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 alle Staaten dieser Welt. Alle gesellschaftlichen Gruppen sind auf funktionierende Informationstechnik angewiesen - sei es für die Produktion, den Konsum, Dienstleistungen oder zur Pflege privater Kontakte. Voraussetzung hierfür ist eine sichere Infrastruktur.

Die jüngere Vergangenheit hat der Öffentlichkeit deutlich vor Augen geführt, dass Digitalisierung, Cyber-Sicherheit und Datenschutz untrennbar miteinander verbunden sind.

Cyber-Angriffe stellen insbesondere für Staat, Wirtschaft und Gesellschaft mithin 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 Chips wie „Meltdown“ und „Spectre“ besonders deutlich. Daneben hat auch der zu Beginn des Jahres 2018 in den Medien bekanntgewordene Angriff auf das Auswärtige Amt 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.

Eine weitere Verschärfung der Bedrohungslage besteht durch die zunehmende Verbreitung von Internet of Things (IoT)-Geräten. Diese Geräte werden regelmäßig nicht unter Sicherheitsaspekten entwickelt und lassen sich hierdurch ohne großen Aufwand zu riesigen Bot-Netzen zusammenschalten.

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

B. Lösung

IT-Sicherheit muss für die Gesellschaft, die Wirtschaft und den Staat ausgeweitet werden. Entsprechend dem Auftrag aus dem Koalitionsvertrag wird daher der mit dem IT-Sicherheitsgesetz geschaffene Ordnungsrahmen durch das Zweite IT-Sicherheitsgesetz erweitert. Das IT-SiG 2.0 stellt den wesentlichen rechtlichen Rahmen der Tätigkeiten der Bundesregierung auf dem Gebiet der IT-Sicherheit in dieser Legislaturperiode dar.

Das Gesetz verfolgt einen ganzheitlichen Ansatz und enthält Maßnahmen zum Schutz der Gesellschaft bzw. der Bürger, zur Stärkung des Staates bzw. zum Schutz der öffentlichen Informationstechnik und für eine resiliente Wirtschaft.

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

Um Cyber-Sicherheitsvorfällen insgesamt zu begegnen, werden die Befugnisse des BSI sowie der Strafverfolgungs- und Sicherheitsbehörden zum Schutz der Bundesverwaltung und der Gesellschaft ausgeweitet. Auch werden Möglichkeiten zur Unterstützung der Länder durch das BSI erweitert, da die Bedrohungen des Cyber-Raums unabhängig von Ländergrenzen bestehen.

Zum Schutz der Bürger sowie besonders schutzbedürftiger Personen, werden ergänzend Anpassungen am materiellen Strafrecht und am Strafverfahrensrecht vorgenommen. So werden Strafrahmen zur besseren Abbildung des Unrechts angepasst, Strafbarkeitslücken geschlossen und Qualifikationstatbestände für Computerstraftaten eingeführt. Durch Anpassungen im Strafverfahrensrecht werden den Strafverfolgungs- und Ermittlungsbehörden effektive Ermittlungsinstrumente zur Bekämpfung der Cyberkri-minalität an die Hand gegeben.

Bei der rechtswidrigen Verbreitung illegal erlangter Daten spielen die Provider eine erhebliche Rolle. Damit die rechtswidrige Verbreitung solcher Daten zukünftig schnell unterbunden werden kann, werden den Providern Verpflichtungen zum Löschen, zum Melden und zu Bestandsauskünften bei Cybercrime-Vorfällen auferlegt.

Zur Verbesserung der Behördenzusammenarbeit bei der Bekämpfung von Cybercrime-Vorfällen auch über Staatsgrenzen hinweg wird in Umsetzung der Cybercrime-Konvention des Europarats eine Regelung zur Vorabsicherung von Daten geschaffen.

Außerdem werden die für die Betreiber Kritischer Infrastrukturen bestehenden Meldepflichten und Verpflichtungen zur Einhaltung der Mindeststandards auf weitere Teile der Wirtschaft ausgeweitet. Hierbei geht es um diejenigen Teile, an welchen ein besonderes öffentliches Interesse besteht, weil z.B. bei deren Beeinträchtigung ein Grundinteresse der Gesellschaft gefährdet wäre.

C. Alternativen

Beibehalten des bisherigen Rechtszustandes.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

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 in der Wirtschaft zu einer Veränderung des jährlichen Erfüllungsaufwands von rund 45,09 Mill. Euro. Rund 31,20 Mill. Euro davon entstehen aus neuen oder geänderten Informationspflichten. Einmalig wird die Wirtschaft mit rund 16,71 Mill. Euro belastet.

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 BDBOS ist verantwortlich für die Kommunikationswege des Bundes. 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 864 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 55,5 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.

Infolge des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl 2015, Teil I Nr. 31, S. 1324) und dem Gesetz zur 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 (EURL2016/1148UmsG) erhielt das BSI Ressourcen als zentrale Anlaufstelle für Betreiber Kritischer Infrastrukturen und Nationale Cyber-Sicherheitsbehörde.

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

Die in § 2 Absatz 13 BSIG eingefügte Ergänzung bezüglich der Zertifizierung der Komponenten für das neue Mobilfunknetz (5G) führt zu einem erhöhten Personalbedarf von 168 Stellen.

- Mit den neuen Aufgaben des BSI zur Förderung des Verbraucherschutzes und der Verbraucherinformation trägt das Gesetz dem Umstand Rechnung, dass die 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 der Verbraucherinnen und Verbraucher 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 169 Planstellen.

- In diesem Kontext kommen auch die Änderungen in § 3 Abs. 1 Satz 2 Nr. 14 sowie § 7 Abs. 1d, sprich die erweiterte Informationsaufgabe und Warnbefugnis im Hinblick auf Produkte zum Tragen, die den Aktivitäten des BSI größere Wirkung verschaffen wird. 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 12 Planstellen 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 im § 3 Abs. 1 Satz 2 Nr. 19 „Pflege und Weiterentwicklung sicherer Identitäten“ alte Ansätze fortzuentwickeln sowie ganz neue Ansätze zu entwickeln, die zur breiten Anwendung kommen. Hierfür benötigt das BSI 8 Planstellen.

- § 4a 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. Diese neue Aufgabe des BSI führt zu einem Personalbedarf von 64 Planstellen.

- § 4b Meldestelle. Die Sammlung von Informationen über Sicherheitslücken, Schadprogrammen 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 existierenden Meldestelle beim Bundesamt zwingend erforderlich. Der organisatorische, rechtliche und technische Ausbau sowie die kontinuierliche Beobachtung, Entgegennahme sowie Auswertung und Analyse der Meldungen führt zu einem zusätzlichen Personalbedarf von 14 Planstellen.

- § 5 Abs. 11: Die Bedrohungslage für die Kommunikationstechnik des Bundes ist quantitativ und qualitativ gestiegenen. Um der gestiegenen Gefahr eine effektive Abwehr entgegenzusetzen, muss das Bundesamt personell verstärkt werden. Die aktuell im Bundesamt zur Verfügung stehenden Personalressourcen ermöglichen nicht, die erforderlichen Detektionsmaßnahmen bei allen Behörden des Bundes in ausreichender Form zum Einsatz zu bringen. Neben der mit gem. Gesetz adressierten gestiegenen Gefahrenlage für die Kommunikationstechnik des Bundes erweitert das Gesetz auch die Möglichkeiten des Bundesamtes in Bezug auf eine Unterstützung der Länder. Um eine angemessene Abwehr von Gefahren für die Kommunikationstechnik des Bundes zu erhalten und die neuen Aufgaben bei der Unterstützung der Länder zu erfüllen, benötigt das Bundesamt zusätzliche 29 Planstellen.

- § 5a: Neben der Analyse von Protokolldaten i.S.d. BSIG ist die Auswertung von behördeninternen Protokollierungsdaten ein wesentlicher Bestandteil einer umfassenden Abwehr von Gefahren für die Sicherheit der Informationstechnik. Die geplante Änderung am BSIG erlaubt es dem BSI auf gesetzlicher Grundlage, nun

auch behördeninterne Protokollierungsereignisse von vor allem IT-Systemen auszuwerten. Hieraus ergibt sich, dass nun in einem sehr viel größeren Maßstab auch Behörden, die noch nicht durch die 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. Für die Detektion von Cyber-Angriffen durch eine systematische Analyse dieser Daten ist ein Aufwuchs des Bundesamtes um 29 Planstellen zu realisieren.

- In der heutigen Bedrohungslage sind präventive Schutz- und Abwehrmaßnahmen alleine nicht mehr ausreichend. Längst ist klar, dass Angriffe auch bei bestmöglicher Prävention erfolgreich sein werden, 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 oder die Betreiber Kritischer Infrastrukturen) bei der Bewältigung von Sicherheitsvorfällen unterstützen. Die Erfahrung nach der Einrichtung dieser MIRTs hat gezeigt, dass auch die Länder in diesem Bereich einen erheblichen Unterstützungsbedarf haben. Um eine regelmäßige Unterstützung durch das Bundesamt zu ermöglichen, wird durch dieses Gesetz die Betroffenheit eines Landes von einem IT-Sicherheitsvorfall als Einsatz-Regelfall festgelegt. Durch die damit einhergehende Erweiterung des Adressatenkreises entsteht für das Bundesamt ein personeller Mehrbedarf von 41 Planstellen.

- § 5c, § 8b Abs. 2: Kommt es bei Betreibern Kritischer Infrastrukturen oder bei weiterer Anlagen 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 Krisenreaktionspläne zu erarbeiten sowie eine solche Struktur zwischen Bundesbehörden und den KRITIS-Betreibern aufzubauen, zu pflegen und zu betreiben, sind beim Bundesamt 44 Planstellen/Stellen erforderlich.

- § 5d 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 Verwaltungsaufwand von 2 Planstellen.

- Das Bundesamt muss in der Lage sein, technische Untersuchungen nach § 7a BSIG zur Erfüllung aller seiner gesetzlichen Aufgaben durchzuführen. Dies wird durch dieses Gesetz ermöglicht. Zudem wir das Bundesamt mit weitergehenden 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.

- § 7c: 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 Bundesamt 10 Planstellen.

- Um Detektionsmaßnahmen zum besonderen Schutz von Mitgliedern der Verfassungsorgane durchzuführen und hierdurch das BKA zu unterstützen, entsteht dem Bundesamt zudem ein Personalbedarf von zusätzlichen 2 Planstellen.

- Die Vielzahl von Digitalisierungsvorhaben der Bundesregierung erfordert eine konstante Beratung und Begleitung durch das Bundesamt, um bereits ab der Konzeptions- und Planungsphase die Aspekte der IT-Sicherheit in angemessener Weise zu berücksichtigen. Daher ist das Bundesamt durch die jeweils zuständige Stelle frühzeitig bei der Planung und Umsetzung der neuen Digitalisierungsvorhaben des Bundes zu beteiligen. Angesichts der Vielzahl der anstehenden Digitalisierungsprojekte beläuft sich der hierdurch entstehende Beratungsaufwand auf einen Bedarf von 71 Planstellen/Stellen.

- Durch die Erweiterung der KRITIS-Regelungen und die damit verbundene Aufnahme weiterer Branchen in den Regelungsbereich des Gesetzes sowie die Ergänzung des BSIG um den Bereich der Infrastrukturen im besonderen öffentlichen Interesse und die Möglichkeit, bestimmten Betreiben im Einzelfall Pflichten nach §§ 8a und 8b BSGI aufzuerlegen, wenn eine Störung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse dieses Unternehmens zu einer tatsächlichen und hinreichend schweren Gefährdung für ein Grundinteresse der Gesellschaft führen würde, führt zu einem personellen Mehrbedarf des Bundesamtes von insgesamt 56 Planstellen.

- 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. Das IT-Sicherheitskennzeichen des Bundesamts wird es Verbraucherinnen und Verbrauchern ermöglichen, schnell und einfach zu überprüfen, ob das jeweilige IT-Produkt bzw. dessen Hersteller aktuelle Sicherheitsstandards in ausreichender Form berücksichtigt. Um die für die Vergabe des IT-Sicherheitskennzeichens erforderlichen Arbeiten inkl. der im Sinne einer Marktaufsicht anstehenden Prüfungen und Kontrollen durchführen zu können, benötigt das Bundesamt 25 zusätzliche Planstellen.

- Die Erweiterung der Bußgeldvorschriften führt zu einem erhöhten Prüfungs- und Verwaltungsaufwand. Das Bundesamt benötigt zur Bewältigung dieses zusätzlichen Aufwandes 2 weitere Planstellen.

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 BSI-Gesetz in der Fassung der Bekanntmachung vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 1 des Gesetzes vom 23. Juni 2017 (BGBl. I S. 1885) 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) Absatz 9 wird durch folgenden Absatz 9 ersetzt:

   „(9) 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. Protokolldaten nach Absatz 8 sind eine Teilmenge der Protokollierungsdaten. Protokollierungsdaten dienen der Erkennung, Eingrenzung oder Beseitigung von Störungen oder Fehlern bei der Kommunikationstechnik oder von Angriffen.“

   c) Nach Absatz 9 wird folgender Absatz 9a eingefügt:

   „(9a) IT-Produkte sind Softwareprodukte sowie alle einzelnen oder miteinander verbundenen Hardwareprodukte und Hardwarekomponenten, inklusive der zur einwandfreien Funktion eingesetzten Software.“

   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) Kernkomponenten für Kritische Infrastrukturen (KRITIS-Kernkomponenten) sind IT-Produkte, die zum Betrieb von Kritischen Infrastrukturen im Sinne dieses Gesetzes dienen und für diesen Zweck besonders entwickelt oder geändert werden. KRITIS-Kernkomponenten sind:

1. im Sektor Energie IT-Produkte für die Kraftwerksleittechnik, für die Netzleittechnik oder für die Steuerungstechnik zum Betrieb von Anlagen oder Systemen zur Stromversorgung, Gasversorgung, Kraftstoff- oder Heizölversorgung oder Fernwärmeversorgung,

2. im Sektor Wasser IT-Produkte für die Leit-, Steuerungs- oder Automatisierungstechnik von Anlagen zur Trinkwasserversorgung oder Abwasserbeseitigung,

3. im Sektor Informationstechnik und Telekommunikation IT-Produkte zum Betrieb von Anlagen oder Systemen zur Sprach- und Datenübertragung oder zur Datenspeicherung und -verarbeitung. Soweit IT-Produkte und deren Einsatz dem Anwendungsbereich des TKG unterfallen, gelten diese nur dann als KRITIS-Kernkomponenten im Sinne dieser Vorschrift, wenn sie durch den Sicherheitskatalog nach § 109 Absatz 6 TKG als solche festgelegt sind.

4. im Sektor Ernährung IT-Produkte zum Betrieb von Anlagen oder Systemen zur Lebensmittelversorgung.

5. im Sektor Gesundheit IT-Produkte zum Betrieb eines Krankenhausinformationssystems, zum Betrieb von Anlagen oder Systemen zum Vertrieb von verschreibungspflichtigen Arzneimitteln sowie zum Betrieb eines Laborinformationssystems,

6. im Sektor Finanz- und Versicherungswesen IT-Produkte zum Betrieb von Anlagen oder Systemen der Bargeldversorgung, des kartengestützten Zahlungsverkehrs, des konventionellen Zahlungsverkehrs, zur Verrechnung und der Abwicklung von Wertpapier- und Derivatgeschäften oder zur Erbringung von Versicherungsdienstleistungen,

7. im Sektor Transport und Verkehr IT-Produkte zum Betrieb von Anlagen oder Systemen zur Beförderung von Personen und Gütern im Luftverkehr, im Schienenverkehr, in der See- und Binnenschifffahrt, im Straßenverkehr, im öffentlichen Personennahverkehr oder in der Logistik,

8. im Sektor Entsorgung IT-Produkte zum Betrieb von Anlagen oder Systemen zur Abfallentsorgung.

(14) Infrastrukturen im besonderem öffentlichen Interesse sind Anlagen oder Teile davon, die

dem Bereich Rüstung angehören und nach § 60 der Außenwirtschaftsverordnung in der jeweils geltenden Fassung wesentlich für die Sicherheitsinteressen der Bundesrepublik Deutschland sind,

1. dem Bereich Kultur und Medien angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung eine Gefährdungen für die öffentliche Sicherheit eintreten würde, oder

2. nicht von Absatz 10 erfasst sind, aber dennoch von erheblicher Bedeutung sind, weil durch ihren Ausfall oder ihre Beeinträchtigung die Geschäftstätig-

keit von Unternehmen mit Zulassung zum Teilbereich des regulierten Marktes mit weiteren Zulassungsfolgepflichten (Prime Standard) nach § 48 Börsenordnung der Frankfurter Wertpapierbörse eingeschränkt und dadurch erhebliche volkswirtschaftliche Schäden eintreten würden.

Die Infrastrukturen 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 folgender Nummer 5a eingefügt:

„5a. Erteilung der Befugnis nach § 1 Absatz 2 des Gesetzes über die Akkreditierungsstelle, als Konformitätsbewertungsstelle im Bereich der IT-Sicherheit tätig zu sein. Im Bereich der hochwertigen IT-Sicherheitszertifizierung Anerkennung der hierfür erforderlichen Sachkenntnis der Konformitätsbewertungsstelle nach § 9 Absatz 6;".

c) 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;".

d) 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;".

e) Nummer 17 wird durch folgende Nummer 17 ersetzt:

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

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

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

„19. Entwicklung von Anforderungen an Identifizierungs- und Authentisierungsverfahren und Bewertung dieser Verfahren unter dem Gesichtspunkt der Informationssicherheit;

20. Entwicklung und Veröffentlichung sicherheitstechnischer 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 überwiegende Sicherheitsinteressen oder Geheimschutzinteressen entgegenstehen.

(2) Ferner ist dem Bundesamt 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 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 IT-Sicherheit, insbesondere zur Beseitigung der festgestellten Mängel, verbinden.

§ 4b

Meldestelle für die Sicherheit in der Informationstechnik

(1) Das Bundesamt fördert die Sicherheit in der Informationstechnik. Hierzu sammelt es Informationen über Sicherheitsrisiken in der Informationstechnik 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 Dritte im Rahmen der Meldung verlangen,

dass die Daten nur anonymisiert weitergegeben werden dürfen. In diesem Fall gilt § 5 Absatz 5 und Absatz 6 Satz 1 entsprechend.

(3) Das Bundesamt kann die gemäß Absatz 2 gemeldeten Informationen zur Aufgabenerfüllung verarbeiten. Insbesondere kann es die 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. 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.

Eine Weitergabe erfolgt nicht, wenn 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,

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

Sonstige gesetzliche Übermittlungshindernisse und Regelungen zum Geheimschutz bleiben unberührt.

(4) Erlangt das Bundesamt im Rahmen einer Meldung nach Absatz 2 Kenntnis von der Identität eines Dritten, 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 Dritte diese Erkenntnisse gewonnen hat, die schutzwürdigen Interessen des Dritten das Allgemeininteresse an der Übermittlung überwiegen. Die Entscheidung nach Satz 1 muss dem behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem weiteren Bediensteten des Bundesamtes, der die Befähigung zum Richteramt hat, zur vorherigen Entscheidung vorgelegt werden.

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

5. § 5 wird wie folgt geändert:

a) In Absatz 1 Satz 4 werden nach den Wörtern „Schnittstellendaten nach Satz 1 Nummer 2“ die Wörter „nach Maßgabe des § 4a“ eingefügt.

b) 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 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, soweit dies automatisiert möglich ist. Eine nicht automatisierte Auswertung oder eine personenbezogene Verwendung ist nur nach Maßgabe der nachfolgenden Absätze zulässig. Soweit hierzu die Wiederherstellung oder vorübergehende Erhaltung des Personenbezugs pseudonymisierter Daten erforderlich ist, muss diese durch den Präsidenten des Bundesamtes angeordnet werden. Der Präsident kann diese Aufgabe an einen Bediensteten des Bundesamtes mit der Befähigung zum Richteramt delegieren. Die Entscheidung über die Wiederherstellung oder vorübergehende Erhaltung des Personenbezugs ist zu protokollieren. Entscheidet der Delegierte über die Wiederherstellung oder vorübergehende Erhaltung des Personenbezugs pseudonymisierter Daten, sind der Präsident und die behördliche Datenschutzbeauftragte unverzüglich zu informieren.“

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

„(2a) Protokolldaten dürfen vor ihrer Pseudonymisierung und Speicherung nach Absatz 2 sowie stichprobenartig nach ihrer Pseudonymisierung und Speicherung manuell verarbeitet werden, sofern diese Verarbeitung zur Sicherstellung einer fehlerfreien Pseudonymisierung oder fehlerfreien automatisierten Auswertung verhältnismäßig ist. Absatz 2 Satz 5 bis 8 gilt entsprechend. Die Entscheidung ist zu protokollieren.“

d) Nach Absatz 10 wird folgender Absatz 11 eingefügt:

„(11) Das Bundesamt darf Maßnahmen nach Absatz 1

1. zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes bei IT-Dienstleistern und Diensteanbietern durchführen, die wesentliche IT-Dienstleistungen oder IT-Dienstleistungen in sicherheitssensiblen Bereichen für den Bund erbringen und

2. zur Abwehr von Gefahren für die Kommunikationstechnik der Länder auf deren Ersuchen durchführen.

