Referentenentwurf

des Bundesministeriums des Innern, für Bau und Heimat

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

(IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0)

A. Problem und Ziel

Die Gewährleistung der Cyber- und Informationssicherheit ist ein Schlüsselthema für Staat, Wirtschaft und Gesellschaft. Sie sind auf funktionierende Informationstechnik angewiesen - sei es für den Informationsaustausch, die Produktion, den Konsum, Dienstleistungen oder zur Pflege privater Kontakte. Voraussetzung hierfür ist eine sichere Infrastruktur.

Cyber-Angriffe stellen für Staat, Wirtschaft und Gesellschaft nach wie vor ein großes Gefahrenpotential dar. Zwar stagniert die Gesamtzahl der Angriffe auf hohem Niveau, jedoch werden sie qualitativ immer ausgefeilter und somit für alle Betroffenen auch gefährlicher. Dies wurde durch Vorfälle wie die Ransomware „WannaCry“ und die Aufdeckung von Schwachstellen in Computerchips wie „Meltdown“ und „Spectre“ besonders deutlich. Daneben hat auch der zu Beginn des Jahres 2018 in den Medien bekanntgewordene Angriff auf die Kommunikationsinfrastrukturen des Auswärtigen Amtes deutlich gemacht, dass der Staat seine Schutzmaßnahmen anpassen muss. Vorfälle, bei denen persönliche Daten unter anderem aus sozialen Netzwerken ohne Einverständnis und Wissen der Betroffenen weit verbreitet werden (Datenleak-Vorfall Anfang des Jahres 2019), zeigen, dass nicht nur Staat, Wirtschaft und Gesellschaft, sondern auch Individualinteressen betroffen sind.

Die zunehmende Verbreitung von Internet of Things (IoT)-Geräten verschärft die Situation zusätzlich. Diese Geräte werden teilweise nicht unter Sicherheitsaspekten entwickelt und lassen sich hierdurch zu großen Bot-Netzen zusammenschalten. Dieser Gefahr gilt es zu begegnen.

Insgesamt ist Cyber-Sicherheit niemals statisch. Ein aktuelles Schutzniveau ist kein Garant für eine erfolgreiche Abwehr der Angriffe von morgen. Vielmehr ist eine ständige Anpassung und Weiterentwicklung der Schutzmechanismen und der Abwehrstrategien erforderlich. Dieses Gesetz dient daher dem Schutz von Staat, Wirtschaft und Gesellschaft.

B. Lösung

IT-Sicherheit muss für Staat, Wirtschaft und Gesellschaft ausgeweitet werden. Entsprechend dem Auftrag aus dem Koalitionsvertrag wird daher der mit dem IT-Sicherheitsgesetz geschaffene Ordnungsrahmen durch das Zweite IT-Sicherheitsgesetz erweitert (IT-SiG 2.0). Das Gesetz verfolgt einen ganzheitlichen Ansatz.

Zum Schutz der Bürgerinnen und Bürger werden insbesondere Voraussetzungen für ein einheitliches IT-Sicherheitskennzeichen geschaffen, welches die IT-Sicherheit der Produkte erstmals sichtbar macht. Hierdurch wird eine fundierte Kaufentscheidung ermöglicht. Außerdem wird Verbraucherschutz im Bereich der Informationssicherheit als zusätzliche Aufgabe des Bundesamtes in der Informationstechnik (BSI) gesetzlich etabliert.

Um Cyber-Sicherheitsvorfällen insgesamt zu begegnen, werden zudem die Befugnisse des BSI zum Schutz der Bundesverwaltung, beispielsweise mit der Schaffung von Befugnissen zur Detektion von Schadprogrammen zum Schutz der Regierungsnetze ausgeweitet.

Bei der rechtswidrigen Verbreitung illegal erlangter Daten tragen die Diensteanbieter nach dem Telekommunikationsgesetz (TKG) und dem Telemediengesetz (TMG) Mitverantwortung, da die von ihnen angebotenen Dienste Mittel der Verbreitung sind.Damit die rechtswidrige Verbreitung solcher Daten zukünftig schnell unterbunden werden kann, werden den Diensteanbietern Verpflichtungen zum Löschen, zum Melden und zu Bestandsauskünften auferlegt.

Zum Schutz der Wirtschaft werden die für die Betreiber Kritischer Infrastrukturen bestehenden Meldepflichten und Verpflichtungen zur Einhaltung der Mindeststandards auf weitere Teile der Wirtschaft ausgeweitet.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

Mehrbedarfe durch den Erfüllungsaufwand sind finanziell und stellenplanmäßig in den jeweiligen Einzelplänen zu erwirtschaften.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Durch das geplante Regelungsvorhaben kommt es bei Bürgerinnen und Bürgern zu keiner Änderung des Erfüllungsaufwands.

E.2 Erfüllungsaufwand für die Wirtschaft

Durch das geplante Regelungsvorhaben der Bundesregierung kommt es für die Wirtschaft zu einer Veränderung des jährlichen Erfüllungsaufwands von rund 45,09 Millionen Euro. Rund 31,20 Millionen Euro davon entstehen aus neuen oder geänderten Informationspflichten. Einmalig wird die Wirtschaft mit rund 16,71 Millionen Euro belastet.

Soweit durch das Regelungsvorhaben für die Wirtschaft zusätzlicher laufender Erfüllungsaufwand entsteht, wird dieser durch geeignete Entlastungsmaßnahmen kompensiert.

E.3 Erfüllungsaufwand der Verwaltung

Der Verwaltung entsteht für die Erfüllung der im Gesetz vorgesehenen zusätzlichen Aufgaben ein Aufwand von insgesamt xxxxxxxx Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund xxxxxxxx Millionen Euro.

Die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS) ist verantwortlich für die Kommunikationswege des Bundes. Es ist ein Erfüllungsaufwand in Höhe von insgesamt 54 Planstellen erforderlich, sofern eine Protokollierung nicht über DaaS möglich ist. Hierfür fallen jährlich Personalkosten in Höhe von rd. 3,35 Mio. Euro und einmalige Sachkosten in Höhe von rd. 5 Mio. Euro an.

Sollte das DaaS in Anspruch genommen werden, so reduziert sich der Personalmehrbedarf um ca. 28 Planstellen, sodass insgesamt ein Mehraufwand in Höhe von 26 Planstellen erforderlich ist. Dies entspricht jährlichen Personalkosten von rd. 1,62 Mio. Euro.

Es ist ein Erfüllungsaufwand in Höhe von insgesamt 10 Planstellen erforderlich. Hierfür fallen jährlich Personalkosten in Höhe von 620.800 Euro und Sachkosten in Höhe von rd. 10,2 Mio. Euro an.

Beim BSI ist ein Erfüllungsaufwand in Höhe von 583 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund xxx Millionen Euro notwendig. Darin ist bereits eine OPH-Quote enthalten. Zusätzlich sind zur Umsetzung des Gesetzes Sachkosten in Höhe von einmalig 28 Mio. Euro und jährlich in Höhe von rd. 47,5 Mio. Euro zu berücksichtigen.

Der Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen wird finanziell und stellenmäßig im Gesamthaushalt ausgeglichen.

Für die Umsetzung des Zweiten IT-Sicherheitsgesetzes kommen für das BSI folgende neue Aufgaben, die zusätzlichen Personalbedarf nach sich ziehen, hinzu:

- Mit den neuen Aufgaben des BSI zur Förderung des Verbraucherschutzes und der Verbraucherinformation im Bereich der Informationssicherheit trägt das Gesetz dem Umstand Rechnung, dass Fragen der IT-Sicherheit durch die Digitalisierung alltäglicher Lebensabläufe – insbesondere durch die steigende Vernetzung der privaten Haushalte – bei Verbraucherinnen und Verbrauchern eine steigende Bedeutung zukommt. Mit seiner technischen Expertise und Erfahrung kann das BSI einerseits durch Beratung, Sensibilisierung und Unterstützung von Verbraucherinnen und Verbrauchern zum Schutz dieser vor den mit der Digitalisierung verbundenen Gefahren für die IT-Sicherheit beitragen. Andererseits will das BSI seine Kompetenzen, Fähigkeiten und etablierten Arbeitsbeziehungen dazu einsetzen, Security by Design am Markt durchzusetzen, sodass den Verbraucherinnen und Verbrauchern sichere Produkte zur Verfügung stehen, was heute oft nicht der Fall ist. Um diese wichtige Aufgabe sachgerecht durchführen zu können, benötigt das BSI 163 Planstellen/Stellen.

- In diesem Kontext kommen auch die Änderungen in § 3 Abs. 1 Satz 2 Nr. 14 sowie § 7 Abs. 1d BSIG-E (erweiterte Informationsaufgabe und Warnbefugnis im Hinblick auf Produkte) zum Tragen, die den Aktivitäten des BSI größere Wirkung verschaffen werden. Um in relevantem Umfang vor unsicheren Produkten warnen zu können, müssen die Untersuchungskapazitäten für Produkte deutlich ausgeweitet und die rechtskonformen Prozesse zur Verbraucherinformation und -warnung ausgebaut und fortentwickelt werden. Hierfür werden 18 Planstellen/Stellen benötigt.

- Identitätsdiebstahl entwickelt sich immer mehr zum Massenphänomen und Massenproblem. Der Appell zu sicheren Passwörtern kann das grundlegende Problem nicht mehr lösen, Identifizierungs- und Authentisierungsverfahren müssen

nutzerfreundlicher werden und zugleich das angemessene, notwendige Maß an Sicherheit bieten. Hier gilt es im Rahmen der neuen Aufgabe in § 3 Abs. 1 Satz 2 Nr. 19 BSIG-E, „Pflege und Weiterentwicklung sicherer Identitäten“, bestehende Ansätze fortzuentwickeln sowie neue Ansätze zu entwickeln und in die Anwendung zu überführen. Hierfür benötigt das BSI 8 Planstellen/Stellen.

- § 4a BSIG-E, Kontrolle der Kommunikationstechnik: Staatliche Stellen sind in besonderem Maße auf eine zuverlässige und sichere Kommunikation angewiesen. Daher sind an die Kommunikationstechnik des Bundes besonders hohe Sicherheitsanforderungen zu stellen. Diese besondere Sicherheit erfordert eine effektive und schnelle Kontrollmöglichkeit des Bundesamtes, um Gefahren für die Kommunikationstechnik früh zu erkennen und in der Folge zu beseitigen. Die Ausübung der neuen Kontroll- und Prüfbefugnisse, die für jede Einrichtung der Bundesverwaltung wahrgenommen werden kann, führt zu einem Personalbedarf von 64 Planstellen/Stellen.

- § 4b BSIG-E, Meldestelle: Die Sammlung von Informationen über Sicherheitslücken, Schadprogramme und IT-Sicherheitsvorfälle ist für ein Gesamtlagebild von besonderer Bedeutung. Um eine zentrale Sammlung und systematische Auswertung der an das Bundesamt gerichteten Hinweise auch angesichts der Vielzahl mit dem IT-SiG 2.0 hinzukommender Regelungsbereiche in angemessener Weise sicherzustellen, ist der Ausbau der Meldestelle beim BSI zwingend erforderlich. Der organisatorische und technische Ausbau sowie die kontinuierliche Beobachtung, Entgegennahme sowie Auswertung und Analyse der Meldungen führt zu einem zusätzlichen Personalbedarf von 14 Planstellen/Stellen.

- § 5 BSIG-E: Die Gefahr für die Kommunikationstechnik des Bundes ist quantitativ und qualitativ gestiegen. Um dieser eine effektive Abwehr entgegenzusetzen, muss das Bundesamt personell verstärkt werden. Die aktuell zur Verfügung stehenden Personalressourcen ermöglichen es nicht, die erforderlichen Detektionsmaßnahmen bei allen Behörden des Bundes in ausreichender Form zum Einsatz zu bringen. Neben Maßnahmen zur Sicherung der Kommunikationstechnik des Bundes erweitert das Gesetz auch die Möglichkeiten des Bundesamtes zur Unterstützung der Länder. Hierfür benötigt das BSI zusätzliche 29 Planstellen/Stellen.

- § 5a BSIG-E: Neben der Analyse von Protokolldaten im Sinne des BSIG ist zukünftig die Auswertung behördeninterner Protokollierungsdaten ein wesentlicher Bestandteil einer umfassenden Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes. Hieraus ergibt sich, dass nun in einem sehr viel größeren Maßstab auch Behörden, die noch nicht von der IT-Konsolidierung erfasst werden, Protokollierungsdaten an das BSI übermitteln müssen und das BSI diese bei dem gesamten Prozess (Planen, Sammeln, Detektieren, Auswerten) nach Mindeststandard zur Protokollierung und Detektion unterstützen muss. Hierbei ist zu beachten, dass eine sehr heterogene IT-Systemlandschaft besteht, welche eine individuelle Betreuung der Behörden erfordert. Die Detektion von Cyber-Angriffen durch eine systematische Analyse dieser Daten führt zu einem zusätzlichen Personalbedarf von 29 Planstellen/Stellen.

- In der heutigen Bedrohungslage sind präventive Schutz- und Abwehrmaßnahmen allein nicht mehr ausreichend. Angriffe werden auch bei bestmöglicher Prävention erfolgreich sein, sodass die Planung und Durchführung reaktiver Maßnahmen unerlässlich ist. Zu diesen zählt eine möglichst schnelle und sachkundige Zurückführung angegriffener Systeme und Netze in einen „sauberen“ Zustand, um die weitere Nutzbarkeit und Sicherheit der betroffenen Systeme und Netze sicherzustellen. Das Bundesamt hat zu diesem Zweck Mobile Incident Response

Teams (MIRTs) eingerichtet, die betroffenen Behörden der Bundesverwaltung sowie weiterer Bedarfsträger (andere Verfassungsorgane, Länder oder die Betreiber Kritischer Infrastrukturen) bei der Bewältigung von Sicherheitsvorfällen unterstützen. Durch die Erweiterung des Adressatenkreises entsteht für das BSI ein personeller Mehrbedarf von 41 Planstellen/Stellen.

- § 5c, § 8b Abs. 2 BSIG-E: Kommt es bei Betreibern Kritischer Infrastrukturen oder bei Unternehmen im besonderen öffentlichen Interesse zu größeren (IT-) Störungen, hat dies sehr schnell negative Auswirkungen auf große Teile der Bevölkerung. Zur Aufrechterhaltung oder Wiederherstellung von IT-Systemen im Falle einer erheblichen Störung ist eine bestehende, auch in Krisenlagen funktionsfähige Kommunikationsinfrastruktur von wesentlicher Bedeutung. Um die notwendigen Krisenreaktionsmaßnahmen zu erarbeiten sowie eine Struktur zwischen Bundesbehörden und den Betreibern Kritischer Infrastrukturen aufzubauen, zu pflegen und zu betreiben, sind beim BSI 44 Planstellen/Stellen erforderlich.

- § 5d BSIG: Die schnelle Information der Opfer eines Cyber-Angriffs und die Möglichkeit so früh wie möglich Unterstützung bei der Bewältigung anzubieten, ist eine elementare Aufgabe des Bundesamtes. Um die Opfer eines Angriffs identifizieren zu können, ist eine Bestandsdatenabfrage häufig unerlässlich. Zur effektiven Durchführung der damit verbundenen Aufgaben entsteht ein zusätzlicher Personalbedarf von 2 Planstellen/Stellen.

- Das Bundesamt muss in der Lage sein, technische Untersuchungen nach § 7a BSIG-E zur Erfüllung seiner gesetzlichen Aufgaben durchzuführen. Das Bundesamt wird mit Befugnissen ausgestattet, die zugleich auch zu weitergehenden und tieferen Prüfungen führen und damit einen Mehraufwand erzeugen. Durch die Erweiterung der Untersuchungsbefugnis entsteht ein Bedarf von 5 Planstellen/Stellen.

- § 7b BSIG-E: Um schnell und effektiv vor Sicherheitsrisiken für die Netz- und Informationssicherheit zu warnen, ist eine Detektion bestehender Risiken unerlässlich. Insbesondere für die Planung, Entwicklung und Wartung der Scanner als auch für die fachliche Begleitung aller Prüfungen sowie für die notwendigen Auswertungen und die Einschätzung der Ergebnisse werden weitere Fachkräfte benötigt. Um diese neue Aufgabe effektiv umzusetzen, benötigt das BSI 10 Planstellen/Stellen.

- § 7c BSIG-E: Um Detektionsmaßnahmen zum besonderen Schutz von Mitgliedern der Verfassungsorgane durchzuführen und hierdurch das Bundeskriminalamt zu unterstützen, entsteht dem Bundesamt zudem ein Personalbedarf von zusätzlichen 2 Planstellen/Stellen.

- § 8 BSIG-E: Die Digitalisierungsvorhaben der Bundesregierung erfordern eine konstante Beratung und Begleitung durch das Bundesamt, um bereits ab der Konzeptions- und Planungsphase die Aspekte der IT-Sicherheit zu berücksichtigen. Angesichts der Vielzahl der anstehenden Digitalisierungsprojekte entsteht, aufgrund des hierdurch entstehenden Beratungsaufwands, ein Personalbedarf von 71 Planstellen/Stellen.

- Durch die Aufnahme weiterer Branchen in den Regelungsbereich des Gesetzes sowie die Ergänzung des BSIG um den Bereich der Unternehmen im besonderen öffentlichen Interesse entsteht ein personeller Mehrbedarf des BSI von insgesamt 56 Planstellen/Stellen.

- Die in § 8a Absatz 6 eingefügte Vertrauenswürdigkeitserklärung für kritische Komponenten (im Rahmen von Zertifizierungen) führt zu einem erhöhten Personalbedarf von XX Stellen (wird nachgereicht)

- § 9a BSIG-E: Durch die Konzeption und Vergabe eines IT-Sicherheitskennzeichens sollen insbesondere Verbraucherinnen und Verbraucher in die Lage versetzt werden, den Aspekt der IT-Sicherheit bei der Auswahl ihrer IT-Produkte in einfacher Form berücksichtigen zu können, indem sie schnell und einfach überprüfen können, ob das jeweilige IT-Produkt bzw. dessen Hersteller aktuelle Sicherheitsstandards in ausreichender Form berücksichtigt. Um die für die Vergabe des IT-Sicherheitskennzeichens erforderlichen Arbeiten inklusive der im Sinne einer Marktaufsicht anstehenden Prüfungen und Kontrollen durchführen zu können, benötigt das Bundesamt 25 zusätzliche Planstellen/Stellen.

- § 14 BSIG-E: Die Erweiterung der Bußgeldvorschriften führt zu einem erhöhten Prüfungs- und Verwaltungsaufwand. Das BSI benötigt zur Bewältigung dieses zusätzlichen Aufwandes 2 weitere Planstellen/Stellen.

Für die Umsetzung des Zweiten IT-Sicherheitsgesetzes kommen für die BDBOS folgende neue Aufgaben hinzu:

- § 4a BSIG-E: Die Kontrollbefugnisse des BSI verursachen Mitwirkungs-, Unterstützungs- und Berichtspflichten auf Seiten der BDBOS, die zu einem Personalbedarf von 6 Planstellen führen.

- § 5 Absatz 11 und § 5a BSIG-E: Durch die neue Regelung darf das BSI Protokolldaten von Infrastrukturen erheben und auswerten, wofür neue Prozesse und Schnittstellen geschaffen werden müssen. Die hierfür erforderlichen Mehraufwendungen ergeben sich bereits aus dem Mindeststandard zur Protokollierung. Hier fällt ein Personalaufwand von einmalig 1-2 Personenwochen sowie 12 Personentage p.p.a. für die Einrichtung, Wartung und Pflege der Infrastruktur an. Für die Daueraufgabe der Protokollierung erfordert mindestens 1 Planstelle, sofern die BDBOS die Protokollierung über die vom BSI angebotenen Dienstleistungen zur Detektion nicht möglich ist.

  Andernfalls sind die Aufwände deutlich größer. Die BDBOS muss in diesem Fall für die von ihr betriebenen Infrastrukturen Technik, Organisation und Prozesse aufsetzen und anpassen, um die notwendigen Protokolldaten systematisch zu erfassen, auszuwerten und an das BSI weitergeben zu können. Insgesamt ist für die Umsetzung dieser Änderungen in § 5 und § 5a ein Personalmehrbedarf von 30 Planstellen in der BDBOS anzusetzen. Zusätzlich entstehen hier einmalige technische Aufwände in Höhe von 5 Mio. Euro.

- §§ 5c, 8b BSIG-E: Für die Änderungen betreffend die Krisenkommunikation mit KRITIS-Unternehmen und deren Integration in die Kommunikationsnetze und Betriebsinfrastrukturen der BDBOS ist ein Personalbedarf von 8 Planstellen erforderlich. Dies ergibt sich aus der Unterstützung des BSI bei insbesondere folgenden Aufgaben:
  - Erstellung von Krisenreaktionsplänen
  - Anhörung der Betroffenen
  - Fachliche Beratung und Einbindung in Gesamtkonzepte
  - Pflegeaufwand nach Abstimmung
  - Unterstützung der Beübung
- § 8 BSIG: Zur Umsetzung der besonders hohen Sicherheitsanforderungen und sich stetig fortentwickelnden Mindeststandards für die Kommunikationstechnik des

Bundes erhöhen sich bei der BDBOS die Aufwände für die technische Konzeption der von ihr betriebenen Netze sowie für die Erstellung und Sicherstellung der Umsetzung der erforderlichen Sicherheitskonzepte für die einzelnen KRITIS-Kernkomponenten der Netze und für die Netze in ihrer jeweiligen Gesamtheit. Es entsteht bei der BDBOS ein Personalbedarf von 10 Planstellen.

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe wirkt mit bei der Erstellung und Änderung des Gesamtplans für die Reaktionsmaßnahmen des Bundes gemäß § 5c, bei der Prüfung von Standards gemäß § 8a Abs. 2, in der Erstellung von Auswirkungsanalysen nach § 8b Abs. 2 sowie im Bereich Krisenkommunikationssystem nach § 8b Abs. 2. Aufgrund der Ausweitung des Adressatenkreises um den Bereich Entsorgung (§ 2 Abs. 10) sowie Unternehmen im besonderen öffentlichen Interesse (§ 2 Abs. 14), was sich auf die Wahrnehmung der bestehenden Aufgaben nach § 8a und § 8b auswirken wird, und aufgrund der neuen Aufgaben im Bereich Gesamtplan für Reaktionsmaßnahmen und Krisenkommunikationssystem ist ein Erfüllungsaufwand in Höhe von insgesamt 47 Planstellen erforderlich. Hierfür fallen jährlich Personalkosten in Höhe von XXX Euro an.

F. Weitere Kosten

Keine.

Referentenentwurf der Bundesregierung

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

(Zweites IT-Sicherheitsgesetz – IT-SiG 2.0)

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)

Das Gesetz über das Bundesamt für die Sicherheit in der Informationstechnik (BSIG-BSI-Gesetz) in der Fassung der Bekanntmachung vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 13 des Gesetzes vom 20. November 2019 (BGBl. I S. 1626) geändert worden ist, wird wie folgt geändert:

1. § 2 wird wie folgt geändert:

   a) Absatz 3 Satz 1 wird durch folgenden Satz ersetzt:

   „Kommunikationstechnik des Bundes im Sinne dieses Gesetzes ist die Informationstechnik, die von einer oder mehreren Bundesbehörden oder im Auftrag einer oder mehrerer Bundesbehörden betrieben wird und der Kommunikation oder der Datenverarbeitung innerhalb einer Bundesbehörde, der Bundesbehörden untereinander oder mit Dritten dient.“

   b) Nach Absatz 8 wird nachfolgender Absatz 8a eingefügt:

   „(8a) Protokollierungsdaten sind Aufzeichnungen über die Art und Weise, wie die Informationstechnik genutzt wurde, über technische Ereignisse oder Zustände innerhalb eines informationstechnischen Systems und wie dieses mit anderen kommuniziert hat. Protokollierungsdaten dienen der Erkennung, Eingrenzung oder Beseitigung von Störungen oder Fehlern bei der Kommunikationstechnik oder von Angriffen.“

   c) Nach Absatz 9 werden folgende Absätze 9a und 9b eingefügt:

   „(9a) IT-Produkte sind Software sowie alle einzelnen oder miteinander verbundenen Hardwareprodukte.

   (9b) Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten.“

d) In Absatz 10 Satz 1 Nummer 1 werden nach dem Wort „Versicherungswesen“ die Wörter „oder Entsorgung“ eingefügt.

e) Nach Absatz 12 werden folgende Absätze 13 und 14 eingefügt:

„(13) Kritische Komponenten im Sinne dieses Gesetzes sind IT-Produkte, die in Kritischen Infrastrukturen eingesetzt werden und die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit dieser IT-Produkte zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können. Die kritischen Komponenten im Sinne dieses Gesetzes werden für Betreiber nach § 8d Abs. 2 Nr. 1 durch den Katalog von Sicherheitsanforderungen nach § 109 Abs. 6 TKG näher bestimmt. Alle übrigen kritischen Komponenten werden in einem Katalog des Bundesamtes näher bestimmt. Das Bundesamt gibt den Betreibern Kritischer Infrastrukturen Gelegenheit zur Stellungnahme. Der Katalog wird vom Bundesamt veröffentlicht.

(14) Unternehmen im besonderem öffentlichen Interesse sind Unternehmen, die nicht Betreiber Kritischer Infrastrukturen nach Absatz 10 sind,

1. deren Geschäftstätigkeit unter § 60 Absatz 1 Nummer 1 bis 5 der Außenwirtschaftsverordnung in der jeweils geltenden Fassung fällt,

2. die aufgrund ihrer volkswirtschaftlichen Bedeutung und insbesondere ihrer erbrachten Wertschöpfung von besonderem öffentlichen Interesse sind oder

3. die einer Regulierung nach der Verordnung zum Schutz vor Gefahrstoffen in der jeweils geltenden Fassung unterliegen

Die Unternehmen im besonderem öffentlichen Interesse nach Nummer 2 werden durch die Rechtsverordnung nach § 10 Absatz 5 näher bestimmt.“

2. § 3 Absatz 1 Satz 2 wird wie folgt geändert:

a) In Nummer 2 wird das Wort „oder“ gestrichen.

b) Nach Nummer 5 wird folgende Nummer 5a eingefügt:

„5a. Erteilung von Befugnissen nach § 1 Absatz 2 des Gesetzes über die Akkreditierungsstelle als Konformitätsbewertungsstelle im Bereich der IT-Sicherheit tätig zu sein, insbesondere durch Anerkennung sachverständiger Stellen zur Durchführung von Prüfungen und Bewertungen im Rahmen der Zertifizierung. nach § 9 Absatz 3;“

c) Nach Nummer 5a wird folgende Nummer 5b eingefügt:

„5b. Wahrnehmung der Aufgaben und Befugnisse nach Artikel 58 Absatz 7 und 8 der Verordnung (EU) 2019/881 vom 17. April 2019 als nationale Behörde für die Cybersicherheitszertifizierung;“

d) Nummer 14 wird durch die folgende Nummer 14 ersetzt:

„14. Beratung, Information und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik, insbesondere unter besonderer Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;“

e) Nach Nummer 14 wird folgende Nummer 14a eingefügt:

„14a. Förderung des Verbraucherschutzes und der Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik, insbesondere durch Wahrnehmung der Aufgabe nach Nummer 14 gegenüber Verbrauchern;“

f) Nummer 17 wird durch folgende Nummer 17 ersetzt:

„17. Aufgaben nach den §§ 8a bis 8f als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen, digitaler Dienste, der Unternehmen im besonderen öffentlichen Interesse und der Hersteller von IT-Produkten;“

g) In Nummer 18 wird der Punkt durch ein Semikolon ersetzt.

h) Nach Nummer 18 werden folgende Nummern 19 und 20 eingefügt:

„19. Empfehlungen für Identifizierungs- und Authentisierungsverfahren und Bewertung dieser Verfahren unter dem Gesichtspunkt der Informationssicherheit;

20. Entwicklung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte.“

3. In § 4 Absatz 2 Nummer 1 werden nach dem Wort „Informationen,“ ein Komma und die Wörter „einschließlich personenbezogener Daten,“ eingefügt.

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

„§ 4a

Kontrolle der Kommunikationstechnik des Bundes

(1) Das Bundesamt ist befugt, die Sicherheit der Kommunikationstechnik des Bundes und ihrer Komponenten, einschließlich technischer Infrastrukturen, die zu deren Betrieb erforderlich sind, zu überprüfen und zu kontrollieren. Es kann hierzu die Bereitstellung aller zur Aufgabenerfüllung erforderlichen Informationen, insbesondere zu technischen Details, zu Strategien, Planungen und Regelungen mit Bezug zur Kommunikationstechnik des Bundes einschließlich Aufbau- und Ablauforganisation, verlangen sowie Unterlagen und Datenträger des Betreibers der jeweiligen Kommunikationstechnik des Bundes oder eines mit Betriebsleistungen beauftragten Dritten einsehen und hiervon unentgeltlich Abschriften, Auszüge, Ausdrucke oder Kopien, auch von Datenträgern, anfertigen oder Ausdrucke von elektronisch gespeicherten Daten verlangen, soweit nicht Geheimschutzinteressen oder überwiegende Sicherheitsinteressen entgegenstehen.

(2) Dem Bundesamt ist in den Zeiten, zu denen die Räume normalerweise für die jeweilige geschäftliche oder betriebliche Nutzung zur Verfügung stehen, zu den Grundstücken und Betriebsräumen, einschließlich Datenverarbeitungsanlagen und -geräten, die für die Kommunikationstechnik des Bundes verwendet werden, Zugang zu gewähren, soweit dies zur Erfüllung der Zwecke nach Absatz 1 erforderlich ist.

(3) Bei Einrichtungen von Dritten, bei denen Schnittstellen zur Kommunikationstechnik des Bundes bestehen, kann das Bundesamt auf der Schnittstellenseite der Einrichtung im Einvernehmen mit dem Dritten die Sicherheit der Schnittstelle überprüfen und kontrollieren. Es kann hierzu im Einvernehmen mit dem Dritten die zur Aufgabenerfüllung erforderlichen Informationen, insbesondere zu technischen Details, zu Strategien, Planungen und Regelungen sowie Unterlagen und

Datenträger des Betreibers einsehen und hiervon unentgeltlich Abschriften, Auszüge, Ausdrucke oder Kopien, auch von Datenträgern, oder Ausdrucke von elektronisch gespeicherten Daten anfertigen.

