurch zu erwartenden Grundrechtsbeeinträchtigungen für den Gesetzgeber und die Öffentlichkeit nicht nachvollziehbar gemacht werden können, und

r. der das IT-Sicherheitsgesetz auf die parallel in Verhandlung befindliche EU-Richtlinie zur Netz- und Informationssicherheit (NIS) hin anpasst

2. und sich auf EU-Ebene insbesondere in den laufenden Verhandlungen und die NIS-Richtlinie für einheitliche und hohe Standards der IT-Sicherheit einzusetzen.

3. mittelfristig gesetzlich dafür Sorge zu tragen, dass

a. der Aufbau, Betrieb und das Angebot von Ende-zu-Ende-Verschlüsselungen gefördert und zum Kernstück eines umfassenderen Regelungsansatzes gemacht wird,

b. eine langfristige Strategie zur Prüfung und Sicherstellung von Bausteinen einer sicheren Hard- und Softwareinfrastruktur auf der Grundlage etwa von Open Source-Elementen (offene und überprüfbare Quelltexte) erarbeitet und umgesetzt wird, beispielsweise durch die Finanzierung von regelmäßigen und unabhängigen Überprüfungen von sicherheitsrelevanter Software („bug bountys“),

c. in einer ganzheitlichen Perspektive die Hersteller von Hard- und Software (nicht nur Betreiber) berücksichtigt und Anreize zur Qualitätssicherung durch Haftungsverpflichtungen geschaffen werden,(beispielsweise für die fahrlässige Implementierung oder Nichtbeseitigung von Sicherheitslücken),

d. das Vergaberecht der öffentlichen Hand angepasst wird, so dass grundsätzlich nur auditierte, zertifizierte sowie open sourcegemäße Produkte berücksichtigt werden,

e. eine Beförderung des Schwarzmarktes für Sicherheitslücken durch den staatlichen Aufkauf und die Zurückhaltung von Sicherheitslücken (bspw. zero-day-exploits), welchedie Integrität digitaler Infrastrukturen gefährden, zu verbieten und stattdessen auf die konsequente Beseitigung von Sicherheitslücken hinzuwirken,

f. mittels eines übergreifenden Regelungsansatzes für einen hohen Datenschutz durch Technik gesorgt wird, beispielsweise durch Verpflichtungen zu „Security and Privacy by Design and Default“

g. der Schutz von Whistleblowern (Hinweisgebern) gesetzlich gestärkt wird.

IV. Begründung

Im Folgenden werden die vom Innenausschuss empfohlenen Änderungen auf Grundlage des Änderungsantrags der Koalitionsfraktionen auf Ausschussdrucksache 18(4)326 gegenüber der ursprünglichen Fassung des Gesetzentwurfs erläutert. Soweit der Ausschuss die unveränderte Annahme des Gesetzentwurfs empfiehlt, wird auf die Begründung in Drucksache 18/4096 verwiesen.

Zu Nummer 1

Buchstabe a)

Aktuell in der Presse diskutierte Beispiele von Schadprogrammen wie REGIN oder Schadsoftwareplattformen der Equation Group verdeutlichen einen erneuten Qualitätssprung in der Bedrohung der IT des Bundes. Es handelt sich hierbei um hochkomplexe, multifunktionale und modular aufgebaute Spionageprogramme, die an Stellen ansetzen, auf die beispielsweise gängige Virenschutzprogramme bisher nicht zugreifen können. Die Erkennung solcher Schadprogramme kann wirksam nur durch neue und auf die jeweilige konkrete Gefährdungssituation angepasste, umfangreiche sowie komplexe Detektionsmethoden zur Erkennung von Anomalien innerhalb der zu schützenden Netzwerke erfolgen. Das technische und personelle Know-how für ein derartiges Monitoring befindet sich in der Regel nicht in den einzelnen Behörden der Bundesverwaltung, sondern ist zentral im BSI verankert.

Derzeit erfüllt das BSI sein bestehendes Mandat zur zentralen Abwehr und Detektion von Angriffen durch ein zentrales Monitoring der behördenübergreifenden Regierungsnetze. Um neue Bedrohungen zuverlässig detektieren und abwehren zu können, muss dieses Monitoring ausgebaut werden. Hierfür benötigt das BSI auch Protokolldaten aus der internen IT der Behörden.