Hierbei gelten die Absätze 2 bis 10 entsprechend. Im Falle des Satzes 1 Nummer 2 ist dies nur möglich, soweit dies nach jeweiligem Landesrecht ausdrücklich vorgesehen ist.“

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

„§ 5a

Verarbeitung behördeninterner Protokollierungsdaten

Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes behördeninterne Protokollierungsdaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, erheben 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 überwiegende Sicherheitsinteressen oder Geheimschutzinteressen nicht entgegen stehen. Die Bundesbehörden sind verpflichtet, das Bundesamt bei Maßnahmen nach Satz 1 zu unterstützen und hierbei den unbeschränkten Zugang des Bundesamtes zu behördeninternen Protokollierungsdaten nach Satz 1 sicherzustellen. § 5 Absatz 2 bis 4 sowie Absatz 8 und 9 gelten entsprechend.“

7. Der bisherige „§ 5a“ wird „§ 5b“ und wie folgt geändert:

a) Absatz 1 wird wie folgt gefasst:

„(1) Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Stelle des Bundes oder eines Betreibers einer Kritischen Infrastruktur oder eines Betreibers einer weiteren Anlage im besonderen öffentlichen Interesse um einen herausgehobenen Fall, so kann das Bundesamt auf Ersuchen der betroffenen Stelle oder des betroffenen Betreibers die Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind.“

b) In Absatz 7 wird folgender Satz angefügt:

„Ein begründeter Einzelfall liegt in der Regel vor, wenn einem Betreiber von Anlagen nach § 8g die Pflichten nach § 8a und § 8b auferlegt wurden oder eine Stelle eines Landes betroffen ist.“

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

Krisenreaktionspläne auf, um die Aufrechterhaltung oder Wiederherstellung der informationstechnischen Systeme, Komponenten oder Prozesse bei Betreibern Kritischer Infrastrukturen oder Betreibern weiterer Anlagen 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.

(2) Die Krisenreaktionspläne sollen die an der Krisenreaktion beteiligten Behörden, Betreiber Kritischer Infrastrukturen und Betreiber weiterer Anlagen im besonderen öffentlichen Interesse in die Lage versetzen, im Notfall unverzüglich abgestimmte Entscheidungen zu treffen und die angemessenen Maßnahmen rechtzeitig durchzuführen.

(3) Bei der Erstellung und bei wesentlichen Änderungen der Krisenreaktionspläne soll eine Abstimmung mit den Betroffenen sichergestellt werden. Die Krisenreaktionspläne werden regelmäßig unter Berücksichtigung von Erkenntnissen aus bewältigten Krisen im Bereich der Sicherheit in der Informationstechnik sowie den Verände-

rungen des Stands der Technik und der Rechtslage überprüft und gegebenenfalls angepasst.

(4) Während einer erheblichen Störung gemäß § 8b Absatz 4 Nummer 2 kann das Bundesamt im 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 erforderlich informationstechnischen Maßnahmen für die Wiederherstellung der Sicherheit und der Funktionsfähigkeit ihrer informationstechnischen Systeme anordnen, um erhebliche Versorgungsengpässe oder Gefährdungen für andere 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 selbst nicht unverzüglich beseitigen kann.

§ 5d

Bestandsdatenauskunft

(1) Das Bundesamt darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Auskunft über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten verlangen (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes), 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 möglichst 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 (§ 113 Absatz 1 Satz 3, §113c Absatz 1 Nummer 3 des Telekommunikationsgesetzes).

(3) Das Bundesamt übermittelt Auskunftsverlangen nach Absatz 1 oder Absatz 2 in Textform. Auf Grund eines Auskunftsverlangens nach Absatz 1 oder 2 hat derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich an das Bundesamt zu übermitteln. Für die Entschädigung der Diensteanbieter ist § 23 des Justizvergütungs- und -entschädigungsgesetzes entsprechend anzuwenden.

(4) 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 Aus-

kunft 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 eine Benachrichtigung an den Betroffenen.

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

(6) 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 5.“

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 von diese Produkte betreffenden Warnungen zu informieren. Diese Informationspflicht besteht nicht, 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. 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 anhand sachlicher Kriterien einschränken; sachliche Kriterien können insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere Zuverlässigkeit des Empfängers sein.“

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 die Frist für die Übermittlung der Auskünfte fest. Das Auskunftsverlangen enthält ferner einen Hinweis auf die in § 14 vorgesehenen Sanktionen.

(3) 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 dieser Aufgaben erforderlich ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben.

(4) 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 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 und Auswertung 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 ist ungeschützt im Sinne des Absatzes 1, wenn öffentlich bekannte Sicherheitslücken bestehen oder wenn auf Grund offensichtlich unzureichender Sicherheitsvorkehrungen von unbefugten Dritten auf das System zugegriffen werden kann.

(3) Wird im Falle des Absatzes 1 ein Schadprogramm, eine Sicherheitslücke oder ein anderes Sicherheitsrisiko in einem informationstechnischen System erkannt, sind die hierfür Verantwortlichen oder 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 jeweils zuständige 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) Ferner darf das Bundesamt 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 erreichbaren und ungeschützten informationstechnischen Systemen unterstützen. § 7b Absatz 2 und 3 gelten entsprechend.“

12. § 8 wird wie folgt geändert:

a) Absatz 1 wird wie folgt gefasst:

„(1) Das Bundesamt erarbeitet im Benehmen mit den Ressorts Mindeststandards für die Sicherheit der Informationstechnik des Bundes, welche 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 in vollem Eigentum des Bundes stehen und die IT-Dienstleistungen für die Bundesverwaltung erbringen,

zu berücksichtigen 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 sowie der Konferenz der IT-Beauftragten der Ressorts mit. Für andere öffentlich- oder privatrechtlich or-

ganisierte 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 und Duldung der Kontrolle durch das Bundesamt verpflichtet. 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 eingefügt:

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

13. § 8a wird wie folgt geändert:

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

„(1a) Die Verpflichtung der Betreiber Kritischer Infrastrukturen, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind, umfasst auch den Einsatz von Systemen zur Angriffserkennung. Die Betreiber Kritischer Infrastrukturen dürfen die hierzu erforderlichen Daten verarbeiten. Die im Rahmen des Einsatzes von Systemen zur Angriffserkennung erhobenen Daten sind unverzüglich zu löschen, wenn sie nicht für die Vermeidung von Störungen nach Absatz 1 Satz 1 erforderlich sind. Die übrigen Daten dürfen nicht länger als zehn Jahre gespeichert werden. Die Ausgestaltung des Einsatzes von Systemen zur Angriffserkennung legt das Bundesamt in einer Technischen Richtlinie fest. Hierzu muss die oder der Bundesbeauftrage für den Datenschutz und die Informationsfreiheit angehört werden. Die Betreiber Kritischer Infrastrukturen müssen der oder dem betrieblichen Datenschutzbeauftragten, dem Bundesamt, der jeweiligen Aufsichtsbehörde und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am Ende eines Quartals detailliert über die Verfahren und Umstände von Maßnahmen nach Satz 1 in diesem Zeitraum schriftlich berichten."

b) Nach Absatz 5 wird folgender Absatz 6 eingefügt:

„(6) KRITIS-Kernkomponenten dürfen nur von solchen Herstellern bezogen werden, die vor dem erstmaligen Einsatz der Komponenten eine Erklärung über ihre Vertrauenswürdigkeit gegenüber dem Betreiber der Kritischen Infrastruktur abgeben haben (Vertrauenswürdigkeitserklärung). Diese Verpflichtung erstreckt sich auf die gesamte Lieferkette des Herstellers. Das Bundesministerium des Innern, für Bau und Heimat erlässt die Mindestanforderungen für die Vertrauenswürdigkeitserklärung durch Allgemeinverfügung, die im Bundesanzeiger bekannt zu machen ist. Diese Verpflichtung gilt ab der Bekanntmachung der Allgemeinverfügung nach Satz 3."

14. § 8b wird wie folgt geändert:

a) In Absatz 2 wird folgender Satz 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, 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."

b) 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."

c) Nach Absatz 3 wird folgender Absatz 3a 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 und der Betreiber seiner 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, kann das Bundesamt die erfolgte Registrierung eines Betreibers aus tatsächlichen oder rechtlichen Gründen ablehnen."

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

16. Nach § 8e werden die folgenden §§ 8f bis 8h eingefügt:

„§ 8f

Anforderungen für Betreiber von Infrastrukturen im besonderen öffentlichen Interesse

Die Pflichten nach den §§ 8a und 8b gelten entsprechend für Betreiber von Anlagen oder Teilen davon

1. nach § 2 Absatz 14 Nummer 2 spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 5.

2. nach § 2 Absatz 14 Nummer 1 und 3 spätestens zwei Jahre nach Inkrafttreten dieses Gesetzes.

§ 8g

Cyberkritikalität

(1) Das Bundesamt kann im Einzelfall Betreibern von Anlagen die Pflichten nach §§ 8a und 8b auch auferlegen, wenn

1. die betriebenen Anlagen oder Teile davon den Sektoren oder Bereichen nach § 2 Absatz 10 Satz 1 Nummer 1 sowie § 2 Absatz 13 Nummer 2 oder 3 zuzuordnen sind und

2. die Voraussetzungen des § 2 Absatz 10 Nummer 2 sowie § 2 Absatz 14 Nummer 1, 2 oder 3 im Übrigen nicht vorliegen, aber Störungen der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, insbesondere wegen des hohen Grades an Vernetzung der eingesetzten Informationstechnik, zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der betroffenen Dienstleistung insgesamt führen würden (Cyberkritikalität).

(2) Das Bundesamt kann im Einzelfall einem Unternehmen die Pflichten nach §§ 8a und 8b auferlegen, wenn eine Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse dieses Unternehmens zu einer tatsächlichen und hinreichend schweren Gefährdung für ein Grundinteresse der Gesellschaft führen würde.

(3) Das Bundesamt hat bei der Auferlegung der Pflichten dem Adressaten nach Absatz 1 und 2 mitzuteilen, ab wann die Pflichten nach §§ 8a und 8b gelten. Die Frist darf ein Jahr nicht unterschreiten.

§ 8h

Hersteller von IT-Produkten

(1) Hersteller von IT-Produkten haben erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Produkte unverzüglich dem Bundesamt zu melden, wenn die Anwendung des IT-Produkts zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit von Anlagen nach § 2 Absatz 10 oder 14 führen kann. Die Meldung muss Angaben zu der Störung des betroffenen IT-Produkts, zu möglichen grenzüberschreitenden Auswirkungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache sowie zu den Auswirkungen der Störung enthalten.

(2) Hersteller von KRITIS-Kernkomponenten nach § 2 Absatz 13 haben Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der Software dem Bundesamt unverzüglich zu melden, wenn die Anwendung der KRITIS-Kernkomponenten Software zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit von Kritischen Infrastrukturen nach § 2 Absatz 10 führen kann. Die Meldung muss Angaben zu der Störung der betroffenen Software, zu möglichen grenzüberschreitend Auswirkungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache sowie zu den Auswirkungen der Störung enthalten.

(3) Die Verpflichtung der Hersteller nach Absatz 1 und 2 beginnt spätestens ein Jahr nach Inkrafttreten des Gesetzes.“

17. In § 9 wird folgender Absatz 8 eingefügt:

„(8) Sind KRITIS-Kernkomponenten im Sinne von § 2 Absatz 13 durch Gesetze oder aufgrund eines Gesetzes einer Zertifizierung zu unterziehen, ist die Abgabe der Vertrauenswürdigkeitserklärung nach § 8 Absatz 6 Satz 3 Voraussetzung für die Zertifizierung.“

18. Nach § 9 wird folgender §9a eingefügt:

„§ 9a

Freiwilliges IT-Sicherheitskennzeichen

(1) Zur Umsetzung des Auftrages aus § 7 Absatz 1 Satz 1 Nummer 1a in Verbindung mit § 3 Absatz 1 Satz 2 Nummer 14 erteilt das Bundesamt nach Maßgabe einer Rechtsverordnung gemäß § 10 Absatz 2a (RVO IT-Sicherheitskennzeichen) für verschiedene Produktkategorien auf Antrag ein einheitliches IT-Sicherheitskennzeichen. Die umfassten Produktkategorien sind in der Rechtsverordnung nach § 10 Abs. 2a 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).

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 2a bestimmt.

(3) 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 2a bestimmt ist, mit. Die summarische Prüfung 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. Den weiteren Ablauf und die notwendigen Informationen regelt die Rechtsverordnung nach § 10 Absatz 2a.

(4) Das IT-Sicherheitskennzeichen ist körperlich mit dem jeweiligen Produkt oder mit dessen Umverpackung zu verbinden. Das IT-Sicherheitskennzeichen kann vom Hersteller oder Verkäufer 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 2a festzulegen.

(5) 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 2a erfüllen. 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 2 a entspricht.

(6) 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.

(7) Wird das IT-Sicherheitskennzeichen ohne Freigabe genutzt, kann das Bundesamt die Nutzung untersagen. Dem Hersteller ist vor einer Maßnahme nach Absatz 6 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.“

19. § 10 wird wie folgt geändert:

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

„(2a) 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 be-

troffenen 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 Anlagen oder Teilen davon ein besonderes öffentliches Interesse nach § 2 Absatz 14 Nummer 2 besteht und ob die Betreiber nach § 8f Nummer 2 den Pflichten der §§ 8a und 8b unterfallen.“

20. § 11 wird wie folgt gefasst:

„§ 11

Einschränkung von Grundrechten

Das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) wird durch die §§ 4a, 5, 5b, 5c und 5d Absatz 2 eingeschränkt. Das Grundrecht auf Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) wird durch § 4a eingeschränkt.“

21. § 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 in Verbindung mit einer Rechtsverordnung nach § 10 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 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine Registrierung nicht oder nicht rechtzeitig vornimmt oder eine Kontaktstelle nicht oder nicht rechtzeitig benennt,

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 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. 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 § 109 wird nach Absatz 2 folgender Absatz 2a eingefügt:

„Maßnahmen nach Absatz 2 Satz 2 umfassen auch den Einsatz von Systemen zur Angriffserkennung - nach Vorgaben des Bundesamtes für Sicherheit in der Informaitonstechnik. Details legt das Bundesamt in einer Technischen Richtlinie im Benehmen mit der Bundesnetzagentur fest. Die Diensteanbieter und das Bundesamt dürfen die hierzu erforderlichen Daten verarbeiten. Soweit erforderlich, dürfen Diensteanbieter und das Bundesamt insoweit Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis nach § 88 Absatz 2 unterliegen, für diesen Zweck verarbeiten. Daten, die für die Aufklärung des Angriffs, den Schutz der Informationstechnik und die Strafverfolgung der Angreifer erforderlich sind, haben die Diensteanbieter von sich aus und auf Anforderung den dazu zuständigen Behörden zu übermitteln. Die im Rahmen des Einsatzes von Systemen zur Angriffserkennung erhobenen Daten sind unverzüglich zu löschen, wenn sie nicht für die Vermeidung von Störungen im Sinne von Absatz 1 Satz 1 erforderlich sind. Die übrigen Daten dürfen nicht länger als zehn Jahre gespeichert werden. Hierzu muss die oder der Bundesbeauftrage für den Datenschutz und die Informationsfreiheit angehört werden. Die Diensteanbieter müssen der oder dem betrieblichen Datenschutzbeauftragten, dem Bundesamt für Sicherheit in der Informationstechnik, der Bundesnetzagentur und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am Ende eines Quartals detailliert über die Verfahren und Umstände von Maßnahmen nach Satz 1 in diesem Zeitraum schriftlich berichten.“

2. § 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) Stellt der Erbringer öffentlich zugänglicher Telekommunikationsdienste fest, dass die bei ihm gespeicherten Daten unrechtmäßig übermittelt worden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, so hat er hierüber unverzüglich das Bundeskriminalamt zu unterrichten.“

c) Nach Absatz 7 wird folgender Absatz 8 eingefügt:

„(8) Zur Abwehr von erheblichen 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 den Diensteanbietern anordnen, sofern diese dazu technisch in der Lage sind und es ihnen 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.“

3. Nach § 109a wird folgender § 109b eingefügt:

„§ 109b

Pflicht der Provider zur Meldung und Löschung

(1) Stellt der Erbringer öffentlich zugänglicher Telekommunikationsdienste fest, dass sein Dienst zur rechtswidrigen Weitergabe oder Veröffentlichung rechtswidrig erlangter Daten genutzt wird, so hat er unverzüglich das Bundeskriminalamt zu unterrichten.

(2) Liegen zureichende 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 Diensteerbringer im Sinne des Absatzes 1 zu sperren. Der betroffene Nutzer ist zu benachrichtigen. Sofern der betroffene Nutzer nach seiner Benachrichtigung innerhalb angemessener Frist widerspricht, hat der Diensteerbringer die Daten zu löschen. Die zuständigen Stellen können eine Sperrung oder Löschung 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 Diensteerbringer im Sinne des Absatzes 1 muss eine unverzügliche Bearbeitung der Anordnung nach Absatz 2 sicherstellen.“

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 er 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 § 149 Absatz 1 werden nach der Nummer 21c die folgenden Nummern 21d bis 21f 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 trifft, 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,

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

21i. entgegen § 109b Absatz 2 trotz Anordnung durch die zuständigen Stellen den Zugang zu den unrechtmäßig erlangten und veröffentlichten Daten nicht sperrt oder die Daten auf Anordnung nicht löscht.

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. In § 13 wird nach Absatz 7 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.“

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

„Stellt der Diensteanbieter fest, dass bei ihm gespeicherte Bestands- oder Nutzungsdaten unrechtmäßig übermittelt worden oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind, so hat er hierüber unverzüglich das Bundeskriminalamt zu unterrichten. Drohen aufgrund der unrechtmäßigen Kenntniserlangung der Daten nach Satz 1 schwerwiegende Beeinträchtigungen für die Rechte oder schutzwürdigen Interessen des betroffenen Nutzers, gilt § 42a des Bundesdatenschutzgesetzes entsprechend.“

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 hat er unverzüglich das Bundeskriminalamt zu unterrichten. § 109b Absatz 2 und 3 Telekommunikationsgesetzes gelten entsprechend.

(2) § 110 Absatz 1a des Telekommunikationsgesetzes gilt entsprechend.“

4. In § 16 Absatz 2 wird in Nummer 5 der Punkt durch ein Komma ersetzt und nach Nummer 5 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 des Strafgesetzbuchs

Das Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 14 des Gesetzes vom 18. Dezember 2018 (BGBl. I S. 2639) geändert worden ist, wird wie folgt geändert:

1. § 99 Absatz 2 wird wie folgt gefasst:

„(2) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von einem Jahr bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. fremde Geheimnisse, namentlich ein Betriebs- oder Geschäftsgeheimnis oder Tatsachen, Gegenstände oder Erkenntnisse, die von einer amtlichen Stelle oder auf deren Veranlassung geheim gehalten werden, mitteilt oder liefert und wenn er

2. eine verantwortliche Stellung missbraucht, die ihn zur Wahrung solcher Geheimnisse besonders verpflichtet, oder

3. in ein informationstechnisches System, in dem das Geheimnis gespeichert ist, eindringt oder

4. durch die Tat die Gefahr eines schweren Nachteils für die Bundesrepublik Deutschland herbeiführt, einschließlich der Vorbereitung derart schädigender Folgehandlungen.“

2. Nach § 126 wird folgender § 126a eingefügt:

„§ 126a

Zugänglichmachen von Leistungen zur Begehung von Straftaten

(1) Wer Dritten eine internetbasierte Leistung zugänglich macht, deren Zweck oder Tätigkeit darauf ausgerichtet ist, die Begehung von rechtswidrigen Taten zu ermöglichen, zu fördern oder zu erleichtern, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

(2) Die Strafe darf nicht schwerer sein, als die für die Tat im Sinne von Absatz 1 angedrohte Strafe.

(3) Mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren wird bestraft, wer die Tat gewerbsmäßig oder als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten im Sinne dieser Vorschrift verbunden hat, begeht.

(4) Absatz 1 gilt nicht für Handlungen

1. wenn die Begehung von Straftaten nur einen Zweck oder eine Tätigkeit von untergeordneter Bedeutung darstellt, oder

2. die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Dazu gehören insbesondere beruflichen Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 der Strafprozessordnung genannten Personen.“

3. Die §§ 202a, 202b, 202c, 202d, 303a, 303b werden jeweils wie folgt geändert:

In § 202a Absatz 1 werden die Wörter „bis zu drei Jahren“ durch die Wörter „bis zu fünf Jahren“ ersetzt.

In § 202b Absatz 1 werden die Wörter „bis zu zwei Jahren“ durch die Wörter „bis zu fünf Jahren“ ersetzt.

In § 202c Absatz 1 werden die Wörter „bis zu zwei Jahren“ durch die Wörter „bis zu fünf Jahren“ ersetzt.

In § 202d Absatz 1 werden die Wörter „bis zu drei Jahren“ durch die Wörter „bis zu fünf Jahren“ ersetzt.

In § 303a Absatz 1 werden die Wörter „bis zu zwei Jahren“ durch die Wörter „bis zu fünf Jahren“ ersetzt.

In § 303b Absatz 1 werden die Wörter „bis zu drei Jahren“ durch die Wörter „bis zu fünf Jahren“ ersetzt.

In § 303b Absatz 2 werden die Wörter „bis zu fünf Jahren oder Geldstrafe“ durch die Wörter „von sechs Monaten bis zu fünf Jahren“ ersetzt.