(4) Das Bundesamt teilt sein Ergebnis der Überprüfung und Kontrolle nach Absatz 1 der jeweiligen überprüften Stelle sowie im Falle einer öffentlichen Stelle des Bundes ihrer jeweiligen Rechts- und Fachaufsicht mit. Damit kann es Vorschläge zur Verbesserung der Informationssicherheit, insbesondere zur Beseitigung der festgestellten Mängel, verbinden.

§ 4b

Allgemeine Meldestelle für die Sicherheit in der Informationstechnik

(1) Das Bundesamt fördert die Sicherheit in der Informationstechnik. Hierzu nimmt es als allgemeine Meldestelle Informationen über Sicherheitsrisiken in der Informationstechnik entgegen und wertet diese aus.

(2) Das Bundesamt kann zur Wahrnehmung der in Absatz 1 Satz 1 genannten Aufgabe Informationen zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweisen entgegennehmen. Das Bundesamt richtet hierzu geeignete Meldemöglichkeiten ein. Die Meldungen können anonym erfolgen. Soweit die Meldung nicht anonym erfolgt, kann der Meldende im Rahmen der Meldung verlangen, dass seine Daten nur anonymisiert weitergegeben werden dürfen. In diesem Fall gelten § 5 Absatz 5 und Absatz 6 Satz 1 entsprechend.

(3) Das Bundesamt kann die gemäß Absatz 2 gemeldeten Informationen verarbeiten, um:

1. Dritte über bekanntgewordene Sicherheitslücken, Schadprogramme, erfolgte oder versuchte Angriffe auf die Sicherheit in der Informationstechnik zu informieren, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist,

2. im Benehmen mit der zuständigen Aufsichtsbehörde die Öffentlichkeit gemäß § 7 zu warnen,

3. Bundesbehörden gemäß § 4 Absatz 2 Nummer 2 über die sie betreffenden Informationen zu unterrichten,

4. Betreiber Kritischer Infrastrukturen gemäß § 8b Absatz 2 Nummer 4 Buchstabe a) über die sie betreffenden Informationen zu unterrichten.

(4) Eine Weitergabe nach Absatz 3 Nummern 1, 2 und 4 erfolgt nicht, soweit die gemäß Absatz 2 gemeldeten Informationen:

1. Betriebs- und Geschäftsgeheimnisse von Dritten beinhalten und die Maßnahmen nach Absatz 3 Satz 1 nicht ohne Bekanntgabe dieser Betriebs- und Geschäftsgeheimnisse durchgeführt werden können oder

2. auf Grund von Vereinbarungen mit Dritten nicht übermittelt werden dürfen.

Sonstige gesetzliche Übermittlungshindernisse und Regelungen zum Geheimschutz bleiben unberührt.

(5) Erlangt das Bundesamt im Rahmen einer Meldung nach Absatz 2 Kenntnis von der Identität des Meldenden, so kann eine Übermittlung dieser personenbezogenen Daten unterbleiben, wenn für das Bundesamt erkennbar ist, dass unter Berücksichtigung der Schwere einer gemeldeten Sicherheitslücke, eines Schadprogramms, eines erfolgten oder versuchten Angriffs auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweisen sowie der Art und Weise, mittels derer der Meldende diese Erkenntnisse gewonnen hat, die schutzwürdigen Interessen des Meldenden das Allgemeininteresse an der Übermittlung überwiegen. Die Entscheidung nach Satz 1 muss dem oder der behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem oder einer weiteren Bediensteten des Bundesamtes, der oder die die Befähigung zum Richteramt hat, zur vorherigen Entscheidung vorgelegt werden.

(6) Bestehende gesetzliche Meldepflichten und Übermittlungsregelungen bleiben unberührt.“

5. § 5 wird wie folgt geändert:

a) Absatz 2 wird wie folgt gefasst:

„(2) Protokolldaten nach Absatz 1 Satz 1 Nummer 1 dürfen über den für die automatisierte Auswertung nach Absatz 1 Satz 1 Nummer 1 erforderlichen Zeitraum hinaus, längstens jedoch für 18 Monate, gespeichert werden. Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Auswertung der nach diesem Absatz gespeicherten Daten nur automatisiert erfolgt und dass ein Zugriff auf Daten, die länger als drei Monate gespeichert sind, nur beim Vorliegen tatsächlicher Erkenntnisse über die Betroffenheit des Bundes mit einem Schadprogramm erfolgt. Die Daten sind zu pseudonymisieren. Eine nicht automatisierte Verarbeitung ist nur nach Maßgabe der nachfolgenden Absätze zulässig. Soweit hierzu die Wiederherstellung pseudonymisierter Protokolldaten erforderlich ist, muss diese durch die Präsidentin oder den Präsidenten des Bundesamtes oder der Vertretung im Amt angeordnet werden.“

b) Nach Absatz 2 wird folgender Absatz 2a eingefügt:

„(2a) Protokolldaten dürfen vor ihrer Pseudonymisierung und Speicherung nach Absatz 2 zur Sicherstellung einer fehlerfreien automatisierten Auswertung manuell verarbeitet werden. Liegen Hinweise vor, dass die fehlerfreie automatisierte Auswertung wegen eines erheblichen Fehlers erschwert wird, darf der Personenbezug von Protokolldaten zur Sicherstellung der fehlerfreien automatisierten Auswertung wiederhergestellt werden, sofern dies im Einzelfall erforderlich ist. Absatz 2 Satz 5 bis 8 gilt entsprechend.“

c) Nach Absatz 10 wird folgender Absatz 11 angefügt:

„(11) Zur Abwehr von Gefahren für die Kommunikationstechnik der Länder darf das Bundesamt Maßnahmen nach Absatz 1 auf deren Ersuchen durchführen. Hierbei gelten die Absätze 2 bis 10 entsprechend.“

6. Nach § 5 wird folgender § 5a eingefügt:

„§ 5a

Verarbeitung behördeninterner Protokollierungsdaten

Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes Protokollierungsdaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, verarbeiten und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist und Geheimschutzinteressen oder überwiegende Sicherheitsinteressen nicht entgegen stehen. Die Bundesbehörden sind verpflichtet, das Bundesamt bei Maßnahmen nach Satz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu behördeninternen Protokollierungsdaten nach Satz 1 sicherzustellen. § 5 Absatz 2 bis 4 sowie Absatz 8 und 9 gelten entsprechend.“

7. Der § 5a wird wie folgt geändert:

a) Die Bezeichnung „§ 5a“ wird durch die Bezeichnung „§ 5b“ ersetzt.

b) In Absatz 1 Satz 1 werden nach den Wörtern „Kritischen Infrastruktur“ die Wörter „oder eines Unternehmens im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1, 2 oder 3“ eingefügt.

c) Nach Absatz 7 Satz 1 wird der Satz „Ein begründeter Einzelfall liegt in der Regel vor, wenn eine Stelle eines Landes betroffen ist.“ eingefügt:

8. Nach § 5b werden die folgenden §§ 5c und 5d eingefügt:

„§ 5c

Sicherheit und Funktionsfähigkeit informationstechnischer Systeme im Falle erheblicher Störungen

(1) Das Bundesamt stellt im Einvernehmen mit

1. dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und

2. der jeweils zuständigen Aufsichtsbehörde des Bundes

einen Gesamtplan für die Reaktionsmaßnahmen des Bundes auf, um die Aufrechterhaltung oder Wiederherstellung der informationstechnischen Systeme, Komponenten oder Prozesse bei Betreibern Kritischer Infrastrukturen oder Unternehmen im besonderen öffentlichen Interesse für den Fall einer erheblichen Störung im Sinne des § 8b Absatz 4 Nummer 2, die zu erheblichen Versorgungsengpässen oder Gefährdungen für die öffentliche Sicherheit führen können, sicherzustellen. Sofern nach Satz 1 keine zuständige Aufsichtsbehörde des Bundes benannt ist, ist das zuständige Ressort zu beteiligen.

(2) Der Gesamtplan soll die an der Krisenreaktion beteiligten Behörden, Betreiber Kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse in die Lage versetzen, im Notfall unverzüglich Entscheidungen zu treffen und die erforderlichen Maßnahmen rechtzeitig durchzuführen.

(3) Bei der Erstellung und bei wesentlichen Änderungen des Gesamtplans wird das Benehmen mit den Betroffenen hergestellt. Die Krisenreaktionspläne werden regelmäßig unter Berücksichtigung von Erkenntnissen aus bewältigten Krisen im

Bereich der Sicherheit in der Informationstechnik sowie den Veränderungen des Stands der Technik und der Rechtslage überprüft und falls erforderlich angepasst.

(4) Während einer erheblichen Störung gemäß § 8b Absatz 4 Nummer 2 kann das Bundesamt im Benehmen mit den jeweils im Einzelfall nach § 5 Absatz 5 zu beteiligenden Stellen

1. den Betroffenen die zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten übermitteln,

2. von den Betroffenen die Herausgabe der zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten verlangen,

3. im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe gegenüber den Betroffenen die erforderlichen informationstechnischen Maßnahmen für die Wiederherstellung der Sicherheit und der Funktionsfähigkeit ihrer informationstechnischen Systeme anordnen, um erhebliche Versorgungsengpässe oder Gefährdungen für wichtige Rechtsgüter, insbesondere für Leib und Leben sowie für die öffentliche Sicherheit, abzuwenden, wenn der Betroffene die erhebliche Störung nicht unverzüglich selbst beseitigt oder zu erwarten ist, dass der Betroffene die erhebliche Störung nicht selbst unverzüglich beseitigen kann.

§ 5d

Bestandsdatenauskunft

(1) Das Bundesamt darf nach dem in der Rechtsverordnung nach § 112 Absatz 3 des Telekommunikationsgesetzes geregelten Verfahren von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den § 111 des Telekommunikationsgesetzes erhobenen Daten verlangen, wenn das Bundesamt im Rahmen seiner gesetzlichen Aufgabenerfüllung von ziel- und zweckgerichteten Beeinträchtigungen der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme Dritter Kenntnis erlangt hat, die schutzwürdigen Interessen des betroffenen Dritten eine unmittelbare Kontaktaufnahme durch das Bundesamt mit ihm als erforderlich erscheinen lassen, um im Einzelfall weitergehende Angriffe auf die Sicherheit oder Funktionsfähigkeit informationstechnischen Systeme zu verhindern oder sonstige Schäden vom betroffenen Dritten abzuwenden, und die Auskunft für die Kontaktaufnahme erforderlich ist.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden.

(3) Nach erfolgter Auskunft weist das Bundesamt den Betroffenen auf die bei ihm festgestellten Beeinträchtigungen hin. Nach Möglichkeit weist das Bundesamt den Betroffenen auf angemessene, wirksame und zugängliche technische Mittel hin, mittels derer die festgestellten Beeinträchtigungen durch den Betroffenen selbst beseitigt werden können. In den Fällen des Absatzes 2 ist der Betroffene über die Auskunft zu benachrichtigen. Im Falle der Weitergabe der Information nach § 5 Absatz 5 oder wenn Tatsachen die Annahme rechtfertigen, dass die Voraussetzungen einer Weitergabe nach § 5 Absatz 5 vorliegen, ergeht keine Benachrichtigung an den Betroffenen.

(4) Das Bundesamt kann personenbezogene Daten, die es im Rahmen dieser Vorschrift verarbeitet, entsprechend § 5 Absatz 5 und 6 übermitteln.

(5) Das Bundesamt unterrichtet die oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über

1. die Anzahl der Vorgänge, in denen Daten nach Absatz 1 oder Absatz 2 an das Bundesamt übermittelt wurden,

2. Übermittlungen nach Absatz 4.“

9. § 7 wird wie folgt geändert:

a) Absatz 1 wird wie folgt gefasst:

„(1) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 und Nummer 14a 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 und

d) Informationen über sicherheitsrelevante IT-Eigenschaften der Produkte.

2. Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte, informationstechnischer Produkte und Dienste empfehlen.

Das Bundesamt kann zur Wahrnehmung der Aufgaben nach Satz 1 Dritte einbeziehen, wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist. Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung der Warnungen zu informieren. Diese Informationspflicht besteht nicht, wenn hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks gefährdet wird oder wenn berechtigterweise davon ausgegangen werden kann, dass der Hersteller an einer vorherigen Benachrichtigung kein Interesse hat. Soweit entdeckte Sicherheitslücken oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern oder weil das Bundesamt gegenüber Dritten zur Vertraulichkeit verpflichtet ist, kann es den Kreis der zu warnenden Personen einschränken; Kriterien hierfür sind insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere Zuverlässigkeit des Empfängers.“

b) Absatz 2 Satz 1 wird wie folgt geändert:

aa) Nach der Angabe „Nummer 14“ wird die Angabe „und Nummer 14a“ eingefügt.

bb) Nach den Wörtern „sowie den Einsatz bestimmter“ werden die Wörter „informationstechnischer Produkte und Dienste“ eingefügt.

10. § 7a wird wie folgt gefasst:

„§ 7a

Untersuchung der Sicherheit in der Informationstechnik

(1) Das Bundesamt kann zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen.

(2) Soweit erforderlich kann das Bundesamt für Untersuchungen nach Absatz 1 von Herstellern informationstechnischer Produkte und Systeme alle notwendigen Auskünfte, insbesondere auch zu technischen Details, verlangen. Bei der Versendung des Auskunftsverlangens an einen Hersteller gibt das Bundesamt die Rechtsgrundlage, den Zweck des Auskunftsverlangens und die benötigten Auskünfte an und legt eine angemessene Frist für die Übermittlung der Auskünfte fest. Das Auskunftsverlangen enthält ferner einen Hinweis auf die in § 14 vorgesehenen Sanktionen.

(3) Das Bundesamt gibt Auskünfte sowie die aus den Untersuchungen gewonnen Erkenntnisse unverzüglich an die zuständigen Aufsichtsbehörden des Bundes oder sofern keine Aufsichtsbehörde vorhanden ist, an das jeweilige Ressort weiter, wenn Anhaltspunkte bestehen, dass diese sie zur Erfüllung ihrer Aufgaben benötigen.

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

(5) Kommt ein Hersteller der Aufforderung des Bundesamtes nach Absatz 2 Satz 1 nicht oder nur unzureichend nach, kann das Bundesamt hierüber die Öffentlichkeit informieren. Es kann hierbei den Namen des Herstellers sowie die Bezeichnung des betroffenen Produkts oder Systems angeben, und darlegen inwieweit der Hersteller seiner Auskunftspflicht nicht nachgekommen ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu gewähren. § 7 Absatz 2 Satz 2 gilt entsprechend.“

11. Nach § 7a werden folgende §§ 7b und 7c eingefügt:

„§ 7b

Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden

(1) Das Bundesamt kann zur Erfüllung seiner Aufgaben Maßnahmen zur Detektion von Schadprogrammen, Sicherheitslücken und anderen Sicherheitsrisiken in öffentlich erreichbaren informationstechnischen Systemen durchführen, wenn Tatsachen die Annahme rechtfertigen, dass diese ungeschützt sind und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können. Erlangt es dabei Informationen, die dem Fernmeldegeheimnis unterliegen, darf es diese nur entsprechend § 5 Absatz 5 und 6 BSIG übermitteln.

(2) Ein informationstechnisches System im Sinne des Absatzes 1 ist ungeschützt, wenn auf diesem öffentlich bekannte Sicherheitslücken bestehen oder wenn auf Grund

sonstiger offensichtlich unzureichender Sicherheitsvorkehrungen unbefugt von Dritten auf das System zugegriffen werden kann.

(3) Wird durch Maßnahmen gemäß Absatz 1 ein Schadprogramm, eine Sicherheitslücke oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt, sind die für das informationstechnische System Verantwortlichen oder hilfsweise der betreibende Dienstleister des jeweiligen Netzes oder Systems unverzüglich zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßige weitere Ermittlungen möglich ist und überwiegende Sicherheitsinteressen nicht entgegenstehen. Das Bundesamt kann anordnen, dass der Diensteanbieter Maßnahmen gemäß § 109a Absatz 4 des Telekommunikationsgesetzes ergreift. Das Bundesamt unterrichtet die oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kalenderjährlich jeweils bis zum 30. Juni des Folgejahres über die Anzahl der Vorgänge gemäß Absatz 1.

(4) Das Bundesamt darf zur Erfüllung seiner Aufgaben Systeme und Verfahren einsetzen, welche einem Angreifer einen erfolgreichen Angriff vortäuschen, um Schadprogramme und andere Angriffsmethoden zu erheben und auszuwerten. Das Bundesamt darf die hierzu erforderlichen Daten verarbeiten.

§ 7c

Detektion zum Schutz der Mitglieder der Verfassungsorgane

Das Bundesamt kann das Bundeskriminalamt auf dessen Ersuchen zur Erfüllung der Aufgaben nach § 6 Bundeskriminalamtsgesetzes mit Maßnahmen zur Detektion und Auswertung von Sicherheitslücken und anderen Sicherheitsrisiken in öffentlich zugänglichen und ungeschützten informationstechnischen Systemen unterstützen. § 7b Absätze 2 und 3 gelten entsprechend.“

12. § 8 wird wie folgt geändert:

a) Absatz 1 wird wie folgt gefasst:

„(1) Das Bundesamt legt im Benehmen mit den Ressorts Mindeststandards für die Sicherheit der Informationstechnik des Bundes fest, die von

1. Stellen des Bundes,

2. Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihrer Vereinigungen ungeachtet ihrer Rechtsform auf Bundesebene, soweit von der jeweils zuständigen obersten Bundesbehörde angeordnet, sowie von

3. öffentlichen Unternehmen, die mehrheitlich im Eigentum des Bundes stehen und die IT-Dienstleistungen für die Bundesverwaltung erbringen,

umzusetzen sind. Abweichungen von den Mindeststandards sind nur in sachlich gerechtfertigten Fällen zulässig, sie sind zu dokumentieren und zu begründen. Das Bundesministerium des Innern, für Bau und Heimat kann im Benehmen mit der Konferenz der IT-Beauftragten der Ressorts bei bedeutenden Mindeststandards die Überwachung und Kontrolle ihrer Einhaltung durch das Bundesamt anordnen. Das Bundesamt teilt das Ergebnis seiner Kontrolle der jeweiligen überprüften Stelle, deren jeweiliger zuständiger Aufsichtsbehörde sowie der Konferenz der IT-Beauftragten der Ressorts mit. Für andere öffentlich- oder privatrechtlich organisierte Stellen

dürfen nur dann Schnittstellen zur Kommunikationstechnik des Bundes eingerichtet werden, soweit die für die Einrichtung verantwortliche Stelle vertraglich sicherstellt, dass die öffentlich- oder privatrechtlich organisierte Stelle sich zur Einhaltung der Mindeststandards verpflichtet. Das Bundesamt kann im Einvernehmen mit dem Dritten die Einhaltung der Mindeststandards überprüfen und kontrollieren. Das Bundesamt berät die unter Satz 1 und 6 genannten Stellen 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.“

b) In Absatz 3 Satz 4 wird das Wort „Bundesbehörden“ durch die Wörter „Stellen des Bundes oder von ihnen beauftragte Dritte“ ersetzt.

c) Nach Absatz 3 wird folgender Absatz 4 angefügt:

„(4) Zur Gewährleistung der Sicherheit in der Informationstechnik bei der Planung und Umsetzung von Digitalisierungsvorhaben des Bundes ist das Bundesamt durch die jeweils verantwortliche Stelle frühzeitig zu beteiligen und dem Bundesamt Gelegenheit zur Stellungnahme zu geben.“

13. § 8a wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) Nach Satz 2 wird folgender Satz 3 eingefügt:

„Zur Umsetzung von Maßnahmen nach Satz 1 können Betreiber Kritischer Infrastrukturen auch geeignete Prozesse vorsehen, um die Vertrauenswürdigkeit der Beschäftigten zu überprüfen, die in Bereichen tätig sind, in denen in besonderem Maße auf die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit informationstechnischer Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der Kritischen Infrastruktur maßgeblich sind, eingewirkt werden kann.“

bb) Der bisherige Satz 3 wird Satz 4.

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

„(1a) Die Verpflichtung der Betreiber Kritischer Infrastrukturen, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen nach Absatz 1 Satz 1 zu treffen, umfasst auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung haben dem jeweiligen Stand der Technik zu entsprechen. Die Einhaltung des Standes der Technik wird vermutet, wenn die Systeme der Technischen Richtlinie [Bezeichnung] des Bundesamtes in der jeweils geltenden Fassung entsprechen.

(1b) Die Betreiber Kritischer Infrastrukturen dürfen die für den Einsatz von Systemen zur Angriffserkennung erforderlichen Daten verarbeiten. Die im Rahmen des Einsatzes von Systemen zur Angriffserkennung verarbeiteten Daten sind unverzüglich zu löschen, wenn sie für die Vermeidung von Störungen nach Absatz 1 Satz 1 nicht mehr erforderlich sind, spätestens jedoch nach zehn Jahren.

(1c) Im Rahmen des Einsatzes von Systemen zur Angriffserkennung erhobene Daten, die für den Schutz vor Angriffen auf Informationstechnik oder die Aufklärung und Strafverfolgung eines Angriffs erforderlich sind, haben die Betreiber den dafür zuständigen Behörden zu übermitteln.“

c) Absatz 3 wird wie folgt geändert:

aa) Nach Satz 3 wird folgender Satz 4 eingefügt:

„Die Betreiber übermitteln dem Bundesamt dabei zusätzlich eine Liste aller IT-Produkte, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen von Bedeutung sind, weil Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit dieser IT-Produkte zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit einer Kritischen Infrastruktur oder zu einer Gefährdung der öffentlichen Sicherheit und Ordnung führen können.“

bb) Die bisherigen Sätze 4 und 5 werden die Sätze 5 und 6.

14. § 8b wird wie folgt geändert:

a) In Absatz 2 Nummer 3 werden nach den Wörtern „Kritischen Infrastrukturen“ die Wörter „oder Unternehmen im besonderen öffentlichen Interesse“ angefügt.

b) In Absatz 2 Nummer 4 wird der Buchstabe a wie folgt ersetzt:

„a) die Betreiber Kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse über sie betreffende Informationen nach den Nummern 1 bis 3“

c) An Absatz 2 werden folgende Sätze angefügt:

„Es regelt die Anspruchsberechtigungen für den Zugang von Betreibern Kritischer Infrastrukturen zu einem einheitlichen Krisenkommunikationssystem, welches eine geeignete Kommunikationsinfrastruktur zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung bereitstellt, ohne dass hierdurch Doppelstrukturen zu den Netzinfrastrukturen und Diensten der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben geschaffen werden. Die zuständigen Aufsichtsbehörden, das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, die sonst zuständigen Behörden des Bundes und die zuständigen Aufsichtsbehörden der Länder haben dem Bundesamt unverzüglich vorliegende Informationen nach Satz 1 Nummer 1 bis 4 zu melden, soweit nicht gesetzliche Regelungen entgegenstehen.“

d) Der Absatz 3 wird wie folgt gefasst:

„(3) Betreiber Kritischer Infrastrukturen sind verpflichtet, die von ihnen betriebenen Kritischen Infrastrukturen im Sinne des § 2 Absatz 10 in Verbindung mit der Rechtsverordnung nach § 10 Absatz 1 beim Bundesamt zu registrieren und eine Kontaktstelle zu benennen. Die Betreiber haben sicherzustellen, dass sie über die benannte Kontaktstelle jederzeit erreichbar sind. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Kontaktstelle.“

e) Nach dem Absatz 3 werden die folgenden Absätze 3a, 3b, 3c und 3d eingefügt:

„(3a) Rechtfertigen Tatsachen die Annahme, dass eine Anlage oder Teile davon nach der Rechtsverordnung nach § 10 Absatz 1 eine Kritische Infrastruktur nach diesem Gesetz ist oder sind und der Betreiber seine Pflicht zur Registrierung nach Absatz 3 nicht erfüllt, so hat der Betreiber dem Bundesamt auf Verlangen die für die Bewertung aus Sicht des Bundesamtes erforderlichen Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen und Auskunft zu erteilen. Ist eine Anlage oder Teile davon nach der Rechtsverordnung

nach § 10 Absatz 1 eine Kritische Infrastruktur im Sinne dieses Gesetzes, kann das Bundesamt die Registrierung auch selbst vornehmen (Ersatzvornahme), wenn der Betreiber seine Pflicht zur Registrierung nicht erfüllt. Rechtfertigen Tatsachen die Annahme, dass im Falle einer Registrierung nach Absatz 3 Satz 1 die Anlage oder Teile davon keine Kritische Infrastruktur im Sinne dieses Gesetzes ist oder sind, kann das Bundesamt die erfolgte Registrierung eines Betreibers aus tatsächlichen oder rechtlichen Gründen ablehnen.

(3b) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1 und 2 sind verpflichtet, sich beim Bundesamt zu registrieren und eine zu den üblichen Geschäftszeiten erreichbare Stelle zu benennen. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Stelle.

(3c) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 3 können eine freiwillige Registrierung beim Bundesamt und Benennung einer zu den üblichen Geschäftszeiten erreichbaren Stelle vornehmen. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Stelle.

(3d) § 8a Absatz 1 Satz 3 gilt auch für Unternehmen im öffentlichen Interesse nach § 2 Absatz 14 Nummer 1, 2 und 3.“

f) Nach dem Absatz 4 werden die folgenden Absätze 4a und 4b eingefügt:

„(4a) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1 und 2 haben die folgenden Störungen unverzüglich an das Bundesamt zu melden

1. Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung geführt haben,

2. erhebliche Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung führen können.

Die Meldung muss Angaben zu der Störung, zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und der Art der betroffenen Einrichtung oder Anlage enthalten.

(4b) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 3 haben die folgenden Störungen unverzüglich an das Bundesamt zu melden:

1. Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einer erheblichen Gefahr für die öffentliche Sicherheit und Ordnung geführt haben,

2. erhebliche Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einer erheblichen Gefahr für die öffentliche Sicherheit und Ordnung führen können.

Die Meldung muss Angaben zu der Störung, zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und der Art der betroffenen Einrichtung oder Anlage enthalten.“

g) In Absatz 6 werden nach den Wörtern „Störung nach Absatz 4“ ein Komma und die Angaben „4a oder 4b“ eingefügt.

15. In § 8c Absatz 3 Satz 4 wird die Angabe „Absatz 3“ durch die Angabe „Absatz 4“ ersetzt.

16. In § 8d Absatz 2 werden die Wörter „§8a ist nicht anzuwenden auf“ durch die Wörter „§8a Absatz 1 bis 5 ist nicht anzuwenden auf“ ersetzt.

17. § 8e wird wie folgt geändert:

a) Der Absatz 1 wird wie folgt gefasst:

„ (1) Das Bundesamt kann Dritten auf Antrag Auskunft zu den im Rahmen von § 8a Absatz 2 und 3, § 8c Absatz 4 und § 8f erhaltenen Informationen sowie zu den Meldungen nach § 8b Absatz 4, 4a und 4b sowie § 8c Absatz 4 nur erteilen, wenn schutzwürdige Interessen des betroffenen Betreibers Kritischer Infrastrukturen, des Unternehmens im besonderen öffentlichen Interesse oder des Anbieters digitaler Dienste dem nicht entgegenstehen und durch die Auskunft keine Beeinträchtigung von Sicherheitsinteressen eintreten kann. Zugang zu personenbezogenen Daten wird nicht gewährt.“

b) Der Absatz 2 wird wie folgt gefasst:

„(2) Zugang zu den Akten des Bundesamtes in Angelegenheiten nach den §§ 8a bis 8c und §§ 8f wird bei Vorliegen der Voraussetzungen des § 29 des Verwaltungsverfahrensgesetzes nur gewährt, wenn schutzwürdige Interessen des betroffenen Betreibers Kritischer Infrastrukturen, des Unternehmens im besonderen öffentlichen Interesse oder des Anbieters digitaler Dienste dem nicht entgegenstehen und durch den Zugang zu den Akten keine Beeinträchtigung von Sicherheitsinteressen eintreten kann.“

18. Nach § 8e wird der folgende § 8f eingefügt:

„§ 8f

Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse

(1) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1 sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten dieses Gesetzes ein IT-Sicherheitskonzept beim Bundesamt vorzulegen, aus dem hervorgeht,

1. welche Informationstechnischen Systeme, Komponenten und Prozesse für die Erbringung der Wertschöpfung des Unternehmens maßgeblich sind,

2. welche organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ebendieser vorgenommen wurden,

3. inwieweit bei Vornahme der organisatorischen und technischen Vorkehrungen nach Nummer 2 der Stand der Technik eingehalten wurde.

(2) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 2 sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 5 ein IT-Sicherheitskonzept beim Bundesamt vorzulegen, das den in Absatz 1 Nummer 1 bis 3 genannten Voraussetzungen genügt.

(3) Das Bundesamt kann auf Grundlage des IT-Sicherheitskonzepts und dessen Anforderungen nach Absatz 1 Hinweise zu angemessenen organisatorischen und technischen Vorkehrungen nach Nummer 3 zur Einhaltung des Stands der Technik geben.

(4) Unternehmen im besonderen öffentlichen Interesse gemäß § 2 Absatz 14 Nummer 1 und 2 haben das IT-Sicherheitskonzept nach Absatz 1 Nummer 1 bis 3 mindestens alle zwei Jahre vorzulegen.“

19. Nach § 9 werden folgende § 9a und § 9b eingefügt:

„§ 9a

Freiwilliges IT-Sicherheitskennzeichen

(1) Zur Umsetzung des Auftrages aus § 3 Absatz 1 Satz 2 Nummer 14 erteilt das Bundesamt nach Maßgabe einer Rechtsverordnung gemäß § 10 Absatz 3 (RVO IT-Sicherheitskennzeichen) für verschiedene Produktkategorien auf Antrag ein einheitliches IT-Sicherheitskennzeichen. Die umfassten Produktkategorien sind in der Rechtsverordnung nach § 10 Absatz 3 aufzuführen und zu beschreiben. Die Nutzung des IT-Sicherheitskennzeichens ist für die Hersteller der Produkte freiwillig.

(2) Das Kennzeichen beinhaltet

1. eine Erklärung des Herstellers der jeweiligen Produkte, in welcher dieser das Vorliegen bestimmter IT-Sicherheitseigenschaften des Produkts für zutreffend erklärt (Herstellererklärung), und

2. eine Information des Bundesamtes über Sicherheitslücken oder sonstige Informationen über sicherheitsrelevante IT-Eigenschaften (BSI-Sicherheitsinformation).