Das BSI kann die Behörden bisher nicht verpflichten, entsprechende Daten zu erheben, die dafür erforderlichen Schritte einzuleiten oder diese dem BSI zur Verfügung zu stellen.

Mit der Ergänzung in Satz 5 wird dem besonderen Schutz der richterlichen Unabhängigkeit Rechnung getragen.

Buchstabe b)

Die Änderung von § 7a Absatz 2 des BSI-Gesetzes stellt die insgesamt enge Zweckbindung der Vorschrift klar und bedient sich dabei der im BSI-Gesetz üblichen Verweistechnik (vergleiche zum Beispiel § 7 Absatz 1 Satz 1, § 7 Absatz 2 Satz 1, § 8 Absatz 2 Satz 1 des BSI-Gesetzes in seiner geltenden Fassung).

§ 7a des BSI-Gesetzes nimmt mit der Änderung nunmehr in allen seinen Aspekten konkret Bezug auf die Erfüllung folgender Aufgaben des BSI:

- Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes (§ 3 Absatz 1 Satz 2 Nummer 1 des BSI-Gesetzes),
- Beratung und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen (§ 3 Absatz 1 Satz 2 Nummer 14 des BSI-Gesetzes),
- Aufgaben nach den §§ 8a und 8b des BSI-Gesetzes als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen (§ 3 Absatz 1 Satz 2 Nummer 17 des BSI-Gesetzes).

Diese Zweckbindung gilt nunmehr ausdrücklich für

- die Untersuchung von auf dem Markt bereitgestellten oder zur Bereitstellung auf dem Markt vorgesehenen informationstechnischen Produkten und Systemen (Absatz 1),
- die Nutzung der aus den Untersuchungen gewonnenen Erkenntnisse (Absatz 2 Satz 1) sowie
- die Weitergabe und Veröffentlichung dieser Erkenntnisse (Absatz 2 Satz 2).

Buchstabe c)

Die Änderung in Satz 1 dient der Klarstellung, dass die Erarbeitung von Mindeststandards für die IT-Sicherheit des Bundes eine Pflichtaufgabe des BSI ist.

Die Änderung in Satz 2 stärkt die Befugnisse des BSI. Das bisher vorgesehene Zustimmungserfordernis hat den Erlass verbindlicher Mindeststandards für die IT-Sicherheit des Bundes und damit die Schaffung eines hinreichenden und einheitlichen (Mindest-)Sicherheitsniveaus in der Bundesverwaltung faktisch verhindert. In den letzten Jahren hat sich die IT-Sicherheitslage des Bundes immer weiter verschärft. Gezielte Angriffe auf die Informationstechnik des Bundes werden zahlreicher, professioneller und komplexer. Zugleich erhöht die steigende Abhängigkeit des Staates von Informationstechnik deren wesentliche Bedeutung für die Funktionsfähigkeit der staatlichen Verwaltung.

Satz 3 stellt klar, dass sich der Beratungsauftrag des BSI auch auf die Umsetzung der Mindestsicherheitsstandards in der Bundesverwaltung erstreckt.

Buchstabe d)

Doppelbuchstabe aa)

Dreifachbuchstabe aaa)

Durch die Änderung werden die Betreiber Kritischer Infrastrukturen bei der Sicherung ihrer Systeme, Komponenten und Prozesse stärker als bisher auf die Einhaltung des Standes der Technik verpflichtet.

Die Ausgestaltung als Soll-Vorschrift trägt dem Umstand Rechnung, dass Betreiber Kritischer Infrastrukturen teilweise Maßnahmen nicht ergreifen können, die aus reiner IT-Sicherheitssicht als Stand der Technik anzusehen wären. Dies gilt beispielsweise für zeitnahe Sicherheits-Updates von Betriebssystemen, deren Auswirkungen auf die notwendigen Betriebsprozesse bei komplexen Systemen nicht von vornherein absehbar sind. Das Einspielen solcher Updates könnte zu einem Ausfall der Kritischen Dienstleistungen führen, deren Schutz die gesetzliche Verpflichtung auf den Stand der Technik eigentlich bezweckt. Erforderlich ist daher eine gewisse Flexibilität in der Umsetzung von Maßnahmen, die dem Stand der Technik entsprechen.