4. Nach § 202d werden folgende §§ 202e und 202f eingefügt:

„§ 200e

Unbefugte Nutzung informationstechnischer Systeme

(1) Wer unbefugt

1. sich oder einem Dritten den Zugang zu einem informationstechnischen System verschafft,

2. ein informationstechnisches System in Gebrauch nimmt oder

3. einen Datenverarbeitungsvorgang oder einen informationstechnischen Ablauf auf einem informationstechnischen System beeinflusst oder in Gang setzt,

wird mit Geldstrafe oder Freiheitsstrafe bis zu einem Jahr bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist. Die Tat nach Satz 1 ist nur strafbar, wenn sie geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen.

(2) Der Versuch ist strafbar.

(3) Im Sinne dieser Vorschrift ist informationstechnisches System nur ein solches, das

1. zur Verarbeitung personenbezogener Daten geeignet oder bestimmt ist oder

2. Teil einer Einrichtung oder Anlage ist, die wirtschaftlichen, öffentlichen, wissenschaftlichen, künstlerischen, gemeinnützigen oder sportlichen Zwecken dient oder die den Bereichen Energie, Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung, Versorgung, Haustechnik oder Haushaltstechnik angehört;

(5) Ist ein Angehöriger, der Vormund oder der Betreuer verletzt oder lebt der Verletzte mit dem Täter in häuslicher Gemeinschaft, so wird die Tat nur auf Antrag verfolgt.

§202f

Besonders schwerer Fall einer Straftat gegen die Vertraulichkeit oder Integrität informationstechnischer Systeme

(1) Mit Freiheitsstrafe von sechs Monaten bis zu zehn Jahren wird bestraft, wer

1. eine Tat nach den §§ 202a bis 202e

   a) für eine fremde Macht,

   b) gewerbsmäßig oder

   c) als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach den §§ 202a, 202b, 202c, 202d, 202e StGB verbunden hat, begeht,

2. sich bei einer Tat nach § 202e den Zugang zu einer großen Anzahl von informationstechnischen Systemen verschafft oder eine große Anzahl von informationstechnischen Systemen in Gebrauch nimmt oder eine große Anzahl von Daten-

verarbeitungsvorgängen oder informationstechnischen Abläufen beeinflusst oder in Gang setzt oder

3. bei einer Tat nach den §§ 202a bis 202d in der Absicht handelt,

   a) eine Gefahr für die öffentliche Sicherheit,

   b) eine gemeingefährliche Straftat oder

   c) eine besonders schwere Straftat gegen die Umwelt nach § 330 herbeizuführen oder zu ermöglichen.

(2) Handelt der Täter einer Tat nach den §§ 202a bis 202e in der Absicht, einen Aus-fall oder eine wesentliche Beeinträchtigung der Funktionsfähigkeit kritischer Infrastrukturen zu bewirken, so wird er mit Freiheitsstrafe nicht unter einem Jahr bestraft. Eine kritische Infrastruktur im Sinne dieser Vorschrift ist eine Einrichtung, Anlage oder Teile davon im Sinne von § 2 Absatz 10 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik.

(3) Ebenso wird bestraft, wer

1. sich in den Fällen des § 202a, b und d Daten, die den Kernbereich der privaten Lebensgestaltung einer anderen Person betreffen, in der Absicht verschafft, diese in einer Weise zu verbreiten oder der Öffentlichkeit zugänglich zu machen, die geeignet ist, dem Betroffenen erhebliche Nachteile zuzufügen.

2. eine Tat nach den §§ 202a bis 202e als Mitglied einer Bande, die sich zur fortgesetzten Begehung von Straftaten nach diesen Vorschriften verbunden hat, gewerbsmäßig begeht.

(4) In minder schweren Fällen der Absätze 2 und 3 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren.

(5) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von einem Jahr bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. fremde Geheimnisse, namentlich ein Betriebs- oder Geschäftsgeheimnis oder Tatsachen, Gegenstände oder Erkenntnisse, die von einer amtlichen Stelle oder auf deren Veranlassung geheimgehalten werden, mitteilt oder liefert und wenn er

2. eine verantwortliche Stellung missbraucht, die ihn zur Wahrung solcher Geheimnisse besonders verpflichtet, oder

3. in ein informationstechnisches System, in dem das Geheimnis gespeichert ist, eindringt oder

4. durch die Tat die Gefahr eines schweren Nachteils für die Bundesrepublik Deutschland herbeiführt, einschließlich der Vorbereitung derart schädigender Folgehandlungen.“

Artikel 5

Änderung der Strafprozessordnung

Die Strafprozessordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 12 des Gesetzes vom 18. Dezember 2018 (BGBl. I S. 2639) geändert worden ist, wird wie folgt geändert.

1. § 100a Absatz 2 Nummer 1 wird wie folgt geändert:

   a) Nach Buchstabe a wird eine weitere Aufzählung eingefügt:

   „Zugänglichmachen von Leistungen zur Begehung von Straftaten nach § 126a“

   b) Nach Buchstabe g wird eine weitere Aufzählung eingefügt:

   „Straftaten gegen die Vertraulichkeit oder Integrität informationstechnischer Systeme nach §§ 202a, 202b, 202c, 202d, 202e, 202f Absatz 2 und 3, §§ 303a, 303b.“

2. § 100b Absatz 2 Nummer 1 wird wie folgt geändert:

   a) Nach Buchstabe a wird eine weitere Aufzählung eingefügt:

   „Zugänglichmachen von Leistungen zur Begehung von Straftaten nach § 126a Absatz 3“

   b) Nach Buchstabe e wird eine weitere Aufzählung eingefügt:

   „Straftaten gegen die Vertraulichkeit oder Integrität informationstechnischer Systeme nach § 202f Absatz 2 und 3.“

3. § 100g Absatz 2 Satz 2 Nummer 1 wird wie folgt geändert:

   a) Nach Buchstabe a wird eine neue Aufzählung eingefügt:

   „Zugänglichmachen von Leistungen zur Begehung von Straftaten nach § 126a Absatz 3“

   b) Nach Buchstabe d wird eine neue Aufzählung eingefügt:

   „Straftaten gegen die Vertraulichkeit oder Integrität informationstechnischer Systeme nach § 202f Absatz 2 und 3.“

4. Nach § 163f wird folgender § 163g eingefügt:

„§ 163g

Begründen bestimmte Tatsachen den Verdacht, dass jemand Täter oder Teilnehmer einer Straftat im Sinne von § 100g Absatz 1 StPO ist, so dürfen die Staatsanwaltschaft sowie die Behörden und Beamten des Polizeidienstes auch gegen den Willen des Inhabers auf Nutzerkonten oder Funktionen, die ein Anbieter eines Telekommunikations- oder Telemediendienstes dem Verdächtigen zur Verfügung stellt und mittels derer der Verdächtige im Rahmen der Nutzung des Telekommunikations-

oder Telemediendienstes eine dauerhafte virtuelle Identität unterhält, zugreifen. Sie dürfen unter dieser virtuellen Identität mit Dritten in Kontakt treten. Der Verdächtige ist verpflichtet, die zur Nutzung der virtuellen Identität erforderlichen Zugangsdaten herauszugeben. § 95 Absatz 2 gilt entsprechend mit der Maßgabe, dass die Zugangsdaten auch herauszugeben sind, wenn sie geeignet sind, eine Verfolgung wegen einer Straftat oder einer Ordnungswidrigkeit herbeizuführen. Jedoch dürfen die durch Nutzung der Zugangsdaten gewonnenen Erkenntnisse in einem Strafverfahren oder in einem Verfahren nach dem Gesetz über Ordnungswidrigkeiten gegen den Verdächtigen oder einen in § 52 Absatz 1 der Strafprozessordnung bezeichneten Angehörigen des Verdächtigen nur mit Zustimmung des Verdächtigen verwendet werden."

Artikel 6

Änderung des Gesetzes über die internationale Rechtshilfe in Strafsachen

An § 67 des Gesetzes über die internationale Rechtshilfe in Strafsachen in der Fassung der Bekanntmachung vom 27. Juni 1994 (BGBl. I S. 1537), das zuletzt durch Artikel 3 des Gesetzes vom 27. August 2017 (BGBl. I S. 3295) geändert worden ist, wird folgender Absatz 5 angefügt:

„(5) Auch schon vor Eingang des Ersuchens um Herausgabe können die Staatsanwaltschaft sowie die Behörden und Beamten des Polizeidienstes anordnen, dass der Sicherstellung oder Beschlagnahme nach § 67 Absatz 1 unterliegende oder nach § 100g Absatz 1 oder Absatz 2 StPO, § 100j StPO, oder §§ 161, 163 StPO, 14, 15 TMG zu erhebende Daten bei dem Anbieter von Telekommunikation- oder Telemediendiensten für höchstens 180 Tage vor Veränderungen geschützt gespeichert und verwahrt werden müssen. Der Zeitraum der Speicherung bei dem Anbieter kann einmal um weitere 180 Tage verlängert werden. Die Herausgabe und die Benachrichtigung des Nutzers darf nur nach Maßgabe der allgemeinen Vorschriften erfolgen."

Artikel 7

Änderung des Justizvergütungs- und -entschädigungsgesetzes

Das Justizvergütungs- und -entschädigungsgesetz vom 5. Mai 2004 (BGBl. I S. 718, 776), das zuletzt durch Artikel 5 Absatz 2 des Gesetzes vom 11. Oktober 2016 (BGBl. I S. 2222) geändert worden ist, wird wie folgt geändert:

Der Anlage 3 (zu § 23 Absatz 1) wird in Abschnitt 4 folgende Nummer 403 angefügt:

„403. Vorabsicherung gemäß § 67 des Gesetzes über die internationale Rechtshilfe in Strafsachen: je Tag der tatsächlich erfolgten Vorabsicherung … 0,35 EURO, mindestens jedoch 35,00 EURO"

Artikel 8

Änderung des Artikel 10-Gesetzes

In § 3 Absatz 1 Satz 1 Nummer 8 des Artikel 10-Gesetzes vom 26. Juni 2001 (BGBl. I S. 1254, 2298), das zuletzt durch Artikel 12 des Gesetzes vom 14. August 2017 (BGBl. I S. 3202) geändert worden ist, wird nach der Angabe „202b“ ein Komma und die Angabe „202f“ eingefügt.

Artikel 9

Änderung des Bundeskriminalamtsgesetzes

In § 4 Absatz 1 Nummer 5 des Bundeskriminalamtsgesetzes vom 1. Juni 2017 (BGBl. I S. 1354) wird nach der Angabe „202c“ ein Komma und die Angabe „202e, 202f,“ eingefügt.

Artikel 10

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 „KRITIS-Kernkomponenten nach § 2 Absatz 13 des BSI-Gesetzes in der jeweils geltenden Fassung“ ersetzt.

2. Satz 3 wird gestrichen.

Artikel 11

Inkrafttreten

Dieses Gesetz tritt am Tag nach seiner Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

In der vergangenen Legislaturperiode wurden bereits mehrere Vorhaben zur Erhöhung der IT-Sicherheit umgesetzt. Insbesondere wurde im Jahr 2015 das erste Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) verkündet. Dies wurde durch die BSI-Kritis-Verordnung und die Umsetzung der EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen (NIS-Richtlinie) ergänzt.

Cyber-Sicherheit ist jedoch niemals statisch. Ein ausreichendes Schutzniveau heute ist kein Garant für adäquate Schutzmechanismen und eine erfolgreiche Abwehr der Angriffe von morgen. Eine ständige Anpassung und Weiterentwicklung der Abwehrstrategien ist erforderlich. Entsprechend dem Koalitionsvertrag zwischen CDU, CSU und SPD, Zeile 1969 f., wird daher das IT-Sicherheitsgesetz fortgeschrieben und der Ordnungsrahmen erweitert, um den 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 Bedrohungslage betrifft die Gesellschaft bzw. den Bürger selbst, den Staat und auch die Wirtschaft. Daher verfolgt das Gesetz einen ganzheitlichen Ansatz und enthält Maßnahmen zum Schutz all dieser Adressaten. Wesentlicher Akteur hierfür ist das BSI. Entsprechend dem Koalitionsvertrag zwischen CDU, CSU und SPD, Zeile 6004, wird die Rolle des BSI gestärkt.

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

Zur Begegnung von Cyber-Sicherheitsvorfällen insgesamt werden die Befugnisse des BSI zum Schutz der Bundesverwaltung und der Gesellschaft ausgeweitet. Auch werden Möglichkeiten zur Unterstützung der Länder durch das BSI geschaffen, da die Bedrohungen des Cyber-Raums unabhängig von Ländergrenzen bestehen.

Außerdem werden die für die Betreiber Kritischer Infrastruktur bestehenden Meldepflichten und Verpflichtungen der Mindeststandards auf weitere Teile der Wirtschaft ausgeweitet. Hierbei geht es um diejenigen Teile, an welchen ein besonderes öffentliches Interesse besteht bzw. bei deren Beeinträchtigung ein Grundinteresse der Gesellschaft gefährdet

würde. Hierdurch 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 im Telekommunikationsgesetz (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 (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 länderübergreifende Wirtschaftstätigkeit zur Folge hätten. Internationale Abkommen zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten setzen voraus, dass in jedem Staat nur eine einzige 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 in 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]

4. Erfüllungsaufwand

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

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

Die BDBOS ist verantwortlich für die Kommunikationswege des Bundes. 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 864 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 55,5 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 rund 47,5 Mio. Euro zu berücksichtigen.

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

Infolge des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl 2015, Teil I Nr. 31, S. 1324) und dem Gesetz zur 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 (EURL2016/1148UmsG) erhielt das BSI Ressourcen als zentrale Anlaufstelle für Betreiber Kritischer Infrastrukturen und Nationale Cyber-Sicherheitsbehörde.

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

- Die in § 2 Absatz 13 BSIG eingefügte Ergänzung bezüglich der Zertifizierung der Komponenten für das neue Mobilfunknetz (5G) führt zu einem erhöhten Personalbedarf von 168 Stellen.

- Mit den neuen Aufgaben des BSI zur Förderung des Verbraucherschutzes und der Verbraucherinformation trägt das Gesetz dem Umstand Rechnung, dass die 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 der Verbraucherinnen und Verbraucher 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 169 Planstellen.

- In diesem Kontext kommen auch die Änderungen in § 3 Abs. 1 Satz 2 Nr. 14 sowie § 7 Abs. 1d, sprich die erweiterte Informationsaufgabe und Warnbefugnis im Hinblick auf Produkte zum Tragen, die den Aktivitäten des BSI größere Wirkung verschaffen wird. 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 12 Planstellen 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 im § 3 Abs. 1 Satz 2 Nr. 19 „Pflege und Weiterentwicklung sicherer Identitäten“ alte Ansätze fortzuentwickeln sowie ganz neue Ansätze zu entwickeln, die zur breiten Anwendung kommen. Hierfür benötigt das BSI 8 Planstellen

- § 4a 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. Diese neue Aufgabe des BSI führt zu einem Personalbedarf von 64 Planstellen.

- § 4b Meldestelle. Die Sammlung von Informationen über Sicherheitslücken, Schadprogrammen 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 existierenden Meldestelle beim Bundesamt zwingend erforderlich. Der organisatorische, rechtliche und technische Ausbau sowie die kontinuierliche Beobachtung, Entgegennahme sowie Auswertung und Analyse der Meldungen führt zu einem zusätzlichen Personalbedarf von 14 Planstellen.

- § 5 Abs. 11: Die Bedrohungslage für die Kommunikationstechnik des Bundes ist quantitativ und qualitativ gestiegenen. Um der gestiegenen Gefahr eine effektive Abwehr entgegenzusetzen, muss das Bundesamt personell verstärkt werden. Die aktuell im Bundesamt zur Verfügung stehenden Personalressourcen ermöglichen nicht, die erforderlichen Detektionsmaßnahmen bei allen Behörden des Bundes in ausreichender Form zum Einsatz zu bringen. Neben der mit gem. Gesetz adressierten gestiegenen Gefahrenlage für die Kommunikationstechnik des Bundes erweitert das Gesetz auch die Möglichkeiten des Bundesamtes in Bezug auf eine Unterstützung der Länder. Um eine angemessene Abwehr von Gefahren für die Kommunikationstechnik des Bundes zu erhalten und die neuen Aufgaben bei der Unterstützung der Länder zu erfüllen, benötigt das Bundesamt zusätzliche 29 Planstellen.

- § 5a: Neben der Analyse von Protokolldaten i.S.d. BSIG ist die Auswertung von behördeninternen Protokollierungsdaten ein wesentlicher Bestandteil einer umfassenden Abwehr von Gefahren für die Sicherheit der Informationstechnik. Die geplante Änderung am BSIG erlaubt es dem BSI auf gesetzlicher Grundlage, nun auch behördeninterne Protokollierungsereignisse von vor allem IT-Systemen auszuwerten. Hieraus ergibt sich, dass nun in einem sehr viel größeren Maßstab auch Behörden, die noch nicht durch die 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. Für die Detektion von Cyber-Angriffen durch eine systematische Analyse dieser Daten ist ein Aufwuchs des Bundesamtes um 29 Planstellen zu realisieren.

- In der heutigen Bedrohungslage sind präventive Schutz- und Abwehrmaßnahmen alleine nicht mehr ausreichend. Längst ist klar, dass Angriffe auch bei bestmöglicher Prävention erfolgreich sein werden, 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 oder die Betreiber Kritischer Infrastrukturen) bei der Bewältigung von Sicherheitsvorfällen unterstützen. Die Erfahrung nach der Einrichtung dieser MIRTs hat gezeigt, dass auch die Länder in diesem Bereich einen erheblichen Unterstützungsbedarf haben. Um eine regelmäßige Unterstützung durch das Bundesamt zu ermöglichen, wird durch dieses Gesetz die Betroffenheit eines Landes von einem IT-Sicherheitsvorfall als Einsatz-Regelfall festgelegt. Durch die damit einhergehende Erweiterung des Adressatenkreises entsteht für das Bundesamt ein personeller Mehrbedarf von 41 Planstellen.

- § 5c, § 8b Abs. 2: Kommt es bei Betreibern Kritischer Infrastrukturen oder bei weiterer Anlagen 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 Krisenreaktionspläne zu erarbeiten sowie eine solche Struktur zwischen Bundesbehörden und den KRITIS-Betreibern aufzubauen, zu pflegen und zu betreiben, sind beim Bundesamt 44 Planstellen/Stellen erforderlich.

- § 5d 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 Verwaltungsaufwand von 2 Planstellen.

- Das Bundesamt muss in der Lage sein, technische Untersuchungen nach § 7a BSIG zur Erfüllung aller seiner gesetzlichen Aufgaben durchzuführen. Dies wird durch dieses Gesetz ermöglicht. Zudem wir das Bundesamt mit weitergehenden 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.

- § 7c: 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 Bundesamt 10 Planstellen.

- Um Detektionsmaßnahmen zum besonderen Schutz von Mitgliedern der Verfassungsorgane durchzuführen und hierdurch das BKA zu unterstützen, entsteht dem Bundesamt zudem ein Personalbedarf von zusätzlichen 2 Planstellen.

- Die Vielzahl von Digitalisierungsvorhaben der Bundesregierung erfordert eine konstante Beratung und Begleitung durch das Bundesamt, um bereits ab der Konzeptions- und Planungsphase die Aspekte der IT-Sicherheit in angemessener Weise zu berücksichtigen. Daher ist das Bundesamt durch die jeweils zuständige Stelle frühzeitig bei der Planung und Umsetzung der neuen Digitalisierungsvorhaben des Bundes zu beteiligen. Angesichts der Vielzahl der anstehenden Digitalisierungsprojekte beläuft sich der hierdurch entstehende Beratungsaufwand auf einen Bedarf von 71 Planstellen/Stellen.

- Durch die Erweiterung der KRITIS-Regelungen und die damit verbundene Aufnahme weiterer Branchen in den Regelungsbereich des Gesetzes sowie die Ergänzung des BSIG um den Bereich der Infrastrukturen im besonderen öffentlichen Interesse und die Möglichkeit, bestimmten Betreiben im Einzelfall Pflichten nach §§ 8a und 8b BSGI aufzuerlegen, wenn eine Störung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse dieses Unternehmens zu einer tatsächlichen und hinreichend schweren Gefährdung für ein Grundinteresse der Gesellschaft führen würde, führt zu einem personellen Mehrbedarf des Bundesamtes von insgesamt 56 Planstellen.

- 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. Das IT-Sicherheitskennzeichen des Bundesamts wird es Verbraucherinnen und Verbrauchern ermöglichen, schnell und einfach zu überprüfen, ob das jeweilige IT-Produkt bzw. dessen Hersteller aktuelle Sicherheitsstandards in ausreichender Form berücksichtigt. Um die für die Vergabe des IT-Sicherheitskennzeichens erforderlichen Arbeiten inkl. der im Sinne einer Marktaufsicht anstehenden Prüfungen und Kontrollen durchführen zu können, benötigt das Bundesamt 25 zusätzliche Planstellen.

- Die Erweiterung der Bußgeldvorschriften führt zu einem erhöhten Prüfungs- und Verwaltungsaufwand. Das Bundesamt benötigt zur Bewältigung dieses zusätzlichen Aufwandes 2 weitere 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 nicht vorgesehen, da nach Artikel 10 des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 ohnehin eine Evaluierung durchgeführt wird, in welche die Erfahrungen aus diesem Gesetzesentwurf einfließen können.