(3) Hersteller ist, wer die Voraussetzungen des § 2 Nummer 14 des Gesetzes über die Bereitstellung von Produkten auf dem Markt erfüllt. Die Herstellererklärung soll sich insbesondere aus einer die Produktkategorie umfassenden Technischen Richtlinie ergeben, soweit diese vom Bundesamt bereits veröffentlicht wurde. Branchenabgestimmte IT-Sicherheitseigenschaften können im Rahmen der Herstellererklärung verwendet werden, sofern das Bundesamt feststellt, dass sie geeignet sind, ausreichende IT-Sicherheitseigenschaften für die Produktkategorie abzubilden. Das Verfahren zur Feststellung der Eignung branchenabgestimmter IT-Sicherheitseigenschaften wird durch Rechtsverordnung nach § 10 Absatz 3 bestimmt.

(4) Der Antrag auf Freigabe zur Nutzung des IT-Sicherheitskennzeichens ist beim Bundesamt zu stellen. Das Bundesamt bestätigt den Eingang und teilt die Freigabe zur Nutzung oder die Verweigerung schriftlich innerhalb einer angemessenen Frist, die abhängig von der jeweiligen Produktkategorie in der Rechtsverordnung nach § 10 Absatz 3 bestimmt wird, mit. Die Plausibilitätsprüfung der eingereichten Dokumente des Herstellerversprechens kann auch durch einen qualifizierten Dritten erfolgen. Dem Antrag sind die erklärten IT-Sicherheitseigenschaften über das Produkt, sowie alle Unterlagen aus denen sich diese ergeben, beizufügen. Die Freigabe des IT-

Sicherheitskennzeichens nach Satz 1 ist zu verweigern, wenn bekannte Tatsachen die Annahme rechtfertigen, dass die Voraussetzungen des Absatz 7 Satz 2 Nummer 2 bereits bei Antragsstellung vorliegen. Den weiteren Ablauf und die notwendigen Informationen regelt die Rechtsverordnung nach § 10 Absatz 3.

(5) Das IT-Sicherheitskennzeichen ist körperlich mit dem jeweiligen Produkt oder mit dessen Umverpackung zu verbinden. Das IT-Sicherheitskennzeichen kann vom Hersteller oder Verkäufer zusätzlich auch auf elektronischem Wege veröffentlicht werden. Die Herstellererklärung sowie auch die bestehenden Sicherheitsinformationen nach Absatz 2 Satz 1 werden über einen elektronischen Verweis auf einer Webseite des Bundesamtes abrufbar gemacht. Das genaue Verfahren ist in der Rechtsverordnung nach § 10 Absatz 3 festzulegen.

(6) Das IT-Sicherheitskennzeichen darf verwendet werden, wenn das Produkt die Anforderungen für die Verwendung des IT-Sicherheitskennzeichens nach Maßgabe der Regelungen nach den Absätzen 1 bis 4 sowie der Rechtsverordnung nach § 10 Absatz 3 erfüllt. Das IT-Sicherheitskennzeichen darf auch für die Werbung für die Produkte genutzt werden, soweit die Darstellung den Vorgaben der Absatz 1 bis 4 sowie der Rechtsverordnung nach § 10 Absatz 3 entspricht.

(7) Das Bundesamt soll in regelmäßigen Abständen sowie anlassbezogen prüfen, ob die Vorgaben des IT-Sicherheitskennzeichens eingehalten werden. Werden bei einem das IT-Sicherheitskennzeichen tragenden Produkt Abweichungen vom abgegeben Herstellerversprechen oder Sicherheitslücken festgestellt, kann das Bundesamt die geeigneten Maßnahmen treffen, insbesondere

1. Informationen über den elektronischen Verweis in geeigneter Weise darstellen (BSI-Sicherheitsinfo),

2. die Freigabe zur Nutzung des IT-Sicherheitskennzeichens widerrufen und die Werbung mit dem IT- Sicherheitskennzeichen sowie die Nutzung des IT-Sicherheitskennzeichens untersagen.

(8) Wird das IT-Sicherheitskennzeichen ohne Freigabe genutzt, kann das Bundesamt die Nutzung untersagen. Dem Hersteller ist vor einer Maßnahme nach Absatz 7 Satz 2 die Gelegenheit einzuräumen, die Nichterfüllung der Herstellererklärung oder der weiteren Anforderungen des IT-Sicherheitskennzeichens innerhalb eines angemessenen Zeitraumes abzustellen oder Sicherheitslücken zu beseitigen, es sei denn, gewichtige Gründe der Sicherheit der Produkte erfordern eine sofortige Maßnahme.

§ 9b

Untersagung des Einsatzes kritischer Komponenten nicht vertrauenswürdiger Hersteller

(1) Der Einsatz einer kritischen Komponente (§ 2 Absatz 13), für die auf Grund einer spezialgesetzlichen Regelung eine Zertifizierungspflicht besteht, ist durch den Betreiber einer Kritischen Infrastruktur dem Bundesministerium des Innern, für Bau und Heimat vor Einbau anzuzeigen. In der Anzeige ist die kritische Komponente und die Art ihres Einsatzes anzugeben.

(2) Kritische Komponenten nach Absatz 1 dürfen nur von solchen Herstellern eingesetzt werden, die eine Erklärung über ihre Vertrauenswürdigkeit gegenüber dem Betreiber der Kritischen Infrastruktur abgeben haben (Garantieerklärung). Diese

Erklärung erstreckt sich auf die gesamte Lieferkette des Herstellers. Die Garantieerklärung des Herstellers der kritischen Komponente ist der Anzeige nach Absatz 1 beizufügen. Das Bundesministerium des Innern, für Bau und Heimat legt die Mindestanforderungen für die Garantieerklärung unter Berücksichtigung überwiegender öffentlicher Interessen, insbesondere sicherheitspolitischer Belange, durch Allgemeinverfügung fest, die im Bundesanzeiger bekannt zu machen ist. Aus der Garantieerklärung muss hervorgehen, ob und wie der Hersteller hinreichend sicherstellen kann, dass die kritische Komponente über keine technischen Eigenschaften verfügt, die geeignet sind, missbräuchlich auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur (etwa Sabotage, Spionage oder Terrorismus) einwirken zu können. Die Verpflichtung in Satz 1 gilt ab der Bekanntmachung der Allgemeinverfügung nach Satz 5.

(3) Ist der Anwendungsbereich des § 9b eröffnet, ist eine Feststellung nach § 9 Absatz 4 Nr. 2 entbehrlich. Zum Zwecke der Gewährleistung der nationalen Sicherheitsinteressen der Bundesrepublik Deutschland prüft das Bundesministerium des Innern, für Bau und Heimat stattdessen den Einsatz der kritischen Komponente nach Absatz 1 in Hinblick auf die Vertrauenswürdigkeit des Herstellers und kann gegenüber dem Betreiber der Kritischen Infrastruktur im Einvernehmen mit dem jeweils betroffenen Ressort den Einsatz untersagen, wenn der Hersteller der kritischen Komponente nicht vertrauenswürdig ist.

(4) Ein Hersteller einer kritischen Komponente ist nicht vertrauenswürdig, wenn

1. er gegen die in der Garantieerklärung eingegangen Verpflichtungen und Versicherungen verstoßen hat,

2. seine in der Garantieerklärung angegebenen Tatsachen unwahr sind

3. er Sicherheitsüberprüfungen und Penetrationsanalysen nicht im erforderlichen Umfang an seinem Produkt und in der Produktionsumgebung in angemessener Weise unterstützt,

4. er bekannte bzw. bekannt gewordene Schwachstellen oder Manipulationen nicht unverzüglich dem Betreiber der Kritischen Infrastruktur meldet und solche nicht beseitigt,

5. die kritische Komponente über technische Eigenschaften verfügt, die geeignet sind, missbräuchlich auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können. Dies gilt nicht, wenn der Hersteller nachweisen kann, dass er die technische Eigenschaft nicht implementiert hat und er diese jeweils ordnungsgemäß beseitigt hat.

(5) Ist eine Untersagung nach Absatz 3 erfolgt, kann das Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit dem betroffenen Ressort ohne erneute Prüfung der Vertrauenswürdigkeit eines Herstellers nach Absatz 3

1. den angezeigten Einsatz weiterer kritischer Komponenten desselben Typs und desselben Herstellers untersagen und

2. die Nutzung im Einsatz befindlicher kritischer Komponenten desselben Typs und desselben Herstellers innerhalb einer verhältnismäßigen Frist untersagen.

(6) Bei wiederholten Verstößen nach Absatz 4 Nummer 1 bis 3 kann der Einsatz aller kritischen Komponenten des Herstellers untersagt werden.“

20. § 10 wird wie folgt geändert:

a) Nach Absatz 2 wird folgender Absatz 3 eingefügt:

„(3) Das Bundesministerium des Innern, für Bau und Heimat wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie und dem Bundesministerium der Justiz und für Verbraucherschutz, Einzelheiten der Gestaltung und Verwendung des IT-Sicherheitskennzeichens nach § 9a Absatz 1 Satz 1 zu regeln, um eine einheitliche Gestaltung des Kennzeichens und eine eindeutige Erkennbarkeit der gekennzeichneten informationstechnischen Produkte zu gewährleisten, sowie die erfassten Produktkategorien und das Verwaltungsverfahren zur Sicherstellung der Anforderungen im Zusammenhang mit der Verwendung des Kennzeichens festzulegen.“

b) Nach Absatz 4 wird folgender Absatz 5 angefügt:

„(5) Das Bundesministerium des Innern, für Bau und Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, bei welchen Unternehmen ein besonderes öffentliches Interesse nach § 2 Absatz 14 Nummer 2 besteht“

21. § 11 wird wie folgt gefasst:

„§ 11

Einschränkung von Grundrechten

Das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) wird durch die §§ 4a, 5, 5a, 5b, 5c und 5d Absatz 2 eingeschränkt.“

22. § 14 wird wie folgt gefasst:

„§ 14

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 5b Absatz 6 nicht an der Beseitigung einer Störung mitwirkt,

2. einer vollziehbaren Anordnung nach § 5b Absatz 6 zuwiderhandelt,

3. entgegen § 7a Absatz 2 Satz 1 und 2 eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt,

4. entgegen § 8a Absatz 1 Satz 1 eine dort genannte Vorkehrung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig trifft,

5. entgegen § 8a Absatz 3 Satz 1 einen Nachweis nicht richtig, nicht vollständig oder nicht rechtzeitig erbringt,

6. einer vollziehbaren Anordnung nach § 8a Absatz 3 Satz 5 zuwiderhandelt,

7. entgegen § 8a Absatz 4 Satz 2 den Zutritt nicht gestattet, in Betracht kommende Aufzeichnungen, Schriftstücke und sonstige Unterlagen nicht in geeigneter Weise vorlegt oder Auskunft nicht erteilt oder die sonst erforderliche Unterstützung nicht gewährt,

8. entgegen § 8b Absatz 3 Satz 1 oder Absatz 3b Satz 1 eine Kontaktstelle nicht oder nicht rechtzeitig benennt oder eine Registrierung nicht oder nicht rechtzeitig vornimmt,

9. entgegen § 8b Absatz 3 Satz 2 eine Erreichbarkeit nicht sicherstellt,

10. entgegen § 8b Absatz 3a dem Bundesamt die verlangten Unterlagen nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig übermittelt oder die verlangte Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt,

11. entgegen § 8b Absatz 4 Satz 1 Nummer 1 und Nummer 2 oder Absatz 4a Nummer 1 und 2 oder Absatz 4b Nummer 1 und 2 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

12. entgegen § 8b Absatz 6 Satz 1 nicht an der Beseitigung oder Vermeidung einer Störung mitwirkt,

13. einer vollziehbaren Anordnung nach § 8b Absatz 6 zuwiderhandelt,

14. entgegen § 8c Absatz 1 Satz 1 eine dort genannte Maßnahme nicht trifft,

15. entgegen § 8c Absatz 3 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vornimmt oder

16. einer vollziehbaren Anordnung nach § 8c Absatz 4

    a) Nummer 1 oder

    b) Nummer 2

zuwiderhandelt,

17. entgegen § 8f Absatz 1 oder 2 ein IT-Sicherheitskonzept nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorlegt,

18. als Hersteller oder Einführer (§ 2 Nummer 8 des Gesetzes über die Bereitstellung von Produkten auf dem Markt) eines Produktes das IT-Sicherheitskennzeichen nach § 9a

    a) nach einem Widerruf nach § 9a Absatz 6 weiterhin für ein Produkt im geschäftlichen Verkehr nutzt oder damit wirbt oder

    b) ohne vorherige Freigabe nach § 9a Absatz 3 durch das Bundesamt für ein Produkt im geschäftlichen Verkehr nutzt.

(2) Verstöße gegen die Bestimmungen des Absatzes 1 Nummer 2, 6, 13 und 16 können mit Geldbußen von bis zu 20 000 000 EURO oder von bis zu 4 % des gesamten

weltweit erzielten jährlichen Unternehmensumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist, geahndet werden. Verstöße gegen die übrigen Bestimmungen des Absatzes 1 können mit Geldbußen von bis zu 10 000 000 EURO oder von bis zu 2 % des gesamten weltweit erzielten jährlichen Unternehmensumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist, geahndet werden.

(3) In den Fällen des Absatzes 1 Nummer 14 bis 16 wird die Ordnungswidrigkeit nur geahndet, wenn der Anbieter digitaler Dienste seine Hauptniederlassung nicht in einem anderen Mitgliedstaat der Europäischen Union hat oder, soweit er nicht in einem anderen Mitgliedstaat der Europäischen Union niedergelassen ist, dort einen Vertreter benannt hat und in diesem Mitgliedstaat dieselben digitalen Dienste anbietet.

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

Artikel 2

Änderungen des Telekommunikationsgesetzes

Das Telekommunikationsgesetz vom 3. Mai 2013 (BGBl. I S. 1084), das zuletzt durch Artikel 4 des Gesetzes vom 20. Oktober 2015 (BGBl. I S. 1722) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht werden bei der Angabe zu § 109 hinter dem Wort „technische“ die Wörter „und organisatorische“ eingefügt.

2. § 109 wird wie folgt geändert:

   a) In Absatz 2 Satz 2 werden nach dem Wort „Nutzer“ ein Komma und die Wörter „für Dienste“ eingefügt.

   b) Nach Absatz 2 Satz 3 werden folgende Sätze eingefügt:

   „Der Umfang der Maßnahmen nach Satz 1 und 2 richtet sich nach dem jeweiligen Gefährdungspotenzial des öffentlichen Telekommunikationsnetzes oder öffentlich zugänglichen Telekommunikationsdienstes. Sicherheitsrelevante Netz- und Systemkomponenten, die kritische Funktionen erfüllen, (kritische Komponenten) dürfen nur eingesetzt werden, wenn sie von einer anerkannten Prüfstelle überprüft und von einer anerkannten Zertifizierungsstelle zertifiziert wurden. Die Einzelheiten der nach den Satz 1 bis 4 zu treffenden Maßnahmen sowie Einzelheiten der Festlegung kritischer Funktionen und der Bestimmung der kritischen Komponenten nach Satz 5 legt die Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Katalog von Sicherheitsanforderungen nach Absatz 6 fest.“

   c) In Absatz 2 Satz 6 wird die Angabe „§ 11“ durch die Angabe „§ 62“ ersetzt.

   d) Nach Absatz 4 Satz 1 werden folgende Sätze eingefügt:

   „Insbesondere ist im Sicherheitskonzept darzustellen, auf welche Weise die verbindlichen Vorgaben des Katalogs von Sicherheitsanforderungen nach Absatz 6 umgesetzt sind. Sofern der Katalog Sicherheitsziele vorgibt, die auf

unterschiedliche Weise erreicht werden können, ist im Sicherheitskonzept darzulegen, dass mit den ergriffenen Maßnahmen das jeweilige Sicherheitsziel vollumfänglich erreicht wird.“

e) In Absatz 5 Satz 5 und Satz 8 werden jeweils die Wörter „Europäische Agentur für Netz- und Informationssicherheit“ durch die Wörter „Agentur der Europäischen Union für Cybersicherheit“ ersetzt.

f) In Absatz 6 Satz 1 wird das Wort „erstellt“ durch das Wort „legt“ ersetzt, nach den Wörtern „Informationstechnik und“ die Wörter „der oder“ eingefügt und nach der Angabe „nach den Absätzen 1 und 2“ das Wort „fest“ eingefügt.

g) Nach Absatz 6 Satz 1 wird folgender Satz eingefügt:

„Die im Katalog festgelegten Anforderungen sind verbindlich.“

h) In Absatz 6 Satz 2 wird das Wort „Sie“ durch die Wörter „Die Bundesnetzagentur“ ersetzt.

i) In Absatz 6 Satz 3 wird das Wort „veröffentlicht“ durch die Wörter „durch öffentliche Bekanntmachung zugestellt“ ersetzt.

j) Nach Absatz 6 Satz 3 werden folgende Sätze eingefügt:

„Die öffentliche Bekanntmachung wird dadurch bewirkt, dass der Katalog, die Rechtsbehelfsbelehrung und ein Hinweis auf die Veröffentlichung auf der Internetseite der Bundesnetzagentur im Amtsblatt der Bundesnetzagentur bekannt gemacht werden. Der Katalog gilt mit dem Tag als zugestellt, an dem seit dem Tag der Bekanntmachung im Amtsblatt der Bundesnetzagentur zwei Wochen verstrichen sind; hierauf ist in der Bekanntmachung hinzuweisen. Die nach Absatz 1, 2 und 4 Verpflichteten haben die Anforderungen des Katalogs spätestens ein Jahr nach dessen Inkrafttreten zu erfüllen, es sei denn, in dem Katalog ist eine davon abweichende Umsetzungsfrist festgelegt worden.“

k) Nach Absatz 7 Satz 1 werden folgende Sätze eingefügt:

„Unbeschadet von Satz 1 haben sich Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial alle zwei Jahre einer Überprüfung durch eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde zu unterziehen, in der festgestellt wird, ob die Anforderungen nach Absatz 1 bis 3 erfüllt sind. Die Bundesnetzagentur legt den Zeitpunkt der erstmaligen Überprüfung nach Satz 2 fest.“

l) In Absatz 7 Satz 2 wird nach der Angabe „Satz 1“ die Angabe „und 2“ eingefügt und nach dem Wort „Bundesnetzagentur“ die Wörter „und an das Bundesamt für Sicherheit in der Informationstechnik, sofern dieses die Überprüfung nicht vorgenommen hat,“ eingefügt.

m) Nach Absatz 7 Satz 3 wird folgender Satz eingefügt:

„Die Bewertung der Überprüfung sowie eine diesbezügliche Feststellung von Sicherheitsmängeln im Sicherheitskonzept erfolgt durch die Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik.“

3. § 109a wird wie folgt geändert:

a) In Absatz 4 Satz 1 werden nach dem Wort „Störungen“ die Wörter „oder Gefahren“ und nach dem Wort „ausgehen“ die Wörter „oder diesen betreffen“ eingefügt.

b) Nach Absatz 1 wird folgender neuer Absatz 1a eingefügt:

„(1a) Im Falle einer unrechtmäßigen Übermittlung an oder unrechtmäßigen Kenntniserlangung von Daten durch Dritte unterrichtet der Diensteanbieter unverzüglich das Bundeskriminalamt über diesen Sachverhalt, wenn bestimmte Tatsachen die Annahme rechtfertigen, dass

1. jemand Telekommunikations- oder Datenverarbeitungssysteme ohne Erlaubnis oder Billigung des Diensteanbieters verändert, auf diese eingewirkt oder Zugangseinrichtungen zu diesen überwunden hat und

2. dies nicht fahrlässig erfolgt ist.

Die Übermittlung an das Bundeskriminalamt hat elektronisch an eine vom Bundeskriminalamt zur Verfügung gestellte Schnittstelle zu erfolgen.“

c) Nach Absatz 7 wird folgender Absatz 8 eingefügt:

„(8) Zur Abwehr erheblicher Gefahren für die Kommunikationstechnik des Bundes, eines Betreibers einer Kritischen Infrastruktur oder einer Infrastruktur im besonderen öffentlichen Interesse oder für die Verfügbarkeit von Informations- oder Kommunikationsdiensten oder unerlaubten Zugriffen auf eine Vielzahl von Telekommunikations- und Datenverarbeitungssystemen von Nutzern kann das Bundesamt für Sicherheit in der Informationstechnik

1. die Umsetzung der Maßnahmen nach Absatz 4, 5 und 6 und

2. die Bereinigung betroffener Datenverarbeitungssysteme von einem konkret benannten Schadprogramm

gegenüber dem Diensteanbieter anordnen, sofern dieser dazu technisch in der Lage ist und es ihm wirtschaftlich zumutbar ist. Vor Anordnung der Maßnahme durch das Bundesamt für Sicherheit in der Informationstechnik ist Einvernehmen mit der Bundesnetzagentur herzustellen. Widerspruch und Anfechtungsklage gegen die Anordnungen nach Satz 1 haben keine aufschiebende Wirkung.“

4. In § 110 wird nach Absatz 1 folgender Absatz 1a eingefügt:

„(1a) Wer eine Telekommunikationsanlage betreibt, mit der öffentlich zugängliche Telekommunikationsdienste erbracht werden, oder sonst Telekommunikationsdienste erbringt und den Dienst im räumlichen Zuständigkeitsbereich der Bundesnetzagentur anbietet, hat Daten, zu deren Beauskunftung oder Bereitstellung oder Löschung er nach diesem Abschnitt verpflichtet ist, so zu verarbeiten oder zu speichern, dass §112 TKG Auskunfts-, Bereitstellungs- oder Löschungsverlangen unmittelbar gegenüber den zuständigen Behörden ausführen kann. Er ist verpflichtet, im räumlichen Zuständigkeitsbereich der Bundesnetzagentur eine Stelle zur elektronischen und postalischen Entgegennahme dieser Ersuchen einzurichten. Der Bundesnetzagentur ist die elektronische und postalische Erreichbarkeit der Stelle mitzuteilen. Die Bundesnetzagentur stellt die ihr benannten Erreichbarkeiten der Stellen den für Anfragen oder Ersuchen nach diesem Abschnitt zuständigen Behörden zur Verfügung.“

5. In § 112 Absatz 2 wird nach der Nummer 8 folgende Nummer 9 angefügt:

„9. dem Bundesamt für die Sicherheit in der Informationstechnik“.

6. In § 149 Absatz 1 werden nach der Nummer 21c die folgenden Nummern 21d bis 21j eingefügt:

„21d. entgegen § 109a Absatz 4 Satz 1 den Nutzer nicht oder unzureichend benachrichtigt,

21e. entgegen § 109a Absatz 4 Satz 2 den Nutzer nicht oder unzureichend auf angemessene, wirksame und zugängliche technische Mittel hingewiesen hat, mit denen dieser diese Störungen hätte erkennen und beseitigen können, obwohl ihm dies technisch möglich und zumutbar war,

21f. entgegen § 109a Absatz 8 eine Anordnung nicht umsetzt, obwohl er hierzu technisch in der Lage war und die Maßnahme für ihn wirtschaftlich zumutbar war,

21g. entgegen § 109a Absatz 1a trotz hinreichender Anhaltspunkte die unrechtmäßige Kenntniserlangung von Daten nicht an die zuständige Stelle meldet,

21j. entgegen § 110 Absatz 1a eine entsprechende Stelle nicht einrichtet oder die Erreichbarkeit der Bundesnetzagentur nicht mitteilt.“

Artikel 3

Änderung des Telemediengesetzes

Das Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 1 des Gesetzes vom 28. September 2017 (BGBl. I S. 3530) geändert worden ist, wird wie folgt geändert:

1. Der § 13 wird wie folgt geändert:

a) Nach Absatz 7 wird folgender Absatz 7a eingefügt:

„Das Bundesamt für Sicherheit in der Informationstechnik kann zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes oder eines Betreibers einer Kritischen Infrastruktur oder für eine Infrastruktur im besonderen öffentlichen Interesse gegenüber Diensteanbietern in begründeten Ausnahmefällen die Umsetzung erforderlicher technischer und organisatorischer Vorkehrungen zur Sicherstellung der Schutzgüter nach Absatz 7 Satz 1 anordnen, wenn hierdurch eine konkrete Gefahr für Datenverarbeitungssysteme einer Vielzahl von Nutzern durch unzureichend gesicherte Telemedienangebote beseitigt werden kann.“

b) Nach Absatz 8 werden die folgenden Absatze 9 und 10 angefügt:

„(9) Liegen tatsächliche Anhaltspunkte für eine unrechtmäßige Erlangung oder Verbreitung personenbezogener Daten oder Daten, die Geschäftsgeheimnisse beinhalten, vor, so ist der Zugang zu diesen Daten durch den Diensteanbieter zu sperren. Der betroffene Nutzer ist zu benachrichtigen.

(10) Im Falle der unrechtmäßigen Erlangung oder Verbreitung von Geschäftsgeheimnissen können die zuständigen Stellen unter den Voraussetzungen des Absatz 9 eine Sperrung der Daten anordnen. Zuständige Stellen sind die für die Abwehr von Gefahren für die öffentliche Sicherheit oder

Ordnung zuständigen Behörden. Der Diensteanbieter hat die unverzügliche Umsetzung der Anordnung sicherstellen.“

2. Dem § 15 Absatz 2 wird folgender Satz angefügt:

„Im Falle einer unrechtmäßigen Übermittlung an oder unrechtmäßigen Kenntniserlangung von Bestands- oder Nutzungsdaten durch Dritte unterrichtet der Diensteanbieter unverzüglich das Bundeskriminalamt über diesen Sachverhalt, wenn Tatsachen darauf hindeuten, dass

1. jemand Telekommunikations- oder Datenverarbeitungssysteme ohne Erlaubnis oder Billigung des Diensteanbieters verändert, auf diese eingewirkt oder Zugangseinrichtungen zu diesen überwunden hat und

2. dies nicht fahrlässig erfolgt ist.

Die Übermittlung an das Bundeskriminalamt hat elektronisch an eine vom Bundeskriminalamt zur Verfügung gestellte Schnittstelle zu erfolgen“

3. Nach § 15a wird folgender § 15b eingefügt:

„§ 15b

Pflichten der Diensteerbringer

(1) Stellt der Diensteanbieter fest, dass rechtswidrig erlangte personenbezogene Daten oder Geschäftsgeheimnisse über seinen Dienst Dritten unrechtmäßig zur Kenntnis gegeben oder veröffentlicht werden, so meldet er diesen Sachverhalt unverzüglich dem Bundeskriminalamt, wenn Tatsachen darauf hindeuten, dass

1. eine große Zahl von Personen betroffen ist oder ein Datenbestand von großem Ausmaß erlangt wurde oder Dritten zur Kenntnis gebracht worden ist,

2. Gefahren für höchstpersönliche Rechtsgüter wie Leib, Leben oder Freiheit angenommen werden,

3. durch die Weitergabe oder Veröffentlichung eine Gefahr für die Sicherheit und den Bestand des Staates drohen kann oder

4. fremde Geheimnisse, namentlich Betriebs- oder Geschäftsgeheimnisse oder Tatsachen, Gegenstände oder Erkenntnisse, die von einer amtlichen Stelle oder auf deren Veranlassung geheim gehalten werden,

betroffen sind.

Die Übermittlung an das Bundeskriminalamt hat elektronisch an eine vom Bundeskriminalamt zur Verfügung gestellte Schnittstelle zu erfolgen.

(2) Liegen zureichende tatsächliche Anhaltspunkte für eine unrechtmäßige Erlangung oder Verbreitung von Daten, die Geschäftsgeheimnisse beinhalten, vor, so ist der Zugang zu diesen Daten durch den Diensteanbieter zu sperren. Der betroffene Nutzer ist zu benachrichtigen. Sofern der betroffene Nutzer nach seiner Benachrichtigung innerhalb angemessener Frist nicht widerspricht, hat der Diensteanbieter die Daten zu löschen. Die zuständigen Stellen können eine Sperrung der Daten anordnen. Zuständige Stellen nach Satz 1 sind die für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Behörden.

(3) Der Diensteanbieter im Sinne des Absatzes 1 muss die unverzügliche Bearbeitung der Anordnung nach Absatz 2 sicherstellen.“

4. In § 16 Absatz 2 wird in Nummer 5 der Punkt durch ein Komma ersetzt und nach Nummer 5 werden folgende Nummern 6 bis 9 eingefügt:

„6. entgegen § 15a die zuständige Stelle nicht unverzüglich von der unrechtmäßigen Kenntniserlangung unterrichtet.

7. entgegen § 15b Absatz 1 Satz 1 die zuständige Stelle nicht unverzüglich von der unrechtmäßigen Weitergabe unterrichtet.

8. entgegen § 15b Absatz 1 Satz 2 den Zugang zu den Daten nicht sperrt oder die Daten nicht löscht.

9. entgegen § 15b Absatz 2 eine entsprechende Stelle nicht einrichtet oder die Erreichbarkeit der Bundesnetzagentur nicht mitteilt.“

Artikel 4

Änderung der Außenwirtschaftsverordnung

§ 55 Absatz 1 der Außenwirtschaftsverordnung vom 2. August 2013 (BGBl. I S. 2865), die die zuletzt durch Artikel 1 der Verordnung vom 27. Februar 2019 (BGBl. I S. XXXX) geändert worden ist, wird wie folgt geändert:

1. in Satz 2 Nummern 2 werden das Wort „Software“ durch die Wörter „kritische Komponenten nach § 2 Absatz 13 des BSI-Gesetzes in der jeweils geltenden Fassung“ ersetzt.

2. Satz 3 wird gestrichen.

Artikel 5

Inkrafttreten

Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Bereits in der vergangenen Legislaturperiode wurden verschiedene Vorhaben zur Erhöhung der IT-Sicherheit umgesetzt. Hervorzuhaben ist das erste Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), das im Jahr 2015 verkündet wurde. Ergänzt wurde dieses Gesetz durch die BSI-Kritisverordnung und die Umsetzung der EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (NIS-Richtlinie).

Maßnahmen zur Gewährleistung von Cyber-Sicherheit sind jedoch niemals statisch. Ein ausreichendes Schutzniveau heute ist kein Garant für adäquate Schutzmechanismen und die erfolgreiche Abwehr von Angriffen morgen. Eine ständige Anpassung und Weiterentwicklung der Abwehrstrategien sind erforderlich. Entsprechend dem Auftrag aus dem Koalitionsvertrag zwischen CDU, CSU und SPD, Zeile 1969 ff., wird daher das IT-Sicherheitsgesetz fortgeschrieben und der Ordnungsrahmen erweitert, um neuen Gefährdungen angemessen zu begegnen. Die Anpassungen bestehender Regelungen und die Schaffung neuer Regelungen dieses Gesetzes dienen dem Schutz der Gesellschaft, der Wirtschaft und des Staates.