„Soll“ impliziert dabei eine Verpflichtung, von der die Betreiber nur in begründeten Ausnahmefällen abweichen dürfen - zum Beispiel, weil ansonsten das Ziel der Versorgungssicherheit überhaupt erst gefährdet wird.

Dreifachbuchstabe bbb)

Es handelt sich um redaktionelle Anpassungen.

Dreifachbuchstabe ccc)

§ 8a des BSI-Gesetzes sieht vor, dass Betreiber Kritischer Infrastrukturen und ihre Branchenverbände branchenspezifische Sicherheitsstandards vorschlagen können. Das BSI stellt auf Antrag fest, ob diese geeignet sind, die Anforderungen an solche Standards zu erfüllen. Durch dieses Verfahren soll vermieden werden, dass in der Wirtschaft bereits bestehende Sicherungssysteme und Prozeduren ausgehebelt werden. Auch die Art, wie die Einhaltung des Stands der Technik nachgewiesen wird, wurde bewusst offen gelassen, um neben den in den Branchen bereits vorhandenen Prüfungs- und Zertifizierungsverfahren kein zusätzliches kostspieliges Verfahren zu etablieren. Zur Schärfung der Systematik von § 8a und im Interesse größerer Rechtsklarheit soll dem BSI aber in diesem Rahmen durch den neuen Absatz 4 ermöglicht werden, konkrete Vorgaben an die Art und Weise der Durchführung, an die hierüber auszustellenden Nachweise sowie fachliche und organisatorische Anforderungen an die prüfende Stelle zu machen.

Doppelbuchstabe bb)

Dreifachbuchstabe aaa)

Die Ergänzung dient der Klarstellung, dass die Meldung des Betreibers auch Angaben dazu enthalten muss, in welcher Art von Einrichtung oder Anlage die von der Störung betroffene Informationstechnik bei dem Betreiber der Kritischen Infrastruktur zur Anwendung kommt. Durch die Verwendung des Begriffs „Art“ wird klargestellt, dass es sich um allgemeine Angaben etwa zur Funktionalität der Anlage und nicht um unternehmensspezifische

Angaben handelt, die sich auf die konkret durch den Betreiber eingesetzte Anlage beziehen. Die entsprechende Information ist für eine sachgerechte Auswertung der Meldung durch das Bundesamt erforderlich.

Im Hinblick auf § 8b Absatz 4 Satz 3 des BSI-Gesetzes ist eine Angabe zur Art der betroffenen Einrichtung nicht erforderlich, wenn dadurch ein eindeutiger Rückschluss auf den Betreiber der Kritischen Infrastruktur möglich wäre.

Dreifachbuchstabe bbb)

In der Praxis fehlt es häufig an der Mitwirkung der Hersteller von informationstechnischen Produkten und Systemen bei der kurzfristigen Behebung von Sicherheitslücken, etwa durch die Bereitstellung eines erforderlichen Sicherheits-Updates. Das IT-Sicherheitsgesetz gibt Betreibern Kritischer Infrastrukturen durch die Verpflichtung zum Einsatz sicherer IT-Produkte bereits jetzt eine Grundlage, um eine Vereinbarung über die Sicherheit/Fehlerfreiheit der zum Einsatz vorgesehenen IT-Produkte und IT-Systeme gegenüber den Herstellern durchsetzen zu können. Diese soll ergänzt werden um eine Anordnungsbefugnis des BSI, mit der die Hersteller der betroffenen informationstechnischen Produkte und Systeme im zumutbaren Umfang zur Mitwirkung an der Beseitigung oder Vermeidung von Störungen verpflichtet werden können.

Satz 2 stellt klar, dass diese Anordnungsbefugnis des BSI auch bei meldepflichtigen Störungen in den spezialgesetzlich geregelten Bereichen gilt.

Dreifachbuchstabe ccc)

Es handelt sich um eine notwendige Folgeänderung.