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 der Definition zur Kommunikationstechnik des Bundes umfasst bisher nicht die behördeninterne Kommunikation oder den behördeninternen Datenaustausch. Genauso wenig werden allgemeine Datenverarbeitungsvorgänge erfasst. Gerade diese Bereiche sind jedoch, genauso wie die Informationstechnik zur Kommunikation und der Datenaustausch der Behördenuntereinander oder mit Dritten, gleichermaßen Ziele für Angriffe, welche wiederum auch Angriffe auf die eigentlichen Kommunikationssysteme ermöglichen. Durch die Einbeziehung dieser Bereiche steigt das Sicherheitsniveau insgesamt, da mehr Detektionsmöglichkeiten geschaffen werden. Andernfalls ist insbesondere die Detektion von zielgerichteten und nachrichtendienstlichen Angriffen nur schwer möglich. Der Begriff der Datenverarbeitung ist hierbei i.S.d DSGVO weit zu verstehen. Der Datenaustausch bleibt weiterhin umfasst.

Kommunikationstechnik, die im Rahmen des Digitalfunk 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 später nicht mehr verwendet und wird daher gestrichen. An dieser Stelle wird der Begriff der Protokollierungsdaten zur Wahrnehmung der neu geschaffenen Befugnis in § 5a legaldefiniert.

Protokollierungsdaten sind technische Ereignisse und Zustände innerhalb eines IT-Systems, die tatsächliche Anhaltspunkte über die Betroffenheit des Bundes liefern können. 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 Cyber-Angriffe erkennen, welche alle sonstigen Sicherheitsmaßnahmen umgangen haben.

Zu Buchstabe c

IT-Produkte sind möglichst weitgehend zu definieren, da sich Sicherheitslücken auf Grund der verschiedensten Komponenten der Produkte ergeben können. Relevant sind sowohl die Hardware an sich als auch die eingesetzte Software, welche das Funktionieren der Hardware erst bedingt. Daneben können auch alleinstehende Softwareprodukte, welche unabhängig von der Hardware vertrieben und betrieben werden, Sicherheitslücken aufweisen.

Zu Buchstabe d

Die Regelung ergänzt die klassischen KRITIS-Sektoren nach Absatz 10 um den Sektor Entsorgung. Die 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 der 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 Absatz 10 und die Digitalen Dienste in Absatz 11.

Absatz 13 definiert die Kernkomponenten für Kritische Infrastrukturen (KRITIS-Kernkomponenten). Diese sind IT-Produkte, die zum Betrieb von Kritischen Infrastrukturen im Sinne dieses Gesetzes dienen und für diesen Zweck besonders entwickelt oder geändert werden. Die Konkretisierung ist notwendig, um einen Gleichlauf zu den im Sicherheitskatalog nach § 109 Absatz 6 TKG zu definierenden speziellen KRITIS- Kernkomponenten für den Bereich der öffentlichen Telekommunikationsnetze herzustellen.

Absatz 14 regelt die Infrastrukturen im besonderen öffentlichen Interesse. Zu diesen gehören zu den Unternehmen mit Zulassung zum Teilbereich des regulierten Marktes mit weiteren Zulassungsfolgepflichten (Prime Standard) nach § 48 Börsenordnung der Frankfurter Wertpapierbörse, sowie Infrastrukturen aus den Bereichen Chemie, Automobilherstellung, Rüstung und Kultur und Medien. Obwohl diese im Sinne dieses Gesetzes keine Kritischen Infrastrukturen im engeren Sinne des Absatzes 10 sind, stellt ihre Funktionsfähigkeit aus anderen Gründen ein erhebliches Interesse für die Gesellschaft dar

Hier kommt dem Sektor Kultur und Medien eine besondere Bedeutung zu. Die Pressefreiheit, die Freiheit der Berichterstattung und die Pluralität der Medien sind Fundament der freiheitlich demokratischen Grundordnung der Bundesrepublik Deutschland und stehen daher unter dem besonderen Schutz des Grundgesetzes. Der Medienbereich sieht sich erhöhtem Druck auf die eigene Unabhängigkeit durch Versuche ausländischer Beeinflussung im Rahmen vielgestaltiger, hybrider Bedrohungen ausgesetzt. Dazu zählt insbesondere die Nutzung von deutschen Medienorganen, die (teilweise) durch ausländische Investoren übernommen werden, für Zwecke der Desinformation. Eine Einflussnahme auf bzw. die Einschränkung der Pressefreiheit, die Freiheit der Berichterstattung und die Pluralität der Medien kann negative Auswirkungen auf die Gesellschaft und die Regierung haben und die freiheitlich demokratische Grundordnung der Bundesrepublik Deutschland gefährden. Die Klassifizierung bestimmter Unternehmen der Medienbranche als besonders sicherheitsrelevante Unternehmen ist daher angezeigt. Da die Erfassung von Unternehmen aus dem Bereich Kultur und Medien in diesem Gesetz vornehmlich aus Gründen der öffentlichen Sicherheit erfolgt, ist die Zuordnung von Kultur und Medien zu den klassischen Kritischen Infrastrukturen z. B. in der KRITIS-Strategie der Bundesregierung hiervon unbeschadet. Denn die Zuordnung in der KRITIS-Strategie stellt nicht auf Belange der öffentlichen Sicherheit, sondern ausschließlich auf Versorgungsaspekte ab.

An dem Sektor Rüstung besteht kraft Natur der Sache ein besonderes öffentliches Interesse. Dies wird auch an verschiedenen Stellen in Gesetzen deutlich, so insbesondere in § 5 AWG. Entsprechend werden solche Unternehmen erfasst, die in § 60 Absatz 1 der Außenwirtschaftsverordnung gelistet sind.

An den Unternehmen mit Zulassung zum Teilbereich des regulierten Marktes mit weiteren Zulassungsfolgepflichten (Prime Standard) nach § 48 Börsenordnung der Frankfurter Wertpapierbörse besteht wegen der volkswirtschaftlichen Bedeutung ein besonderes öffentliches Interesse.

Wie im Fall der Kritischen Infrastrukturen wird eine Rechtsverordnung die weiteren Infrastrukturen 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 § 5a ist erforderlich, da im Rahmen einer Novelle des Akkreditierungsstellengesetzes eine Bereichsausnahme für die Akkreditierung von Prüfstellen im Bereich der IT-Sicherheit implementiert wurde. Danach kann eine Prüfstelle im Bereich der IT-Sicherheit zukünftig nur dann tätig werden, wenn das BSI hierfür seine Befugnis erteilt hat („rechtliches Dürfen“). Das Verfahren der Erteilung der Befugnis, insbesondere das Verhältnis des BSI zur Deutschen Akkreditierungsstelle (DAkks) bedarf einer Regelung im BSI-Gesetz.

Daraus folgt auch die Klarstellung, dass Gutachten und Überprüfungen nach § 2 Absatz 3 Satz 2 und 3 AkkStelleG nach den Grundsätzen der Befugnis erteilenden Behörde (BeB) erfolgen und das BSI als solche nicht an Weisungen der DAkkS gebunden ist, auch wenn der Wortlaut des § 2 Absatz 3 Satz 2 und 3 AkkStelleG ("Die Akkreditierungsstelle lässt Begutachtungen durch die BeB ...ausführen"; "Die Akkreditierungsstelle bedient sich" der BeB") dies vermuten ließe. Dieser Wortlaut ist insofern irreführend.

Zu Buchstabe c

Die Anpassung dient der Klarstellung, dass gerade im Zusammenhang mit dem Verbraucherschutz Aufgabe des BSI auch die Information der genannten Adressaten ist. Ferner wird klargestellt, dass der letzte Halbsatz in Nummer 14 keine Einschränkung der Aufgaben des BSI darstellt.

Zu Buchstabe d

Mit der Regelung wird das Vorhaben des Koalitionsvertrags der 19. Legislaturperiode umgesetzt, den Verbraucherschutz als zusätzliche Aufgabe des BSI zu etablieren. Die ausdrückliche Aufnahme des Verbraucherschutzes in den Aufgabenkatalog des § 3 trägt die 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 stärkt zugleich die Sichtbarkeit des BSI als bürger- und verbraucherorientierte nationale Cybersicherheitsbehörde.

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 in Fragen der Sicherheit in der Informationstechnik zu beraten, zu warnen und zu sensibilisieren. Hierzu stehen dem BSI insbesondere die Befugnisse der §§ 7, 7a zur Warnung, Empfehlung und Untersuchung auf dem Markt bereitgestellter oder zur Bereitstellung vorgesehener informationstechnischer Produkte und Systeme zur Verfügung.

Der Verweis in Nummer 14a auf § 3 Absatz 1 Satz 2 Nummer 14 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 zielgruppen-

spezifisch auf die Belange der Verbraucherinnen und Verbraucher bzw. 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 (Facebook, Whatsapp, …), Streaming-Dienste (Spotify, Netflix, …), Cloud-Dienste (Dropbox, Onedrive, ...), IoT (Alexa, GoogleHome, Smart Home, …), Hardware-Konsumentenprodukte (Smartphone, Smart-TV, …) oder PC-Hardware (Chips, Grafikkarten, …).

Ein ganzheitlicher 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 durch Nummer 14a vorgesehene 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. Im Gegensatz zu den Verbraucherschutzverbänden ist das BSI jedoch keine Organisation zur Vertretung und Durchsetzung ausschließlich 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 IT-Sicherheit sollte 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 IT-Sicherheit 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 und Pflege 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 Verbraucher“. Durch Sicherheitstests und -analysen von auf dem Markt bereitgestellten IT-Produkten und Systemen kann das BSI zum einen seinen technischen Wissensstand in Bezug auf Funktionalitäten erweitern und aktuelle IT-Sicherheitsrisiken für Verbraucher identifizieren. Zum anderen können Sicherheitstests und -analysen auch zur stichprobenartigen Überprüfung bezüglich einer Einhaltung der Anforderungen nach dem zuvor definierten Stand der Technik dienen.

Stärkung der Sensibilisierung und „Awareness“ der Verbraucher. Um das Problembewusstsein und die Aufmerksamkeit für die Belange der Informationssicherheit zu erhöhen, intensiviert das BSI seine Beratungs- und Unterstützungsangebote im Rahmen einer zielgruppenspezifischen Sensibilisierungskampagne für Verbraucher. 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 Verbraucher auf die 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 zum Verbraucher.

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

Angebot eines IT-Sicherheits-Kennzeichens für verbrauchernahe Produkte und Dienste zur Erhöhung der Verbrauchertransparenz und zur Förderung der Sicherheit in der Informationstechnik im Bereich von Verbraucherprodukten und -diensten. Das Angebot eines Kennzeichens für IT-Sicherheit kann Verbrauchern die Auswahl eines IT-Systems oder Online-Dienstes erleichtern, indem für sie auf einen Blick feststellbar ist, welches System oder welcher Dienst ein konkretes 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 von fremden Projekten zum Verbraucherschutz im Bereich IT-Sicherheit (Zuwendung) und Durchführung von eigenen Forschungsprojekten zum Verbraucherschutz im Bereich IT-Sicherheit.

Zu Buchstabe e

Nach §§ 8d bis 8f werden bestehende Pflichten zur Einhaltung von Mindeststandards und Meldung von Störungen auf weitere Teile der Wirtschaft ausgeweitet. In der Folge sind auch die Aufgaben des BSI anzupassen.

Zu Buchstabe f

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

Zu Buchstabe g

Mit der neu eingefügten Nummer19 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 Be-

wertung 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 Nr. 19 stellt daher sicher, dass das gesetzgeberische Ziel bestmöglich erreicht wird.

Mit der neu eingefügten Aufgabe in Nummer 20 wird die Zuständigkeit des BSI für die Entwicklung von Anforderungen 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 4

Es handelt sich hierbei lediglich um eine Klarstellung. Der Begründung des § 4 in BT-Drs. 18/4096, 28. ist zu entnehmen, dass bei der Konzeption der Regelung 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 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 5

Zu § 4a

Die Regelung in § 4a dient der Stärkung der Rolle des Bundesamtes und gleichzeitig der Gewährleistung eines hohen Sicherheitsniveaus. Dies ist auch im Koalitionsvertrag, z.B. Zeile 6029, vorgesehen. Die Verwirklichung der besonders hohen Sicherheitsanforderungen an die 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 über das aktuelle 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. Bund und Länder können vereinbaren inwieweit das Bundesamt die Befugnisse in den Ländern ausüben kann (Art. 91c Abs. 1 GG).

Das Bundesamt wird neben der jeweils überprüften Stelle 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

Die Vorschrift ergänzt die Regelungen aus § 4 BSIG (Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes) und § 8b BSIG (Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen). Im Rahmen seiner Aufgabe als zentrale Meldestelle für Informationstechnik soll das BSI 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 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 fehlt bislang eine ausdrückliche Rechtsgrundlage, die mit § 4b geschaffen werden soll. Entsprechend legt die Norm klar den Zweck der Datenübermittlung fest. Gleichzeitig sind Dritte nach § 4b nicht dazu verpflichtet, dem BSI entsprechende Informationen zu übermitteln. Ihre Meldungen bzw. ihre Zusammenarbeit mit dem BSI erfolgt ausschließlich auf freiwilliger Basis. Ausdrücklich sollen anonyme Meldungen möglich sein. Hierdurch sollen insbesondere Hemmschwellen seitens Einzelpersonen gesenkt werden, die möglicherweise Bedenken haben, sich einer staatlichen Stelle anzuvertrauen.

Das BSI wird hierzu die notwendigen Meldemöglichkeiten aufbauen. Bei der Zusammenarbeit mit Dritten aus der Wirtschaft dürfte es hierbei sinnvoll sein, auf etablierte Melde- und Austauschmöglichkeiten wie MISP (Malware Information Sharing Plattform) zu setzen, die über datenschutzgerechte Rollen- und Rechtekonzepte verfügen. Hierdurch wird eine genaue Kontrolle im Hinblick auf Art, Umfang und Adressaten der übermittelten Daten erreicht. Gegenüber privaten Dritten kann sich der Betrieb einer anonymen Meldemöglichkeit, wie sie zum Beispiel vom Bundeskartellamt betrieben wird, anbieten.

Absatz 3 regelt die Weitergabe von Informationen zur Aufgabenwahrnehmung; die Regelung eröffnet die Möglichkeit, dass das Bundesamt andere Bundesbehörden, Dritte und die Öffentlichkeit über mögliche Gefahren der Cyber- und Informationssicherheit informieren kann, beispielsweise zum Zweck der Schadensverhinderung oder -verringerung.

Absatz 4 Satz 3 führt einen Schutz zugunsten Dritter ein, die dem BSI Informationen übermitteln. Bestehende gesetzliche Übermittlungsregelungen bleiben hiervon unberührt. Damit wird die Übermittlungsbefugnis nach Satz 1, also für die Aufgabenerfüllung des BSI, beschränkt. Nach Absatz 5 bleiben jedoch bestehende gesetzliche Übermittlungsregelungen, die Aufgaben anderer Behörden dienen, hiervon unberührt. Dies betrifft speziell die Zusammenarbeit mit den in § 5 Absatz 5 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 an verschiedenen Punkten erforderlich. Das BSI nimmt dabei weiterhin sonderordnungsbehördliche Funktionen beim Schutz von Kommu-

nikationstechnik wahr, nicht Aufgaben allgemeiner Gefahrenabwehr, die bei den zuständigen Polizeibehörden liegt.

Zu Buchstabe a

Mit der Änderung in Absatz 1 wird klargestellt, dass die vollumfängliche Unterstützung durch die Bundesbehörden gemäß Satz 4 auch den unverschlüsselten Zugriff des Bundesamtes auf Schnittstellen- und Protokolldaten verschlüsselter Kommunikation einschließt.

Die Verbreitung von verschlüsselter Kommunikation nach standardisierten Verfahren wie z. B. TLS hat in der Vergangenheit sehr stark zugenommen und wird auch in Zukunft weiter zunehmen. Dies hat zur Folge, dass die Daten an den Schnittstellen der Kommunikationstechnik des Bundes sowie Protokolldaten für eine Sicherheitsanalyse durch das Bundesamt nicht mehr verarbeitet werden können. Diese fehlende Analysemöglichkeit führt zu einer erheblichen Beeinträchtigung der Sicherheit der Kommunikationstechnik des Bundes, da standardisierte Verschlüsselungsverfahren auch von Schadprogrammen genutzt werden können, um die Kommunikation mit dem Angreifer zu verschleiern und hierdurch unentdeckt zu bleiben.

Dieser Gefahr für die Sicherheit der Kommunikationstechnik des Bundes muss dadurch begegnet werden, dass auch die verschlüsselte Kommunikation des Bundes geöffnet und hierdurch einer Analyse nach § 5 BSIG zugänglich gemacht werden muss. Hierdurch kann die Abwehr von Gefahren für die Kommunikationstechnik des Bundes weiterhin auf dem erforderlichen und dem Stand der Technik entsprechenden Niveau gewährleistet werden. Hinter den Analysepunkt des BSI müssen die Daten – um die Vertraulichkeit wieder herzustellen und die Kommunikation vor der Kenntnis durch Unbefugte zu schützen – wieder verschlüsselt werden, bevor diese weitergeleitet werden.

Bei Verschlüsselungsverfahren wie z.B. TLS können hierfür sogenannte „TLS-Proxies“ eingesetzt werden. Die Kommunikation ist hierbei durchgängig durch die Verschlüsselung geschützt und vor dem unberechtigten Zugriff Dritter gesichert. Des Weiteren bleiben alle Grundsätze zur Auswertung der Schnittstellen- und Protokolldaten nach § 5 gewahrt, insbesondere in Bezug auf personenbezogene oder dem Fernmeldegeheimnis unterliegende Daten.

Zu Buchstabe b

Mit der Änderung wird die Speicherdauer von pseudonymisierten 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, 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 die spezialisierten Cyberangriffe, so genannte Advanced Persistent Threats (APTs), über einen sehr langen Zeitraum. Die im Namen enthaltene Persistenz bezeichnet 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 Zielerfüllung des APTs, wie z. B. die Ausleitung oder Manipulation von Verschlusssachen, große Zeiträume liegen. Es kann vorkommen, dass ein APT erst zum Ende seiner Laufzeit entdeckt wird. Um die meisten durch den APT hervorgerufenen Kompromittierungen erkennen und entfernen zu können, muss die Speicherdauer der Protokolldaten i.S.v. § 2 Absatz 8 BSIG den Zeitraum des APTs möglichst einschließen. Nur wenn das Vorgehen des Angreifers aufgedeckt werden kann, kann die Kommunikationstechnik des Bundes vor gleichartigen zukünftigen Bedrohungen geschützt werden.

Die Streichung der Beschränkung in Satz 1 trägt dem Umstand Rechnung, dass die Identifikation von tatsächlichen Anhaltspunkten im Vorfeld in der Regel nicht möglich ist. Vielmehr sind Protokolldaten erst im Moment des Erkennens eines Angriffes von erheblicher Bedeutung, da rückwirkend das Vorgehen der Angreifer identifiziert und der Schaden so schnell behoben werden kann. Um diese effektive Nutzung der Protokolldaten zu ermöglichen, ist jedoch zuvor eine vollständige Speicherung zwingend erforderlich.

Die neue Einschränkung in Satz 2 stellt eine Einschränkung des Zugriffs auf die Daten dar, um diesen auf das unbedingt erforderliche Maß zu beschränken. Auch wenn die Daten für 18 Monate gespeichert sind, soll ein Zugriff auf Daten, die älter als drei Monate sind, nur dann zulässig und technisch möglich sein, wenn tatsächliche Anhaltspunkte für einen Angriff vorliegen.

Ferner ist die Regelung zur De-Pseudonymisierung anzupassen. Zur Erfüllung seiner gesetzlichen Aufgabe aus § 3 Absatz 1 Satz 2 Nr. 1 BSIG analysiert das BSI im Rahmen seiner Befugnisse aus § 5 BSIG 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 nach Maßgabe der Regelung in § 5 BSIG zulässig. Soweit hierzu die Wiederherstellung des Personenbezugs pseudonymisierter Daten erforderlich ist, muss diese gemäß § 5 Absatz 2 Satz 5 BSIG durch den Präsidenten des Bundesamtes persönlich angeordnet werden. Die Anordnung der De-Pseudonymisierung kann derzeit nicht auf einen anderen Mitarbeiter des BSI delegiert werden.

Hintergrund dieser gesetzlichen Regelung war es, den Schutz des Rechtes auf informationelle Selbstbestimmung in diesem Sonderfall auf höchstem Niveau zu gewährleisten. Da zum Zeitpunkt des Inkrafttretens der Regelung kaum relevante Angriffsszenarien bekannt waren, bei denen eine nichtpseudonyme Verarbeitung durch das BSI erforderlich war und die Erforderlichkeit der De-Pseudonymisierung somit einen Ausnahmefall darstellte, bestand keine Notwenigkeit für einen anderen Regelungsmechanismus.