II. Wesentlicher Inhalt des Entwurfs

Das zweite IT-Sicherheitsgesetz ist Teil des Koalitionsvertrages zwischen CDU, CSU und SPD für die 19. Legislaturperiode und stellt den wesentlichen rechtlichen Rahmen der Bundesregierung auf dem Gebiet der IT-Sicherheit dar.

Das Gesetz basiert auf Erfahrungen aus dem ersten IT-Sicherheitsgesetz sowie weiteren Erkenntnissen, z.B. aus Cyber-Angriffen und anderen Sicherheitsvorfällen. Die abzuwendenden Cyber-Gefahren betreffen die Gesellschaft bzw. den Bürgerinnen und Bürger selbst, den Staat und auch die Wirtschaft. Das Gesetz verfolgt daher einen ganzheitlichen Ansatz und umfasst Maßnahmen zum Schutz der genannten Adressaten. Wesentlicher Akteur hierfür ist das BSI. Seine Rolle wird ebenfalls entsprechend dem Koalitionsvertrag zwischen CDU, CSU und SPD (Zeile 6004) gestärkt.

Zum Schutz der Bürgerinnen und Bürger werden insbesondere die Voraussetzungen für ein einheitliches IT-Sicherheitskennzeichen geschaffen, welches die IT-Sicherheit von Produkten erstmals für Bürgerinnen und Bürger sichtbar macht. Hierdurch wird ihnen eine fundiertere Kaufentscheidung ermöglicht. Außerdem wird Verbraucherschutz als zusätzliche Aufgabe des BSI gesetzlich etabliert.

Zur Verhütung und Abwehr von Cyber-Sicherheitsvorfällen werden die Befugnisse des BSI zum Schutz der Bundesverwaltung und Gesellschaft ausgeweitet. Auch werden die Möglichkeiten zur Unterstützung der Länder durch das BSI verbessert, da die Gefahren des Cyber-Raums unabhängig von Ländergrenzen bestehen.

Die bestehenden Meldepflichten und verpflichtenden Mindeststandards für Betreiber Kritischer Infrastruktur werden auf weitere Teile der Wirtschaft ausgeweitet. Verpflichtet werden zudem auch weitere Unternehmen, an denen ein besonderes öffentliches Interesse

besteht. Durch diese Maßnahmen wird die IT-Sicherheit der Wirtschaft und der Gesellschaft insgesamt erhöht.

III. Alternativen

Beibehalten des bisherigen Rechtszustandes.

IV. Gesetzgebungskompetenz

Für die Änderungen des BSI-Gesetzes (Artikel 1), die den rein technischen Schutz der Informationstechnik von und für Unternehmen und sonstige Einrichtungen im besonderen öffentliche Interesse betreffen, folgt die Gesetzgebungskompetenz des Bundes aus Artikel 73 Absatz 1 Nummer 7 (Telekommunikation) Grundgesetzes (GG)) beziehungsweise aus Artikel 74 Absatz 1 Nummer 11 GG (Recht der Wirtschaft) in Verbindung mit Artikel 72 Absatz 2 GG. Für Änderungen, welche die Befugnisse des BSI zum Schutz der Bundesverwaltung erweitern, hat der Bund eine Gesetzgebungskompetenz kraft Natur der Sache. Die Zuständigkeit des Bundes für Regelungen zur bundesweiten Information einschließlich eventueller Empfehlungen und Warnungen von Verbraucherinnen und Verbrauchern auf dem Gebiet der Informationssicherheit folgt mit Blick auf die gesamtstaatliche Verantwortung der Bundesregierung ebenfalls aus der Natur der Sache (Staatsleitung), denn Fragen zur Sicherheit in der Informationstechnik haben bei stetig zunehmender Digitalisierung und Vernetzung aller Lebensbereiche regelmäßig überregionale Auswirkungen. Der Bund hat darüber hinaus die ausschließliche Gesetzgebungskompetenz nach Artikel 73 Absatz 1 Nummer 8 GG für die Rechtsverhältnisse der im Dienst des Bundes und der bundesunmittelbaren Körperschaften des öffentlichen Rechts stehenden Personen.

Die Änderungen des Telekommunikationsgesetzes (TKG) in Artikel 2 beruhen auf der Gesetzgebungskompetenz des Bundes aus Artikel 73 Absatz 1 Nummer 7 (Telekommunikation) GG und auf Artikel 74 Absatz 1 Nummer 11 (Recht der Wirtschaft) GG in Verbindung mit Artikel 72 Absatz 2 GG.

Die Gesetzgebungskompetenz des Bundes für die Regelungen der Bußgeldvorschriften und Ordnungswidrigkeiten in den Artikeln 1 und 2 folgt aus Artikel 74 Absatz 1 Nummer 1 GG (Strafrecht).

Die Gesetzgebungskompetenz für die Änderung des Telemediengesetzes (TMG) in Artikel 3 ergibt sich aus der Gesetzgebungskompetenz für das Recht der Wirtschaft (Artikel 74 Absatz 1 Nummer 11 GG) in Verbindung mit Artikel 72 Absatz 2 GG.

Soweit die Regelungen auf Artikel 74 Absatz 1 Nummer 11 GG beruhen, ist eine bundesgesetzliche Regelung zur Wahrung der Wirtschaftseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich (vgl. Artikel 72 Absatz 2 GG). 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 Voraussetzungen für die Vergabe von Sicherheitszertifikaten, erhebliche Wettbewerbsverzerrungen und störende Schranken für die innerdeutsche Wirtschaftstätigkeit zur Folge hätten. Internationale Abkommen zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten setzen voraus, dass in jedem Staat nur eine hoheitliche Zertifizierungsstelle existiert.

V. Vereinbarkeit mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen

Der Gesetzentwurf ist mit dem Recht der Europäischen Union und völkerrechtlichen Verträgen vereinbar. Er ergänzt die Umsetzung der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

VI. Gesetzesfolgen

[wird nachgereicht]

1. Rechts- und Verwaltungsvereinfachung

2. Nachhaltigkeitsaspekte

Der Gesetzentwurf entspricht mit der weiteren Anhebung der Sicherheitsstandards als Teil der deutschen IT-Sicherheitsarchitektur, die zunehmend alle Gesellschaftsbereiche durchdringt, dem Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der nationalen Nachhaltigkeitsstrategie.

3. Haushaltsausgaben ohne Erfüllungsaufwand

[wird nachgereicht]

Mehrbedarfe durch den Erfüllungsaufwand sind finanziell und stellenplanmäßig in den jeweiligen Einzelplänen zu erwirtschaften.

4. Erfüllungsaufwand

Durch das geplante Regelungsvorhaben der Bundesregierung kommt es in der Wirtschaft zu einer Veränderung des jährlichen Erfüllungsaufwands von rund 45,09 Millionen Euro. Rund 31,20 Millionen Euro davon entstehen aus neuen oder geänderten Informationspflichten. Ein-malig wird die Wirtschaft mit rund 16,71 Millionen Euro belastet.

Der Verwaltung entsteht für die Erfüllung der im Gesetz vorgesehenen zusätzlichen Aufgaben ein Aufwand von insgesamt xxxxxxxx Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund xxxxxxxx Millionen Euro.

Beim BSI ist ein Erfüllungsaufwand in Höhe von 583 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund xxx Millionen Euro notwendig. Darin ist bereits eine OPH-Quote (Stellen für den Bereich Organisation, Personal und Haushalt) enthalten. Zusätzlich sind zur Umsetzung des Gesetzes Sachkosten in Höhe von einmalig 28 Mio. Euro und jährlich in Höhe von rund 47,5 Mio. Euro zu berücksichtigen.

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe wirkt mit bei der Erstellung und Änderung des Gesamtplans für die Reaktionsmaßnahmen des Bundes gemäß § 5c, bei der Prüfung von Standards gemäß § 8a Abs. 2, in der Erstellung von Auswirkungsanalysen nach § 8b Abs. 2 sowie im Bereich Krisenkommunikationssystem nach § 8b Abs. 2. Es ist ein Erfüllungs-aufwand in Höhe von insgesamt 47 Planstellen erforderlich. Hierfür fallen jährlich Personalkosten in Höhe von XXX Euro an.

Die BDBOS ist verantwortlich für die Kommunikationswege des Bundes. Es ist ein Erfüllungsaufwand in Höhe von insgesamt 54 Planstellen erforderlich, sofern

eine Protokollierung nicht über DaaS möglich ist. Hierfür fallen jährlich Personalkosten in Höhe von rd. 3,35 Millionen Euro und einmalige Sachkosten in Höhe von rd. 5 Millionen Euro an.

Sollte das DaaS in Anspruch genommen werden, so reduziert sich der Personalmehrbedarf um ca. 28 Planstellen, sodass insgesamt ein Mehraufwand in Höhe von 26 Planstellen erforderlich ist. Dies entspricht jährlichen Personalkosten von rd. 1,62 Millionen Euro.

Der Bedarf an Sach- und Personalmitteln sowie Planstellen und Stellen wird finanziell und stellenmäßig im Gesamthaushalt ausgeglichen.

Für die Umsetzung des Zweiten IT-Sicherheitsgesetzes kommen für das BSI folgende neue Aufgaben hinzu:

- Mit den neuen Aufgaben des BSI zur Förderung des Verbraucherschutzes und der Verbraucherinformation im Bereich der Informationssicherheit trägt das Gesetz dem Umstand Rechnung, dass Fragen der IT-Sicherheit durch die Digitalisierung alltäglicher Lebensabläufe – insbesondere durch die steigende Vernetzung der privaten Haushalte – bei Verbraucherinnen und Verbrauchern eine steigende Bedeutung zukommt. Mit seiner technischen Expertise und Erfahrung kann das BSI einerseits durch Beratung, Sensibilisierung und Unterstützung von Verbraucherinnen und Verbrauchern zum Schutz dieser vor den mit der Digitalisierung verbundenen Gefahren für die IT-Sicherheit beitragen. Andererseits will das BSI seine Kompetenzen, Fähigkeiten und etablierte Arbeitsbeziehungen dazu einsetzen, Security by Design am Markt durchzusetzen, sodass den Verbraucherinnen und Verbrauchern sichere Produkte zur Verfügung stehen, was heute oft nicht der Fall ist. Um diese wichtige Aufgabe sachgerecht durchführen zu können, benötigt das BSI 163 Planstellen/Stellen.

- In diesem Kontext kommen auch die Änderungen in § 3 Abs. 1 Satz 2 Nr. 14 sowie § 7 Abs. 1d BSIG-E (erweiterte Informationsaufgabe und Warnbefugnis im Hinblick auf Produkte) zum Tragen, die den Aktivitäten des BSI größere Wirkung verschaffen werden. Um in relevantem Umfang vor unsicheren Produkten warnen zu können, müssen die Untersuchungskapazitäten für Produkte deutlich ausgeweitet und die rechtskonformen Prozesse zur Verbraucherinformation und -warnung ausgebaut und fortentwickelt werden. Hierfür werden 18 Planstellen/Stellen benötigt.

- Identitätsdiebstahl entwickelt sich immer mehr zum Massenphänomen und Massenproblem. Der Appell zu sicheren Passwörtern kann das grundlegende Problem nicht mehr lösen, Identifizierungs- und Authentisierungsverfahren müssen nutzerfreundlicher werden und zugleich das angemessene, notwendige Maß an Sicherheit bieten. Hier gilt es im Rahmen der neuen Aufgabe in § 3 Abs. 1 Satz 2 Nr. 19 BSIG-E, „Pflege und Weiterentwicklung sicherer Identitäten“, bestehende Ansätze fortzuentwickeln sowie neue Ansätze zu entwickeln und in die Anwendung zu überführen. Hierfür benötigt das BSI 8 Planstellen/Stellen.

- § 4a BSIG-E, Kontrolle der Kommunikationstechnik: Staatliche Stellen sind in besonderem Maße auf eine zuverlässige und sichere Kommunikation angewiesen. Daher sind an die Kommunikationstechnik des Bundes besonders hohe Sicherheitsanforderungen zu stellen. Diese besondere Sicherheit erfordert eine effektive und schnelle Kontrollmöglichkeit des Bundesamtes, um Gefahren für die Kommunikationstechnik früh zu erkennen und in der Folge zu beseitigen. Die

Ausübung der neuen Kontroll- und Prüfbefugnisse, die für jede Einrichtung der Bundesverwaltung wahrgenommen werden kann, führt zu einem Personalbedarf von 64 Planstellen/Stellen.

- § 4b BSIG-E, Meldestelle: Die Sammlung von Informationen über Sicherheitslücken, Schadprogramme und IT-Sicherheitsvorfällen ist für ein Gesamtlagebild von besonderer Bedeutung. Um eine zentrale Sammlung und systematische Auswertung der an das Bundesamt gerichteten Hinweise auch angesichts der Vielzahl mit dem IT-SiG 2.0 hinzukommender Regelungsbereiche in angemessener Weise sicherzustellen, ist der Ausbau der Meldestelle beim BSI zwingend erforderlich. Der organisatorische und technische Ausbau sowie die kontinuierliche Beobachtung, Entgegennahme sowie Auswertung und Analyse der Meldungen führt zu einem zusätzlichen Personalbedarf von 14 Planstellen/Stellen.

- § 5 BSIG-E: Die Gefahr für die Kommunikationstechnik des Bundes ist quantitativ und qualitativ gestiegen. Um dieser eine effektive Abwehr entgegenzusetzen, muss das Bundesamt personell verstärkt werden. Die aktuell zur Verfügung stehenden Personalressourcen ermöglichen es nicht, die erforderlichen Detektionsmaßnahmen bei allen Behörden des Bundes in ausreichender Form zum Einsatz zu bringen. Neben Maßnahmen zur Sicherung der Kommunikationstechnik des Bundes erweitert das Gesetz auch die Möglichkeiten des Bundesamtes zur Unterstützung der Länder. Hierfür benötigt das BSI zusätzliche 29 Planstellen/Stellen.

- § 5a BSIG-E: Neben der Analyse von Protokolldaten im Sinne des BSIG ist zukünftig die Auswertung von behördeninternen Protokollierungsdaten ein wesentlicher Bestandteil einer umfassenden Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes. Hieraus ergibt sich, dass nun in einem sehr viel größeren Maßstab auch Behörden, die noch nicht von der IT-Konsolidierung erfasst werden, Protokollierungsdaten an das BSI übermitteln müssen und das BSI diese bei dem gesamten Prozess (Planen, Sammeln, Detektieren, Auswerten) nach Mindeststandard zur Protokollierung und Detektion unterstützen muss. Hierbei ist zu beachten, dass eine sehr heterogene IT-Systemlandschaft besteht, welche eine individuelle Betreuung der Behörden erfordert. Die Detektion von Cyber-Angriffen durch eine systematische Analyse dieser Daten führt zu einem zusätzlichen Personalbedarf von 29 Planstellen/Stellen.

- In der heutigen Bedrohungslage sind präventive Schutz- und Abwehrmaßnahmen allein nicht mehr ausreichend. Angriffe werden auch bei bestmöglicher Prävention erfolgreich sein, sodass die Planung und Durchführung reaktiver Maßnahmen unerlässlich ist. Zu diesen zählt eine möglichst schnelle und sachkundige Zurückführung angegriffener Systeme und Netze in einen „sauberen“ Zustand, um die weitere Nutzbarkeit und Sicherheit der betroffenen Systeme und Netze sicherzustellen. Das Bundesamt hat zu diesem Zweck Mobile Incident Response Teams (MIRTs) eingerichtet, die betroffenen Behörden der Bundesverwaltung sowie weiterer Bedarfsträger (andere Verfassungsorgane, Länder oder die Betreiber Kritischer Infrastrukturen) bei der Bewältigung von Sicherheitsvorfällen unterstützen. Durch die Erweiterung des Adressatenkreises entsteht für das BSI ein personeller Mehrbedarf von 41 Planstellen/Stellen.

- § 5c, § 8b Abs. 2 BSIG-E: Kommt es bei Betreibern Kritischer Infrastrukturen oder bei Unternehmen im besonderen öffentlichen Interesse zu größeren (IT-) Störungen, hat dies sehr schnell negative Auswirkungen auf große Teile der Bevölkerung. Zur Aufrechterhaltung oder Wiederherstellung von IT-Systemen im Falle einer erheblichen Störung ist eine bestehende, auch in Krisenlagen funktionsfähige Kommunikationsinfrastruktur von wesentlicher Bedeutung. Um die

notwendigen Krisenreaktionsmaßnahmen zu erarbeiten sowie eine Struktur zwischen Bundesbehörden und den Betreibern Kritischer Infrastrukturen und den Unternehmen im besonderen öffentlichen Interesse aufzubauen, zu pflegen und zu betreiben, sind beim BSI 44 Planstellen/Stellen erforderlich.

- § 5d BSIG: Die schnelle Information der Opfer eines Cyber-Angriffs und die Möglichkeit so früh wie möglich Unterstützung bei der Bewältigung anzubieten, ist eine elementare Aufgabe des Bundesamtes. Um die Opfer eines Angriffs identifizieren zu können, ist eine Bestandsdatenabfrage häufig unerlässlich. Zur effektiven Durchführung der damit verbundenen Aufgaben entsteht ein zusätzlicher Personalbedarf von 2 Planstellen/Stellen.

- Das Bundesamt muss in der Lage sein, technische Untersuchungen nach § 7a BSIG-E zur Erfüllung seiner gesetzlichen Aufgaben durchzuführen. Das Bundesamt wird mit Befugnissen ausgestattet, die zugleich auch zu weitergehenden und tieferen Prüfungen führen und damit einen Mehraufwand erzeugen. Durch die Erweiterung der Untersuchungsbefugnis entsteht ein Bedarf von 5 Planstellen/Stellen.

- § 7b BSIG-E: Um schnell und effektiv vor Sicherheitsrisiken für die Netz- und Informationssicherheit zu warnen, ist eine Detektion bestehender Risiken unerlässlich. Insbesondere für die Planung, Entwicklung und Wartung der Scanner als auch für die fachliche Begleitung aller Prüfungen sowie für die notwendigen Auswertungen und die Einschätzung der Ergebnisse werden weitere Fachkräfte benötigt. Um diese neue Aufgabe effektiv umzusetzen, benötigt das BSI 10 Planstellen/Stellen.

- § 7c BSIG-E: Um Detektionsmaßnahmen zum besonderen Schutz von Mitgliedern der Verfassungsorgane durchzuführen und hierdurch das Bundeskriminalamt zu unterstützen, entsteht dem Bundesamt zudem ein Personalbedarf von zusätzlichen 2 Planstellen/Stellen.

- § 8 BSIG-E: Die Digitalisierungsvorhaben der Bundesregierung erfordern eine konstante Beratung und Begleitung durch das Bundesamt, um bereits ab der Konzeptions- und Planungsphase die Aspekte der IT-Sicherheit zu berücksichtigen. Angesichts der Vielzahl der anstehenden Digitalisierungsprojekte entsteht, aufgrund des hierdurch entstehenden Beratungsaufwands, ein Personalbedarf von 71 Planstellen/Stellen.

- Durch die Aufnahme weiterer Branchen in den Regelungsbereich des Gesetzes sowie die Ergänzung des BSIG um den Bereich der Unternehmen im besonderen öffentlichen Interesse entsteht ein personeller Mehrbedarf des BSI von insgesamt 56 Planstellen/Stellen.

- Die in § […] eingefügte Vertrauenswürdigkeitserklärung für kritische Komponenten (im Rahmen von Zertifizierungen) führt zu einem erhöhten Personalbedarf von XX Stellen (wird nachgereicht).

- § 9a BSIG-E: Durch die Konzeption und Vergabe eines IT-Sicherheitskennzeichens sollen insbesondere Verbraucherinnen und Verbraucher in die Lage versetzt werden, den Aspekt der IT-Sicherheit bei der Auswahl ihrer IT-Produkte in einfacher Form berücksichtigen zu können, indem sieschnell und einfach überprüfen können, ob das jeweilige IT-Produkt bzw. dessen Hersteller aktuelle Sicherheitsstandards in ausreichender Form berücksichtigt. Um die für die Vergabe des IT-Sicherheitskennzeichens erforderlichen Arbeiten inklusive der im Sinne einer

Marktaufsicht anstehenden Prüfungen und Kontrollen durchführen zu können, benötigt das Bundesamt 25 zusätzliche Planstellen/Stellen.

- § 14 BSIG-E: Die Erweiterung der Bußgeldvorschriften führt zu einem erhöhten Prüfungs- und Verwaltungsaufwand. Das BSI benötigt zur Bewältigung dieses zusätzlichen Aufwandes 2 weitere Planstellen/Stellen.

Für die Umsetzung des Zweiten IT-Sicherheitsgesetzes kommen für die BDBOS folgende neue Aufgaben hinzu:

- § 4a: Die Kontrollbefugnisse des BSI verursachen Mitwirkungs-, Unterstützungs- und Berichtspflichten auf Seiten der BDBOS, die zu einem Personalbedarf von 6 Planstellen führen.

- § 5 Absatz 11 und § 5a: Durch die neue Regelung darf das BSI Protokolldaten von Infrastrukturen erheben und auswerten, wofür neue Prozesse und Schnittstellen geschaffen werden müssen. Die hierfür erforderlichen Mehraufwendungen ergeben sich bereits aus dem Mindeststandard zur Protokollierung. Hier fällt ein Personalaufwand von einmalig 1-2 Personenwochen sowie 12 Personentage p.p.a. für die Einrichtung, Wartung und Pflege der Infrastruktur an. Für die Daueraufgabe der Protokollierung ist von mindestens einer 1 Planstelle, sofern die BDBOS die Protokollierung über Detection-as-a-Service (DaaS) des BSI in Anspruch nimmt.

  Andernfalls sind die Aufwände deutlich größer. Die BDBOS muss in diesem Fall für die von ihr betriebenen Infrastrukturen Technik, Organisation und Prozesse aufsetzen und anpassen, um die notwendigen Protokolldaten systematisch zu erfassen, auszuwerten und an das BSI weitergeben zu können. Insgesamt ist für die Umsetzung dieser Änderungen in § 5 und § 5a ein Personalmehrbedarf von 30 Planstellen in der BDBOS anzusetzen. Zusätzlich entstehen hier einmalige technische Aufwände in Höhe von 5 Mio. Euro.

- §§ 5c, 8b: Für die Änderungen betreffend die Krisenkommunikation mit KRITIS-Unternehmen und deren Integration in die Kommunikationsnetze und Betriebsinfrastrukturen der BDBOS ist ein Personalbedarf von 8 Planstellen erforderlich. Dies ergibt sich aus der Unterstützung des BSI bei insbesondere folgenden Aufgaben:
  - Erstellung von Krisenreaktionsplänen
  - Anhörung der Betroffenen
  - Fachliche Beratung und Einbindung in Gesamtkonzepte
  - Pflegeaufwand nach Abstimmung
  - Unterstützung der Beübung

- § 8: Zur Umsetzung der besonders hohen Sicherheitsanforderungen und sich stetig fortentwickelnden Mindeststandards für die Kommunikationstechnik des Bundes erhöhen sich bei der BDBOS die Aufwände für die technische Konzeption der von ihr betriebenen Netze sowie für die Erstellung und Sicherstellung der Umsetzung der erforderlichen Sicherheitskonzepte für die einzelnen KRITIS-Kernkomponenten der Netze und für die Netze in ihrer jeweiligen Gesamtheit. Es entsteht bei der BDBOS ein Personalbedarf von 10 Planstellen.

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

5. Weitere Kosten

Keine.

6. Weitere Gesetzesfolgen

Die Cyber- und Informationssicherheit für Verbraucherinnen und Verbraucher wird erhöht. Die ausdrückliche Aufnahme des Verbraucherschutzes in den Aufgabenkatalog des BSI trägt der wachsenden Bedeutung der Cyber- und Informationssicherheit für Verbraucherinnen und Verbraucher - insbesondere durch die steigende Vernetzung privater Haushalte und die Verbreitung vernetzter Verbraucherprodukte - Rechnung. Der ganzheitliche Verbraucherschutz beschränkt sich jedoch nicht auf Maßnahmen, die sich unmittelbar an Verbraucherinnen und Verbraucher richten und auf die Vermittlung von Risikobewusstsein, Beurteilungsfähigkeit und Lösungskompetenz gerichtet sind. Die Förderung des Verbraucherschutzes und der Verbraucherinformation, die sich an den satzungsgemäßen Zielen der Verbraucherschutzverbände (z.B. des Verbraucherzentrale Bundesverband, VZBV) und der Deutschen Stiftung Verbraucherschutz orientiert, geht darüber hinaus und umfasst u.a. auch das Eintreten für die Verbraucherbelange gegenüber Herstellern oder die Förderung von Forschungsvorhaben mit Verbraucherschutzbezug.

Die Regelungen sind inhaltlich geschlechtsneutral und damit ohne Gleichstellungsrelevanz. Die weitere Stärkung der Cyber- und Informationssicherheit betrifft sowohl mittelbar wie unmittelbar Frauen wie Männer gleichermaßen. § 1 Absatz 2 des Bundesgleichstellungsgesetzes, der verlangt, dass Rechts- und Verwaltungsvorschriften des Bundes die Gleichstellung von Frauen und Männern auch sprachlich zum Ausdruck bringen sollen, wurde in die Entwicklung der Gesetzesformulierung miteinbezogen. Gleichzeitig wurde aber auch die Diktion der jeweils zu ändernden Stammgesetze mitberücksichtigt.

Demographische Auswirkungen des Vorhabens − unter anderem auf die Geburtenentwicklung, Altersstruktur, Zuwanderung, regionale Verteilung der Bevölkerung oder das Generationenverhältnis − sind nicht zu erwarten.

VII. Befristung; Evaluierung

Eine Befristung oder gesonderte Evaluierung ist derzeit nicht vorgesehen, da nach Artikel 10 des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 eine Evaluierung des Artikel 1 Nummer 2, 7 und 8 des IT-Sicherheitsgesetztes durchgeführt wird. Die aus dieser Evaluierung gewonnenen Erkenntnisse können in vorliegendem Gesetzentwurf noch nicht einfließen. Erkenntnisse und Erfahrungen aus diesem Gesetzentwurf können in diese Evaluierung einfließen.

B. Besonderer Teil

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

Zu Nummer 1

Zu Buchstabe a

Der derzeitige Wortlaut des § 2 Absatz 3 BSIG zur Definition der Kommunikationstechnik des Bundes umfasst bisher nicht die behördeninterne Kommunikation oder den behördeninternen Datenaustausch. Zudem werden allgemeine Datenverarbeitungsvorgänge nicht erfasst. Diese Bereiche sind jedoch, genauso wie die Informationstechnik zur Kommunikation und der Datenaustausch der Behörden untereinander oder mit Dritten, gleichermaßen Angriffsziele. Durch die Einbeziehung dieser Bereiche steigt das Sicherheitsniveau insgesamt, da mehr Detektionsmöglichkeiten

geschaffen werden. Somit wird insbesondere die Detektion von zielgerichteten und nachrichtendienstlichen Angriffen verbessert. Der Begriff der Datenverarbeitung ist hierbei im Sinne der Datenschutzgrundverordnung (DSGVO) weit zu verstehen. Der Datenaustausch bleibt weiterhin umfasst. Regelungen über den Geheimschutz bleiben unberührt.

Kommunikationstechnik, die im Rahmen des Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) im Eigentum von nicht dem Bund zuzuordnenden Nutzern steht, ist nicht Kommunikationstechnik des Bundes im Sinne von § 2 Absatz 3 S. 1 BSIG.

Zu Buchstabe b

Der bisher in § 2 Absatz 9 BSIG definierte Begriff des Datenverkehrs wird im BSIG nicht mehr verwendet und daher gestrichen. An seiner Stelle wird der Begriff der Protokollierungsdaten in § 5a BSIG-E legaldefiniert.

Protokollierungsdaten sind die Dokumentation technischer Ereignisse und Zustände innerhalb eines IT-Systems, die tatsächliche Anhaltspunkte für die Erkennung und Analyse laufender und die Rekonstruktion vergangener Angriffe auf die Informations- und Kommunikationstechnik des Bundes liefern können. Basierend auf diesen Daten lassen sich die Erkennung und Analyse von Cyber-Angriffen deutlich verbessern.

Zu Buchstabe c

IT-Produkte sind möglichst weitgehend zu definieren, da sich Sicherheitslücken in verschiedensten Komponenten ergeben können. Relevant sind sowohl die Hardware an sich als auch die eingesetzte Software, welche das Funktionieren der Hardware erst bedingt. Mit § 8a Absatz 1a bis 1c BSIG-E werden die Betreiber Kritischer Infrastrukturen verpflichtet, Systeme zur Angriffserkennung einzurichten. Mit § 2 Absatz 9b BSIG-E wird der Begriff des Systems zur Angriffserkennung definiert.

Zu Buchstabe d

Die Regelung ergänzt die klassischen KRITIS-Sektoren nach Absatz 10 um den Sektor Entsorgung. Kritische Dienstleistung im Sektor Entsorgung ist die Entsorgung von Siedlungsabfällen. Aufgabe der Entsorgung von Siedlungsabfällen ist es, die anfallenden Abfälle zu sammeln und anschließend so zu beseitigen oder zu verwerten, dass es dabei nicht zu einer Gefährdung der Bevölkerung und Umwelt kommt. Ein Ausfall oder eine Beeinträchtigung dieser Dienstleistung führt, ähnlich wie bei der Abwasserentsorgung, sowohl zu einem kurzfristigen Anstieg der Seuchengefahr als auch zu einer Verschmutzung der Umwelt mit gefährlichen Stoffen. Ihr Ausfall führt damit sowohl kurz- als auch langfristig zu einer gesundheitlichen Gefährdung der Bevölkerung.

Zu Buchstabe e

Die Regelungen ergänzen die Definition der Kritischen Infrastrukturen in § 2 Absatz 10 BSIG und der Digitalen Dienste in § 2 Absatz 11 BSIG.

§ 2 Absatz 13 BSIG-E definiert kritische Komponenten. Diese sind IT-Produkte, die in Kritischen Infrastrukturen eingesetzt werden und die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit dieser IT-Produkte zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können.