Doppelbuchstabe cc)

§ 8c Absatz 2 Nummer 4 des BSI-Gesetzes verweist in seiner derzeitigen Fassung als Auffangtatbestand pauschal auf vorrangige spezialgesetzliche Anforderungen zur Einhaltung von Mindeststandards, die denen nach § 8a vergleichbar oder weitergehend sind. Die entsprechenden spezialgesetzlichen Rechtsvorschriften zu Sicherheitsstandards können aber unterschiedliche Sicherheitsaspekte auch jenseits von IT-Fragen betreffen. Die Rechtsfolge, nach der § 8a insgesamt für nicht anwendbar erklärt wird, ist daher in der derzeitigen Fassung zu starr und durch Einfügung eines „soweit“ flexibler zu formulieren.

Buchstabe e)

Die Regelung konkretisiert das vorgesehene Verfahren zur Bestimmung der Betreiber Kritischer Infrastrukturen im Wege der Rechtsverordnung und trägt dem Erfordernis der hinreichenden Bestimmtheit der Normadressaten durch die Vorgabe eines konkreten Verfahrens für deren Bestimmbarkeit Rechnung. Danach hat eine sektor- und branchenspezifische Betrachtung dergestalt zu erfolgen, dass der für die Bestimmung der Normadressaten maßgebliche Versorgungsgrad als jeweils branchenspezifischer Schwellenwert für jede als kritisch anzusehende Dienstleistung im jeweiligen Sektor zu ermitteln ist. Nur im Falle einer Überschreitung dieser branchenspezifischen Schwellenwerte ist die konkrete Infrastruktur als kritisch im Sinne des Gesetzes anzusehen.

Buchstabe f)

Der Katalog der Bußgeldvorschriften ergänzt den kooperativen Ansatz der §§ 8a und 8b des BSI-Gesetzes um die Möglichkeit der bußgeldbewehrten Sanktion für den Fall der Nichteinhaltung der in den §§ 8a und 8b des BSI-Gesetzes vorgesehenen Pflichten. In Anlehnung an § 149 Nummer 21a des Telekommunikationsgesetzes ist der Verstoß des Betreibers einer Kritischen Infrastruktur gegen die Pflicht zur Meldung erheblicher Störungen im Sinne von § 8a Absatz 4 des BSI-Gesetzes dabei nur dann bußgeldbewehrt, wenn die betreffende Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat.

Absatz 2 regelt die Höhe der jeweiligen Bußgelder. Sachlich zuständige Verwaltungsbehörde ist gemäß Absatz 3 das BSI.

Zu Nummern 2 und 3

Es handelt sich um redaktionelle Anpassungen.

Zu Nummer 4

Die Evaluierung dient der Überprüfung der mit dem IT-Sicherheitsgesetz im BSI-Gesetz neu eingeführten Regelungen zu Meldepflichten und Mindeststandards. Die Formulierung lehnt sich an das entsprechende Vorgehen zum Antiterrordatei-Gesetz an. Insbesondere wird bei der Auswahl des/der Sachverständigen das Einvernehmen

mit dem Bundestag vorgesehen. Die Evaluierung soll anhand der Konzeption zur Evaluierung neuer Regelungsvorhaben gemäß dem Arbeitsprogramm bessere Rechtssetzung der Bundesregierung vom 28. März 2012, Ziffer II. 3., erfolgen.