Die technischen Möglichkeiten von Angreifern und die Arten der Angriffe, aber auch die Detektionsverfahren des BSI haben sich seit dem Inkrafttreten der Regelung jedoch weiterentwickelt. Dem BSI sind mehrere Angriffsmethoden bekannt, für deren effektive Detektion und Abwehr eine nicht-pseudonyme Verarbeitung von Protokolldaten erforderlich ist. Angreifer können Adressen im Internet erlangen, die dem Opfer einen bekannten und vertrauenswürdigen Kommunikationspartner vortäuschen. Dies können z. B. E-Mail-Adressen oder Domainnamen sein, die zu großen Teilen identisch mit den dem Opfer bekannten Adressen sind. Diese optischen bzw. inhaltlichen Ähnlichkeiten haben zur Folge, dass Angriffe dieser Art für das Opfer nur durch gesteigerte Aufmerksamkeit und besondere Vorsicht überhaupt zu erkennen sind und dabei gleichzeitig technisch und organisatorisch unauffällig bleiben. Zum Erkennen dieser Angriffsformen ist es erforderlich, die kompletten, nicht pseudonymisierten Adressen in ihrer ursprünglichen Form zu betrachten, um diese mit Expertenwissen über derartige Vorgehen von fortgeschrittenen Angreifern zu bewerten.

Eine De-Pseudonymisierung ist unumgänglich, um eine Suche nach Mustern zu ermöglichen oder um im Falle von Verdachtsmomenten eine Bewertung zu erlauben. Die ersten vom BSI erarbeiteten Erkennungsverfahren haben bereits gezeigt, dass eine Anwendung dieser auf den Bestand an Protokolldaten bei einer einmaligen Anwendung des Verfahrens 18.053 De-Pseudonymisierungen erforderlich gemacht hätte. In einer Hochrechnung auf das gesamte Kalenderjahr wären dies 79.389 erforderliche De-Pseudonymisierungen gewesen, um Verdachtsmomente für Angriffe zu be- oder widerlegen. Mit der Erarbeitung von weiteren Detektionsmethoden und der zunehmenden Nutzung des Internets ist hier von einer deutlich zunehmenden Zahl an erforderlichen De-Pseudonymisierungen auszugehen.

Bisherige Detektionsverfahren des BSI für Protokolldaten setzten die Kenntnis von IP-Adressen, Domainnamen oder anderen Inhalten voraus, auf deren Basis daraufhin in den Protokolldaten automatisiert gesucht werden konnte. Aus diesem Grund war eine De-Pseudonymisierung kaum erforderlich, denn das Vorliegen eines Treffers bestätigte unmittelbar einen Angriff. Derzeit in Erprobung befindliche Verfahren (z. B. zur Anomalieerkennung oder zur Erkennung auffälliger Zeichen-Codierungen) erfordern hingegen eine manuelle Verifikation. Zu diesem Zweck müssen auch schon IPAdressen und Domainnamen de-pseudonymisiert werden. Die Erforderlichkeit für eine De-Pseudonymisierung wird somit, aufgrund neuer Angriffs- und Detektionsmethodenmethoden, von der Ausnahme zum Regelfall werden. Vor diesem Hintergrund ist die gesetzliche Regelung der aktuellen Bedrohungslage nicht mehr angemessen und erschwert erheblich eine effektive und zeitnahe Analyse der Daten durch das BSI. Zum einen, weil der Präsident des BSI naturgemäß – aufgrund seiner Vielzahl von Aufgaben und Verpflichtungen – nicht ohne zeitliche Einbußen in vielfach auftretende Detailprüfungen und Arbeitsaufgaben des Hauses unmittelbar eingebunden werden kann. Zum anderen ist die Regelung nicht ausfallsicher, da die Entscheidung nur von einer einzigen Person (ggf. noch deren Stellvertreter) getroffen werden kann. Ist diese Person nicht erreichbar, ist eine nicht-pseudonyme Verarbeitung von Protokolldaten nicht möglich.

Das BSIG muss an die neue Situation angepasst werden. Erforderlich ist eine gesetzliche Lösung, die dem praktischen Erfordernis einer effektiven und zeitnahen Analyse der Daten durch das BSI Rechnung trägt, ohne das bestehende hohe Schutzniveau für den Schutz personenbezogener Daten abzuschwächen.

Zu Buchstabe c

Die Regelung ist erforderlich, damit das BSI Stichproben un-pseudonymisierter Protokolldaten erheben kann. Dies ist erforderlich, um Struktur und Semantik der Protokolldaten festzustellen.

Zur Erfüllung seiner gesetzlichen Aufgabe aus § 3 Absatz 1 Satz 2 Nummer 1 BSIG analysiert das BSI im Rahmen seiner Befugnisse aus § 5 BSIG Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen. Bei der Verarbeitung dieser Protokolldaten ist eine regelmäßige automatisierte Qualitätssicherung der verarbeiteten Daten im Klartext erforderlich, da das BSI die Quelle der Datenerhebung (z. B. den IVBB) nicht unter seiner betrieblichen Hoheit hat. Eine Fehlfunktion des Quellsystems kann so direkt aufgedeckt werden. Die Qualitätssicherung unterstützt ebenfalls bei der Anbindung neuer Datenquellen. Eine effektive Qualitätssicherung der Protokolldaten kann nur erfolgen, wenn hierbei einzelne Datensätze nicht pseudonymisiert und manuell ausgewertet werden könnten. Gem. § 5 Absatz 2 Satz 3 BSIG sind die Protokolldaten jedoch zu pseudonymisieren, soweit dies automatisiert möglich ist. Eine nicht-pseudonyme Verarbeitung personenbezogener Daten ist für das BSI nur in den engen Grenzen des § 5 Abs. 3 BSIG zulässig. Eine regelmäßige Qualitätssicherung wird durch die Regelungen des § 5 Abs. 3 BSIG nicht ermöglicht. Zur Erkennung von Angriffen auf Basis von Protokolldaten ist die Datenqualität äußerst relevant. Dem BSI muss es möglich sein, eine hohe Datenqualität mit vertretbarem Aufwand sicherzustellen, insbesondere wenn verschiedene organisatorische Schnittstellen miteinander interagieren.

Das BSI darf daher Daten in noch un-pseudonymisierter Form auswerten. So wird die Auswertung von Daten in un-pseudonymisierter Form benötigt, um identifizieren zu können, weshalb ein Datensatz eine Fehlermeldung in der automatisierten Qualitätssicherung der Verarbeitungskette verursacht hat. Es ist zwingend notwendig, diese fehlerverursachenden Daten im Klartext einsehen zu können, damit eine Fehlfunktion oder ein Angriff auf die Datenquelle oder die Verarbeitungskette ausgeschlossen werden kann.

Andernfalls besteht die Gefahr, dass gespeicherte pseudonymisierte Protokolldaten wegen semantischer Fehler nicht ausgewertet werden können. In diesem Fall kann das BSI

seine Schutzfunktion nach § 3 Absatz 1 Satz 2 Nummer 1 BSIG nicht erfüllen. Ein Beispiel für semantisch nicht verwertbare Informationen sind degenerierte, vertauschte oder leere Bestandteile von Protokolldateneinträgen.

Weiterhin muss zur Entwicklung der automatisierten qualitätssichernden Verarbeitungskette und zur Anbindung neuer Datenquellen dem BSI die Struktur und Semantik der Daten bekannt sein, insbesondere da sich diese im Laufe der Zeit ändern. Wird dem BSI diese Änderung nicht frühzeitig bekannt, kann das BSI seiner Schutzfunktion nach § 3 Absatz 1 Satz 2 Nummer 1 BSIG nicht mehr nachkommen.

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, auf Ersuchen bei der Sicherung ihrer Informationstechnik unterstützen.

Das BSI betreibt zur Erfüllung seiner Aufgabe aus § 3 Absatz 1 Satz 2 Nummer 1 BSIG auf Basis der Ermächtigung aus § 5 BSIG ein System zur Abwehr von Schadprogrammen und anderen Gefahren für die Kommunikationstechnik des Bundes (SES). Dieses System ist in Deutschland einzigartig. Auch Länder haben Interesse an dieser Leistung des BSI. Daher wird die Möglichkeit eines freiwilligen Anschlusses geschaffen.

Für die Unterstützung der Länder durch das SES fehlt dem BSI derzeit jedoch eine gesetzliche Ermächtigung zur Erfassung und Auswertung des Datenverkehrs der Länder, sofern diese das Bundesamt ersuchen. § 5 BSIG ermöglicht dem BSI nur einen Eingriff in das Fernmeldegeheimnis und eine Verarbeitung personenbezogener Daten, um die Kommunikationstechnik des Bundes zu schützen.

Darüber hinaus ist eine zusätzliche Regelung auf Länderebene erforderlich. Die Länder, die vom bestehenden System des BSI zur Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik profitieren wollen und das BSI um Unterstützung ersuchen, benötigen eine dem § 5 BSIG vergleichbare Ermächtigungsgrundlage, um den mit der Schutzmaßnahme verbundenen Eingriff in das Fernmeldegeheimnis und das Recht auf informationelle Selbstbestimmung zu ermöglichen.

Das BSI benötigt die Befugnis nach Absatz 1, zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes, Maßnahmen bei IT-Dienstleistern und Providern durchzuführen, die wesentliche IT-Dienstleistungen oder IT-Dienstleistungen in sicherheitssensiblen Bereichen für den Bund erbringen. Für den Schutz der Bundesverwaltung kann es keinen Unterschied machen, ob ein IT-Dienstleister oder Provider die entsprechenden Netze betreibt.

Zu Nummer 6

Der Begriff der Protokollierungsdaten wird in § 2 Absatz 9 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 die 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, bei der daher keine Protokolldaten im Sinne des § 2 Absatz 8 BSIG anfallen. Des Weiteren können bei Vorliegen tatsächlicher Anhaltspunkte über die Betroffenheit des Bundes nach § 5 BSIG die Protokollierungsdaten de-pseudonymisiert werden, um die betroffene Informationstechnik des Bundes zu identifizieren und die Kompromittierung zu bestätigen und zu beseitigen.

Durch die Verarbeitung von Protokollierungsdaten findet ein Eingriff in das Recht auf informationelle Selbstbestimmung statt. Ein Eingriff in das Fernmeldegeheimnis erfolgt jedoch nicht.

Der verwendete Begriff „unbeschränkt“ ist hierbei gleichbedeutend mit „unverschlüsseltem Zugang“. Hierdurch wird klargestellt, dass die vollumfängliche Unterstützung durch die Bundesbehörden auch den unverschlüsselten Zugriff des Bundesamtes auf Schnittstellen- und Protokolldaten verschlüsselter Kommunikation einschließt.

Überwiegende Sicherheitsinteressen der Sicherheitsbehörden sowie darüber hinaus datenschutzrechtliche Belange sind vom Bundesamt zu berücksichtigen. 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 lediglich um eine Folgeanpassung, da der neue § 5a systematisch an dieser Stelle zu regeln ist.

Zu Nummer 8

Zu Buchstabe a

Die Änderung in Absatz 1 stellt eine Folgeänderung der neuen Regelungen des § 8f dar. Auch in diesen Fällen liegt ein herausgehobenes Schutzinteresse des Staates vor, welches eine Privilegierung des Einsatzes der „Mobile Incident Response Teams“ (MIRTs) rechtfertigt.

Zu Buchstabe b

Gleiches gilt für die Vermutungsregelung nach Absatz 7 Satz 2; werden einem Betreiber entsprechende Pflichten auferlegt, sind diese auch privilegiert im Zusammenhang mit den mobilen Einsatzteams des Bundesamtes zu betrachten. Ferner ist nun auch eine solche Vermutungsregel für die Länder aufgenommen worden.

Zu Nummer 9

Zu § 5c

§ 5c regelt die Erstellung von Krisenreaktionsplänen für die Aufrechterhaltung oder Wiederherstellung der informationstechnischen Systeme, Komponenten oder Prozesse bei Betreibern Kritischer Infrastrukturen oder Betreibern weiterer Anlagen im besonderen öffentlichen Interesse während oder nach einer erheblichen Störung im Sinne des § 8b Absatz 4 Nummer 2, 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. Hierbei handelt es sich nicht um einzelne Krisenreaktionspläne für die jeweiligen Unternehmen, sondern um einen Gesamtplan für die Reaktionsmaßnahmen des Bundes. Bei der Erstellung der Krisenreaktionspläne wird das Bundesamt im Rahmen seiner gesetzlichen Aufgaben und Befugnisse tätig.

Gleichzeitig werden in Absatz 4 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 über Maßnahmen der Aufrechterhaltung oder Wiederherstellung ins Benehmen mit den betreffenden Sicherheitsbehörden (§ 5 Absatz 5 BSIG).

Zu § 5d

§ 5d regelt die Möglichkeit des BSI zur Bestandsdatenauskunft. Über die reine Information des Angriffsopfers über die Provider hinaus ist es erforderlich, dass das BSI ein Opfer eines Cyber-Angriffes unmittelbar kontaktieren und Unterstützung bei der Angriffsabwehr anbieten kann. 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 Absatz 7 wird eine transparente Umsetzung der Regelung sichergestellt. Das Bundesamt unterliegt einer solchen Berichtspflicht bereits in § 5 Absatz 9 BSIG. Die gemäß Absatz 7 notwendigen Angaben können in den jährlichen Bericht (§ 5 Absatz 9 BSIG) des BSI an die BfDI aufgenommen werden.

Zu Nummer 10

Zu Buchstabe a

Die Anpassungen der Regelungen des § 7 dienen insbesondere der Ausweitung hinsichtlich der neuen Aufgabe des Verbraucherschutzes. 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 (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 Herstellers 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 bestehenden Befugnisse des BSI auf die Erfüllung der in § 3 Absatz 1 Satz 2 Nummer 14a 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 (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.

Zu Nummer 11

Zukünftig kann das BSI zur Erfüllung all seiner Aufgaben Produkte und Systeme untersuchen. Ein Grund für eine Einschränkung nur auf bestimmte Aufgaben ist nicht (mehr) ersichtlich. Als nationale Cyber-Sicherheitsbehörde muss das BSI in der Lage sein, zur Erfüllung seines gesamten Aufgaben-Kataloges auf die eigene technische Kompetenz zurückzugreifen und Produkte, die auf dem Markt erhältlich sind, zu untersuchen. Insbesondere in Bezug auf die Sammlung und Auswertung von Informationen über bestehende Sicherheitsrisiken (Nummer 2) ist dies von Bedeutung. Aber auch für andere Aufgaben, wie die Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik (Nummer 3) oder die eigene Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit in der Informationstechnik (Nummer 4) können Untersuchungen der Sicherheit in der Informationstechnik hilfreich sein. Durch eine Erweiterung auf alle Aufgabe würde der in Absatz 3 geregelte Schutz für eventuell betroffene Unternehmen unverändert beibehalten

Ferner erhält das Bundesamt die Befugnis, von Herstellern notwendige Auskünfte zu verlangen. § 7a Absatz 1 dient dazu, Rechtssicherheit für umfassende Untersuchungen von IT-Produkten (zum Beispiel mittels Reverse-Engineering) und IT-Systemen durch das BSI zur Erfüllung seiner Aufgaben herzustellen. Jedoch wird dieses Untersuchungsrecht nicht von einem Recht auf Auskunft flankiert. Um sicherzustellen, dass das Bundesamt für Sicherheit in der Informationstechnik auch zukünftig seine gesetzlichen Aufgaben erfüllen kann, bedarf das BSI der Zurverfügungstellung von Informationen der IT-Hersteller zu dem zu prüfenden Produkt. Da die Hersteller auch in den Verhandlungen bezüglich der Lieferung von IT für die Bundesverwaltung höchstens im Ansatz die benötigten Informationen zur Verfügung stellen, in der Regel vertiefte Informationen aber verweigern, soll das Bundesamt die rechtliche Befugnis erhalten, notwendige Auskünfte von den IT-Herstellern zu verlangen. Dazu wird ein neuer § 7a Absatz 2 als Ermächtigungsgrundlage in das BSI-Gesetz eingefügt.

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

In vielen anderen Bereichen sind Auskunftsverlangen oder auskunftsähnliche Verlangen 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 kommt der Vertrauenswürdigkeit der IT-Systeme, der Hard- und Software immer größere Bedeutung zu. Es muss sichergestellt sein, dass IT-Systeme nur die herstellerseitig zugesagten Funktionalitäten haben und der Hersteller eingebaute Wartungskanäle, Backdoors etc. offenlegt. Auch bisher - ggf. sogar dem Hersteller - unbekannte Sicherheitslücken stellen eine Gefahr für die IT-Sicherheit des Systems dar. Das BSI hat den Auftrag, die Sicherheit von IT-Produkten zu untersuchen. Hierzu bedarf es der Hilfe der Hersteller mit Informationen zur Architektur des Systems, Wartungskanälen etc. Nur mit diesen Informationen ist es möglich, ggf. bisher unbekannte Sicherheitseinfallslöcher zu

entdecken und zu bewerten. Angesichts der Bedeutung der IT-Sicherheit für das Funktionieren des Gemeinwesens ist es daher nur naheliegend, auch für den IT-Bereich ein gesetzliches Auskunftsverlangen zu schaffen. Sollte es sich bei den Auskünften um Geschäfts- oder Betriebsgeheimnisse handeln, berechtigt das den Verpflichteten nicht, die Auskunft zu verweigern. Dafür bietet der neu eingefügte § 7b ausreichenden Schutz.

Absatz 2 Satz 2 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. Satz 2 konkretisiert die Förmlichkeiten eines Auskunftsverlangens und Satz 3 verweist bei Zuwiderhandlungen auf die Bußgeldvorschriften in § 14 BSIG.

Absatz 3 (ehemals Absatz 2) enthält eine Zweckbindung für die aus der Untersuchung nach Absatz 1 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 Bürgern und Bürgerinnen, 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.

Dem Hersteller ist zuvor die Gelegenheit zu einer Stellungnahme einzuräumen. Wenn der Hersteller in diesem Rahmen - etwa bei einer festgestellten Sicherheitslücke - selbst an die Öffentlichkeit geht oder sonst Abhilfe schafft, ist eine zusätzliche Veröffentlichung der Erkenntnisse durch das BSI nicht erforderlich.

Absatz 4 ermöglicht dem BSI bei Zuwiderhandlungen gegen das Auskunftsverlangen, die Öffentlichkeit über die Vorgehensweise der IT-Hersteller zu informieren. Hierdurch soll gewährleistet werden, dass die Hersteller dem Auskunftsverlangen nachkommen. Diese Möglichkeit ist erforderlich, da in einigen Fällen zur effektiven Umsetzung der Befugnis nach Absatz 2 die Verhängung einer Ordnungswidrigkeit nicht ausreichend sein kann. Dem Hersteller ist auch hier zuvor die Gelegenheit zu einer Stellungnahme einzuräumen.

Zu Nummer 12

Zu § 7b

In § 7b Absatz 1 wird die Befugnis zur Durchführung von Maßnahmen zur Detektion und Auswertung von Schadprogrammen, Sicherheitslücken und anderen Sicherheitsrisiken geregelt. Das BSI darf diese Maßnahmen im Rahmen seiner gesetzlichen Aufgaben zum Schutz der Bundesverwaltung, der Verbraucher und der KRITIS-Betreiber anwenden, um die Verantwortlichen oder den betreibenden Dienstleister des jeweiligen Netzes oder Systems über eine bestehende Gefahr zu informieren. Das Bundesamt darf diese Befugnisse ausüben, sofern Systeme ungeschützt sind und Tatsachen die Annahme rechtfertigen, dass die Sicherheit oder Funktionsfähigkeit der Systeme gefährdet ist. Eine Befugnis zu den genannten Maßnahmen besteht nur unter den genannten Voraussetzungen. Gleichzeitig ist eine Datenverarbeitungsbefugnis enthalten. Hierdurch soll das Bundesamt insbesondere sog. nicht-invasive „Portscans“ und eigenständig sog. „Sinkholes“ betreiben

können. Die Befugnis umfasst nicht das Ausspähen bzw. das Einsehen von auf dem System enthaltenen Daten. Dies gilt auch für Absatz 4.

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. 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.

Um diesen gesetzlichen Aufgaben in erforderlichem Maß nachkommen zu können, sind entsprechende Befugnisse für das Bundesamt erforderlich. Die Maßnahmen sollen 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 aufgrund der zunehmenden Vernetzung die Möglichkeit eines Zugriffs via Internet; beispielsweise bei Industrial Control Systems (ICS-Geräte) oder Internet of Things Systemen (IoT-Geräte), die offene Dienste (Ports) und diverse andere Schwachstellen aufweisen können. Über solche Schwachstellen werden vernetzte Systeme permanent angegriffen. Viele Betreiber von vernetzten IT-Systemen sind sich der Gefahren nicht bewusst, die von offenen Ports und anderen bekannten Schwachstellen ihrer IT-Systeme ausgehen. Das Bundesamt besitzt die fachliche Kompetenz, um offene Ports und andere bekannten Schwachstellen durch gezielte automatisierte Such-Routinen (Scans) schnell zu detektieren, und ist in der Lage, die Ergebnisse des Scans schnell an Betroffene aus Staat und Wirtschaft weiterzugeben. Diese schnelle Information der Betroffenen wird zu einer erheblichen Steigerung der IT-Sicherheit der Bundesverwaltung und der KRITIS-Betreiber führen. Die rechtlich zulässigen Möglichkeiten für dieses sehr effektive Mittel sind de lege lata begrenzt.