§ 2 Absatz 14 BSIG-E regelt Unternehmen im besonderen öffentlichen Interesse. Zu diesen gehören Unternehmen, die aufgrund ihrer volkswirtschaftlichen Bedeutung und

insbesondere ihrer erbrachten Wertschöpfung von besonderem öffentlichen Interesse sind, Rüstungshersteller sowie Hersteller von IT-Produkten für die Verarbeitung staatlicher Verschlusssachen und Unternehmen, die einer Regulierung durch die Verordnung zum Schutz vor Gefahrstoffen unterliegen. Diese gehören nicht zu den Kritischen Infrastrukturen im Sinne des § 2 Absatz 10 BSIG, an ihrer Funktionsfähigkeit besteht aber aus anderen Gründen ein erhebliches Interesse für die Gesellschaft.

Wie im Fall der Kritischen Infrastrukturen wird eine Rechtsverordnung die weiteren Unternehmen im besonderen öffentlichen Interesse konkretisieren.

Zu Nummer 2

Zu Buchstabe a

Es handelt sich lediglich um eine redaktionelle Anpassung.

Zu Buchstabe b

Die Ergänzung des § 3 Absatz 1 Satz 2 BSIG dient der Klarstellung der Zuständigkeit des Bundesamtes im Sinne des § 1 Absatz 2 des Gesetzes über die Akkreditierungsstelle im Bereich der Sicherheit in der Informationstechnik, Stellen die Befugnis zu erteilen, als Konformitätsbewertungsstelle tätig zu werden.

Zu Buchstabe c

Die Ergänzung bezieht sich auf die Wahrnehmung der Aufgaben und Befugnisse des Bundesamtes als nationale Behörde für die Cybersicherheitszertifizierung im Sinne des Artikels 58 der Verordnung (EU) 2019/881 vom 17. April 2019.

Zu Buchstabe cd

Die Anpassung dient der Klarstellung, dass es auch Aufgabe des BSI ist, gerade im Zusammenhang mit dem Verbraucherschutz, die genannten Adressaten zu informieren. Ferner wird mit dem letzten Halbsatz in § 3 Absatz 1 Satze 2 Nummer 14 BSIG-E klargestellt, dass das BSI in dieser Aufgabe nicht eingeschränkt wird.

Zu Buchstabe de

Mit der Regelung wird das Vorhaben des Koalitionsvertrags der 19. Legislaturperiode umgesetzt, den Verbraucherschutz im Bereich der Sicherheit in der Informationstechnik als zusätzliche Aufgabe des BSI zu etablieren. Die ausdrückliche Aufnahme des Verbraucherschutzes in den Aufgabenkatalog des § 3 BSIG trägt der wachsenden Bedeutung der Cyber- und Informationssicherheit für Verbraucherinnen und Verbraucher insbesondere durch die steigende Vernetzung privater Haushalte und die Verbreitung vernetzter Verbraucherprodukte - Rechnung. Der Schutz der Verbraucherinnen und Verbraucher im Sinne des § 2 Absatz 11 Nummer 1 BSIG-E stärkt zugleich die Sichtbarkeit des BSI als bürger- und verbraucherorientierte Cybersicherheitsbehörde im nationalen Bereich.

Das BSI kann mit seiner technischen Expertise und breiten Erfahrung im Bereich des anwenderbezogenen Schutzes der Informationssicherheit einen wichtigen Beitrag zur Unterstützung der Verbraucherinnen und Verbraucher vor Gefahren für die Sicherheit der von ihnen eingesetzten Informationstechnik leisten.

Bereits nach geltendem Recht ist es Aufgabe des BSI, die Anwender, also auch Verbraucherinnen und Verbraucher, nach § 3 Absatz 1 Satz 2 Nummer 14 BSIG in Fragen der Sicherheit in der Informationstechnik zu beraten, zu warnen und zu sensibilisieren.

Hierzu stehen dem BSI insbesondere die Befugnisse der §§ 7, 7a BSIG zur Warnung, Empfehlung und Untersuchung auf dem Markt bereitgestellter oder zur Bereitstellung vorgesehener informationstechnischer Produkte und Systeme zur Verfügung.

Der Verweis in § 3 Absatz 1 Satz 2 Nummer 14a BSIG-E auf § 3 Absatz 1 Satz 2 Nummer 14 BSIG stellt klar, dass die Beratung, Information und Warnung von Verbraucherinnen und Verbrauchern in Fragen der IT-Sicherheit substantieller Bestandteil der Verbraucherschutzaufgabe des BSI ist. Hierdurch kann das BSI seine auf alle Anwender bezogenen Aufgaben und Befugnisse zielgruppenspezifisch auf die Belange der Verbraucherinnen und Verbraucher bzw. auf verbrauchernahe Produkte und Dienste fokussieren und ausbauen. Hierzu zählen u.a. stationäre und mobile Betriebssysteme (Windows 10, IOS, Android), Programme und Apps, Online-Dienste (Homebanking, E-Mail, Hosting-Dienste, Teamviewer), Soziale Netze (z.B. Facebook, Whatsapp), Streaming-Dienste (z.B. Spotify, Netflix), Cloud-Dienste (z.B. Dropbox, Onedrive), IoT (z.B. Alexa, GoogleHome, Smart Home), Hardware-Konsumentenprodukte (z.B. Smartphone, Smart-TV) oder Hardware (z.B. Chips, Grafikkarten).

Ein ganzheitlicher Verbraucherschutz im Bereich der Sicherheit in der Informationstechnik beschränkt sich jedoch nicht auf Maßnahmen, die sich unmittelbar an Verbraucherinnen und Verbraucher richten und auf die Vermittlung von Risikobewusstsein, Beurteilungsfähigkeit und Lösungskompetenz gerichtet sind. Die durch § 3 Absatz 1 Satz 2 Nummer 14a BSIG-E vorgesehene Förderung des Verbraucherschutzes und der Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik, die sich an den satzungsgemäßen Zielen der Verbraucherschutzverbände (z.B. des Verbraucherzentrale Bundesverband, VZBV) und der Deutschen Stiftung Verbraucherschutz orientiert, geht darüber hinaus und umfasst u.a. auch das Eintreten für die Verbraucherbelange gegenüber Herstellern oder die Förderung von Forschungsvorhaben mit Verbraucherschutzbezug. Im Gegensatz zu den Verbraucherschutzverbänden ist das BSI jedoch keine Organisation zur ausschließlichen Vertretung und Durchsetzung von Verbraucherinteressen, sondern hat als nationale Cybersicherheitsbehörde die Interessen aller Stakeholder aus Staat, Wirtschaft und Zivilgesellschaft zu berücksichtigen.

Zur Umsetzung des Verbraucherschutzes im Bereich der im Bereich der Sicherheit in der Informationstechnik soll das BSI mit den Verbraucherzentralen und weiteren Partnern im Bereich des (digitalen) Verbraucherschutzes eng zusammenarbeiten. Als Maßnahmen für eine effektive Umsetzung des Verbraucherschutzes im Bereich der Sicherheit in der Informationstechnik kommen folgende Maßnahmen des BSI in Betracht:

- Systematische Marktbeobachtung im Bereich Verbraucherprodukte und -dienste (internetfähige IT-Systeme und Online-Dienste). Hierdurch wird das BSI in die Lage versetzt, aktuelle Marktentwicklungen zu identifizieren und basierend hierauf auch Prognosen im Hinblick auf zukünftige Trends, Entwicklungen und Auswirkungen auf Verbraucher treffen zu können. Die Ergebnisse der Marktbeobachtung stellen die Grundlage für weitergehende Sicherheitstests und -analysen dar.

- Definition des Stands der Technik für IT-Produktkategorien und Dienste im Verbraucherbereich. Der Stand der Technik wird durch das BSI kontinuierlich weiter gepflegt und aktualisiert.

- Sicherheitstests und -analysen mit dem Schwerpunkt „IT-Sicherheitsrisiken für Verbraucherinnen und Verbraucher“. Durch Sicherheitstests und -analysen von auf dem Markt bereitgestellten IT-Produkten und Systemen kann das BSI aktuelle IT-Sicherheitsrisiken für Verbraucherinnen und Verbraucher identifizieren. Zum anderen können Sicherheitstests und -analysen zur stichprobenartigen Überprüfung

bezüglich der Einhaltung der Anforderungen nach dem zuvor definierten Stand der Technik dienen.

- Um das Problembewusstsein und die Aufmerksamkeit für die Belange der Informationssicherheit zu erhöhen, soll das BSI seine Beratungs- und Unterstützungsangebote, beispielsweise mit einer zielgruppenspezifischen Sensibilisierungskampagne für Verbraucher intensivieren. Insbesondere kann es auf Basis der Ergebnisse von Marktbeobachtung, Sicherheitstests und technischen Bewertungen sowie eines durch das BSI definierten Standes der Technik, Verbrauchern allgemeine Empfehlungen zur sicheren Nutzung von informationstechnischen Produkten und Diensten geben und vor Gefahren im Zusammenhang mit konkreten informationstechnischen Produkten und Diensten sowie vor Herstellern warnen.

- Ergänzung des BSI-Bürger-Angebots um eine Verbraucherschutz-Online-Plattform, auf der Verbraucherinnen und Verbraucher auf Empfehlungen, Warnungen und Informationen des BSI zugreifen und sich umfassend zu den für sie relevanten Themen der Cyber-Sicherheit informieren können. Die Plattform dient zudem als Kommunikationsschnittstelle zu den Verbraucherinnen und Verbrauchern.

- Aufnahme eines kontinuierlichen Verbraucherschutzdialogs zwischen BSI, Herstellern und Diensteanbietern, um einen frühzeitigen und steten Austausch zwischen den Belangen der Verbraucherinnen und Verbraucher und den Interessen der Hersteller und Diensteanbieter zu fördern. Hierzu nutzt das BSI seine Erfahrungen aus der Marktbeobachtung, den Sicherheitstests und -analysen sowie dem Dialog mit den Übrigen im Verbraucherschutz tätigen Akteuren.

- Angebot eines IT-Sicherheitskennzeichens für verbrauchernahe Produkte und Dienste zur Erhöhung der Verbrauchertransparenz und zur Förderung der Sicherheit in der Informationstechnik. Das Angebot eines Kennzeichens für IT-Sicherheit kann Verbraucherinnen und Verbrauchern die Auswahl eines IT-Produktes oder eines Online-Dienstes erleichtern, indem für sie auf einen Blick feststellbar ist, welches IT-Produkt oder welcher Dienst welches konkrete Sicherheitsniveau aufweist. Hierdurch kann der Markt für sichere IT-Systeme und Online-Dienste (z.B. Cloud-Dienste) positiv beeinflusst werden, so dass indirekt zugunsten der Verbraucher ein Beitrag dazu geleistet wird, das Sicherheitsniveau insgesamt zu steigern. Zudem wird ein sichtbares Gütesiegel oder Kennzeichen auch zu einer Sensibilisierung der Verbraucher und damit zu einem Bewusstsein für IT-Sicherheit führen.

- Unterstützung von Abmahnungen und Klagen bei verbraucherrechtswidrigen Praktiken durch das BSI. Das BSI unterstützt mit seiner fachlichen Expertise im Bereich der IT-Sicherheit Abmahnungen und Klagen bei verbraucherrechtswidrigen Praktiken nach dem Unterlassungsklagegesetz (UKlaG) bzw. dem Gesetz gegen unlauteren Wettbewerb (UWG). Gemäß § 7a Absatz 2 BSIG darf das BSI informationstechnische Produkte untersuchen und die hieraus gewonnenen Erkenntnisse u.a. auch den im UKlaG genannten Stellen zur Verfügung stellen. Ebenso darf das BSI diese Stellen in Fragen der Sicherheit der Informationstechnik beraten. Im Ergebnis kann das BSI somit die im UKlaG genannten Stellen bei der Durchsetzung von Ansprüchen gegen verbraucherrechtswidrige Praktiken im Bereich der IT-Sicherheit beraten und unterstützen.

- Förderung fremder Projekte zum Verbraucherschutz im Bereich der Informationssicherheit und Durchführung von eigenen Forschungsprojekten zum Verbraucherschutz im Bereich IT-Sicherheit.

Zu Buchstabe ef

Die bestehenden Pflichten zur Einhaltung von Mindeststandards und zur Meldung von Störungen werden auf weitere Teile der Wirtschaft ausgeweitet. In der Folge sind auch die Aufgaben des BSI anzupassen.

Zu Buchstabe fg

Es handelt sich um eine redaktionelle Anpassung wegen der Ergänzung weiterer Aufgaben.

Zu Buchstabe h

Mit der neu eingefügten Nummer 19 in § 3 Absatz 1 Satz 2 BSIG wird die Zuständigkeit des BSI für die Entwicklung von Vorgaben sowie die abschließende Bewertung von Identifizierungs- und Authentisierungsverfahren unter dem Gesichtspunkt der Informationssicherheit gesetzlich klargestellt. Diese sicherheitstechnisch relevanten Verfahren bedürfen gerade mit Blick auf die Vorgaben der eIDAS-VO auf EU-Ebene einer Konkretisierung sowie abschließenden Bewertung im nationalen Kontext, um eine sichere, nutzerfreundliche und insbesondere einheitliche Ausgestaltung zu gewährleisten. Das BSI ist kraft seines gesetzlichen Auftrags innerhalb der Bundesverwaltung für diesen Bereich zuständig, da der Gesetzgeber mit der Bündelung der Fachkompetenz des Bundes im Bereich der Informationssicherheit beim BSI (§ 1 Satz 2 BSIG) gerade das Ziel verfolgt hat, eine einheitliche Bewertung für sicherheitstechnisch relevante Verfahren und Maßnahmen zu erzielen. Darüber hinaus verfügt das BSI als einzige Behörde innerhalb der Bundesverwaltung über die technische Kompetenz, die für eine abschließende Bewertung solcher Verfahren erforderlich ist. Die neu eingefügte Klarstellung in Nummer 19 stellt daher sicher, dass das gesetzgeberische Ziel erreicht wird.

Mit der neu eingefügten Aufgabe in Nummer 20 in § 3 Absatz 1 Satz 2 BSIG wird die Zuständigkeit des BSI für die Entwicklung von Anforderungen und Empfehlungen nebst entsprechender Konformitätsprüfung und -bestätigung bei IT-Produkten, insbesondere in Gestalt von Technischen Richtlinien, ausdrücklich festgelegt. Mit Blick auf die zunehmende Vernetzung der IT-Produkte sind entsprechende Anforderungen an die IT-Sicherheit zum Zwecke des Verbraucherschutzes unerlässlich. Hierzu müssen durch das Bundesamt einheitliche Vorgaben geschaffen und als zentrale Stelle im Markt etabliert werden.

Zu Nummer 3

Es handelt sich hierbei lediglich um eine Klarstellung. Der Begründung zu § 4 BSIG in BT-Drs. 18/4096, 28. ist zu entnehmen, dass bei der Konzeption der Regelung im Jahr 2009 davon ausgegangen wurde, dass die im Rahmen von § 4 BSIG üblicherweise zu übermittelnden Informationen keinen Personenbezug aufweisen. Durch die kontinuierliche Erweiterung der datenschutzrechtlichen Regelungen auf nationaler und europäischer Ebene und höchstrichterliche Entscheidungen kann heute aber nicht mehr davon ausgegangen werden, dass Informationen technischer Natur in der Regel keinen Personenbezug aufweisen. Im Gegenteil ist in der Regel davon auszugehen, dass sich ein Personenbezug - aufgrund neuer technischer Auswertungsmöglichkeiten und der Erweiterung des Anwendungsbereiches der Regelungen zum Schutz von personenbezogenen Daten - bei einer Vielzahl von technischen Daten nicht vollständig ausschließen lässt. Die Klarstellung ist ferner erforderlich, um die Regelung für die übermittelnden Behörden als eine eindeutige und rechtssichere Rechtsgrundlage für die Übermittlung personenbezogener Daten an das Bundesamt auszugestalten und hierdurch Rechtsunsicherheit zu beseitigen.

Zu Nummer 4

Zu § 4a BSIG-E

Die neue Regelung in § 4a BSIG-E dient der Stärkung der Rolle des Bundesamtes und gleichzeitig der Gewährleistung eines hohen Sicherheitsniveaus. Dies ist auch im Koalitionsvertrag der 19. Legislaturperiode, z.B. Zeile 6029, vorgesehen. Die Umsetzung der besonders hohen Sicherheitsanforderungen bei der Kommunikationstechnik des Bundes erfordert eine effektive, schnelle und jederzeitige Prüf- und Kontrollmöglichkeit durch das für die Sicherheit der Kommunikationstechnik des Bundes zuständige Bundesamt. Die Regelung schafft die hierfür erforderliche Ermächtigung und benennt die dem Bundesamt zur Verfügung stehenden Befugnisse.

Anhaltspunkte zu dem aktuellen Sicherheitsniveau für die Sicherheit der Kommunikationstechnik können Informationen sein, die sich insbesondere aus Konzepten, Regelungen, Dokumenten, bspw. über Netzinfrastrukturen, ergeben.

Sofern sich die Kommunikationstechnik des Bundes nicht in Stellen des Bundes befindet, kann das Bundesamt die Befugnisse nur im Einvernehmen mit den Dritten ausüben. Dies gilt auch, wenn sich Schnittstellen in Einrichtungen bzw. auf Seiten der Länder befinden.

Das Bundesamt wird neben der jeweils überprüften Stelle und der eigenen Fachaufsicht das Ergebnis auch der jeweiligen Rechts- und Fachaufsicht der geprüften Stelle entsprechend dem Ressortprinzip, nach eigenem Ermessen versehen mit Vorschlägen zur Verbesserung der IT-Sicherheit, mitteilen.

Zu § 4b BSIG-E

Die Vorschrift ergänzt die Regelungen des § 4 BSIG (Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes) und des § 8b BSIG (Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen). Im Rahmen seiner Aufgabe als zentrale Meldestelle für Informationstechnik soll das BSI auch als allgemeine Meldestelle umfassend Informationen zu Sicherheitslücken, Schadprogrammen und IT-Sicherheitsvorfällen zentral sammeln und auswerten. Wesentliche Informationsquellen sind hierbei privatwirtschaftlich organisierte Sicherheits- und Computer-Notfallteams (CERTs), die Wirtschaft, aber auch Einzelpersonen wie Forscher, Hacker und IT-Sicherheitsanalysten. Diese Informationen sind für ein Gesamtlagebild der Cyber-Sicherheit in Deutschland von besonderer Bedeutung.

Die im Rahmen von § 4b BSIG-E verarbeiteten Informationen haben regelmäßig einen Personenbezug, da oftmals (dynamische) IP-Adressen oder E-Mail-Adressen, von denen Cyber-Angriffe ausgehen, verarbeitet werden und auch zu Zwecken der Gewährleistung der Netz- und Informationssicherheit verarbeitet werden müssen. Für die Übermittlung solcher Informationen durch Dritte aus der Wirtschaft oder durch Einzelpersonen an das BSI (Meldende) fehlt bislang eine ausdrückliche Rechtsgrundlage, die mit § 4b BSIG-E geschaffen werden soll. Entsprechend legt die Norm klar den Zweck der Datenübermittlung fest. Gleichzeitig sind Meldende nach § 4b BSIG-E nicht dazu verpflichtet, dem BSI entsprechende Informationen zu übermitteln. Ihre Meldungen bzw. ihre Zusammenarbeit mit dem BSI erfolgt ausschließlich auf freiwilliger Basis. Es sollen anonyme Meldungen möglich sein, um hierdurch Hemmschwellen, insbesondere bei Einzelpersonen, zu senken, die möglicherweise Bedenken haben, sich einer staatlichen Stelle anzuvertrauen.

Das BSI wird hierzu die notwendigen Möglichkeiten zur Entgegennahme der Meldungen aufbauen. Bei der Zusammenarbeit mit Dritten aus der Wirtschaft sollte soweit wie möglich auf etablierte Melde- und Austauschmöglichkeiten wie MISP (Malware Information Sharing Plattform) aufgebaut werden, die über datenschutzgerechte Rollen- und Rechtekonzepte verfügen. Gegenüber privaten Dritten kann sich der Betrieb einer anonymen Meldemöglichkeit, wie sie zum Beispiel vom Bundeskartellamt betrieben wird, anbieten.

§ 4a Absatz 3 BSIG-E eröffnet die Möglichkeit, dass das Bundesamt andere Bundesbehörden, Dritte und die Öffentlichkeit über mögliche Gefahren der Cyber- und

Informationssicherheit informieren kann, beispielsweise zu Zwecken der Schadensverhinderung oder -verringerung.

§ 4a Absatz 4 Satz 3 BSIG führt Schutzrechte der Meldenden ein. Nach Absatz 5 bleiben jedoch bestehende gesetzliche Meldepflichten und Übermittlungsregelungen, die den Aufgaben anderer Behörden dienen, hiervon unberührt. Dies betrifft speziell die Zusammenarbeit mit den in § 5 Absatz 5 BSIG genannten Stellen für deren Aufgaben nach Maßgabe der dafür geltenden Übermittlungsregelungen.

Zu Nummer 5

Aus Erfahrungen der Vergangenheit zu verschiedenen Angriffen ist zum Schutz der Regierungsnetze eine Anpassung des § 5 BSIG erforderlich. Das BSI nimmt dabei weiterhin sonderordnungsbehördliche Funktionen beim Schutz von Kommunikationstechnik wahr und nicht Aufgaben der allgemeinen Gefahrenabwehr. Die Zuständigkeit der allgemeinen Gefahrenabwehr, welche grundsätzlich im Rahmen der gesetzlich zugewiesenen Aufgaben auch die Abwehr von Angriffen aus dem Cyberraum umfasst, liegt weiterhin bei den zuständigen Polizeibehörden.

Zu Buchstabe b

Mit der Änderung wird die Speicherdauer pseudonymisierter Protokolldaten i.S.v. § 2 Absatz 8 BSIG von drei auf 18 Monate erhöht. Die automatische Auswertung der Protokolldaten erfolgt weiterhin für die ersten drei Monate. Auf die zusätzlichen 15 Monate darf nur unter Berücksichtigung von § 5 Absatz 2 Satz 5 bis 8 BSIG, also nach Anordnung, und bei Vorliegen tatsächlicher Erkenntnisse über die Betroffenheit des Bundes zugegriffen werden. Wie Cyber-Vorfälle der Vergangenheit innerhalb der Bundesverwaltung zeigen, erstrecken sich insbesondere spezialisierte Cyberangriffe, so genannte Advanced Persistent Threats (APTs), über einen mehrjährigen Zeitraum. Persistenz bezeichnet dabei das Bemühen der Angreifer, sich nachhaltig und unbemerkt in der Kommunikationstechnik des Bundes einzunisten. Hierfür muss der Angreifer vorsichtig und verdeckt vorgehen, so dass zwischen der initialen Infektion der Kommunikationstechnik des Bundes und der Aufdeckung des Angriffs i.d.R. große Zeiträume liegen. Um durch APT hervorgerufenen Kompromittierungen erkennen und entfernen zu können, muss die Speicherdauer der Protokolldaten den Zeitraum des APT-Angriffs einschließen. Nur wenn das Vorgehen des Angreifers – auch im Nachhinein – aufgeklärt werden kann, kann die Kommunikationstechnik des Bundes vor gleichartigen zukünftigen Bedrohungen geschützt werden.

Satz 2 stellt eine Einschränkung des Zugriffs auf die Daten dar, um den Zugriff auf das fachlich gebotene Maß zu beschränken. Ein Zugriff auf Daten, die älter als drei Monate sind, ist nur dann zulässig, wenn tatsächliche Anhaltspunkte für einen Angriff vorliegen. Hierfür sind sowohl technische als auch organisatorische Vorkehrungen zu treffen.

Zu Buchstabe b

Zur Erfüllung seiner gesetzlichen Aufgabe aus § 3 Absatz 1 Satz 2 Nr. 1 BSIG analysiert das BSI Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen. Diese Daten sind gemäß § 5 Absatz 2 Satz 3 BSIG zu pseudonymisieren, soweit dies automatisiert möglich ist. Eine nicht automatisierte Auswertung ist nur zulässig, um einen erheblichen Fehler zu analysieren und zu beheben. Soweit hierzu die Wiederherstellung des Personenbezugs pseudonymisierter Daten erforderlich ist, muss dies durch den Präsidenten oder die Präsidentin des Bundesamtes oder der Vertretung im Amt angeordnet werden.

Bei der Verarbeitung von Protokolldaten ist eine regelmäßige automatisierte Qualitätssicherung der verarbeiteten Daten im Klartext erforderlich, um semantische und

grammatikalische Fehler in den Daten aufzudecken, bevor diese das Gesamtsystem in seiner fehlerfreien Funktion stören. Eine Fehlfunktion des Quellsystems kann i.d.R. nur so aufgedeckt werden. Eine effektive Qualitätssicherung der Protokolldaten kann nur erfolgen, wenn hierbei einzelne Datensätze nicht pseudonymisiert manuell ausgewertet werden könnten. Eine regelmäßige Qualitätssicherung wurde durch die bisherigen Regelungen des § 5 BSIG nicht ermöglicht.

Zu Buchstabe d

Gemäß § 3 Absatz 1 Satz 2 Nummer 13a BSIG ist es die Aufgabe des BSI, die zuständigen Stellen der Länder in Fragen der Abwehr von Gefahren für die Sicherheit in der Informationstechnik zu unterstützen, soweit ein entsprechendes Ersuchen vorliegt. Zudem kann das Bundesamt die Länder, gem. § 3 Absatz 2 BSIG, nach den allgemeinen Grundsätzen bei der Sicherung ihrer Informationstechnik unterstützen. Dies wird hier nunmehr ausdrücklich normiert.

Zu Nummer 6

Der Begriff der Protokollierungsdaten wird in § 2 Absatz 9 BSIG-E neu eingefügt. Für die Erkennung und Analyse laufender und die Rekonstruktion vergangener Angriffe auf die Informations- und Kommunikationstechnik des Bundes sind diese Daten von erheblicher Bedeutung. Basierend auf diesen Daten lassen sich vergangene Cyber-Angriffe rekonstruieren und laufende erkennen, welche alle sonstigen Sicherheitsmaßnahmen umgangen haben. Um Protokollierungsdaten effektiv zu diesem Zweck zu nutzen, ist eine Planung der zu sammelnden Ereignisse und die Speicherung in einem zentralen System die grundlegende Vorbedingung.

Ein Beispiel hierfür ist das Auslesen oder die Änderung von Zugangsdaten, die dem Angreifer höherwertige Rechte innerhalb der IT-Infrastruktur des Bundes verschaffen und eine laterale Ausbreitung des Angriffes erlauben. Derartige Manipulationen können autonom von Schadsoftware ohne jegliche Kommunikation über die Netze des Bundes erfolgen; dabei fallen keine Protokolldaten im Sinne des § 2 Absatz 8 BSIG an.

Bei Vorliegen tatsächlicher Anhaltspunkte über die Betroffenheit des Bundes nach § 5 BSIG können die Protokollierungsdaten nach § 5 Absatz 3 BSIG de-pseudonymisiert werden, um die betroffene Informationstechnik des Bundes zu identifizieren und die Kompromittierung zu bestätigen und zu beseitigen.

Mit dem Verweis auf die Absätze 2 und 4 von § 5 BSIG wird klargestellt, dass für die Verarbeitung der Protokollierungsdaten dieselben Beschränkungen gelten.

Die Voraussetzungen und Verfahren hinsichtlich des Vorliegens überwiegender Sicherheitsinteressen werden zwischen dem Bundesamt, dem Bundeskriminalamt und dem Bundesamt für Verfassungsschutz mittels Verwaltungsvereinbarung bis spätestens zwei Jahre nach Inkrafttreten dieses Gesetzes geregelt.

Zu Nummer 7

Hierbei handelt es sich um Folgeanpassungen, da der neue § 5a BSIG-E systematisch an dieser Stelle zu regeln und die Unternehmen im besonderen Interesse nach § 2 Absatz 14 Nummer 1 oder 2 BSIG-E aufzunehmen sind.

Zu Nummer 88

Zu § 5c

§ 5c BSIG-E regelt die Erstellung eines Gesamtplans für die Reaktionsmaßnahmen des Bundes zur Aufrechterhaltung oder Wiederherstellung der informationstechnischen Systeme, Komponenten oder Prozesse bei Betreibern Kritischer Infrastrukturen oder Unternehmen im besonderen öffentlichen Interesse während oder nach einer erheblichen Störung im Sinne des § 8b Absatz 4 Nummer 2 BSIG-E, die erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit verursacht. Hierbei zielt im Falle der Krisenbewältigung eine aufzubauende Kommunikationsinfrastruktur weniger auf den Schutz der IT-Sicherheit der Kritischen Infrastrukturen, sondern vielmehr auf die Aufrechterhaltung oder Wiederherstellung der IT-Systeme nach einer krisenhaften Störung oder Beeinträchtigung. Bei der Erstellung des Gesamtplans wird das Bundesamt im Rahmen seiner gesetzlichen Aufgaben und Befugnisse tätig.

Gleichzeitig werden in § 5c Absatz 4 BSIG-E Befugnisse des BSI im Falle des Eintritts einer Störung geregelt. Diese sind erforderlich, um im Einzelfall die Aufrechterhaltung oder Wiederherstellung der IT-Systeme zu gewährleisten. Das Bundesamt setzt sich über Maßnahmen der Aufrechterhaltung oder Wiederherstellung mit den betreffenden Sicherheitsbehörden (§ 5 Absatz 5 BSIG) ins Benehmen.

Zu § 5d

§ 5d BSIG-E regelt die Möglichkeit des BSI zur Bestandsdatenauskunft. Die Möglichkeit des BSI Auskunft zu verlangen ist erforderlich für Information des Nutzers (Angriffsopfer) über den Diensteanbieter und darüber hinaus für die unmittelbare Kontaktaufnahme, um dem Opfer eines Cyber-Angriffes Unterstützung bei der Angriffsabwehr anzubieten. Ferner ist dies erforderlich um IP-Adressen einer (juristischen) Person zuzuordnen, z.B. um Betreiber Kritischer Infrastrukturen identifizieren zu können. Nicht umfasst sind Daten im Sinne des § 113 Abs. 1 Satz 2 TKG.

Durch die Berichtspflicht in § 5d Absatz 5 BSIG-E wird eine transparente Umsetzung der Regelung sichergestellt. Die gemäß § 5d Absatz 5 BSIG-E notwendigen Angaben werden in den jährlichen Bericht (§ 5 Absatz 9 BSIG) des BSI an die Beauftragte oder den Beauftragten für den Datenschutz und die Informationsfreiheit (BfDI) aufgenommen.