Die **Koalitionsfraktionen** betonen die große Bedeutung der IT-Sicherheit. Der Gesetzentwurf konzentriere sich dabei auf den Schutz der Kritischen Infrastruktur (KRITIS), der für die Daseinsvorsorge in Deutschland und die Funktionsfähigkeit der Wirtschaft besonders wichtig sei. Mit dem Gesetzentwurf werde festgelegt, dass die Betreiber von KRITIS in Bezug auf die Sicherheit ihrer Systeme bestimmte Anforderungen erfüllen müssten, und das Meldeverfahren bei Cyberangriffen geregelt. Die vorgegebenen Standards würde das BSI zusammen mit der Wirtschaft und den Verbänden erarbeiten. In Konsequenz aus der Anhörung zu dem Gesetzentwurf sei ein Änderungsantrag vorgelegt worden, der unter anderem die Einführung einer Bußgeldvorschrift vorsehe, die Zweckbindung der gewonnenen Daten und Erkenntnisse klarer regle und eine Evaluierung des Gesetzes nach Ablauf von vier Jahren nach Inkrafttreten unter Hinzuziehung externen Sachverstands festlege. Dem Entschließungsantrag der Fraktion BÜNDNIS 90/DIE GRÜNEN könne nicht zugestimmt werden, da er lediglich Wünsche formuliere, ohne Lösungen aufzuzeigen. Teilweise seien die Vorschläge auch bereits mit dem Änderungsantrag der Koalitionsfraktionen umgesetzt. Der Gesetzentwurf in der vorgelegten Fassung sei ein wichtiger Schritt zur Verbesserung der IT-Sicherheit in Deutschland und des Schutzes vor Cyberangriffen. Diesem sollte zugestimmt werden.

Die **Fraktion DIE LINKE.** stimmt darin überein, dass es unerlässlich sei, sich auch gesetzgeberisch dem Schutz von KRITIS zuzuwenden. An dem vorgelegten Gesetzentwurf gebe es jedoch eine Reihe von Kritikpunkten. So wäre es wünschenswert, dass wesentliche Angriffe und Attacken unter Nennung des Namens des Betreibers gemeldet würden, weil dadurch möglicherweise öffentlicher Druck erwachse, bestimmte Sicherheitslücken zu schließen. Auch fehle es in dem Gesetzentwurf an einem Verbot des kommerziellen Handelns mit Sicherheitslücken. Problematisch sei ebenfalls der Bereich der Speicherung von Daten aus Telekommunikationsvorgängen durch die Telekommunikationsanbieter, soweit diese zur Erkennung, Eingrenzung und Beseitigung von Störungen an Telekommunikationsanlagen dienen sollen, da dies ggf. einer Art von Vorratsdatenspeicherung gleichkomme. Daher werde ausdrücklich der Entschließungsantrag der Fraktion BÜNDNIS 90/DIE GRÜNEN unterstützt und die Forderung erhoben, das BSI als unabhängige Institution auszugestalten, um jeden Anschein einer möglichen Kooperation mit Nachrichtendiensten von vornherein auszuschließen. Der Gesetzentwurf in der vorgelegten Fassung werde abgelehnt.

Die **Fraktion BÜNDNIS 90/DIE GRÜNEN** kritisiert, dass der Gesetzentwurf angesichts der massiven Sicherheitslücken im IT-Bereich nicht früher vorgelegt worden sei, zumal derzeit auch auf europäischer Ebene die NIS-Richtlinie erarbeitet werde. An dem Gesetzentwurf sei problematisch, dass die Meldepflichten der öffentlichen Stellen nicht klar geregelt seien. Auch würden die Betreiber von KRITIS nicht klar benannt. Die Nachbesserung bei der Erhebung der Daten und der Zweckbindung sei nicht ausreichend. Hinzu komme, dass die deutsche Industrie wenig Vertrauen in das BSI habe, da es keine unabhängige Behörde, sondern als ein Annex des BMI zu betrachten sei. Es werde dafür geworben, positive Anreizsysteme zu schaffen, indem man Unternehmen, die bestimmte Standards erfüllten oder sich bestimmten Auditierungen aussetzten, fördere. Im Vergleich zu dem Gesetzentwurf der Koalitionsfraktionen sei der Entschließungsantrag der Fraktion BÜNDNIS 90/DIE GRÜNEN wesentlich weitgreifender. Es gehe nicht nur um Unternehmen und KRITIS, sondern vor allem um den Schutz des Grundrechts auf Vertraulichkeit und Integrität von informationstechnischen Systemen. Daher werde dafür plädiert, den nicht ausreichenden Gesetzentwurf zu überdenken. In der vorgelegten Fassung könne diesem nicht zugestimmt werden.

Berlin, den 10. Juni 2015

Clemens Binninger
Berichterstatter

Gerold Reichenbach
Berichterstatter

Martina Renner
Berichterstatterin

Dr. Konstantin von Notz
Berichterstatter