Darüber hinaus wird dem Bundesamt der Betrieb eigener Sinkhole-Server ermöglicht. Der Betrieb eines solchen Sinkhole-Servers stellt eine sehr effektive Maßnahme zur Bekämpfung von Botnetzen dar. Ein klassisches Botnetz besteht typischerweise aus zwei Komponenten: einer beliebigen Anzahl infizierter und somit fernsteuerbarer Systeme (Bots) und einem zentralen Steuerungssystem (Command-and-Control-Server, C&C-Server). Über den C&C-Server kann der Botnetzeigner (Bot-Herder) den infizierten Systemen Befehle erteilen und diese somit für eigene Aktivitäten verwenden. Hierunter fallen typischerweise neben Aktivitäten, die nur dem Systemeigner schaden, wie beispielsweise Identitätsdiebstahl, Abfluss von Daten oder Manipulation von Online-Überweisungen, auch solche, die Dritten einen Schaden zufügen. Diese können beispielsweise die Suche und Infektion weiterer Opfersysteme sein, das Durchleiten von fremdem Datenverkehr (Proxy) oder die Beteiligung an Denial-of-Service-Angriffen (DDoS-Angriffe). Ohne besondere Befugnisse oder unterstützenden Maßnahmen durch Strafverfolgungsbehörden können jedoch nur Domänen registriert werden, die zu dem jeweiligen Zeitpunkt noch frei sind.

Befinden sich bereits Domänen im Besitz der Botnetzbetreiber, so besteht hier keine Zugriffsmöglichkeit. Dies führt dazu, dass die Bots zwischen regulärem C&C-Server und Sinkhole-Server "pendeln" und dem Botnetzbetreiber nicht dauerhaft entzogen werden können. Der Betreiber des Sinkhole hat somit nur eine beschränkte Sicht auf das Botnetz und die Gesamtmenge der infizierten Systeme. Auf Seiten des Sinkhole-Betreibers entstehen nennenswerte Kosten für die Registrierung der mutmaßlich zukünftig genutzten Domänen. Mit der Verpflichtung der Provider zum Umlenken von C&C-Domänen auf eine Sinkhole des BSI kann die Sichtbarkeit auf ein Botnetz nachhaltig gesteigert werden und

dem Betreiber der Zugriff auf einen großen Teil der Bots langfristig entzogen werden. Hierdurch wird präventiv sowohl Schaden von den Inhabern der betroffenen Systeme als auch von Dritten abgewendet. Dies geht einher mit einer deutlichen Kosten- und Zeitersparnis durch den Wegfall notwendiger Domänenregistrierungen.

Absatz 2 definiert den in Absatz 1 verwenden Begriff „ungeschützt“ und greift als Anknüpfungspunkt die legaldefinierten „Sicherheitslücken“ (§ 2 Absatz 6 BSIG) auf. Die Definition beschränkt sich nicht nur auf Kommunikationsnetze und informationstechnische Systeme, die vollständig ohne Schutzmechanismen arbeiten. Neben Kommunikationsnetzen und informationstechnischen Systemen, die gar keine Sicherheitsmechanismen oder Zugangsbeschränkungen besitzen, werden von der Definition auch die Netze und Systeme erfasst, die zwar einen irgendwie gearteten Schutzmechanismus besitzen, der aber faktisch wirkungslos ist.

Dies ist zum einen der Fall, wenn das Netz oder System bzw. der jeweils zum Schutz verwendete Mechanismus eine bereits bekannte Sicherheitslücke besitzt. Durch das Ausnutzen der bekannten Sicherheitslücke ist es für einen unbefugten Dritten einfach, den bestehenden Sicherheitsmechanismus zu umgehen und Zugriff auf das Netz oder System zu erhalten. Für den Dritten, dem die Sicherheitslücke bekannt ist, bestehen somit faktisch keine Sicherheitsmechanismen oder Zugangsbeschränkungen. Zum anderen erfasst die Definition auch Kommunikationsnetze und informationstechnischen Systeme, deren Schutzmechanismus aufgrund unsorgfältiger Einstellung durch den Betreiber bzw. Verantwortlichen wirkungslos sind. Dies ist zum Beispiel dann der Fall, wenn für ein System werkseitig stets ein identisches Passwort („0000“ oder „admin“) vergeben wird oder wenn die werksseitige Vergabe der Passwörter nach einer öffentlich bekannten und einfachen Systematik erfolgt.

In diesen Fällen existiert zwar ein technisch aktiver Mechanismus zum Schutz für das jeweilige Netz oder System. Allerdings entfaltet dieser Mechanismus keine tatsächliche Schutzwirkung, so dass ein Zugriff durch unbefugte Dritte faktisch ohne Hindernis erfolgen kann.

Absatz 3 regelt die Informationspflichten des Bundesamtes. Dies korrespondiert mit einer Anordnungsbefugnis gegenüber Diensteanbietern zu Maßnahmen nach § 109a Absatz 4 TKG. Dies ist erforderlich, um insbesondere eine Benachrichtigung der Betroffenen sicherzustellen und das erfolgreiche sog. „Sinkholing“ auf einen BSI-Server zu gewährleisten.

Daneben wird in Absatz 4 die Befugnis zum Einsatz sog. „aktiver Honeypots“ geschaffen. Zur Erfüllung seiner gesetzlichen Aufgabe ist für das Bundesamt der Einsatz von sog. „aktiven Honeypots“ unbedingt erforderlich. Passive Honeypots werden seit vielen Jahren von Sicherheitsforschern eingesetzt, um Infektionsversuche zu detektieren. Deren Möglichkeiten sind jedoch stark begrenzt. Es ist damit zwar möglich, die ersten Infektionsvektoren zu erkennen (beispielsweise Infektion über schwache Kennwörter mittels des SSH-Dienstes), aber es ist beispielsweise nicht möglich zu erkennen, wie und welche Infektionen bei IoT-Geräten durchgeführt werden. Die Bedeutung von Angriffen auf IoT-Geräte hat stark zugenommen. Hierbei werden in großer Zahl Botnetze aufgebaut, die massiv genutzt werden, um DDoS-Angriffe durchzuführen. Aktive high-interactive Honeypots ermöglichen es dem BSI, dem Angreifer eine möglichst realitätsnahe Umgebung bereitzustellen. Dies ist im Hinblick auf neue Angriffsmöglichkeiten erforderlich.

Beispielsweise versucht die Schadsoftware Mirai, anhand verschiedener Kriterien Honeypots zu erkennen. Im Fall der Erkennung erfolgt keine Infektion. Ohne Infektion ist keine Analyse des Angriffes möglich und folglich sind auch die Maßnahmen zur Begegnung der Bedrohung eingeschränkt.

Im Fall eines Mirai-Honeypots ist ein sog. „aktiver Honeypot“ beispielsweise ein Honeypot, der einen Zugang per Telnet oder SSH mit all den dadurch bereitgestellten Funktionen zur Verfügung stellt. Die Malware wird nach Login von den Angreifern automatisiert nach dem Login heruntergeladen. Um Schaden zu vermeiden bzw. zu begrenzen, kann die Ausführung heruntergeladenen Schadcodes über Kernel-Module verhindert werden. Zudem kann man das System nach mehreren Minuten zurücksetzen, wenn in dieser Zeit keine versuchte Ausführung unbekannten Codes erfolgt. Möglich sind Begrenzungen des Netzwerkverkehrs. Häufig wird bei einem Angriff allerdings nicht die eigentliche Botnetz-Malware platziert, sondern ein so genannter Downloader, der nach Ausführung die eigentliche Botnetz-Malware von einem Download-Server z. B. per HTTP lädt. Ob es sich bei dem im Honeypot platzierten Binary um die endgültige Schadsoftware oder einen Downloader handelt, kann mit vertretbarem Aufwand nicht im Honeypot festgestellt werden. Um diesem Problem zu begegnen, könnte das Binary prinzipiell anschließend manuell untersucht werden. Dies erfordert aber einen hohen Personalaufwand und dauert je nach Malware bis zu mehrere Wochen für die Analyse. Eine zeitnahe Reaktion auf neue Malware ist damit also nicht möglich. Daher ist es sinnvoll, im Honeypot die erste Ausführung eines unbekannten Binaries für wenige Minuten zu erlauben. Dabei kann der Netzwerkverkehr auf Protokolltypen beschränkt werden, die notwendig sind, damit das Nachladen der Schadsoftware erfolgreich ist. Weiterhin kann die Bandbreite eingeschränkt werden (z. B. rate-limit).

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 des BSIG eröffnet diese Möglichkeit bereits, so dass § 7c der Klarstellung dient, dass das BSI auch mit den Maßnahmen nach § 7b unterstützen kann.

Zu Nummer 13

Zu Buchstabe a

Durch die Änderungen in § 8 Absatz 1 werden die Adressaten für Mindeststandards erweitert. Neben den Stellen des Bundes sollen diese zukünftig ausdrücklich auch für IT-Dienstleister und Diensteanbieter gelten, soweit sie IT-Dienstleistungen für die Kommunikationstechnik des Bundes erbringen. Eine solche Erweiterung ist erforderlich, um sicherzustellen, dass das IT-Sicherheitsniveau des Bundes unabhängig von der Organisationsform eines Dienstleister erbracht wird. Ferner werden Anpassungen wegen sich verändernder Rollen in der Bundesverwaltung durchgeführt.

Daneben werden Kontrollrechte des Bundesamtes eingeführt, die für die Einhaltung eines hohen IT-Sicherheitsstandards zwingend erforderlich sind. Dies entspricht auch den Vorgaben des Umsetzungsplans Bund 2017, nach dem die Einhaltung der Mindeststandards bereits ressortübergreifend verpflichtend geregelt ist.

Auch soll diese Regelung sicherstellen, dass die Sicherheit der Kommunikationstechnik des Bundes unabhängig von der Organisationsform eines Dritten gewährleistet wird, insbesondere dann, wenn weitere Stellen an die Schnittstellen zur Kommunikationstechnik des Bundes eingerichtet werden.

Zu Buchstabe b

Gemäß § 3 Absatz 1 Satz 2 Nummer 1 gehört es zu den Aufgaben des BSI, IT-Sicherheitsprodukte für Stellen des Bundes zu entwickeln. Hierauf nimmt § 8 Absatz 3 Satz 1 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 c

Als nationale 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 des Bundes, sondern gestaltet auch gegenüber Unternehmen, der Bürgerschaft oder anderen Trägern der Verwaltung die Informationssicherheit in der Digitalisierung.

Um seiner Rolle Rechnung zu tragen und sicherzustellen, dass die Belange der Cyber- und Informationssicherheit ausreichend und umfassend berücksichtigt werden, ist das BSI von der jeweils zuständigen Stelle des Bundes stets frühzeitig zu beteiligen, wenn Vorhaben zur Gestaltung der Digitalisierung erarbeitet werden. Dem Bundesamt ist insoweit die Gelegenheit zur Stellungnahme einzuräumen. Der Begriff „Digitalisierungsvorhaben“ soll in diesem Zusammenhang weit verstanden werden.

Zu Nummer 14

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.

Durch die Regelung wird Rechtssicherheit geschaffen. Zum Schutz der Betroffenen sind Verfahren unter der Beteiligung der oder des Bundesbeauftragen für den Datenschutz und die Informationsfreiheit und des Bundesamtes vorgesehen. Eine entsprechende Regelung wurde außerdem in § 109 TKG aufgenommen, um dort auch Daten, welche dem Fernmeldegeheimnis nach § 88 Absatz 2 TKG unterliegen, verarbeiten zu können.

Wie in § 3a gilt die sich aus der DSGVO ergebene Verpflichtung zur unverzüglich 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 und dient der Abgrenzung zur im darauffolgenden Satz enthaltenen Speicherbefugnis.

Zu Buchstabe b

Für den Einsatz von KRITIS- Kernkomponenten sind neben der technischen Qualität der Produkte gleichsam auch die Organisationsstruktur und die möglichen - den Schutzzielen dieses Gesetzes widersprechenden - 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 KRITIS-Kernkomponenten 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 nur unmittelbare Wirkung zwischen den Parteien, ist also als privatrechtliche Erklärung zu werten.

Zu Nummer 15

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 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

Absatz 3a 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 KRITIS-Betreibern 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 schwellwert-relevanten Kennzahlen der KRITIS-Betreiber. KRITIS-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 Bertreiber Kritischer Infrastruktur sind.

Zu Nummer 16

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

Zu Nummer 17

Zu § 8f

§ 8f 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 Sektoren, die aus Sicht des Staates für die Gesellschaft von besonderem öffentlichem Interesse sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche volkswirtschaftliche Schäden eintreten würden oder sie wesentlich für die Sicherheitsinteressen der Bundesrepublik Deutschland sind oder sonst von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung eine Gefährdung für die öffentliche Sicherheit eintreten würde. Hierbei handelt es sich zum einen um die nach dem Prime Standard für den DAX, MDAX, TecDax und SDAX zugelassenen deutschen Aktiengesellschaften sowie Unternehmen aus den Sektoren Rüstung sowie Medien und Kultur, für die durch Rechtsverordnung nach § 10 Absatz 5 näher konkretisiert wird, wann eine Anlage oder Teile davon von besonderem öffentlichem Interesse ist. Die Pflichten gelten für die Betreiber dieser Anlagen, wie auch im Falle der Betreiber Kritischer Infrastrukturen, zwei Jahre nach Inkrafttreten der Verordnung.

Zu § 8g

Durch § 8g wird das Bundesamt ermächtigt, die Pflichten nach §§ 8a und 8b auch im Einzelfall einem in Absatz 1 und 2 genannten Adressaten aufzuerlegen.

Zu Absatz 1

Durch die Festlegung von Schwellenwerten durch die Rechtsverordnung nach § 10 Absatz 1 gibt es Fälle, in denen eine Anlage oder Teile davon aus den genannten Sektoren zwar nicht den Schwellenwert erreichen, eine Störung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit eines informationstechnischen System, Komponenten oder Prozesse, insbesondere wegen der Vielzahl an eingesetzter Informationstechnik, dennoch zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der betroffenen Dienstleistung in einem für die Ebene Bund erheblichen Maßen und im Sinne dieses Gesetzes führen kann. Um dieser Problematik zu begegnen, ist es in diesen Fällen gerechtfertigt, den Betreibern dieser Anlage ebenfalls die Pflichten nach §§ 8a und 8b aufzuerlegen. Da es sich hierbei um Ausnahmen handelt, ist eine Auferlegung durch das BSI im Einzelfall gerechtfertigt.

Zu Absatz 2

Absatz 2 regelt, dass das BSI im Einzelfall auch weiteren Unternehmen die Pflichten nach §§ 8a und 8b auferlegen kann, wenn eine Störung der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten oder Prozesse dieses Unternehmens zu einer tatsächlichen und hinreichend schweren Gefährdung für ein Grundinteresse der Gesellschaft führen würde. Diese Formulierung ist an die Regelung des § 5 Absatz 4 AWG angelehnt.

Die Regelung dient als Auffangtatbestand und stellt sicher, dass im Einzelfall insbesondere auch große mittelständische Unternehmen oder Kleine und Mittlere Unternehmen adressiert werden können, die wegen ihrer Größe nicht den Schwellenwerten der Verordnungen nach § 10 Absatz 1 und Absatz 5 sowie nicht der Regelung des § 2 Absatz 13 Nummer 1 unterfallen, aus anderen Gründen allerdings für die Gesellschaft von besonderer Bedeutung sind.

Zu Absatz 3

Durch die Fristsetzung von mindestens einem Jahr wird gewährleistet, dass den Adressaten eine Umsetzung überhaupt ermöglicht wird.

Zu § 8h

§ 8h regelt eine Meldepflicht von Störungen für Hersteller von IT-Produkten. Die Regelung ist der Verpflichtung aus § 8b Absatz 4 Satz1 Nummer 4 nachgebildet und dient dem Schutz von Anlagen nach § 2 Absatz 10 und 14. Oftmals erlangen Hersteller bereits vor den Kunden Kenntnis von Sicherheitslücken. Zum Schutz der Allgemeinheit ist daher auch von den Herstellern zu fordern, dass Sicherheitslücken kurzfristig gemeldet werden, um rechtzeitig Schutzmaßnahmen ergreifen zu können. Da Beeinträchtigungen oder Störungen von KRITIS-Kernkomponenten zum Betrieb von Kritischen Infrastrukturen ein deutlich höheres Schadenspotential zukommt, gelten hier geringe tatbestandliche Anforderungen an die Meldepflicht als bei sonstigen IT-Produkten.

Zu Nummer 18

Für den Einsatz zertifizierter KRITIS-Kernkomponente ist neben der Zertifizierung wesentlich, ob der jeweilige Hersteller der Komponente hinreichend vertrauenswürdig ist. Im Rahmen der Produktzertifizierung prüft das BSI bisher nicht, ob der Hersteller diese Vertrauenswürdigkeit aufweist. Durch die Verpflichtung zur Aufnahme der Vertrauenswürdigkeitserklärung in den Zertifizierungsprozess erhält das BSI die Möglichkeit, für KRITIS-Kernkomponenten auch die in der Erklärung nach § 8a Abs. 6 zugesicherten Eigenschaften in die Zertifizierungsentscheidung einfließen zu lassen.

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 (Z 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 in die EU ist 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 2a 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 2a 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 BSI Sicherheitsinformationen 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 Nummer 20

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 21

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. 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

Zu Nummer 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 wird, ist eine Unterstützung der BSI Aufforderung zur Herstellermitwirkung durch die Möglichkeit der Verhängung eines Bußgeldes angemessen.

Zu Nummer 2

Mit Nummer 2 wird der Fall einer Zuwiderhandlung gegen eine vollziehbare Anordnung erfasst.

Zu Nummer 3

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

Zu Nummer 5

Die neue Nummer 5 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 nur schwer durchsetzbar sind. Diese sind aber erforderlich, um zu erkennen, ob ein Betreiber eine Kritische Infrastruktur betreibt und die notwendigen und geeigneten Sicherungsmaßnahmen für seine Informationstechnischen Systeme bereithält.

Zu Nummer 7

Wie Nr. 5 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.

Zu Nummer 9

Nach Nummer 9 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, dass Betreiber über die registrierte Kontaktstelle in

der Lage sein muss, Informationen (Cyber- Sicherheitswarnungen, Lageinformationen etc.) entgegenzunehmen und diese unverzüglich zu sichten und zu bewerten (Bearbeitung der Informationen auf Zuruf). In der Regel werden Informationen während der normalen Geschäftszeiten versendet. Es ist jedoch nicht auszuschließen, dass in Ausnahmefällen dringende Warnungen auch außerhalb der normalen 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.

Zu Nummer 10

Die neue Nummer 10 sanktioniert ebenfalls den Umstand, dass einer Auskunftspflicht nicht nachgekommen wird.

Zu Nummer 11

In Nummer 11 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.

Zu Nummer 12

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

Zu Nummer 13

Mit Nummer 13 wird der Fall einer Zuwiderhandlung gegen eine vollziehbare Anordnung erfasst.

Zu Nummer 17

Zur Abwendung des Missbrauchs des freiwilligen IT-Sicherheitskennzeichens nach § 9a, wird mit der neuen Nummer 17 sanktioniert, wenn ein Produkt nach Widerruf weiterhin im geschäftlichen Verkehr genutzt oder beworben wird oder vor der Nutzung keine vorherige Freigabe durch das BSI erfolgt ist. Dies ist erforderlich, damit das Vertrauen in das IT-Sicherheitskennzeichen geschaffen werden kann.

Zu Absatz 2

Absatz 2 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 ausmachen können. Nur so können die Sanktionen wirksam, angemessen und abschreckend sein. Andernfalls besteht die Gefahr, dass einzelne Unternehmen sich wegen der geringen Bußgelder gegen eine Meldung entscheiden, weil dies für sie finanziell attraktiver ist. Da sich die Verpflichtungen auf Kritische Infrastrukturen, Betreiber weiterer Anlage 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 der Datenschutzgrundverordnung. Ein Verstoß gegen Maßnahmen zur Absicherung von Anlagen und Diensten der Daseinsvorsorge sollte ebenso schwerwiegend sanktioniert werden können, wie ein datenschutzrechtlicher Ver-

stoß, z. B. durch den Versand von Spam-Mails. Andernfalls droht auch 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

Die Ergänzung des Absatzes konkretisiert die Verpflichtung der Diensteanbieter, Schutzmaßnahmen zu treffen, und entspricht der Ergänzung in § 8a Absatz 1a BSIG. Diese Pflicht umfasst nun auch ausdrücklich den Einsatz von Systemen zur Angriffserkennung und gibt den Unternehmen Rechtssicherheit. Diese Systeme stellen eine effektive Maßnahme zu Begegnung von Cyber-Angriffen dar.

Die Regelung rechtfertigt einen Eingriff in das Fernmeldegeheimnis nach § 88 Absatz 2 TKG und stellt eine hinreichende Datenverarbeitungsbefugnis dar. Hierdurch wird Rechtssicherheit geschaffen. Zum Schutz der Betroffenen sind Verfahren unter der Beteiligung der oder des Bundesbeauftragen für den Datenschutz und die Informationsfreiheit und des Bundesamtes vorgesehen.

Zu Nummer 2

Zu Buchstabe a

Die Regelung ist zur Information von Betroffenen erforderlich. Aktuell informieren die Provider Kunden darüber, wenn einer der Rechner des Nutzers mit einer Botnetzschadsoftware infiziert ist, die einen C&C-Server kontaktiert. Dazu sind die Provider 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 Provider 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 Provider die Betreiber des Shopsystems nicht informiert. Nach einer Klärung mit einem der großen Provider 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.