Zu Nummer 99

Zu Buchstabe a

Die Anpassungen der Regelungen des § 7 dienen insbesondere der Ausweitung hinsichtlich der neuen Aufgabe des Verbraucherschutzes im Bereich der Sicherheit in der Informationstechnik. Nach § 7 Absatz 1 Satz 1 Nummer 2 und Absatz 2 Satz 1 BSIG kann das BSI bislang lediglich Produktempfehlungen für IT-Sicherheitsprodukte im Sinne des § 3 Absatz 1 Satz 2 Nummer 3 BSIG (z.B. Virenscanner) aussprechen. Zur Erhöhung der Verbrauchertransparenz wird diese Befugnis allgemein auf informationstechnische Produkte und Dienste im Sinne des § 7 Absatz 1 Satz 1 Nummer 1 Buchstabe a), z.B. Router oder SmartTV, ausgeweitet.

Ferner ist eine Flexibilisierung des Verfahrens enthalten. So wird zukünftig geregelt, dass die Informationspflicht nicht besteht, wenn hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks gefährdet wird oder wenn berechtigter Weise davon ausgegangen werden kann, dass der Hersteller an einer vorherigen Benachrichtigung kein Interesse hat. Dies kann z. B. der Fall sein, wenn die Information durch den Hersteller selbst erfolgt ist. Durch die Einschränkung der Informationspflicht sollen die Aufgaben der Sicherheitsbehörden nicht eingeschränkt werden.

Zu Buchstabe b

Zu Doppelbuchstabe aa

Es handelt sich um Folgeänderungen, durch welche die in § 7 und 7a Absatz 1 und 3 BSIG bestehenden Befugnisse des BSI auf die Erfüllung der in § 3 Absatz 1 Satz 2 Nummer 14a BSIG-E eingefügten Aufgabe des Verbraucherschutzes erweitert werden.

Zu Doppelbuchstabe bb

Nach § 7 Absatz 1 Satz 1 Nummer 2 und Absatz 2 Satz 1 BSIG kann das BSI bislang lediglich Produktempfehlungen für IT-Sicherheitsprodukte im Sinne des § 3 Absatz 1 Satz 2 Nummer 3 BSIG (z.B. Virenscanner) aussprechen. Zur Erhöhung der Verbrauchertransparenz wird diese Befugnis allgemein auf informationstechnische Produkte und Dienste im Sinne des § 7 Absatz 1 Satz 1 Nummer 1 Buchstabe a) BSIG, z.B. Router oder SmartTV, ausgeweitet.

Zu Nummer 100

Zu § 7a

Das BSI kann zur Erfüllung seiner Aufgaben Produkte und Systeme untersuchen. Mit der Änderung in § 7a Absatz 1 BSIG-E wird die Untersuchung von IT-Produkten nicht mehr auf bestimmte Aufgabenbereiche beschränkt. Dies ist insbesondere für die umfassende Auswertung von Informationen über bestehende Sicherheitsrisiken von Bedeutung.

Für Aufgaben, wie die Untersuchung von Sicherheitsrisiken bei der Anwendung der Informationstechnik (§ 3 Absatz 1 Satz 2 Nummer 3 BSIG) oder die eigene Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit in der Informationstechnik (§ 3 Absatz 1 Satz 2 Nummer 4 BSIG) können Untersuchungen der Sicherheit in der Informationstechnik von Bedeutung sein.

Ferner erhält das Bundesamt die Befugnis, von Herstellern die zur Untersuchung notwendigen Auskünfte zu verlangen. § 7a Absatz 1 BSIG dient dazu, Rechtssicherheit für umfassende Untersuchungen von IT-Produkten (zum Beispiel mittels Reverse-Engineering) und IT-Systemen durch das BSI zur Erfüllung seiner Aufgaben – insbesondere auch für den Verbraucherschutz im Bereich der Informationssicherheit – herzustellen. Um sicherzustellen, dass das BSI seine gesetzlichen Aufgaben erfüllen und bspw. mögliche Sicherheitsrisiken bewerten kann, bedarf es der aktiven Mitarbeit der IT-Hersteller durch Bereitstellung von Informationen zu dem zu prüfenden Produkt.

§ 7a Absatz 2 BSIG-E ermöglicht dem Bundesamt, für Untersuchungen nach § 7a Absatz 1 BSIG-E von IT-Herstellern alle notwendigen Auskünfte, insbesondere zu technischen Details, zu verlangen. Das BSI muss regelmäßig Sicherheitsbewertungen durchführen, um den sicheren Einsatz von IT-Produkten und IT-Systemen zu gewährleisten. Daher ist die Befugnis Auskünfte zu verlangen, ein notwendiger Schritt in Richtung mehr Sicherheit in der Informationstechnik.

In vielen anderen Bereichen, in denen die Sicherheit einzelner Erzeugnisse oder Produkte (lebenswichtige) Bedeutung hat sind Auskunftsverlangen oder auskunftsähnliche Verlangen an den Hersteller bereits geregelt (z.B. im Lebensmittel- und Futtermittelgesetzbuch, im Chemikaliengesetz und im Gesetz über die Errichtung einer Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben).

Im Rahmen der zunehmenden Digitalisierung haben die Sicherheit und die Vertrauenswürdigkeit von IT-Systemen, von Hard- und Software eine für den Einzelnen

ebenso große Bedeutung. Es muss sichergestellt sein, dass IT-Produkte nur die herstellerseitig zugesagten Funktionalitäten haben und der Hersteller eingebaute Wartungskanäle, Backdoors etc. offenlegt und unbekannte - sogar dem Hersteller unbekannte - Sicherheitslücken nicht zu einer Gefahr für die IT-Sicherheit werden.

§ 7a Absatz 2 Satz 2 BSIG-E wurde von Artikel 18 Absatz 2 der Verordnung (EG) Nr. 1/2003 des Rates vom 16. Dezember 2002 zur Durchführung der in den Artikeln 81 und 82 des Vertrags niedergelegten Wettbewerbsregeln übernommen. § 7a Absatz 2 Satz 2 BSIG-E konkretisiert die Förmlichkeiten eines Auskunftsverlangens; § 7a Absatz 2 BSIG-E Satz 3 verweist bei Zuwiderhandlungen auf die Bußgeldvorschriften in § 14 BSIG.

§ 7a Absatz 3 BSIG-E (§ 7a Absatz 2 BSIG alt) enthält eine Zweckbindung für die aus der Untersuchung nach § 7a Absatz 1 BSIG-E gewonnenen Erkenntnisse. Diese wurde um die aus den Auskünften erlangten Erkenntnisse erweitert. Soweit erforderlich, ist zudem eine Weitergabe und Veröffentlichung dieser Erkenntnisse durch das BSI zulässig.

Im Zeitalter der Digitalisierung hat die Informationstechnik zunehmend eine zentrale Bedeutung für die Lebensführung. Um diese Entwicklung dauerhaft zu fördern, braucht es hohe Sicherheitsstandards. Die Öffentlichkeit hat ein hohes Interesse daran, zu wissen, welche IT-Produkte und Systeme unsicher sind. Die öffentlichen Warnungen fördern zudem die Wahrnehmung der Öffentlichkeit in Fragen der sicheren Informationstechnik und ermöglichen ein hohes Maß an Transparenz. Des Weiteren hat der Staat auch eine Schutzpflicht gegenüber den Bürgerinnen und Bürgern, indem er diese vor jeglichen Gefahren warnen und schützen muss. Sofern es zu einer Veröffentlichung von Informationen kommen sollte, die Geschäfts- oder Betriebsgeheimnisse beinhalten, ist sicherzustellen, dass diese vertraulichen Informationen unkenntlich gemacht werden. Das BSI kann sich dafür auch der Hilfe des entsprechenden Herstellers bedienen.

Gemäß § 7a Absatz 4 BSIG-E ist dem Hersteller zuvor die Gelegenheit zur Stellungnahme zu geben. Wenn der Hersteller in diesem Rahmen - etwa bei einer festgestellten Sicherheitslücke - selbst an die Öffentlichkeit geht oder sonst Abhilfe schafft, unterbleibt die zusätzliche Veröffentlichung der Erkenntnisse durch das BSI.

§ 7a Absatz 5 BSIG-E ermöglicht dem BSI, für den Fall, dass der Hersteller die Auskunft verweigert oder der Aufforderung nicht hinreichend nachkommt, , die Öffentlichkeit über die Vorgehensweise des IT-Herstellers zu informieren. Hierdurch soll gewährleistet werden, dass die Hersteller dem Auskunftsverlangen nachkommen. Diese Möglichkeit ist zur effektiven Umsetzung erforderlich, da die Verhängung einer Ordnungswidrigkeit nach Absatz 2 nicht ausreichend sein kann. Dem Hersteller ist auch hier zuvor die Gelegenheit zu einer Stellungnahme einzuräumen.

Zu Nummer 11

Zu § 7b

Mit § 7b Absatz 1 BSIG-E wird die Befugnis zur Durchführung von Maßnahmen zur Detektion und Auswertung von Schadprogrammen, Sicherheitslücken und anderen Sicherheitsrisiken geschaffen. Das Bundesamt darf diese Maßnahmen zum Schutz der Bundesverwaltung, der Verbraucher und der Betreiber Kritischer Infrastrukturen anwenden, um den Verantwortlichen oder hilfsweise den mit dem Betrieb beauftragten Dritten des jeweiligen Netzes oder Systems über eine bestehende Gefahr zu informieren. Es darf diese Befugnis ausüben, sofern Systeme ungeschützt sind und Tatsachen die Annahme rechtfertigen, dass die Sicherheit oder Funktionsfähigkeit der Systeme gefährdet ist.

Das Bundesamt soll insbesondere sog. „Portscans“, ohne weiteren Zugriff auf das informationstechnische System zu nehmen, durchführen. Des Weiteren ist das Bundesamt

befugt, „Sinkholes“ und „Honeypots“ zu betreiben. Die Befugnis umfasst somit weder das Ausspähen noch das Eindringen in IT-Systeme. Dies gilt auch für Absatz 4.

Die Befugnis ist erforderlich, weil das Bundesamt gemäß § 3 Absatz 1 Satz 2 Nummer 2 BSIG den Auftrag zur Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen und Zurverfügungstellung der gewonnenen Erkenntnisse für andere Stellen hat. Soweit dies zur Erfüllung ihrer Aufgaben sowie für Dritte und zur Wahrung ihrer Sicherheitsinteressen erforderlich ist. Zudem hat das Bundesamt gem. § 3 Absatz 1 Satz 2 Nummer 14 BSIG die Aufgabe, Stellen des Bundes, der Länder sowie Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherungsvorkehrungen zu warnen. Hierfür muss das Bundesamt in der Lage sein, aktiv Sicherheitsrisiken erheben und analysieren zu können.

Die Maßnahmen dürfen ausschließlich mit dem Ziel durchgeführt werden, die Verantwortlichen oder betreibenden Dienstleister des jeweiligen Netzes oder Systems über eine bestehende Gefahr zu informieren.

Bei vielen IT-Systemen besteht die Möglichkeit eines Zugriffs via Netzwerk (z. B. Internet). Dazu gehören beispielsweise Industrial Control Systems (ICS-Geräte) oder Internet of Things-Systemen (IoT-Geräte), die offene Dienste (Ports) und diverse andere Schwachstellen aufweisen können. Viele Betreiber von vernetzten IT-Systemen sind sich der Gefahren nicht bewusst, die von offenen Ports und anderen bekannten Schwachstellen ihrer IT-Systeme ausgehen. Mit der Befugnis ist es dem Bundesamt möglich, offene Ports und andere bekannten Schwachstellen durch gezielte automatisierte Such-Routinen (Scans) schnell zu detektieren, und diese an Betroffene aus Staat und Wirtschaft weiterzugeben. Vor dem Hintergrund der technischen Entwicklung ist die Information der Betroffenen zu potentiellen Schwachstellen ein zentraler Baustein heutiger IT-Sicherheit.

Der Betrieb sog. Sinkhole-Server ist eine effektive Maßnahme zur Bekämpfung von Botnetzen.

Mittels eines Sinkholes werden an ein Zielsystem gerichtete Daten zum einen umgeleitet und zum anderen zu Auswertungszwecken gespeichert. Dies versetzt den Sinkhole-Betreiber in die Lage, die Kommunikation zwischen sog. Bots und dem Command- and-Control-Server (C&C-Server) zu unterbinden. Je nachdem, ob Kennungen für C&C-Server oder Bots verwendet werden, wird jeweils eine der Kommunikationsrichtungen unterbunden und der Datenverkehr erhoben.

Durch die Umleitung der Kommunikation wird der Betrieb des Botnetzes in wesentlichen Teilen unterbunden. Zugleich ermöglicht die Auswertung der gespeicherten Kommunikation die Analyse der Funktionsweise des Botnetzes. Damit wird das Bundesamt in die Lage versetzt zielgerichtet Hinweise zu geben, wie ein Botnetz u.a. deinstalliert werden kann. Für die Anordnung nach § 109a Absatz 8 Nummer 2 TKG sind diese Hinweise von zentraler Bedeutung, um dem Diensteanbieter nach TKG bei seiner Verpflichtung zur Bereinigung betroffener Datenverarbeitungssysteme von einem konkret benannten Schadprogramm zu unterstützen.

§ 7b Absatz 2 BSIG-E definiert den in Absatz 1 verwenden Begriff „ungeschützt“ und greift als Anknüpfungspunkt die Legaldefinition von „Sicherheitslücken“ (§ 2 Absatz 6 BSIG) auf. Die Definition erfasst sowohl Kommunikationsnetze als auch informationstechnische Systeme, die vollständig ohne Schutzmechanismen arbeiten. Daneben werden von der Definition auch die Kommunikationsnetze und informationstechnische Systeme erfasst, die zwar Schutzmechanismen verwenden, die aber faktisch wirkungslos sind.

Dies ist zum einen der Fall, wenn das Netz oder System bzw. der jeweils zum Schutz verwendete Mechanismus eine bereits bekannte Sicherheitslücke besitztoder in

Kommunikationsnetzen und informationstechnischen Systemen, deren Schutzmechanismen wirkungslos sind. Dies wäre zum Beispiel dann der Fall, wenn für ein System werkseitig stets ein identisches Passwort („0000“ oder „admin“) vergeben würde oder wenn die werksseitige Vergabe der Passwörter nach einer öffentlich bekannten und einfachen Systematik erfolgte.

§ 7b Absatz 3 BSIG-E regelt die Informationspflichten des Bundesamtes. Dies korrespondiert mit der Anordnungsbefugnis gegenüber Diensteanbietern zu Maßnahmen nach § 109a Absatz 4 TKG.

In § 7b Absatz 4 BSIG-E wird die Befugnis zum Einsatz sog. „aktiver Honeypots“ geschaffen. Bei einem Honeypot handelt es sich um ein informationstechnisches System, das vom Bundesamt in öffentlichen Netzen betrieben wird und bewusst Schwachstellen aufweist. Wird dieses System von einer Schadsoftware infiziert, ist es dem Bundesamt durch Analyse des Systems möglich, insbesondere Art, Funktionsweise und Infektionsweg nachzuvollziehen. Diese Erkenntnis kann wiederum genutzt werden, um Nutzer informationstechnischer Systeme im Rahmen der gesetzlichen Aufgaben des Bundesamtes zu warnen oder Systeme Kritischer Infrastrukturen oder des Bundes geeignet zu schützen.

Der Analyse von Schadsoftware mittels Honeypots kommt durch die Verbreitung von IoT-Geräten eine zunehmende Bedeutung zu, insbesondere, weil IoT-Geräte ihre eigentliche Funktion beibehalten und dennoch von Schadsoftware infiziert sein können. Für die Nutzenden gestaltet es sich somit häufig schwierig, infizierte IoT-Geräte zu erkennen. Durch die aktive Analyse des Bundesamtes mittel Honeypots kann das erforderliche Wissen generiert und den Nutzenden zur Abwehr der Gefahren von ihren informationstechnischen Systemen zur Verfügung gestellt werden, so dass diese in die Lage versetzt werden, die Systeme in einen ordnungsgemäßen Zustand zu versetzen.

Zu § 7c

Das Bundesamt kann das Bundeskriminalamt zur frühen Erkennung von Gefahren für die in § 6 BKAG betroffenen Personen unterstützen. § 3 Absatz 13 Buchstabe a BSIG eröffnet diese Möglichkeit bereits, so dass § 7c BSIG-E der Klarstellung dient, dass das BSI auch mit den Maßnahmen nach § 7b BSIG-E unterstützen kann.

Zu Nummer 12

Zu Buchstabe a

Durch die Änderungen des § 8 Absatz 1 BSIG werden die Verbindlichkeit der Mindeststandards und der Adressatenkreis erweitert. Neben den Stellen des Bundes sollen die Mindeststandards zukünftig ausdrücklich auch für IT-Dienstleister gelten, soweit sie IT-Dienstleistungen für die Kommunikationstechnik des Bundes erbringen. Eine solche Erweiterung ist erforderlich, um sicherzustellen, dass ein gleich hohes IT-Sicherheitsniveau bei jeder Einrichtung des Bundes – unabhängig von der Organisationsform des IT-Dienstleisters – erreicht wird. Abweichungen von den Mindeststandards sind zugunsten eines einheitlichen Sicherheitsniveaus nur in sachlich begründeten Einzelfällen zulässig.

Daneben werden Kontrollrechte des Bundesamtes eingeführt, die für die Einhaltung eines hohen IT-Sicherheitsstandards zwingend erforderlich sind. Für die Durchführung der Kontrollen obliegt die Fachaufsicht dem Bundesministerium des Innern, für Bau und Heimat. Die Kontrollrechte dienen der Prüfung, ob die Mindeststandards und damit die Voraussetzungen für ein einheitliches IT-Sicherheitsniveau eingehalten werden.

Der Bedrohungslage kann nur begegnet werden, wenn in der gesamten Bundesverwaltung durch die Einhaltung der Mindeststandards ein einheitliches Schutzniveau hergestellt und

damit eine wirksame Prävention erreicht wird. Vergangene Cyber-Sicherheitsvorfälle zeigen, dass trotz der Vorgaben des Umsetzungsplans Bund 2017, nach dem die Einhaltung der Mindeststandards bereits ressortübergreifend verpflichtend geregelt ist, es einer gesetzlichen Regelung im Hinblick auf alle Stellen sowie der öffentlichen Unternehmen des Bundes bedarf, um die Mindeststandards innerhalb der Bundesverwaltung umzusetzen.

Auch soll diese Regelung sicherstellen, dass die Sicherheit der Kommunikationstechnik des Bundes unabhängig von der Organisationsform eines Dritten gewährleistet wird, insbesondere dann, wenn für weitere Stellen Schnittstellen zur Kommunikationstechnik des Bundes eingerichtet werden (bspw. zu internationalen Einrichtungen). Sofern Schnittstellen zu Dritten bestehen, kann die Einhaltung der Mindeststandards für die Schnittstellenseite beim Dritten nur im Einvernehmen mit diesem kontrolliert werden.

Zu Buchstabe bb

Gemäß § 3 Absatz 1 Satz 2 Nummer 1 BSIG gehört es zu den Aufgaben des BSI, IT-Sicherheitsprodukte für Stellen des Bundes zu entwickeln. Hierauf nimmt § 8 Absatz 3 Satz 1 BSIG-E Bezug, so dass analog dazu im Folgenden Satz 4 „Bundesbehörden“ durch „Stellen des Bundes“ ersetzt wird.

Die Ergänzung, dass die IT-Sicherheitsprodukte auch von entsprechend beauftragten Dritten für die Stellen des Bundes abgerufen werden können, regelt nun explizit, dass auch Dienstleister, die die IT der abrufberechtigten Körperschaft betreiben, für ihren Auftraggeber auf die IT-Sicherheitsprodukte des BSI zugreifen können.

Zu Buchstabe cc

Als Cyber-Sicherheitsbehörde ist das BSI zuständig für die Informationssicherheit auf nationaler Ebene (vgl. § 1 BSIG). In dieser Funktion gewährleistet das Bundesamt nicht nur die Sicherheit der Informationstechnik der Bundesverwaltung, sondern ist auch Ansprechpartner für wesentliche Digitalisierungsmaßnahmen.

Um sicherzustellen, dass die Belange der Cyber- und Informationssicherheit ausreichend und umfassend berücksichtigt werden, ist das BSI bei der Planung und Umsetzung von Digitalisierungsvorhaben von der jeweils zuständigen Stelle des Bundes stets frühzeitig zu beteiligen. Dem BSI ist insoweit die Gelegenheit zur Stellungnahme einzuräumen. Der Begriff „Digitalisierungsvorhaben“ soll in diesem Zusammenhang weit verstanden werden.

Zu Nummer 13

Zu Buchstabe a

Die Ergänzung des Absatzes konkretisiert die Verpflichtung der Betreiber Kritischer Infrastrukturen, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Diese Pflicht umfasst nun auch ausdrücklich den Einsatz von Systemen zur Angriffserkennung und gibt den Unternehmen Rechtssicherheit. Diese Systeme stellen eine effektive Maßnahme zur Begegnung von Cyber-Angriffen dar.

Wie in § 3a gilt die sich aus der DSGVO ergebene Verpflichtung zur unverzüglichen Löschung von Daten, sobald diese für die Aufgabenerfüllung nicht mehr erforderlich sind (Artikel 5 und 6 DSGVO). Die in der Regelung enthaltene unverzügliche Löschverpflichtung ist daher deklaratorisch.

Zu Buchstabe b

Für kritische Komponenten sind neben der technischen Qualität der Produkte gleichsam auch die Organisationsstruktur und mögliche – den Schutzzielen dieses Gesetzes widersprechende – rechtlichen Verpflichtungen des Herstellers relevant. Neben technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse, muss durch die Betreiber der Kritischen Infrastrukturen daher auch eine Erklärung des Herstellers eingeholt werden, dass dieser in der Lage ist, die gesetzlich geforderten Bestimmungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme selbst einzuhalten. Dies ist der Tatsache geschuldet, dass mit zunehmender informationstechnischer Komplexität der eingesetzten kritischen Komponenten ein wesentlicher Teil der Beherrschbarkeit der Technologie im Rahmen der Produktpflege (Softwareupdates, Firmware-Updates) beim Hersteller selbst oder auch der weiteren Lieferkette verbleibt. Die Erklärung des Herstellers entfaltet dabei unmittelbare Wirkung nur zwischen den Parteien, ist also als privatrechtliche Erklärung zu werten.

Zu Nummer 144

Zu Buchstabe a und b

Die Änderung ist erforderlich wegen der Erweiterung des Anwendungsbereichs auf weitere Unternehmen im besonderen öffentlichen Interesse.

Zu Buchstabe a

Im Falle der Krisenbewältigung zielt eine aufzubauende Kommunikationsinfrastruktur weniger auf den Schutz der IT-Sicherheit der Kritischen Infrastrukturen, sondern auf die Aufrechterhaltung oder Wiederherstellung der IT-Systeme nach einer krisenhaften Störung oder Beeinträchtigung. Daher wird geregelt, dass Betreiber Kritischer Infrastrukturen Zugang zu einem einheitlichen Krisenkommunikationssystem erhalten, welches eine geeignete Kommunikationsinfrastruktur zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung ermöglicht. Dies gilt durch die in § 8f BSIG-E enthaltene Verweisung entsprechend auch für die Betreiber weiterer Anlagen im besonderen öffentlichen Interesse.

Zu Buchstabe b

Die Regelung ist erforderlich, weil das BSIG bisher keine unmittelbare Pflicht zur Registrierung einer Kritischen Infrastruktur umfasst. Vielmehr besteht die Pflicht zur Registrierung einer Kontaktstelle für die Kritische Infrastruktur. Im auszufüllenden Formular sind dann anlagenspezifische Informationen zur jeweiligen Kritischen Infrastruktur anzugeben. Aus Gründen der Rechtssicherheit für die Registrierung als Kardinalpflicht des Betreibers wird neben der Pflicht zur Registrierung einer Kontaktstelle eine Pflicht zur Registrierung einer Kritischen Infrastruktur unmittelbar verankert werden.

Zu Buchstabe c

§ 8 b Absatz 3a BSIG-E regelt die Befugnis des Bundesamtes, die Herausgabe der für eine Bewertung erforderlichen Unterlagen zu verlangen. Das BSI-Gesetz beinhaltet derzeit keine eigenständige Rechtsgrundlage, um von Betreibern Kritischer Infrastrukturen Auskünfte zu Kennzahlen bezüglich der jeweiligen Schwellwerte zu verlangen. Das BSI ist unterhalb eines Ordnungswidrigkeitsverfahrens daher auf die Mitwirkung der KRITIS-Betreiber angewiesen und muss deren Bewertungsergebnisse akzeptieren. Daraus können Probleme resultieren, wenn Betreiber Anlagen nicht registrieren, obwohl diese Kritische Infrastrukturen nach § 2 Absatz 10 i. V. m. der BSI-KritisV sind oder Angaben unvollständig oder erläuterungsbedürftig sind.

Das Bundesamt erhält daher die Befugnis zur Abfrage von schwellwertrelevanten Kennzahlen der Betreiber. Betreiber werden verpflichtet, dem Auskunftsersuchen unverzüglich nachzukommen. Zudem kann das Bundesamt nach abgeschlossener Bewertung die Anlage im Wege der Ersatzvornahme registrieren, wenn der Betreiber seiner Pflicht nicht nachkommt.

Ferner wird ausdrücklich der Fall geregelt, dass das BSI die Registrierung des Betreibers aufgrund tatsächlicher oder rechtlicher Gründe ablehnt. Nur hierdurch kann sichergestellt werden, dass nur diejenigen Unternehmen den Pflichten nach § 8a und 8b unterliegen, die auch tatsächlich Betreiber Kritischer Infrastrukturen sind.

Zu Buchstabe f

Die neuen Absätze 4a und 4b in § 8b BSIG-E regeln in Anlehnung an § 8b Absatz 4 BSIG die Anwendung der Meldepflichten auf die Unternehmen im besonderen öffentlichen Interesse. Abweichend von § 8b Absatz 4 BSIG sind sowohl Störungen, die zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung als auch zu einer erheblichen Gefahr für die öffentliche Sicherheit und Ordnung führen können, zu melden. Die Regelung wurde abweichend formuliert, weil die bestehende Regelung für die Kritischen Infrastrukturen nicht unmittelbar auf die genannten Bereiche übertragbar ist, weil es sich bei den Unternehmen nicht in jedem Fall um Infrastrukturen handelt.

Zu Nummer 15

Der vorherige Verweis war fehlerhaft und wurde durch die Neufassung korrigiert.

Zu Nummer 156

Es handelt sich um eine Folgeanpassung.

Zu Nummer 157

Es handelt sich um eine Folgeanpassung.

Zu Nummer 18

Zu § 8f

§ 8f BSIG-E regelt die Ausweitung der Pflichten nach §§ 8a und 8b auf weitere Teile der Wirtschaft. Bislang gelten diese Pflichten nur für Betreiber Kritischer Infrastrukturen. Neben Betreibern Kritischer Infrastrukturen gibt es weitere Wirtschaftsbereiche, die für die Gesellschaft von besonderem öffentlichem Interesse sind, weil ihr Ausfall oder ihre Beeinträchtigung zu erheblichen volkswirtschaftlichen Schäden, zu einer Gefährdung für die öffentliche Sicherheit und Ordnung oder zu einer Beeinträchtigung der wesentlichen Sicherheitsinteressen der Bundesrepublik Deutschland führen können. Eine Rechtsverordnung nach § 10 Absatz 5 BSIG wird näher konkretisieren, welche Unternehmen aufgrund ihrer volkswirtschaftlichen Bedeutung und insbesondere ihrer erbrachten Wertschöpfung von besonderem öffentlichem Interesse im Sinne dieses Gesetzes sind. Die Pflichten gelten für die Unternehmen in diesem Bereich, wie auch im Falle der Betreiber Kritischer Infrastrukturen, zwei Jahre nach Inkrafttreten der Verordnung.

Zu Nummer 19

zu § 9a

Absatz 1

Das Bundesamt hat nach § 7 Absatz 1 Nummer 1a i.V.m. § 3 Absatz 1 Satz 2 Nummer 14 BSIG die Aufgabe, Anwender von Produkten im Bereich der Sicherheit der Informationstechnik zu warnen und zu beraten. Dieser Auftrag soll gemäß dem Koalitionsvertrag der 19. Legislaturperiode (Ziffer 1987-1997) und dem Auftrag des Bundestages vom März 2017 (BT-Drucksache 18/11808) im Sinne eines einheitlichen „IT-Gütesiegels“ konkretisiert und umgesetzt werden. Das „IT-Gütesiegel“ wird im Rahmen der Neuregelung des § 9a BSIG als einheitliches IT-Sicherheitskennzeichen umgesetzt. Das IT-Sicherheitskennzeichen (zum Begriff sogleich) wird es ermöglichen, die IT-Sicherheit von verschiedenen Verbraucherprodukten oder auch Dienstleistungen im IT-Bereich verständlich, transparent, einheitlich und aktuell darzustellen. Es besteht zu diesem Zweck aus zwei Komponenten: Der Herstellererklärung und einer dynamischen BSI-Sicherheitsinformation zum Produkt. Die hybride Ausgestaltung bedeutet, dass neben der reinen Herstellererklärung gegen eine technische Vorschrift (bspw. eine TR) gleichsam eine weiterführende Information gegenüber dem Verbraucher über einen Verweis (QR Code, Link) erfolgt, welchen dieser bei Kauf unmittelbar abrufen kann. Über den Verweis werden auf einer Produktinformationsseite die weiterführenden Sicherheitsinformationen dargestellt (sog. „elektronischer Beipackzettel“). Der Begriff des Gütesiegels wird auf Grund der rechtlichen und tatsächlichen Ausgestaltung des IT-Sicherheitskennzeichens nicht mehr verwendet. Ein „Gütesiegel“ setzt voraus, dass eine unabhängige Stelle die objektiven Kriterien einer Aussage - hier der IT-Sicherheitseigenschaften - vorab prüft und darauf basierend ein „Siegel“ vergibt. Eine Selbstauskunft und eine Herstellererklärung - worauf das IT-Sicherheitskennzeichen basiert - genügt der Erwartung der angesprochenen Verkehrskreise an die objektive Prüfung der für die Vergabe erforderlichen Kriterien nicht (vgl. OLG Köln Beschl. v. 5.3.2018 – 6 U 151/17, BeckRS 2018, 4892, beck-online).

Aufbauend auf den gesetzten Zielen und den rechtlichen Rahmenbedingungen kann das IT-Sicherheitskennzeichen nicht den klassischen Ansatz eines Gütesiegels abbilden. Ein solches wäre ein einfaches Siegel, welches auf dem Produkt den Hinweis darstellt, dass eine bestimmte Sicherheit des Produktes gegeben ist. Die Schwierigkeit läge bei dieser klassischen Ausgestaltung darin, dass – unabhängig von der letztlichen Ausgestaltung – nur eine Momentaufnahme gegeben wäre. Eine solche Momentaufnahme ist nicht geeignet, die IT-Sicherheit im Verbraucherbereich nachhaltig abzubilden. Daneben sind die Informationen, welche auf einem einfachen Siegel dargestellt werden können, begrenzt. Der Verbraucher müsste sich schlicht auf die im Siegel verkörperten statischen Informationen verlassen. Das Ziel der substantiierten Verbraucherinformation könnte kaum erreicht werden. Auch besteht wie dargestellt die Gefahr, dass die Glaubwürdigkeit und das Vertrauen in das Siegel bei nachträglich auftretenden und durch den Hersteller nicht behobenen Sicherheitslücken stark beeinträchtigt würden. Ein statisches Siegel ist nicht geeignet, die genannten Zielvorgaben aus dem Koalitionsvertrag zu erfüllen.

Eine verpflichtende Einführung eines IT-Sicherheitskennzeichens ist auf nationaler Ebene nicht möglich. Der Marktzugang von Produkten ist in der EU vollharmonisiert. Jede verpflichtende und rein nationale Regelung würde gegen geltendes Recht verstoßen. Entsprechend wird die Freiwilligkeit ausdrücklich festgeschrieben. Anreiz zur Nutzung seitens der Hersteller soll allein die Darstellung der IT-Sicherheit der Produkte sein, wodurch eine Abgrenzung zu weniger sichereren Produkten erfolgen kann.

Die Einführung des IT-Sicherheitskennzeichens erfolgt schrittweise für verschiedene Produktkategorien. Die Auswahl der relevanten Produktkategorien im Verbraucherbereich obliegt dem Ermessen des BSI. Die Produktkategorien werden in der Rechtsverordnung nach § 10 Absatz 3 aufgeführt.

zu Absatz 2

Das IT-Sicherheitskennzeichen setzt sich zur Verwirklichung des Zwecks des Absatzes 1 aus zwei Komponenten zusammen, der Herstellererklärung und den BSI-Sicherheitsinformationen. Die Herstellererklärung – ein gängiges Instrument im

Produkthaftungsrecht – obliegt allein der Sphäre des Herstellers, d.h. nur dieser ist für deren Wahrheitsgehalt verantwortlich und haftbar. In dieser Erklärung drückt der Hersteller aus, dass die in den zu Grunde liegenden IT-Sicherheitseigenschaften festgelegten IT-Sicherheitsvorgaben im konkreten Produkt erfüllt sind. Die IT-Sicherheitseigenschaften, welche zur Abgabe einer Aussage über die IT-Sicherheit Grundvoraussetzung sind, können sich entweder aus einer Technischen Richtlinie des BSI ergeben oder aus branchenabgestimmten IT-Sicherheitsvorgaben, soweit das BSI diese für geeignet hält, die notwendigen IT-Sicherheitsanforderungen der Produktkategorie abzubilden. Details zum Verfahren werden in der Rechtsverordnung nach § 10 Absatz 3 geregelt.

zu Absatz 3

Die Vergabe des IT-Sicherheitskennzeichens wird in Absatz 3 nur grundlegend geregelt. Die genauen Verfahrensschritte und die konkreten Fristen sind abhängig von der Produktkategorie. Die einzuhaltenden IT-Sicherheitseigenschaften für das jeweilige Produkt werden durch die zugrundeliegende Technische Richtlinie bzw. branchenabgestimmte Sicherheitseigenschaften bestimmt. Näheres regelt die Rechtsverordnung.

zu Absatz 4

Das IT-Sicherheitskennzeichen kann nur dann die gewünschte Wirkung im Rahmen der Kaufentscheidung entfalten, wenn dieses körperlich mit dem Produkt oder dessen Umverpackung verbunden wird. Wichtig ist gerade die Sichtbarkeit für den Verbraucher. Da ein Großteil der Käufe auch über Fernabsatzmodelle erfolgt, ist das IT-Sicherheitskennzeichen auch auf elektronischem Weg nutzbar. Herstellererklärung und die BSI-Sicherheitsinformation bilden gemeinsam einen „elektronischen Beipackzettel“, welcher auf einer Webseite des BSI abrufbar gemacht wird. Das genaue Verfahren und die Inhalte der Herstellererklärung werden in der Rechtsverordnung nach § 10 Absatz 2a festgelegt. Die Herstellererklärung muss die für den Verbraucher relevanten Produktinformationen enthalten, um eine Vergleichbarkeit zu ermöglichen.

zu Absatz 5

Die Nutzung des IT-Sicherheitskennzeichens zu Werbezwecken ist ausdrücklich erlaubt und erwünscht. Die Sichtbarkeit für die Verbraucher ist wesentliche Voraussetzung für die informierte Kaufentscheidung.

Absatz 6 und Absatz 7

Das BSI erhält die Möglichkeit (nicht die Pflicht), die Aussagen des IT-Sicherheitskennzeichens, mithin die Herstellererklärung, sowie die sonstigen möglichen Sicherheitslücken in regelmäßigen Abständen oder auch anlassbezogen zu prüfen. Dieses Recht ist notwendig, um die Validität des IT-Sicherheitskennzeichens aufrechterhalten zu können.

Wenn und soweit bei dieser Prüfung Missstände auffallen, kann das BSI diese auch im Rahmen der BSISicherheitsinformationen zum Produkt einblenden, so dass diese auf dem elektronischen Beipackzettel sichtbar werden. In Ausübung des pflichtgemäßen Ermessens kann das BSI alternativ auch die weitere Nutzung des IT-Sicherheitskennzeichens untersagen und das Recht zur Nutzung widerrufen.

zu § 9b

Auf Grund der hohen Virtualisierung der 5G-Netze und der zu erwartenden stetigen Software-/Firmware-Updates kritischer Komponenten und Dienste bieten weder eine Komponentenzertifizierung, noch eine Überprüfung von Sicherheitskonzepten eine

100%ige Sicherheit dahingehend, dass die Hersteller keine missbräuchlichen Zugriffmöglichkeiten auf Hard- und Software implementieren, die Sabotage oder Spionage ermöglichen. Geeignete technische Maßnahmen können derartige Risiken zwar minimieren bzw. in den möglichen Auswirkungen abschwächen. Die letztlich im Raum stehende Frage der Vertrauenswürdigkeit von Herstellern und Dienstleistern – in diesem Sinne – kann hierdurch jedoch nicht abschließend geklärt werden. Eine Produktzertifizierung beispielsweise bestätigt im Rahmen einer Typprüfung nur, dass eine Produktversion bestimmte funktionale und Sicherheitseigenschaften erfüllt, die in Schutzprofilen, Sicherheitsvorgaben oder Technischen Richtlinien spezifiziert sind.

Um sicherzustellen, dass die Aussagen der Vertrauenswürdigkeitserklärung eingehalten werden bzw. werden können, ist es notwendig, diese in einem geeigneten Verfahren einer angemessenen Prüfung und Bewertung zu unterziehen. Dies kann nicht im Rahmen einer nur technischen Zertifizierung erfolgen. Darüber hinaus werden Zertifizierungen im Cyberbereich zukünftig einer erweiterten europäischen Harmonisierung unterliegen.

Das Verfahren nach § 9b BSIG-E steht auch im Einklang mit der EU-Risikobewertung zu 5G, die deutlich herausstellt, dass neben einer auf europäischer Ebene abzustimmenden sogenannten Toolbox (z.B. mit gemeinsamen Standards für die Zertifizierung) weitere individuelle Maßnahmen in den einzelnen Mitgliedstaaten wegen entgegenstehender Sicherheitsinteressen des Mitgliedstaates zu ergreifen sind. Dies ist auch erforderlich – und daher muss eine nationale Regelung an den expliziten Zuständigkeiten der Mitgliedstaaten für die nationale Sicherheit angeknüpft sein–, um eine Abgrenzung zum vergemeinschafteten Recht und damit ein eigenständiges Handeln der Mitgliedstaaten zu ermöglichen.

Die Abgrenzung durch nationale Sicherheitsinteressen bedingt gleichzeitig ein diesbezügliches Prüfrecht (im Sinne des Verwaltungsverfahrensrechts), das einer Untersagung im Einzelfall vorausgehen muss und gleichzeitig die Rechtsgrundlage für zu ergreifende Rechtsmittel (z.B. für einen öffentlich-rechtlichen Vertrag zur Mitigation identifizierter Risiken oder aber auch – als ultima ratio – für eine Untersagung) schafft.

Darüber hinaus wären aufgrund der europäischen Cybersicherheitsgesetzgebung („Cybersecurity Act (CSA)") Zertifikate in der EU gegenseitig anzuerkennen. Ein Sicherheitszertifikat einer 5G-Komponente oder eines -Dienstes unter dem CSA aus einem Mitgliedstaat würde damit grundsätzlich die Vorgaben einer nationalen gesetzlichen Zertifizierungspflicht erfüllen. Durch ein von der Zertifizierung unabhängiges Verfahren zur Prüfung der Vertrauenswürdigkeit kann dem Risiko begegnet werden, dass nicht vertrauenswürdige Hersteller unter dem Cybersecurity Act Zertifikate in anderen Mitgliedstaaten der EU erhalten, die ohne weiteres unter spezialgesetzlichen Zertifizierungserfordernissen (wie im TKG für kritische Komponenten vorgesehen) anzuerkennen wären.

Vor diesem Hintergrund ist die Prüfung und Bewertung der Einhaltung der Vertrauenswürdigkeitserklärung der Hersteller bzw. Dienstleister nicht allein im Rahmen der Zertifizierung selbst durchzuführen. Durch die systematische Trennung der Prüfung der technischen Sicherheitsanforderungen (z.B. Einhaltung des Sicherheitskataloges nach § 109 Abs. 6 TKG) von der Schaffung eines Verfahrens zur Prüfung der Einhaltung der Aussagen der Vertrauenswürdigkeitserklärung – auch im laufenden Betrieb – wird gewährleistet, dass die Sicherheitsaussagen der technischen Zertifizierung und Evaluierung systematisch nicht mit einer Bewertung der Vertrauenswürdigkeit vermischt werden.

Die Anzeige hat durch den Betreiber zu erfolgen, da nur dieser beurteilen kann, ob die Komponente im Kontext des Einsatzes als kritisch zu bewerten ist (zum Beispiel aufgrund des Schutzbedarfes bestimmter Teile eines Kommunikationsnetzes nach TKG). Die

Anzeigepflicht besteht auch unabhängig von eventuellen Übergangsfristen, welche für das Vorlegen von Sicherheitszertifikaten bestehen.

Der Untersagung des Einsatzes einer kritischen Komponente muss zugrunde liegen, dass das entsprechende Produkt Funktionen (z.B. Schwachstellen oder sogenannte „Hintertüren“) enthält, die missbräuchlich Verwendung finden können. Die Untersagung kann auch erfolgen, wenn der Hersteller gegen Verpflichtungen (zum Beispiel die missbräuchliche Weitergabe von Daten an Dritte) aus der Vertrauenswürdigkeitserklärung verstößt oder bestimmten Zusicherungen nicht nachkommt (z.B. Nachweise zu vertrauenswürdigem Personal).

Die erfolgte Untersagung des Einsatzes einer kritischen Komponente eines Herstellers kann zur Untersagung des Einsatzes anderer kritischer Komponenten desselben Typs desselben Herstellers oder bei einem wiederholten Verstoß auch zu Untersagungen weiterer kritischer Komponenten dieses Herstellers – ggf..auch in Kritischen Infrastrukturen anderer Betreiber – führen.

Zu Nummer 1920

Zu Buchstabe a

Die Verordnungsermächtigung ist notwendig, um das Verwaltungsverfahren zur Vergabe und die genauen Inhalte des IT-Sicherheitskennzeichens im Detail abbilden zu können. Die Regelungen sind auf Ebene einer Verordnung notwendig, um die verschiedenen Produktkategorien schrittweise rechtssicher zur Nutzung des IT-Sicherheitskennzeichens einführen zu können. Daneben werden in der Verordnung die Details der Ausgestaltung (grafische Darstellung, Aufbau des elektronischen Beipackzettels usw.) festgelegt.

Zu Buchstabe b

Die Regelung ist dem Absatz 1 nachgebildet und ermächtigt das Bundesministerium des Innern, für Bau und Heimat zum Erlass einer Rechtsverordnung, durch welche konkretisiert wird, bei welchen Anlagen oder Teile davon ein besonderes öffentliches Interesse im Sinne des § 2 Absatz 14 Nummer 2 und 3 besteht. Bei der Bestimmung der Anlagen oder Teile davon ist die Systematik zur Bestimmung Kritischer Infrastrukturen nach § 10 Absatz 1 i. V. m. der BSI-KritisV entsprechend anzuwenden im Sinne von qualitativen und quantitativen Kriterien.

Zu Nummer 201

Durch diese Änderung wird dem Zitiergebot des Artikels 19 Absatz 1 Satz 2 GG Genüge getan und ins bisherige Gefüge des § 11 BSIG eingefügt.

Zu Nummer 22

Der Katalog der Bußgeldvorschriften wurde insgesamt überarbeitet. Dies umfasst eine Systematisierung und Ergänzung der Bußgeldtatbestände sowie die Erhöhung von Bußgeldern selbst.

Die bisherigen Sanktionen haben nur einen Teil der Pflichten aus den §§ 8a ff. BSIG abgedeckt. Es war daher erforderlich, zur besseren Durchsetzung insbesondere von Auskunfts- und Nachweispflichten den Katalog der Tatbestände zu präzisieren und zu erweitern. Außerdem wird Wertungswidersprüchen der Bußgeldhöhen zu Verstößen gegen die DSGVO begegnet.

Zu Absatz 1

Die neue Nummer 1 ermöglicht es, ein Bußgeld für den Fall zu verhängen, dass Hersteller eines informationstechnischen Systems, entgegen dem Verlangen des Bundesamtes, nicht oder in unzureichender Form an der Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen Systems mitwirken.

Die Mitwirkung der Hersteller ist in vielen Fällen bei Störungen und Ausfall von komplexen IT-Systemen von Kritischen Infrastrukturen von erheblicher Bedeutung für eine schnelle Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen Systems, da in der Regel nur bei den Herstellern der vollständige Zugang zur Dokumentation von Hard- und Softwarekomponenten vorhanden ist.

Vor dem Hintergrund, dass durch Störung oder Ausfall des Systems eine Vielzahl von Bürgerinnen und Bürger in erheblicher Weise betroffen sein wird, ist die Androhung eines Bußgeldes zur Unterstützung der BSI Aufforderung zur Herstellermitwirkung angemessen.

Mit § 14 Absatz 1 Nummer 2 BSIG-E wird der Fall einer Zuwiderhandlung gegen eine vollziehbare Anordnung erfasst.

Mit § 14 Absatz 1 Nummer 3 BSIG-E wird die Pflicht der Hersteller zur Auskunftserteilung aus § 7 Absatz 2 Satz 1 BSIG sanktioniert. Da das BSI regelmäßig auf Auskünfte der Hersteller angewiesen ist, ist zur Durchsetzung des Auskunftsrechts eine Sanktionsmöglichkeit erforderlich.

Die neue Nummer 5 des § 14 Absatz 1 BSIG-E ermöglicht es, ein Bußgeld für den Fall zu verhängen, dass Auskünfte und Dokumente zu Kennzahlen nicht vorgelegt werden oder Nachweise nicht oder nicht geeignet erbracht werden. Dies ist erforderlich, da ansonsten die Auskunfts- und Nachweispflichten nicht oder nur schwer durchsetzbar sind. Diese sind aber notwendig, um zu erkennen, ob ein Betreiber eine Kritische Infrastruktur betreibt und die notwendigen und geeigneten Sicherungsmaßnahmen für seine Informationstechnischen Systeme bereithält.

Wie mit § 14 Absatz 1 Nummer 5 BSIG-E soll mit der neuen Nummer 7 gewährleistet werden, dass Auskunftsverlangen besser durchgesetzt werden können, wobei sich Nummer 7 insbesondere auf Auskünfte bei Vor-Ort-Kontrollen bezieht.

Nach § 14 Absatz 1 Nummer 9 BSIG-E handelt ordnungswidrig, wer nicht sicherstellt, dass die einzurichtende Kontaktstelle jederzeit erreichbar ist. Dies ist erforderlich, um die unverzügliche Weiterleitung wichtiger Sicherheitsinformationen an betroffene Betreiber sicherzustellen. Die Ordnungsvorschrift hält Betreiber zur Einhaltung dieser Verpflichtung an. Dabei heißt „jederzeit erreichbar“ i.S.d. § 8b Absatz 3 BSIG-E, dass Betreiber Kritischer Infrastrukturen über die registrierte Kontaktstelle in der Lage sein müssen, Informationen (Cyber- Sicherheitswarnungen, Lageinformationen etc.) entgegenzunehmen und diese unverzüglich auszuwerten (Bearbeitung der Informationen auf Zuruf). In der Regel werden Informationen während der üblichen Geschäftszeiten versendet. Es ist jedoch nicht auszuschließen, dass in Ausnahmefällen dringende Warnungen auch außerhalb der üblichen Geschäftszeiten (an Feiertagen, Wochenenden oder nachts) versendet werden. Für diese Fälle können bereits existierende dauerhaft erreichbare Stellen in der Organisation, z. B. Pforte, Werkschutz oder sonstige Bereitschaftsdienste, akuten Handlungsbedarf erkennen und ggf. eine Alarmierung bzw. Weiterleitung vornehmen, um die Erreichbarkeit zu gewährleisten.

§ 14 Absatz 1 Nummer 10 BSIG-E sanktioniert, dass einer Auskunftspflicht nicht nachgekommen wird.

Durch § 14 Absatz 1 Nummer 11 BSIG-E wird zusätzlich neben § 8b Abs. 4 Nr. 2 auch die Nr. 1 mit einem Bußgeld bewehrt. Dies ist erforderlich, um zu verhindern, dass Meldungen, die erst nach Eintritt einer Gefahrenlage gemacht werden müssen, von Betreibern dann nicht mehr erfolgen.

Durch § 14 Absatz 1 Nummer 12 BSIG-E wird die fehlende Mitwirkung bei der Bekämpfung einer IT-Bedrohungslage mit einem Bußgeld bewehrt. Dies soll die Betreiber dazu anhalten, in Krisenfällen das Erforderliche zu unternehmen, um die Gefahrenlage zu beenden.

Mit § 14 Absatz 1 Nummer 13 BSIG-E wird der Fall einer Zuwiderhandlung gegen eine vollziehbare Anordnung erfasst.

Zur Abwendung des Missbrauchs des freiwilligen IT-Sicherheitskennzeichens nach § 9a BSIG-E, wird mit § 14 Absatz 1 Nummer 17 BSIG-E sanktioniert, wenn ein Produkt nach Widerruf weiterhin im geschäftlichen Verkehr genutzt oder beworben wird oder vor der Nutzung keineFreigabe durch das BSI erfolgt ist.

Zu Absatz 2

§ 14 Absatz 2 BSIG-E regelt die Höhe der jeweiligen Bußgelder und orientiert sich hierbei an den Regelungen der DSGVO. Die Bußgelder sollen sich an der Wirtschaftskraft des Unternehmens orientieren und bis zu vier Prozent des Umsatzes des Unternehmens ausmachen können. Nur so können die Sanktionen generalpräventiv wirken. Andernfalls bestünde die Gefahr, dass einzelne Unternehmen sich wegen einer nur geringen Bußgeldhöhegegen eine Meldung entscheiden, weil die Zahlung eines Bußgeldes nach Abwägung der möglichen Aufwände für das Unternehmen dies für sie finanziell attraktiver ist. Da sich die Verpflichtungen auf die Betreiber Kritischer Infrastrukturen, von Infrastrukturen oder Unternehmen in Wirtschafsbereichen im besonderen öffentlichen Interesse und Anbieter Digitaler Dienste beziehen, sind die bisherigen Bußgelder in Höhe von maximal 100.000 € verglichen zur Wirtschaftskraft zu gering, um eine lenkende Wirkung erzielen zu können.

Die neue Höhe orientiert sich an den Regelungen der DSGVO. Ein Verstoß gegen Maßnahmen zur Absicherung von Kritischen Infrastrukturen oder Infrastrukturen oder Unternehmen in Wirtschafsbereichen im besonderen öffentlichen Interesse und Diensten der Daseinsvorsorge sollte ebenso schwerwiegend sanktioniert werden können, wie ein datenschutzrechtlicher Verstoß, z. B. durch den Versand von Spam-E-Mails. Andernfalls droht ein Wertungswiderspruch.

Die Androhung des erhöhten Bußgeldrahmens soll dem erhöhten Unwertgehalt einer Missachtung behördlich angeordneter Maßnahmen gerecht werden. Dies entspricht auch Artikel 21 der NIS-Richtlinie, wonach die vorgesehenen Sanktionen wirksam, angemessen und abschreckend sein müssen.

Zu Artikel 2 (Änderungen des Telekommunikationsgesetzes)

Zu Nummer 1

§ 109 TKG erfasst bereits in der aktuellen Fassung sowohl technische als auch organisatorische Schutzmaßnahmen, die von Netzbetreibern und Diensteerbringern zu ergreifen sind. Die Ergänzung der Angabe zu § 109 stellt insofern keine inhaltliche Änderung dar. Vielmehr gibt die künftige Bezeichnung den tatsächlichen Regelungsinhalt der Norm wieder.

Zu Nummer 2

§ 109 TKG stellt die zentrale Vorschrift hinsichtlich der technischen und organisatorischen Schutzmaßnahmen, die von Netzbetreibern und Diensteerbringern zu ergreifen sind, dar. Dabei ist sie auch Ermächtigungsgrundlage für den Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten. Gerade im Hinblick auf den bereits begonnenen und noch anstehenden Aufbau der Mobilfunknetze der 5. Generation und den damit verbundenen Anstieg der Kritikalität der Netze ist es angezeigt, die Sicherheitsanforderungen für Betreiber öffentlicher Telekommunikationsnetze zu erhöhen.

Zu Buchstabe a

Die Ergänzung „für Dienste“ stellt klar, dass die von den verpflichteten Unternehmen zu ergreifenden Maßnahmen auch die Auswirkungen von Sicherheitsverletzungen für Dienste minimieren sollen. Dies entspricht auch der bis zum 21.12.2020 umzusetzenden Vorgabe in Artikel 40 Richtlinie (EU) 2018/1972, die die Sicherheit von Netzen und Diensten betrifft.

Zu Buchstabe b

Die ergänzend eingeführte Regelung gibt ausdrücklich vor, dass sich der Umfang der zu ergreifenden technischen und organisatorischen Schutzmaßnahmen nach dem Gefährdungspotenzial des jeweiligen Netzes/ Dienstes richtet. Dementsprechend sind mit steigendem Gefährdungspotenzial auch gesteigerte Sicherheitsanforderungen zu erfüllen.

Bislang unterliegen Netz- und Systemkomponenten keinerlei Zertifizierungsverpflichtungen. Künftig sind kritische Komponenten zu überprüfen und zu zertifizieren. Als kritische Komponenten werden solche Netz- und Systemkomponenten eingestuft, die kritische Funktionen erfüllen. Einzelheiten zum Zertifizierungsverfahren werden – wie bisher – im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG) geregelt.

Zudem wird klargestellt, dass Einzelheiten der nach Satz 1 bis 4 zu treffenden Maßnahmen gemeinsam durch BNetzA, BSI und BfDI im Sicherheitskatalog festgelegt werden. Darüber hinaus sind auch Einzelheiten der Festlegung kritischer Funktionen und der Bestimmung der kritischen Komponenten im Sicherheitskatalog festzulegen. Dabei legen die zuständigen Behörden insbesondere fest, welche Funktionen eines Netzes /Dienstes als kritisch eingestuft werden und wie die Netzbetreiber und Diensteerbringer ausgehend von dieser behördlichen Festlegung ableiten, ob eine bestimmte Komponente eine kritische Funktion erfüllt und folglich der Zertifizierungspflicht unterfällt.

Zu Buchstabe c

Anpassung an die aktuelle Rechtslage.

Zu Buchstabe d

Die ergänzend eingefügten Sätze konkretisieren die im Sicherheitskonzept vorzunehmenden Darstellungen der Netzbetreiber und Diensteerbringer. Dabei sind künftig bei der Erstellung des Sicherheitskonzepts deutliche Bezüge zu den Vorgaben des Sicherheitskatalogs nach Absatz 6 aufzunehmen.

Der neue Satz 3 stellt klar, dass die Netzbetreiber/Diensteerbringer in Fällen, in denen der Sicherheitskatalog lediglich ein Sicherheitsziel vorgibt, ohne eine entsprechende Schutzmaßnahme vorzuschreiben, darzulegen haben, dass durch die jeweils gewählte Maßnahme das vorgegebene Sicherheitsziel vollumfänglich erreicht wird. Dies führt zu mehr Transparenz hinsichtlich der getroffenen technischen und organisatorischen

Schutzmaßnahmen und stellt eine Erleichterung bei der Überprüfung der Sicherheitskonzepte dar.

Zu Buchstabe e

Es erfolgt die Anpassung der offiziellen Bezeichnung der ENISA. Diese hat seit Juli 2019 eine neue Bezeichnung.

Zu Buchstabe f

Es handelt sich um eine sprachliche Anpassung, die die Verbindlichkeit der im Katalog formulierten Sicherheitsanforderungen hervorhebt.

Zu Buchstabe g

Es handelt sich um eine ausdrückliche Klarstellung, dass die im Katalog festgelegten Anforderungen verbindlich sind.

Zu Buchstabe h

Sprachliche Folgeanpassung.

Zu Buchstabe i

Die Änderung betrifft die Regelung zur Zustellung des Sicherheitskatalogs durch öffentliche Bekanntmachung. Damit wird die in § 131 TKG vorgesehene Zustellung nach Verwaltungszustellungsgesetz (VwZG) durch öffentliche Bekanntmachung ersetzt.

Zu Buchstabe j

Die Änderung betrifft die Regelung, wie die öffentliche Bekanntmachung zu erfolgen hat. Sie enthält auch eine Zustellfiktion und eine Regelung zur Umsetzungsfrist. Vorgaben des Katalogs sind spätestens ein Jahr nach Inkrafttreten zu erfüllen (übliche technische Umsetzungsfrist) sofern im Katalog selbst keine abweichende Umsetzungsfrist geregelt ist.

Zu Buchstabe k

Neben der Anordnungsbefugnis der Bundesnetzagentur besteht künftig für Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial eine Pflicht, sich alle zwei Jahre einer Überprüfung durch eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde zu unterziehen. Diese neue Verpflichtung ist insbesondere angesichts des Gefährdungspotenzials dieser Netze erforderlich und angemessen. Die Pflicht zur Aktualisierung der Sicherheitskonzepte nach Absatz 4 besteht unabhängig davon.

Derzeit ist noch nicht absehbar, wann eine erstmalige Durchführung der Überprüfung sinnvoll erscheint. Daher wird der Bundesnetzagentur die Festlegung des Zeitpunkts der erstmaligen Überprüfung übertragen.

Zu Buchstabe l

Folgeänderung sowie Vorgabe, dass der Überprüfungsbericht an die BNetzA und das BSI zu übersenden ist, da BSI künftig in die Bewertung einbezogen wird.

Zu Buchstabe m

Künftig sollen die Bundesnetzagentur und das Bundesamt für Sicherheit in der Informationstechnik gemeinsam die Bewertung einer von der Bundesnetzagentur angeordneten oder einer regelmäßigen Überprüfung durch eine qualifizierte unabhängige Stelle vornehmen. In diesem Rahmen bewerten die Behörden ebenfalls gemeinsam das Sicherheitskonzept des betreffenden Unternehmens, das regelmäßig auch Bestandteil der Überprüfung durch eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde ist. Sofern die Behörden Sicherheitsmängel feststellen, liegt die Befugnis zur Anordnung von Abhilfemaßnahmen bei der Bundesnetzagentur.

Zu Nummer 3

Zu Buchstabe a

Die Regelung ist zur Information von Betroffenen erforderlich. Aktuell informieren die Diensteanbieter Kunden darüber, wenn Datenverarbeitungssysteme der Nutzer mit einer Botnetzschadsoftware infiziert sind, die einen C&C-Server kontaktiert. Dazu sind die Diensteanbieter gemäß § 109a Absatz 4 TKG verpflichtet, wenn diesen bekannt wird, dass von den Datenverarbeitungssystemen der Nutzer Störungen ausgehen, was bei vielen Botnetzen der Fall ist. Allerdings informieren nicht alle Diensteanbieter die Inhaber der Datenverarbeitungssysteme, wenn Schwachstellen bei Systemen erkannt werden, aber keine unmittelbare Störung erkennbar ist. So haben beispielsweise bei der Meldung des BSI zu Schwachstellen des Online-Shopsystems Magento in vielen Fällen die informierten Diensteanbieter die Betreiber des Shopsystems nicht informiert. Hierzu wurde dem BSI mitgeteilt, dass man keine Veranlassung sehe, bei Schwachstellen von Datenverarbeitungssystemen (z.B. Shopsystemen) Dritter zu warnen, insbesondere, wenn sich diese nicht in angeschlossenen Kundennetzen befinden.

Angreifer scannen das Internet auf Schwachstellen, um festzustellen, welche Datenverarbeitungssysteme angreifbar sind, um diese anschließend zu übernehmen oder mit Schadsoftware zu infizieren. Teilweise ist ein eigener Scan nicht notwendig, da es im Internet frei verfügbare Dienste gibt, die als Dienstleistung Systeme scannen und somit Informationen über mögliche Schwachstellen bereitstellen (z.B. Shodan). Auf diese Weise wird weltweit täglich eine hohe Zahl von Systemen infiziert. Ein aus dem Internet erreichbares Datenverarbeitungssystem, welches bekannte Schwachstellen besitzt, wird daher mit hoher Wahrscheinlichkeit infiziert und als Folge zu einem System, von dem zukünftig Störungen ausgehen.