Das Problem besteht hierbei darin, dass ein Angreifer das Internet auf Schwachstellen scannen, um festzustellen, welche Datenverarbeitungssysteme angreifbar sind und diese anschließend übernehmen oder mit Schadsoftware infizieren. Teilweise ist ein eigener Scan nicht notwendig, da es im Internet frei verfügbar 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 von Angreifern infiziert. Ein aus dem Internet erreichbares Datenverarbeitungssystem, welches bekannte Schwachstellen besitzt, wird damit 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 präventiv 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 Provider 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 Verwendung von E-Mailadresse bei Online-Shops genutzt wurde).

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 die BfDI für Fälle der Verletzung des Schutzes bei dem Dienste 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 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.).

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, Daten-

verkehr 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 Datenver-

kehr 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.

Die Beteiligung des Bundeskriminalamtes und der Bundesnetzagentur dient der Sicherstellung der Abstimmung der Behörden untereinander.

Zu Nummer 3

Der sogenannte Datenleak-Vorfall (unbefugte Veröffentlichung persönlicher Daten und Dokumente von Politikern und anderen Personen des öffentlichen Lebens im Internet) verdeutlicht erneut, welche schwerwiegenden Folgen die unberechtigte und unkontrollierte Verbreitung unrechtmäßig erlangter Daten haben kann.

Um größeren Schaden soweit wie möglich zu vermeiden, ist es für die Betroffenen von höchster Priorität, dass die unrechtmäßige Verbreitung ihrer Daten schnellstmöglich gestoppt wird. Wichtigster Ansatzpunkt ist die Verhinderung der weiteren Verbreitung der Daten durch den Provider, über dessen Plattform die Weitergabe erfolgt. Daher müssen die Host-Provider die Pflicht – aber auch das Recht – haben, rechtswidrig weiterverbreitete Daten unverzüglich von ihren Plattformen zu löschen.

Zu Absatz 1

Regelungsadressat in §109b ist der TK-Diensteerbringer, bei dem die Daten gespeichert, zwischengespeichert, übertragen, veröffentlicht oder weitergegeben werden. Im Unterschied zu § 109a muss es sich hierbei nicht um Daten handeln, deren Schutz bei dem Diensteerbringer selbst verletzt worden ist. Folglich ist für die zusätzliche Verpflichtung des Host-Providers, bei dem die unrechtmäßig erlangten Daten (weiter-)verbreitet wurden, eine neue Regelung in §109b TKG-neu (sowie entsprechend im TMG, s.u.) 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.

Die Norm knüpft die Verpflichtung zur Unterrichtung des Bundeskriminalamts an eine positive Kenntniserlangung des Diensteerbringers. Auf welche Weise diese Kenntniserlangung erfolgt, ist unerheblich (z.B. eigene Recherche, Hinweise von Nutzern o.ä.). Eine eigene anlasslose Recherchepflicht wird dem Diensteerbringer durch diese Norm nicht auferlegt.

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. Auf eine Pflicht zur Benachrichtigung der von der Verletzung betroffenen Personen wird an dieser Stelle verzichtet, weil dies einen u.U. erheblichen Auswerteaufwand auf Seiten des Providers hervorrufen würde. 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 aufrecht erhalten, 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. Aufgrund der Zweckrichtung der Regelung (Gefahrenabwehr) sind die zuständigen Stellen die Polizeien der Länder. Bei Vorliegen von zu-

reichenden 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. Es wird deshalb erforderlich sein, dass die Diensteerbringer auch eine Erreichbarkeit außerhalb der üblichen Bürozeiten sicherstellen.

Zu Nummer 4

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. Ebenso ist sie zur Entgegennahme von Ersuchen nach § 109b TKG verpflichtet.

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 5

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

Zu Nummer 21d

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.

Zu Nummer 21e

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.

Zu Nummer 21f

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.

Zu Nummer 3

Es handelt sich um eine zu § 109a Abs. 1a spiegelbildliche Norm, die eine zur Regelung des TKG parallele Pflicht auch für TMG-Anbieter einführt.

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 des Strafgesetzbuchs)

Zu Nummer 1

Besonderes Gefährdungspotential liegt darüber hinaus auch in Konstellationen vor, in denen Täter Cyberangriffe für eine fremde Macht durchführen. Ein signifikanter Teil der

Cyberbedrohungen weist – u.a. in Form der APT – einen staatlich motivierten bzw. nachrichtendienstlichen Hintergrund auf.

Auf diese Entwicklung muss mit Nachjustierungen in zwei Bereichen des materiellen Strafrechts regiert werden: Durch eine Anpassung des § 99 StGB (Geheimdienstliche Agententätigkeit) und durch Aufnahme des Tätigwerdens „für eine fremde Macht“ in den Katalog der Regelbeispiele für einen besonders schweren Fall in § 202f StGB.

§ 99 StGB stellt das Tätigwerden für eine fremde Macht – unabhängig davon, ob die Tätigkeit in der Realwelt oder im Cyberraum stattfindet – unter Strafe. Die Änderung ergänzt die Regelbeispiele der Strafzumessungsbestimmung in Anpassung an die Entwicklung des Phänomenbereichs um neuere typische Sachverhalte, die entsprechend gewichtige unrechts- und schuldqualifizierende Tatumstände bezeichnen. Zudem werden die qualifizierenden Elemente einerseits der Tatbegehung und der andererseits der Tatfolgen als eigenständige Alternativen geregelt. Mit der neuen Nummer 1 wird der besondere Schutz von Geheimnissen auch auf den Schutz von Wirtschaft und Wissenschaft erstreckt. Außerdem wird die bisherige Nummer 2 nunmehr als selbständiges Regelbeispiel gefasst, bei dem sich die besondere Schwere aus den Tatfolgen unabhängig davon ergibt, ob die beschafften Informationen für sich Geheimnisqualität besitzen.

Vor dem Hintergrund des aufgezeigten Gefährdungspotentials genügt jedoch eine bloße Anpassung des § 99 StGB nicht allein. In diesem Zusammenhang wird ausschließlich auf die Gewinnung von Informationen oder Gegenständen abgestellt. Andere Formen nachrichtendienstlicher Tätigkeit, wie beispielsweise (Des-)Informationsoperationen oder Sabotagehandlungen werden von § 99 StGB nicht umfasst. Gerade dafür werden aber häufig Cyberoperationen durchgeführt. Um auch diese Fälle abzudecken (z.B. Cyberangriffe nur gegen Einzelpersonen, um an deren Daten zum Zwecke einer weiterführenden Informationsoperation zu gelangen), muss das Kriterium des Tätigwerdens für eine fremde Macht ebenfalls als Regelbeispiel für einen besonders schweren Fall aufgenommen werden.

Zu Nummer 2

Die Norm sowie die nachstehende Begründung entspricht dem Entwurf des Bundesrats gem. BR-Drs. 33/19 in der Fassung der BR-Drs. 33/1/19.

Der – nicht selten anonyme und mittels Krypto-Währungen abgewickelte – Handel mit illegalen Waren und Dienstleistungen (insbesondere mit Betäubungsmitteln, Kinderpornographie, Schadsoftware, Falschgeld, Ausweispapieren oder Waffen) über das Internet hat aufgrund der Möglichkeit der Anonymisierung, die das Internet bietet, erheblich zugenommen. Entsprechende Handelsplattformen finden sich im für jedermann ohne weiteres zugänglichen Bereich des Internets (sogenanntes Surface-Web), vermehrt aber auch im sogenannten Darknet.

Der Zugang zum Darknet erfolgt insbesondere über das „The Onion Router“ (Tor)-Netzwerk, das aus einer Vielzahl von weltweit verteilten Servern besteht, über die Datenpakete in ständig wechselnder Form geleitet werden. Beim Verbindungsaufbau wird durch das Programm eine zufällige Route über einen Teil der Server festgelegt, ohne dass Herkunft oder Ziel der Daten protokolliert werden. Durch die Verschlüsselung der Nutzerdaten und die dynamische Routenwahl wird die Feststellung von Anfangs- und Endpunkten eines Datentransfers erheblich erschwert. Zugang und Erreichbarkeit der Darknet-Angebote sind durch das Erfordernis besonderer Programme, wie des Tor-Browsers, beschränkt.

Die Angebote im Darknet umfassen, wie auch auf andere Weise zugangsbeschränkte Dienste, neben Foren für Whistleblower oder Chatrooms für politisch Verfolgte in autoritär geführten Staaten auch Inhalte bekannter Servicebetreiber. Ebenso finden sich jedoch Angebote mit strafrechtlicher Relevanz, darunter Handel mit Betäubungsmitteln, Kinder-

pornographie oder Waffen, mit Schadsoftware und Ausweispapieren. Vergleichbare Angebote finden sich auch in weiteren Bereichen des Internets.

Die Zentralstellen für die Verfolgung von Cybercrime der Länder haben in den vergangenen Jahren zahlreiche Ermittlungsverfahren mit überwiegend internationalen Bezügen geführt und einschlägige Foren sowie Handelsplattformen schließen können. In der Praxis zeigt sich jedoch, dass Anbieter und Kunden ihre Aktivitäten mit allenfalls geringem zeitlichem Verzug über alternative Plattformen fortführen. Die Verfahren lassen im Übrigen durchweg ein arbeitsteiliges Zusammenwirken von Plattformbetreibern und Nutzern der Plattform, also sowohl Händlern als auch Käufern, erkennen. Die Erfahrungen zeigen zudem, dass die klassischen Organisationsdelikte und die historischen gesetzgeberischen Vorstellungen von Täterschaft und Teilnahme auf moderne, internetbasierte Täterstrukturen kaum übertragbar sind. Die Betreiber selbst stellen lediglich eine technische Infrastruktur zur Verfügung. Ihr Verdienst entsteht durch Werbung oder einen Treuhand-Service im Rahmen der Zahlungsabwicklung.

Das Kriminalitätsphänomen beschränkt sich auch nicht auf wenige Einzelfälle. Bereits im Jahr 2016 waren dem Bundeskriminalamt circa 50 einschlägige Plattformen bekannt (BT-Drucks. 18/9487, S. 2). Das dort betriebene Geschäftsmodell des „Cybercrime-as-a-Service“ wird in der kriminellen Szene weiter ausgebaut (Lagebild Cybercrime des Bundeskriminalamtes 2016, abrufbar unter www.bka.de, dort S. 16 ff.). Illegale Onlinehandelsplattformen stellen aus Sicht von EUROPOL eine der zentralen Schnittstellen von Cybercrime und weiteren Formen - auch organisierter - Kriminalität dar (Internet Organised Crime Threat Assessment 2017, abrufbar unter www.europol.eu). Gegenüber den bereits etablierten Handelsgütern, wie z. B. Betäubungsmitteln, sei eine deutliche Zunahme bei Angeboten von Hackertools und -dienstleistungen zu verzeichnen. Diese Aspekte hat auch die Europäische Kommission in der gemeinsamen Mitteilung mit der Hohen Vertreterin der Union für Außen- und Sicherheitspolitik an das Europäische Parlament und den Rat „Abwehrfähigkeit, Abschreckung und Abwehr: die Cybersicherheit in der EU wirksam erhöhen“ vom 13.09.2017 betont und auf das derzeit nur geringe Risiko der Tatentdeckung hingewiesen [JOIN(2017) 450, dort S. 18].

In der strafrechtlichen Praxis stellt sich das Problem, dass eine Beihilfe gemäß § 27 StGB zu den über die Plattform begangenen Straftaten oft nicht nachweisbar ist, da die Haupttaten bilateral zwischen den Beteiligten über verschlüsselte Kommunikationskanäle abgewickelt werden, jedenfalls aber nicht offen im Forum sichtbar sind. Zudem sind bei vielen Foren die Arten von Straftaten, die über sie abgewickelt werden sollen, zu Beginn nicht klar definiert. Die Täter stellen eine informationstechnische Struktur zur Verfügung und wissen um die strafrechtliche Relevanz der über den Dienst abgewickelten Geschäfte. Welche Art von Gütern konkret gehandelt wird, spielt für die Täter dabei keine Rolle. Moderne Foren verfügen zudem häufig über vollautomatisierte Verkaufssysteme, bei denen eine Beihilfe zu einer konkreten Haupttat noch schwieriger nachzuweisen ist. Ungeachtet dessen erfasst die strafrechtliche Ahndung unter dem Gesichtspunkt der Beihilfe in der Regel nicht hinreichend den aktiven Charakter der Tathandlung, die die Grundlagen der Underground-Economy schafft.

Auch eine Zurechnung von Einzeltaten unter dem Gesichtspunkt einer bandenmäßigen Tatbegehung ist häufig nicht möglich, da in der Regel kriminelle Foren und Marktplätze der Underground Economy von nur einer Person oder zwei Personen geführt werden. Bei Foren und Marktplätzen mit mehreren Personen in der Führungsebene ist überdies zu berücksichtigen, dass sich die Betreiber regelmäßig nicht persönlich kennen und oftmals kein übergeordnetes, homogenes Interesse vorliegt. Ist im Einzelfall eine Bande im strafrechtlichen Sinne anzunehmen, ist im Weiteren für jede einzelne Tat nach den allgemeinen Kriterien festzustellen, ob sich die anderen Bandenmitglieder hieran als Mittäter, Anstifter oder Gehilfen beteiligt oder ob sie gegebenenfalls überhaupt keinen strafbaren Tatbeitrag geleistet haben. Letzteres kann insbesondere dann in Betracht kommen, wenn einzelne Betreiber nur für die Aufrechterhaltung und Wartung der technischen Infrastruk-

tur oder die Administration nicht strafrechtlich relevanter Bereiche zuständig sind und glaubhaft versichern, keine Kenntnis von oder jedenfalls kein Interesse an den über das Forum abgeschlossenen oder angebahnten illegalen Verkaufstätigkeiten gehabt zu haben. In derartigen Konstellationen kommt auch die Annahme eines uneigentlichen Organisationsdelikts durch den Aufbau und die Aufrechterhaltung eines auf Straftaten ausgerichteten Geschäftsbetriebs regelmäßig nicht in Betracht.

Eine effektive Strafverfolgung kommt schließlich auch unter dem Gesichtspunkt der Bildung einer kriminellen Vereinigung im Sinne des § 129 StGB nicht stets in Betracht. Die Anforderungen an den Nachweis konkreter Einzeltaten sind bei dem abstrakten Gefährdungsdelikt zwar erleichtert, in der Regel wird jedoch die für den Tatbestand erforderliche Festigkeit der Struktur nicht erreicht. Dies gilt ungeachtet der durch das 54. Gesetz zur Änderung des Strafgesetzbuches – Umsetzung des Rahmenbeschlusses 2008/841/JI des Rates vom 24. Oktober 2008 zur Bekämpfung der organisierten Kriminalität vom 17. Juli 2017 (BGBl. I S. 2440) erfolgten Ausweitung des Vereinigungsbegriffs im Sinne des § 129 Absatz 2 StGB, denn Voraussetzung einer Vereinigung ist weiterhin ein organisierter Zusammenschluss. Dies erfordert zumindest eine gewisse Organisationsstruktur sowie eine instrumentelle Vorausplanung und Koordinierung. Zusammenschlüsse, die sich zufällig zur unmittelbaren Begehung einer Straftat bilden, wie dies bei den hier relevanten Cyberstrukturen oft der Fall ist, dürften dem Vereinigungsbegriff des § 129 Absatz 2 StGB nicht unterfallen.

Weil der Zugang zu den einschlägigen Angeboten in der Regel keinen besonderen technischen Anforderungen unterliegt und die Erreichbarkeit teilweise zwar beschränkt, aber ohne erheblichen technischen Aufwand möglich ist, bieten die Handelsplattformen somit einen niedrigschwelligen Zugriff auf logistische Infrastrukturen für die Begehung von Straftaten auch für Personen, die herkömmliche Beschaffungswege für Waffen, Betäubungsmittel oder kriminelle Dienstleistungen nicht beschreiten. Auf diese Weise wird einer unbestimmten Vielzahl von Personen die Möglichkeit verschafft, eine unbestimmte Vielzahl von Straftaten zu begehen. Diese Angebote stellen eine erhebliche Gefahr für die öffentliche Sicherheit dar, ohne dass die geltende Rechtslage ausreichende Möglichkeiten für eine angemessene strafrechtliche Verfolgung bietet.

Diese Lücken sollen durch die Einführung der neuen Vorschrift geschlossen werden. Der Entwurf zielt darauf, das Betreiben von auf die Förderung, Ermöglichung oder Erleichterung illegaler Zwecke ausgerichteten Plattformen unabhängig von dem Nachweis der Beteiligung an einzelnen konkreten Handelsgeschäften unter Strafe zu stellen. Die Vorschrift soll die öffentliche Sicherheit und die staatliche Ordnung schützen, daher erfolgt die Aufnahme in den sechsten Abschnitt. Die Aufnahme eines Tatbestands in das Strafgesetzbuch fördert eine einheitliche Rechtsanwendung und erscheint daher gegenüber spezialgesetzlichen Einzelregelungen vorzugswürdig. Soweit vereinzelt bereits Strafvorschriften das Verschaffen einer Gelegenheit zur Begehung von Straftaten erfassen, zum Beispiel § 29 Absatz 1 Nummer 10 BtMG, regelt § 126a StGB-E den Sonderfall der internetbasierten Tatbegehung. Dem Konkurrenzverhältnis wird insoweit durch eine Subsidiaritätsklausel in § 126a Absatz 1 StGB-E Rechnung getragen.

Eine Einschränkung auf nur bestimmte, für das geschützte Rechtsgut besonders gefährlich einzustufende szenetypische Delikte ist aus Gründen der Verhältnismäßigkeit nicht erforderlich und nicht sachgerecht. Ein solcher Katalog liefe – ähnlich einer Neuregelung in einzelnen Spezialgesetzen – Gefahr, unvollständig zu bleiben. Zum anderen ist die Zugänglichmachung jedes internetbasierten Angebots, das auf die Begehung jeglicher Straftaten gerichtet ist, gleichermaßen strafwürdig. Dies gilt zum Beispiel auch für Plattformen, welche auf die Begehung von Äußerungsdelikten gerichtet sind. Dem Verhältnismäßigkeitsgrundsatz wird durch die ausdrückliche Beschränkung des Absatzes 2 Rechnung getragen, die sicherstellt, dass die Strafe nicht schwerer sein darf als die für die ermöglichten rechtswidrigen Taten angedrohte Strafe. Die Gefährlichkeit der Delikte wird durch die internetbasierte Begehung erheblich erhöht, da die Leistungen quasi ohne Be-

schränkung zugänglich sind. Der potentielle Adressatenkreis ist damit praktisch unbegrenzt. Die Täter des § 126a StGB-E eröffnen durch die Handelsplattformen einen örtlich, zeitlich und sachlich unbegrenzten Zugang zu illegalen Waren und Dienstleistungen, der in der analogen Welt auch nicht annähernd vergleichbar besteht oder möglich wäre und Grundlage weiterer digitaler oder analoger Handelsketten sein kann.

Die Vorschrift ist hinsichtlich ihres sachlichen Anwendungsbereichs auch zur Ermöglichung der Berücksichtigung der weiteren technischen Entwicklung weit gefasst und erfasst jegliche internetbasierte Zugänglichmachung von Leistungen. Der Begriff „internetbasiert“ ist hierbei technikbezogen auszulegen und erfasst alle Dienste, die auf der Netzwerkschicht des OSI-Referenzmodells über das Internet-Protokoll (IP) vermittelt werden. Über den allgemeinen Sprachgebrauch zum Begriff „Internet“ hinaus fallen damit nicht nur solche Dienste in den Anwendungsbereich der Norm, die zum Beispiel über das World Wide Web oder per E-Mail erbracht werden, sondern auch per Voice-over-IP Dienste. Eine Beschränkung des Anwendungsbereichs auf auf technische Weise zugangsbeschränkte Internetplattformen wäre demgegenüber nicht sachgerecht, würde doch gerade derjenige, der solche Dienste offen und für jeden zugänglich feilbietet, insoweit straflos bleiben. Die Dreistigkeit des unverdeckt Handelnden würde damit belohnt werden. Das für die Öffentlichkeit bestehende Gefährdungspotential ist zudem deutlich größer, wenn jedermann unabhängig von seinem technischen Know-how auf eine internetbasierte Zugänglichmachung illegaler Leistungen zugreifen könnte. Zur Abgrenzung der durch den Tatbestand erfassten Angebote von legalen Handelsplattformen, die ohne den Willen der Betreiber für strafrechtlich relevante Zwecke genutzt werden, wird – in Anlehnung an die Formulierung des § 129 StGB – überdies auf den Zweck und die Ausrichtung der Tätigkeit abgestellt. Damit sind Betreiber, deren Angebote ohne entsprechende Zielrichtung zur Förderung von Straftaten genutzt werden, vom Tatbestand ausgenommen. Dies gewährleistet eine Beschränkung schon des Tatbestands auf strafwürdige Online-Angebote. Die Prüfung der Ausrichtung der Plattform hat anhand des konkreten Einzelfalls zu erfolgen und ist allgemein verbindlichen Kriterien nicht zugänglich. Auf Grundlage der bisherigen praktischen Erfahrungen dürften indizielle Bedeutung in diesem Zusammenhang erlangen zum Beispiel das tatsächliche Angebot einer Online-Plattform, der Umgang mit Hinweisen auf Handel mit illegalen Waren und Dienstleistungen und auch die etwa in Allgemeinen Geschäftsbedingungen (AGB) enthaltenen Vorgaben. Schon im Rahmen der Prüfung eines Anfangsverdachts dürften diese Umstände ohne erheblichen Aufwand feststellbar sein.