Eine Lösung des Problems ist, die Anwender dieser Datenverarbeitungssysteme bei erkannten Schwachstellen vor einer Infektion durch ihre Diensteanbieter über die Schwachstelle zu informieren, damit diese ihr System absichern können (z. B. Softwareupdate).

Die direkte Information der Nutzer durch das BSI scheidet aus, da das BSI nicht über die Nutzerinformationen verfügt, um diese informieren zu können. Das BSI kann zwar eine IP-Adresse einem Diensteanbieter zuordnen, hat aber beispielsweise bei dynamischen IP-Adressen keine Information darüber, welcher Nutzer diese IP-Adresse zu dem entsprechenden Zeitpunkt genutzt hat. Es ist daher sinnvoll, dass Nutzer durch ihre Diensteanbieter auch dann informiert werden, wenn das BSI dem Diensteanbieter Schwachstellen meldet, deren Ausnutzung sehr wahrscheinlich ist.

Ein weiteres Anwendungsfeld sind Fälle des Identitätsdiebstahls. Es wird klargestellt, dass Diensteanbieter ihre Kunden warnen müssen, wenn ihnen (z. B. durch das dem BSI) bekannt wird und es wahrscheinlich ist, dass ihre Kunden von einem Identitätsdiebstahl betroffen sind. Hier besteht das Problem, dass gefundene Identitätsdaten häufig aus E-Mailadresse und Kennwort bestehen, wobei die E-Mailadresse zwar einem bestimmten

Provider zugeordnet werden kann, der aber selber nicht betroffen ist (also z. B. die als Benutzerkennung verwendete E-Mailadresse bei Online-Shops).

Das BSI verfügt über die fachliche Expertise, um im Falle des Bekanntwerdens einer Schwachstelle oder eines Identitätsdiebstahls den Providern die entsprechenden Informationen zur Warnung der Nutzer bereitzustellen. Die Informationslücke, die für die Bürgerinnen und Bürger durch die fehlende Warnung der Provider vor bekannten Gefahren entsteht, wird durch die erweiterte Informationspflicht geschlossen.

Zu Buchstabe b

§ 109a TKG sieht bereits eine Benachrichtigungspflicht für TK-Dienste an die BNetzA und den oder die BfDI für Fälle der Verletzung des Schutzes bei dem Diensteanbieter selbst gespeicherter personenbezogener Daten vor.

Eine solche Meldepflicht genügt aber nicht, um auch eine schnelle Strafverfolgung und Gefahrenabwehr (z.B. Information der Betroffenen, Schutzmaßnahmen) sicherstellen zu können. Deshalb muss in entsprechenden Fällen auch eine Benachrichtigung der Strafverfolgungsbehörden sichergestellt werden. Als zentrale Stelle im Sinne der Vorschrift wird das Bundeskriminalamt definiert. Das Bundeskriminalamt ist in der Lage, entsprechende Hinweise schnell zu bewerten und entsprechende Folgemaßnahmen – etwa die Information zuständiger Dienststellen bei den Ländern – einzuleiten. Auf diese Weise kann sichergestellt werden, dass die negativen Folgen der strafbaren Verletzung des Schutzes personenbezogener Daten minimiert werden. Die Meldepflicht gegenüber dem Bundeskriminalamt ist beschränkt, sodass nur strafrechtlich relevante Sachverhalte erfasst werden (z.B. § 202a StGB). Eine Meldepflicht wird erst dann ausgelöst, wenn der Diensteanbieter Anhaltspunkte dafür hat, dass an seinen Telekommunikations- oder Datenverarbeitungssystemen unberechtigte Eingriffe vorgenommen wurden. Fahrlässiges Verhalten durch z.B. Mitarbeiter des Telekommunikationsdienstes wird somit nicht erfasst. Die Norm knüpft die Verpflichtung zur Unterrichtung des Bundeskriminalamts an eine positive Kenntniserlangung des Providers. Auf welche Weise diese Kenntniserlangung erfolgt, ist unerheblich (z.B. eigene Recherche, Hinweise von Nutzern o.ä.).

Die Meldung hat auf elektronischem Wege zu erfolgen über eine von der Zentralstelle des BKA einzurichtende und dort zu definierende Schnittstelle. Hiermit wird auch sichergestellt, dass die Meldungen in gleicher Weise von den Anbietern vorgenommen werden. Die weitergehende Umsetzung der Meldepflichten durch die Anbieter eines sozialen Netzwerks bleibt deren Organisationshoheit überlassen. Nach Inkrafttreten der Regelung beginnt die Meldepflicht der Anbieter damit erst zu dem Zeitpunkt, in dem das BKA den technischen Zugang zur Schnittstelle eingerichtet und freigeschaltet hat.

Zu Buchstabe c

Nach dem neuen Absatz 8 kann das BSI zur Abwehr einer erheblichen Gefahr für die Kommunikationstechnik des Bundes, des Betreibers einer Kritischen Infrastruktur oder für die Verfügbarkeit von Informations- oder Kommunikationsdiensten oder unerlaubten Zugriffen auf eine Vielzahl von Telekommunikations- und Datenverarbeitungssystemen von Nutzern die Diensteanbieter zur Durchführung von Schutzmaßnahmen verpflichten.

Nummer 1 betrifft die Umsetzung der Befugnisse nach Absatz 4 bis 6. Absatz 4 umfasst hierbei insbesondere Maßnahmen zur Benachrichtigung der Nutzer. Für Anbieter von Telekommunikationsdiensten (Provider) bestehen nach § 109a Absatz 5 oder Absatz 6 TKG Pflichten, um bestimmte Schutzmaßnahmen zum Schutz der Netz- und Informationssicherheit zu ergreifen. Allerdings machen die Provider nicht oder nicht in ausreichender Form von diesen Möglichkeiten Gebrauch. Das BSI hat derzeit keine Befugnis die Provider zu Maßnahmen nach § 109a Absatz 5 oder Absatz 6 TKG anzuweisen, Datenverkehr zu blockieren oder umzuleiten. Damit fehlt dem BSI die

Ermächtigung bei folgenden Problemen effektiv zu reagieren und schnell Schutzmaßnahmen einzuleiten:

a) Sind IP-Adresse oder Domänennamen von Internet-Systemen bekannt, die von Kriminellen zur Steuerung infizierter Nutzersysteme (z. B. Bots) genutzt werden, beispielsweise C&C-Server, können Provider momentan nicht angewiesen werden, den Datenverkehr zu diesen Systemen zu blockieren, umzuleiten oder zu beschränken. Eine schnelle Entscheidung über eine solche Umleitung oder Beschränkung kann insbesondere wichtig sein, um bei Botnetzinfektionen Nutzer zu schützen, damit deren Rechner nicht ferngesteuert werden. Für das BSI besteht derzeit nur die Möglichkeit, die Provider über CERT-Bund zu bitten, erkannte C&C-Server abzuschalten oder über DNS-Registries oder DNS-Registrate die entsprechenden Domänen zu blockieren oder auf Sinkholes umzuleiten, was in der Regel eine richterliche Anordnung des zuständigen Staates des Domänennamens erfordert. Dies ist nicht in allen Staaten möglich und sehr zeitaufwändig.

Eine effektivere Reaktion wäre hier, die deutschen Provider anzuweisen, die Malwaredomänen bei den eigenen DNS-Resolvern/DNS-Nameservern zu blockieren oder auf Sinkholes umzuleiten, also keine Auflösung des DNS-Namen zu der IP-Adresse zuzulassen, die im Internet für diese Namensauflösung konfiguriert ist. Damit können infizierte Nutzersysteme geschützt werden. Bevorzugt sollte dabei bei den Schadsoftwaredomänen eine Umleitung auf eine vom BSI vorgegebene Sinkhole erfolgen, um die so erkannten infizierten Systeme über die zuständigen Provider benachrichtigen zu können.

Diese Maßnahme bei den Providern greift zwar nur dann, wenn die Systeme des Nutzers die DNS-Resolver bzw. DNS-Nameserver des betreffenden Providers nutzen. Bei den meisten Nutzern ist dies aber die Standardkonfiguration, so dass es sich grundsätzlich um eine effektive Maßnahme handelt.

Um die oben beschriebene Maßnahme im Wege der Anordnung zielführend einzusetzen, ist eine fachliche Expertise des Anordnenden erforderlich. Diese Maßnahme kann bei fehlerhafter Prüfung dazu führen, dass reguläre, nicht kriminelle Dienste im Internet eingeschränkt werden.

Vor der Anordnung muss daher geprüft werden, ob die angegebene Schaddomäne ausschließlich für kriminelle Zwecke eingesetzt wird, um mögliche Kollateralschäden auszuschließen. Die hierfür erforderliche Expertise ist beim BSI bereits vorhanden. Im Rahmen seiner Tätigkeit hat das BSI Prüfungen dieser Art schon mehrfach durchgeführt (CERT-Bund sowie Avalanche-Takedown in Zusammenarbeit mit Europol und FBI). Aufgrund der bereits bestehenden fachlichen Kompetenz sollte die oben beschriebene Anordnungsbefugnis daher zweckmäßigerweise beim BSI angesiedelt werden.

b) Ferner mangelt es dem BSI an hinreichenden Befugnissen zum Schutz von Betreibern Kritischer Infrastrukturen: Werden dem BSI Angriffe im Internet bekannt, die zu einem erheblichen Schaden einer Kritischen Infrastruktur führen oder führen könnten, kann das BSI die Provider momentan nicht anweisen, den Datenverkehr, der diesem Angriff zugeordnet werden kann, zu blockieren. Eine solche Anweisungsbefugnis zu Maßnahmen nach § 109a Absatz 5 und Absatz 6 TKG würde das BSI in die Lage versetzen, bei aktuellen Krisenvorfällen schnell und unmittelbar reagieren zu können. Ein Beispiel für ein Anordnungsszenario wäre, dass Systeme einer Kritischen Infrastruktur über einen aus dem Internet verfügbaren Dienst zur Steuerung von Wasserkraftwerken massiv angegriffen werden und es bereits zu Ausfällen gekommen ist. In diesem Fall könnte das BSI die Provider anweisen, den Angriffsverkehr zu diesem Dienst zu blockieren, um den Krisenvorfall abzuwenden.

Die Provider selbst haben bereits die Befugnis gemäß § 109a Absatz 5 bei Störungen die Nutzung des Telekommunikationsdienstes bis zur Beendigung der Störung

einzuschränken, umzuleiten oder zu unterbinden. Gemäß § 109a Absatz 6 dürfen Provider Datenverkehr zu Störungsquellen auch einschränken oder unterbinden soweit dies zur Vermeidung von Störungen in den Telekommunikations- und Datenverarbeitungssystemen der Nutzer erforderlich ist. Aber auch wenn die Provider die Möglichkeit haben, die Maßnahmen durchzuführen, besteht die Gefahr, dass dies einige aus Aufwandsgründen oder anderen fiskalischen Gründen nicht tun. Gerade im Bereich des Sinkholings von Botnetzen und der Filterung von (D)DoS-Angriffen ist dies zur Abwehr von Gefahren jedoch manchmal unumgänglich.

Es wird daher eine Weisungsbefugnis des BSI benötigt, um die Provider anzuweisen, Datenverkehr zu Domänen oder IP-Adressen – im Rahmen ihrer Handlungsmöglichkeiten nach § 109a Absatz 5 und Absatz 6 TKG – zu blockieren oder auf (BSI-)Sinkholes umzuleiten. Ferner wird so eine koordinierte Abwehr von Cyber-Angriffen sichergestellt. Daher ist auch eine Beteiligung des BKA erforderlich.

Die Anweisungsbefugnis des BSI ist zudem so ausgestaltet, dass die Aufgaben des BSI zum Schutz von Kritischen Infrastrukturen verbessert werden. Die Ermächtigung enthält vor diesem Hintergrund eine konkrete Regelung zum Datenverkehr, der einem Angriff zugeordnet werden kann, welcher eine Gefahr für eine Kritische Infrastruktur darstellt oder kausal für einen Schaden an einer Kritischen Infrastruktur ist, um dem BSI die Möglichkeit einzuräumen, Angriffen auf KRITIS schneller und effektiver zu begegnen und den Datenverkehr schnell blockieren zu lassen.

Darüber hinaus ist in Nummer 2 die Anordnungsbefugnis zur Bereinigung betroffener Datenverarbeitungssystemen von einem konkret benannten Schadprogramm enthalten. Eine solche Befugnis zur Installation von lückenschließender Software (Patches) bzw. zur Löschung von Schadsoftware wird zum Zwecke einer effektiven Bekämpfung der Gefahren durch Bot-Netze (insbesondere gegen die Bedrohung durch „Ransomware of Things“) benötigt. Diese Befugnis soll vor allem im Rahmen der internationalen Kooperation bei der Bekämpfung von Bot-Netzen genutzt werden können und jeweils nur, soweit dies erforderlich, verhältnismäßig (insb. technisch risikoarm) ist. Bei solchen Zugriffen geht es nicht etwa um ausforschendes Eindringen des BSI in PCs und Smartphones etc., sondern es geht um das Problem, dass im Zusammenhang mit der Stilllegung bzw. Übernahme von Botnetzen die meisten IT-Nutzer überhaupt nicht wissen (können), dass z. B. ihr IoT-Kühlschrank Teil eines Botnetzes ist und sie die dadurch bestehende Gefahr für andere in aller Regel gar nicht selbst bereinigen (können). Auch solche Situationen müssen aber bereinigt werden können.

Entsprechende Technik wird bereits im europäischen Ausland bei Takedowns von Botnetzen eingesetzt.

Hierbei wird auf durch die zuständigen Behörden übernommenen URL-Pack-Cluster ein so genannter „Dropper“ hinterlegt. Verbindet sich intervallmäßig ein Bot mit diesem Server, wird überprüft, ob der Bot mit einer dem Zuständigkeitsbereich der jeweiligen Behörde unterfallenden IP-Adresse auftritt. Ist dies der Fall, wird der „Dropper“ an den Bot ausgeliefert. Hat der Bot eine andere IP-Adresse, so erfolgt keine weitere Interaktion mit dem Bot. Auf Bots, die den „Dropper“ heruntergeladen haben, wird dieser automatisch ausgeführt. Er lädt nach kurzer Analyse eine vorbereitete passende „Bereinigungssoftware“ herunter. Diese bereinigt ohne weiteres Zutun des Bots oder dessen Benutzers anschließend das System von der Schadsoftware.

Die Regelung ist wegen der engen Tatbestandsvoraussetzung und dadurch, dass die Diensteanbieter nur verpflichtet werden können, wenn sie dazu technisch in der Lage sind und es ihnen wirtschaftlich zumutbar ist, verhältnismäßig.

Zu Nummer 2

Telekommunikationsdienstleister, die ihren Sitz im Ausland haben und die Daten auf Servern im Ausland speichern, ihre Dienste aber auch in Deutschland erbringen, sollten gesetzlich verpflichtet werden, eine Kontaktstelle für die deutschen Ermittlungs- und Sicherheitsbehörden einzurichten. Bisher besteht in der Regel - abgesehen von der Erhebung von Bestandsdaten in bestimmten Sachverhalten - keine Möglichkeit für eine direkte Zusammenarbeit mit Dienstleistern, die sich auf einen juristischen Sitz im Ausland berufen. Vielmehr verweisen die Unternehmen bei Anfragen deutscher Behörden auf den Rechtshilfeweg. Es kann jedoch nicht hingenommen werden, dass Unternehmen, die Dienstleistungen im Bundesgebiet für Nutzer im Bundesgebiet erbringen, sich hinsichtlich der Einhaltung der im Bundesgebiet geltenden Verpflichtungen als ausgenommen betrachten.

Diese Kontaktstelle muss Ersuchen zur Datenherausgabe usw. zeitnah beantworten.

Im Schwerpunkt betrifft dies die großen Internetdienstleister wie Amazon, Telegram, Facebook, Google und Microsoft. Diese Firmen bieten ihre Leistungen in Deutschland an. Dennoch werden die dabei anfallenden Daten, die für die Durchsetzung des staatlichen Anspruchs auf Strafverfolgung benötigt werden, in der Regel nicht auf ein entsprechendes Ersuchen der Strafverfolgungsbehörden herausgegeben. Vielmehr ziehen sich die Firmen auf eine Position zurück, wonach sie aufgrund ihres formellen Sitzes im Ausland nicht zur unmittelbaren Zusammenarbeit mit deutschen Ermittlungsbehörden verpflichtet wären.

Das Netzwerkdurchsetzungsgesetz enthält bereits eine entsprechende Verpflichtung für Soziale Netzwerke in § 5 Absatz 2 NetzDG. Allerdings werden hiervon nur die in § 1 Absatz 1 NetzDG definierten Dienste erfasst.

Teilweise vergleichbare Regelungen werden auch in den EU-Dossiers „e-evidence“ und „terrorist content online“ verfolgt. Allerdings ist bei beiden Dossiers ein Abschluss noch nicht absehbar. Deshalb müssen entsprechende Regelungen zunächst im nationalen Recht verfolgt werden. Für die Unternehmen hat dies den Vorteil, dass die Umsetzung entsprechender Regelungen auf EU-Ebene sie nicht unvorbereitet träfe, sondern geeignete Strukturen in Deutschland bereits bestünden. Viele Unternehmen könnten zudem die bereits zur Umsetzung des NetzDG geschaffenen Strukturen mit geringen Anpassungen nutzen.

Um sicherzustellen, dass die Ansprechstellen zentral erfasst und die Erreichbarkeiten für die anfrageberechtigten Behörden verfügbar sind, wird die Bundesnetzagentur mit der Zusammenstellung und Zurverfügungstellung der Erreichbarkeiten beauftragt. Die Anfragen selbst werden jedoch von den Behörden direkt an die Unternehmen gestellt.

Zu Nummer 3

Es handelt sich um eine Folgeänderung aufgrund des § 5d BSIG-E.

Zu Nummer 4

Es handelt sich um Folgeänderungen, mit denen die neu geschaffenen Verpflichtungen als Ordnungswidrigkeit bußgeldbewehrt und damit abgesichert werden.

Nach § 109a Absatz 4 TKG haben Diensteanbieter Pflichten gegenüber den Nutzern. Zur effektiven Durchsetzung dieser Pflichten ist, insbesondere wegen der besonderen Bedeutung der Cyber-Sicherheit, eine Bußgeldbeschwerung erforderlich.

Die Ergänzung in Nummer 21d ist erforderlich, um die Pflicht von Diensteanbietern, Nutzer zu informieren und auf Schutzmöglichkeiten hinzuweisen, mit einem Bußgeld zu flankieren. Auf diese Weise werden Hersteller stärker in die Pflicht genommen.

Die Anordnungsbefugnis des BSI ist mit einem Bußgeld zu flankieren, um Diensteanbietern das besondere Erfordernis deutlich zu machen, Anordnungen zum Schutze von IT-Systemen umgehend umzusetzen.

Zur Durchsetzung der neuen Verpflichtung nach § 109a Absatz 8 TKG wird eine korrespondiere Bußgeldvorschrift geschaffen. Die Verpflichtung nach Absatz 8 besteht nur in außergewöhnlichen Bedrohungsszenarien. Daher ist eine entsprechende Bußgeldregung gerechtfertigt.

Zu Artikel 3 (Änderung des Telemediengesetzes)

Zu Nummer 1

Das Bundesamt hat gemäß § 3 Absatz 1 Satz 2 Nummer 2 BSIG den gesetzlichen Auftrag zur Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen und Zurverfügungstellung der gewonnenen Erkenntnisse für andere Stellen, soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist, sowie für Dritte, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist.

Wenn das Bundesamt die Betroffenen über die gesammelten Informationen unterrichtet, ergreifen diese jedoch oftmals nicht die notwendigen Absicherungsmaßnahmen. Das Bundesamt hat derzeit keine Befugnis, die Diensteanbieter zu Maßnahmen nach § 13 Absatz 7 TMG anzuweisen, die von ihnen angebotenen Dienste auf Hardware- und/oder Softwareebene unter Berücksichtigung des jeweiligen Stands der Technik in angemessener Art und Weise abzusichern, wenn von einem konkreten Telemediendienst – in der Regel einer Website – eine erhebliche Gefahr ausgeht. Im Hinblick auf die nachfolgenden Beispielszenarien fehlen dem Bundesamt somit konkrete Möglichkeiten zur Beseitigung bzw. Eindämmung von IT-Gefährdungslagen:

a) Cyber-Kriminelle haben großflächig eine Sicherheitslücke der E-Commerce-Software „Magento“ ausgenutzt, um durch Einschleusen von schädlichem Code Zahlungsinformationen von Kunden sowie weitere personenbezogene Kundendaten auszuspähen („Online-Skimming“). In der Bundesrepublik waren mehrere hundert Webshops betroffen. Für das BSI besteht in einem solchen Fall nur die Möglichkeit – wie im vorliegenden Fall geschehen –, über CERT-Bund die Netzbetreiber / Provider zu informieren, bei denen die betroffenen Shopbetreiber ihrerseits Kunden sind. Eine Befugnis des Bundesamtes, die Shopbetreiber anzuweisen, konkrete Absicherungsmaßnahmen durchzuführen, besteht seitens des BSI nicht.

b) Einer der häufigsten Infektionswege für Schadsoftware ist die vom Anwender unbemerkte Infektion über sog. „Drive-by-Downloads“. Hierbei handelt es sich um Schadsoftware, die (oftmals vom Webseitenbetreiber unbemerkt) Anwender beim Aufrufen einer Webseite infiziert. Auch an dieser Stelle besteht für das Bundesamt lediglich die Möglichkeit der Warnung unter gleichzeitiger Information des jeweils zuständigen Netzbetreibers / Providers / Hosters. Es besteht allerdings – wie im vorgenannten Fall auch – keine zielgerichtete Möglichkeit des Bundesamtes, die Webseitenbetreiber zur Absicherung ihrer Hardware und/oder Software sowie zur Beseitigung der Infektion zu verpflichten bzw. eine entsprechende Weisung auszusprechen.

§ 13 Absatz 7 TMG verpflichtet Dienstanbieter zu technisch organisatorischen Selbstschutzmaßnahmen. Dienstanbieter sind gemäß § 2 Nummer 1 TMG erfasst, soweit diese ihre Dienste „geschäftsmäßig“ anbieten. Erfasst sind auch Hostingunternehmer, die z. B. sog. „Webbaukästen“ oder vorkonfigurierte Webshop- bzw. CMS-Systeme anbieten.

Diese sind dann ihren Kunden gegenüber verpflichtet, die Anforderungen des § 13 Absatz 7 TMG umzusetzen.

Zwar sind Verstöße gegen § 13 Absatz 7 TMG gemäß § 16 Absatz 2 Nummer 3 TMG bußgeldbewehrt, was jedoch einen eingetretenen Verletzungserfolg voraussetzt. Zu diesem Zeitpunkt hat sich die Gefährdung der IT-Sicherheit also bereits realisiert.

Es wird daher eine Anordnungsbefugnis des Bundesamtes benötigt, Dienstanbieter zur Umsetzung konkreter Maßnahmen gemäß § 13 Absatz 7 TMG zu verpflichten.

Die Regelung ist verhältnismäßig, da dem Bundesamt eine Weisung nur dann möglich sein soll, wenn eine Vielzahl von Nutzern durch eine identische Sicherheitslücke gefährdet wird, die sich auf einer ebensolchen Vielzahl von Diensten findet. Weiterhin soll vermieden werden, dass Dienstanbieter zukünftig ihre Verantwortung für die von ihnen angebotenen Dienste auf das Bundesamt „überlagern“, weil dieses in jedweder Gefährdungslage eine Weisung erteilt. Nur diese Fälle sind insbesondere dazu geeignet, massive IT-Gefährdungslagen zu produzieren.

Zu Nummer 2

Es handelt sich um eine zu § 110 Abs. 1a TKG spiegelbildliche Norm, die eine zur Regelung des TKG parallele Pflicht auch für TMG-Anbieter einführt. Die Meldung an das Bundeskriminalamt über eine elektronische Schnittstelle soll genauso wie bei § 109a Abs. 1a TKG ausgestaltet werden.

Zu Nummer 3

Bei dem sogenannte Datenleak-Vorfall Anfang 2019 hat der Täter unbefugt persönlicher Daten und Dokumente von Politikern und anderen Personen des öffentlichen Lebens im Internet veröffentlicht. Hierzu verwendete er u.a. Daten aus E-Mail bzw. Social Media Accounts der betroffenen Personen, indem er sich zunächst die Zugangsdaten –- dieser Accounts verschaffte (z.B. über eine veranlasste Zurücksetzung der Passwörter und unter Nutzung von wieder freigegebenen E-Mail-Adressen der betroffenen Personen) und im Anschluss diese übernahm. Bereits nach Art. 5 Abs. 1 Bst. d DSGVO sind die Diensteanbieter verpflichtet, personenbezogene Daten auf dem neuesten Stand zu halten und angemessene Maßnahmen zu treffen, damit unrichtige personenbezogene Daten unverzüglich gelöscht oder berichtigt werden. Der Vorfall verdeutlich aber, welche schwerwiegenden Folgen die unberechtigte und unkontrollierte Verbreitung unrechtmäßig erlangter Daten haben kann. Mit der vorgesehenen Meldepflicht soll ein schnelles und adäquates Handeln der Ermittlungsbehörden sichergestellt werden.

Zu Absatz 1

Regelungsadressat sind Diensteerbringer, bei denen die Daten gespeichert, zwischengespeichert, übertragen, veröffentlicht oder weitergegeben werden. Im Unterschied zu § 15a muss es sich hierbei nicht um Daten handeln, deren Schutz bei dem Diensteerbringer selbst verletzt worden ist. Folglich ist für die zusätzliche Verpflichtung der Diensteanbieter, bei dem die unrechtmäßig erlangten Daten (weiter-)verbreitet wurden, eine neue Regelung in § 15b erforderlich.

Die Norm umfasst alle personenbezogenen Daten gem. Art. 4 Nr. 1 DSGVO. Daneben sind auch Betriebs- und Geschäftsgeheimnisse umfasst (vgl. RegE eines Gesetzes zur Umsetzung der Richtlinie (EU) 2016/943 zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung). Im Rahmen der Benachrichtigung sind die inkriminierten Daten mit zu übermitteln, damit die Behörde die Daten prüfen und entsprechende Folgemaßnahmen einleiten kann.

Das Bundeskriminalamt ist in der Lage, entsprechende Hinweise schnell zu bewerten und entsprechende Folgemaßnahmen – etwa die Information zuständiger Dienststellen bei den Ländern – einzuleiten.

Um eine unverhältnismäßige Ausgestaltung der Meldepflicht für die Diensteanbieter zu vermeiden, sollen dem Bundeskriminalamt nur die näher in der Norm bestimmte Fälle gemeldet werden. Diese Fälle sind durch eine große Anzahl der möglicherweise betroffenen Personen, der Art der Daten oder des Schädigungspotentials etwa für die Sicherheit und den Bestand des Staates gekennzeichnet. Damit wird sichergestellt, dass nur strafrechtlich relevante Sachverhalte erfasst werden. Notwendig ist zudem eine positive Kenntniserlangung des Providers. Fahrlässiges Verhalten durch z.B. Mitarbeiter des Diensteanbieters werden somit nicht erfasst.

Die Norm knüpft die Verpflichtung zur Unterrichtung des Bundeskriminalamts an eine positive Kenntniserlangung des Providers. Auf welche Weise diese Kenntniserlangung erfolgt, ist unerheblich (z.B. eigene Recherche, Hinweise von Nutzern o.ä.).

Die Meldung an das Bundeskriminalamt über eine elektronische Schnittstelle soll genauso wie bei § 109a Absatz 1a TKG ausgestaltet werden.

Zu Absatz 2

Die Norm knüpft an die Kenntniserlangung zunächst die Verpflichtung des Diensterbringers, den Zugang zu den Daten für Dritte zu sperren. Anschließend ist der betroffene Nutzer - also derjenige, auf dessen Handeln die Veröffentlichung zurückgeht - auf geeignete Weise zu benachrichtigen. Eine Benachrichtigung der von der Verletzung betroffenen Person aufgrund von Art. 34 DSGVO bleibt hiervon unberührt. Widerspricht der benachrichtigte Nutzer der Entfernung der Daten innerhalb einer angemessenen Frist nicht, so sind die Daten anschließend zu löschen. Die Frist muss angemessen sein und nicht übermäßig kurz; weil der Zugang zu den Daten zu diesem Zeitpunkt bereits gesperrt ist, besteht während des Laufens der Frist keine Gefahr einer Vertiefung der der Verletzung. Erfolgt ein Widerspruch des Nutzers, muss zwischen dem Provider und dem Nutzer eine Klärung nach den allgemeinen Regeln erfolgen. Der Provider darf auch trotz des Widerspruchs die Sperrung aufrechterhalten, wenn er zutreffend weiterhin von einer Verletzung des Schutzes personenbezogener Daten ausgeht.

Ergänzend zu den o.g. Verfahren kann eine Sperrung des Zugangs auch durch die zuständige Stelle angeordnet werden. Bei Vorliegen von zureichenden tatsächlichen Anhaltspunkten einer Straftat nach §§ 202 a bis f (in der Fassung nach diesem Gesetz), 303a StGB (Anfangsverdacht) können die zuständigen Stellen anordnen, dass der Provider den Zugang zu den unrechtmäßig erlangten Daten sperrt.

Zu Absatz 3

Für eine effektive Ausgestaltung der Regelung ist zudem eine sehr kurzfristige Bearbeitung durch den Erbringer des Dienstes sicherzustellen. Wenn die Verbreitung nicht sehr kurzfristig unterbrochen wird, ist diese häufig nicht mehr aufzuhalten.

Zu Nummer 4

Es handelt sich um Folgeänderungen, mit denen die neu geschaffenen Verpflichtungen als Ordnungswidrigkeit bußgeldbewehrt und damit abgesichert werden.

Zu Artikel 4 (Änderung der Außenwirtschaftsverordnung)

Zu Nummer 1 und Nummer 2

Die Änderung trägt der Einführung der kritischen Komponenten im BSIG Rechung und ist eine Folgeänderung.

Zu Artikel 115 (Inkrafttreten)

Wegen der steigenden Bedrohungslage und der damit verbundenen Bedeutung des Vorhabens wird das Inkrafttreten auf den frühestmöglichen Zeitpunkt gelegt.