Im Zusammenspiel mit den zum 1. Juli 2017 durch das Gesetz zur Reform der strafrechtlichen Vermögensabschöpfung vom 13. April 2017 (BGBl. I S. 872) neu gefassten Abschöpfungsvorschriften sichert die Einführung des neuen Tatbestands zudem die effektive Bekämpfung auch der wirtschaftlichen Grundlagen der Underground-Economy.

Der Grundtatbestand des § 126a Absatz 1 StGB-E ist aufgrund der potentiell erheblichen Gefährdung des Rechtsfriedens mit Geldstrafe oder Freiheitsstrafe von bis zu fünf Jahren bedroht. Der Täter des § 126a StGB-E schafft durch den Betrieb der Plattform Aktionsraum und niedrigschwelligen Zugriff auf Infrastruktur für die Begehung auch schwerer Straftaten durch eine unbestimmte Vielzahl anderer Straftäter und dadurch eine andauernde und ganz erhebliche Gefahr für die öffentliche Sicherheit und Ordnung. Bei erhöhten Strafdrohungen in anderen Tatbeständen, zum Beispiel § 29 Absatz 1 Nummer 10 BtMG, greift die Subsidiaritätsklausel des § 126a Absatz 1 StGB-E. Aus Gründen der Verhältnismäßigkeit begrenzt § 126a Absatz 2 StGB-E die Strafdrohung auf die für die Straftat im Sinne von § 126a Absatz 1 StGB-E angedrohte Strafe. Neben dem Grundtatbestand sieht § 126a Absatz 3 StGB-E bei gewerbsmäßiger oder bandenmäßiger Begehung aufgrund der erhöhten kriminellen Energie eine mit im Mindestmaß erhöhter Strafdrohung bewehrte Qualifikation vor. Die Erfahrungen der Praxis zeigen, dass nicht jede Tathandlung im Sinne des § 126a StGB-E gewerbsmäßig begangen wird, Anbieter stellen Handelsmöglichkeiten auch oft kostenfrei aus ideellen Gründen oder zur Mehrung des eigenen Ansehens in der Szene bereit. Auch bei Tauschbörsen für Schriften mit kinder-

pornographischen Inhalten fehlt es ferner regelmäßig an einem gewerbsmäßigen Handeln. Das Kriterium der Gewerbsmäßigkeit rechtfertigt daher die in der Qualifikation vorgesehene höhere Strafdrohung.

Die erhöhte Strafdrohung verdeutlicht überdies, dass die Qualifikation des § 126a Absatz 3 StGB-E dem Bereich der schweren Kriminalität zuzurechnen ist. Dies begründet in Verbindung mit den Besonderheiten der Tatbegehung mittels internetbasierter Leistung die Aufnahme des Qualifikationstatbestands in den Katalog der Ermittlungsmaßnahme des § 100a Absatz 2 Nr. 1 d) StPO. Die Ermittlungen wegen eines ausschließlich den Grundtatbestand des § 126a Absatz 1 StGB-E erfüllenden Sachverhalts dürften zwar ohne die technischen Überwachungsmaßnahme des § 100a StPO nachhaltig erschwert werden, aus Gründen der Verhältnismäßigkeit ist jedoch die Aufnahme nur der Qualifikation sachgerecht.

Zu Absatz 1

Die Vorschrift trägt der besonderen Gefährlichkeit des Zugänglichmachens internetbasierter Leistungen Rechnung, die sich ohne zeitliche, sachliche oder räumliche Grenzen an Personen jeden Alters richten. Die Vorschrift ist hinsichtlich ihres sachlichen Anwendungsbereichs weit gefasst, um künftige technische Entwicklungen berücksichtigen zu können, und erfasst jegliche internetbasierte Zugänglichmachung von Leistungen. Der Begriff „internetbasiert“ ist hierbei technikbezogenen auszulegen und erfasst alle Dienste, die auf der Netzwerkschicht des OSI-Referenzmodells über das Internet-Protokoll (IP) vermittelt werden. Über den allgemeinen Sprachgebrauch zum Begriff „Internet“ hinausgehend fallen damit nicht nur solche Dienste in den Anwendungsbereich der Norm, die zum Beispiel über das World Wide Web oder per E-Mail erbracht werden, sondern beispielsweise auch Voice-over-IP Dienste. Eine Beschränkung des Anwendungsbereichs auf Internetplattformen, deren Zugang und Erreichbarkeit durch besondere technische Vorkehrungen beschränkt ist, wäre demgegenüber nicht sachgerecht, würde doch gerade derjenige, der solche Dienste offen und für jeden zugänglich feilbietet, insoweit straflos bleiben. Die Dreistigkeit des unverdeckt Handelnden würde damit belohnt werden. Unter dem Aspekt der Strafwürdigkeit ist die Einschränkung auf das Darknet nicht geboten, da eine etwaige Verschleierung der Täteridentität nichts über das durch die Tat begangene Unrecht aussagt. Das für die Öffentlichkeit bestehende Gefährdungspotential ist zudem deutlich größer, wenn jedermann von überall unabhängig von seinem technischen Know-how auf eine internetbasierte illegale Leistung zugreifen könnte.

Der Begriff der Leistung beschreibt alle Angebote, die sich an einen oder mehrere Nutzer richten, ohne stets auf Dauer und wiederholte Nutzung abzuzielen. Ein Zugänglichmachen liegt entsprechend der zu § 184 Absatz 1 Nummer 1 StGB entwickelten Grundsätze dann vor, wenn den Nutzern die Möglichkeit der Wahrnehmung der Leistung eröffnet wird. So stellt zum Beispiel der Betrieb eines sogenannten „bulletproof hosters“, der keine eigenen Angebote online stellt, sondern lediglich den Speicherplatz und das Routing für (kriminelle) Dritter anbietet, ein Fall des „Zugänglichmachens“ dar. Zur Abgrenzung der vom Tatbestand erfassten von den nicht strafwürdigen Angeboten ist auf die Ausrichtung des Zwecks oder der Tätigkeit abzustellen. So soll sichergestellt werden, dass ordnungsgemäß eingerichtete Online-Angebote, die entgegen ihrer Zielsetzung auch für den Handel mit illegalen Waren oder Dienstleistungen genutzt werden, nicht der Gefahr strafrechtlicher Verfolgung ausgesetzt werden. Ziel der Zugänglichmachung im Sinne des § 126a Absatz 1 StGB-E muss das Ermöglichen, Fördern oder Erleichtern von rechtswidrigen Straftaten sein. Dem steht nicht entgegen, dass auch legale Aktivitäten abgewickelt werden sollen, soweit dies lediglich dem Verschleiern der tatsächlichen Zielrichtung dient. Die Prüfung der Ausrichtung einer Online-Plattform hat anhand des konkreten Einzelfalls zu erfolgen und ist allgemein verbindlichen Kriterien nicht zugänglich. Hierbei kann auf die zu § 202c Absatz 1 Nummer 2 StGB entwickelten Maßstäbe abgestellt werden. Auf Grundlage der bisherigen praktischen Erfahrungen dürften indizielle Bedeutung in diesem Zusammenhang erlangen zum Beispiel das tatsächliche Angebot einer Online-Plattform, der

Umgang mit Hinweisen auf Handel mit illegalen Waren und Dienstleistungen und auch die etwa in Allgemeinen Geschäftsbedingungen (AGB) enthaltenen Vorgaben. Schon im Rahmen der Prüfung eines Anfangsverdachts dürften diese Umstände ohne erheblichen Aufwand aufzuklären sein. Stellt die Begehung von Straftaten nur einen Zweck untergeordneter Bedeutung dar, so findet der Tatbestandsausschluss des § 126a Absatz 4 StGB-E Anwendung.

§ 126a StGB-E soll sämtliche rechtswidrige Taten (§ 11 Absatz 1 Nummer 5 StGB) erfassen. Eine Beschränkung auf einzelne Tatbestände birgt die Gefahr der Unvollständigkeit und trägt ferner nicht der Strafwürdigkeit der Zugänglichmachung jedes internetbasierten Angebots Rechnung, das auf die Begehung jeglicher Straftaten gerichtet ist. Die Erfahrungen in der Praxis zeigen, dass Schwerpunkte des illegalen Online-Handels die Bereiche Betäubungsmittel, Waffen, Falschgeld beziehungsweise gefälschte Urkunden, Kinderpornographie und Cyberwerkzeuge, insbesondere Hacker-Programme, sind. Daneben können aber auch Plattformen nicht außen vor bleiben, die zum Beispiel auf die Begehung von Äußerungsdelikten gerichtet sind oder als Dienstleistungen die Begehung von Straftaten gegen die körperliche Unversehrtheit und gegen das Leben vermitteln.

Der größte Anteil der Handelsaktivitäten fällt nach den praktischen Erfahrungen im Bereich der Betäubungsmittel an. Im Bereich gefälschter Urkunden sind besonders Identitätsnachweise zu nennen, die vor allem für betrügerische Bestellungen und die Anlage finanztransaktionsverschleiernder Tarnkonten genutzt werden. Abgeschottete Plattformen im Netz sind zudem einer der vorherrschenden Absatz- und Verteilmechanismen kinderpornographischer Schriften, deren Verbreitungsgrad ohne die dahinterstehenden technischen Infrastrukturen kaum denkbar wäre. Im Bereich der Cyberwerkzeuge werden über Online-Plattformen zum Beispiel Schadsoftwareprogramme angeboten, mit denen Schwachstellen von IT-Systemen ausgenutzt und Sicherungen überwunden werden können. Ebenso wird sogenannte Ransomware, das heißt Software, die Nutzdaten verschlüsselt, um von den Nutzern Zahlungen zur Aufhebung der Verschlüsselung zu erlangen, angeboten. Des Weiteren wird die unmittelbare Durchführung von Cyberangriffen als Dienstleistung offeriert. Hier stehen die sogenannten Botnetze im Fokus, das heißt eine Vielzahl gekaperter Drittrechner, die unter Täterkontrolle koordinierte Überlastangriffe auf legitime Webseiten und -services durchführen.

Eine Abgrenzung zu den nicht dem Tatbestand unterfallenden legalen Handelsplattformen gelingt über das Tatbestandsmerkmal der Ausrichtung des Zwecks oder der Tätigkeit unter Heranziehung der entwickelten Kriterien zu § 202c Absatz 1 Nummer 2 StGB sowie ferner über eine Anwendung des Tatbestandsauschlusses nach § 126a Absatz 4 Nummer 1 StGB-E. Etwaigen Abgrenzungsproblemen im Bereich der beruflichen Handlungen, insbesondere der in § 53 Absatz 1 Satz 1 Nummer 5 StPO genannten Personen, wird durch die Schutzklausel des § 126a Absatz 4 Nummer 2 StGB-E begegnet.

Zu Absatz 2

Aus Gründen der Verhältnismäßigkeit begrenzt § 126a Absatz 2 StGB-E die Strafdrohung auf die für die rechtswidrige Tat im Sinne von § 126a Absatz 1 StGB-E angedrohte Strafe. Dieses Vorgehen orientiert sich an den Regelungen in vergleichbaren Vorschriften, zum Beispiel §§ 202d Absatz 2, 257 Absatz 2, 258 Absatz 3 StGB.

Zu Absatz 3

Neben dem Grundtatbestand sieht § 126a Absatz 3 StGB-E für Täter, welche die Tat nach § 126a Absatz 1 StGB-E gewerbsmäßig oder als Mitglied einer Bande begehen, die sich zur fortgesetzten Begehung von Straftaten im Sinne von § 126a Absatz 1 StGB-E verbunden hat, aufgrund der erhöhten kriminellen Energie eine mit im Mindestmaß erhöhter Strafdrohung bewehrte Qualifikation vor. Aufgrund des bestehenden Organisationsaufwands der Betreiber wird die Intention der Bertreiber nicht selten auf eine Gewinnerzie-

lung ausgerichtet sein. Die Erfahrungen der Praxis zeigen, dass nicht jede Tathandlung im Sinne des § 126a StGB-E gewerbsmäßig begangen wird, Anbieter stellen Handelsmöglichkeiten auch oft kostenfrei aus ideellen Gründen oder zur Mehrung des eigenen Ansehens in der Szene bereit. Auch bei Tauschbörsen für Schriften mit kinderpornographischen Inhalten fehlt es ferner regelmäßig an einem gewerbsmäßigen Handeln. Das Kriterium der Gewerbsmäßigkeit rechtfertigt daher die vorgesehene höhere Strafdrohung, die zudem verdeutlicht, dass die Qualifikation des § 126a Absatz 3 StGB-E dem Bereich der besonders schweren Kriminalität zuzurechnen ist.

Der Strafrahmen orientiert sich auf Grundlage der erhöhten kriminellen Energie von auf Dauer angelegten, gewinnorientierten Strukturen an denen für vergleichbare Delikte bei gewerbsmäßiger oder bandenmäßiger Begehungsweise, zum Beispiel § 260 Absatz 1 Nummer 1 und 2 StGB (Hehlerei), § 263 Absatz 3 Satz 2 Nummer 1 StGB (Betrug) – auch in Verbindung mit § 263a Absatz 2 StGB (Computerbetrug) –, § 267 Absatz 3 Satz 2 Nummer 1 StGB (Urkundenfälschung) und § 303b Absatz 4 Satz 2 Nummer 2 StGB (Computersabotage). Das Delikt ist, anders als einige der vorgenannten Beispiele, als Qualifikation ausgestaltet, um dem Umstand Rechnung zu tragen, dass Online-Plattformen für illegale Waren und Dienstleistungen den Nährboden weiter Bereiche des Cybercrime darstellen. Die Bedeutung der Plattformen entspricht dabei der vergleichbarer Einrichtungen im legalen Bereich. Der Unternehmensgegenstand zahlreicher, auch international erfolgreicher Unternehmen besteht im Unterhalt einer Infrastruktur für den örtlich und zeitlich ungebundenen Austausch von Waren und Dienstleistungen. Ebenso stellen sich Funktion und Bedeutung der illegalen Plattformen dar, denen eine erhebliche Ausstrahlwirkung im Bereich des Cybercrime zukommt.

Zu Absatz 4

§ 126a Absatz 4 Nummer 1 StGB-E sieht einen Tatbestandsausschluss für die Fälle vor, in denen die Begehung von Straftaten nur einen Zweck oder eine Tätigkeit von untergeordneter Bedeutung darstellt. Die Vorschrift stellt damit klar, dass insbesondere Leistungen von legalen Handelsplattformen, die von Dritten für strafrechtlich relevante Zwecke genutzt werden, nicht unter § 126a Absatz 1 StGB-E fallen. Im Übrigen können die in der Rechtsprechung zu § 129 Absatz 3 Nummer 2 StGB entwickelten Abgrenzungskriterien herangezogen werden. § 126a Absatz 4 Nummer 2 StGB-E nimmt entsprechend zu § 202d Absatz 3 Satz 2 Nummer 2 StGB aus Gründen der Verhältnismäßigkeit und zum Schutze bestimmter Berufsgruppen solche Handlungen von der Strafbarkeit aus, die ausschließlich der Erfüllung rechtmäßiger dienstlicher oder beruflicher Pflichten dienen. Hierzu zählen insbesondere berufliche Handlungen der in § 53 Absatz 1 Satz 1 Nummer 5 StPO genannten Personen.

Zu Nummer 3

Die Computerstraftaten der §§ 202a ff., 303a ff. StGB sind aktuell als bloße „Bagatellkriminalität“ ausgestaltet. Sie weisen – abgesehen von den Qualifikationen des § 303b Abs. 2 und 4 StGB – Strafrahmen auf, die im Höchstmaß zwei oder drei Jahre betragen und damit dem einer Beleidigung oder dem unbefugten Gebrauch eines Fahrzeugs entsprechen. Die erheblich gestiegene Bedeutung dieser Straftaten in der immer weiter vernetzten Gesellschaft wird nicht adäquat abgebildet.

Der bisherige Strafrahmen bei den Computerstraftaten berücksichtigt nicht die besonderen und technisch bedingten Umstände bei der Entwendung von Daten. In der Gesamtschau wiegt etwa das Delikt des Ausspähens von Daten (§ 202a StGB) daher mindestens ebenso schwer – wenn nicht schwerer – wie der „klassische“ Diebstahl.

Das Opfer eines „Datenklaus“ kann nicht mehr alleine über seine Daten verfügen. Diese können gegen seinen Willen verwendet, ggfls. sogar veröffentlicht werden. Hinzu kommt, dass ein Diebstahl in der Regel dadurch ungeschehen gemacht werden kann, indem die

entwendete Sache zurückgegeben wird. Dies ist beim „Datenklau“ nicht möglich: Das Opfer muss stets damit rechnen, dass weitere Kopien der Daten existieren. Eine Ausspähung von Daten kann damit nie rückgängig gemacht werden, das Opfer muss dauerhaft mit dem belastenden Zustand leben, dass seine privaten Daten für immer potentiell öffentlich sind. Insoweit übersteigt der Unrechtsgehalt sogar den des Diebstahls.

In Fällen, in denen der Täter auch Daten aus dem Privat- oder gar Intimbereich des Opfers erlangt, kann für das Opfer die Situation sogar vergleichbar mit dem Wohnungseinbruchdiebstahl sein, der einen Verbrechenstatbestand darstellt. Die Strafschärfung ist hier darin begründet, dass der Täter zum Zwecke der Ausführung der Tat in die Privatwohnung und damit den höchstpersönlichen Lebensbereich des Opfers eindringt und damit größeres Unrecht verwirklicht als bei einem einfachen Diebstahl. Folglich muss dieses erhöhte Unrecht auch einen Abbildung im Strafrahmen finden, etwa durch Einführung von Qualifikationstatbeständen.

Private Daten sind insbesondere durch das Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme (Artikel 2 Absatz 1 i.V.m. Artikel 1 Absatz 1 des Grundgesetzes) gegen staatliche Zugriffe besonders geschützt. Dieses Grundrecht stellt auch eine objektiv-rechtliche Wertentscheidung der Verfassung dar, die für alle Bereiche der Rechtsordnung gilt und aus der sich Richtlinien für Gesetzgebung ableiten lassen. Danach ist der Staat auch in der Pflicht, rechtswidrigen Datenzugriff durch Private auch durch entsprechende Strafnormen effektiv zu verhindern.

Aufgrund der Vergleichbarkeit des verwirklichten Unrechts ist es deshalb angemessen, für Delikte wie das Ausspähen von Daten und die verwandten Delikte einen höheren Strafrahmen – jeweils ähnlich dem Diebstahl – vorzusehen, um dem erhöhten Unrecht Rechnung zu tragen.

Zu Nummer 4

Die vorgeschlagene Regelung soll als neuer § 202e StGB in den Fünfzehnten Ab-schnitt (Verletzung des persönlichen Lebens- und Geheimbereichs) des Besonderen Teils des Strafgesetzbuchs eingefügt werden. Für eine systematische Regelung an dieser Stelle spricht, dass das geschützte Rechtsgut der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme dem persönlichen Lebens-und Geheimbereich zuzuordnen ist. Die Regelung entspricht im Grunddelikt und hinsichtlich der nachfolgenden Ausführungen dem Vorschlag des Landes Hessen für ein entsprechende Anpassung (BR-Drs. 338/16 und 47/18).

Zu Absatz 1

Das Merkmal der Unbefugtheit als allgemeines Rechtfertigungselement entspricht dem in § 201 verwendeten Begriff. Es stellt klar, dass eine Strafbarkeit bei wirksamer ausdrücklicher oder konkludenter Einwilligung ausgeschlossen ist. Dadurch ist es z. B. nicht strafbar, wenn Betreiber von Internetseiten Cookies (Ein Cookie (engl. "Keks") ist eine Textinformation, die eine besuchte Website (hier "Server") über den Browser im Rechner des Betrachters ("Client") platziert. Der Client sendet die Cookie-Information bei späteren, neuen Besuchen dieser Seite mit jeder Anforderung wieder an den Server.) verwenden und darauf, wie es datenschutzrechtlich geboten und üblich ist, hinweisen. Auch das Aufspielen von Softwareupdates o. ä. ist hierdurch von Strafbarkeit ausgenommen, ebenso wie z. B. das Aufspüren von Sicherheitslücken im EDV-System eines Unternehmens, soweit der "Hacker" vom Inhaber des Unternehmens mit dieser Aufgabe betraut wurde. Auch sonst sozialadäquate Handlungen sind nicht "unbefugt" im Sinne von § 202e StGB-E (zur Sozialadäquanz bei anderen Delikten im 15. Ab-schnitt vgl. Fischer, StGB, 63. Auflage, Erläuterungen zu § 201).

Durchaus erfasst sind hingegen beispielsweise Applikationen (Apps) für Endgeräte, die einen größeren Funktionsumfang haben als in der jeweiligen Beschreibung oder Datenschutzerklärung angegeben, bei deren Installation die Nutzer mithin bewusst über die eingeräumten Zugriffsrechte getäuscht werden.

§ 202e StGB-E erfüllt insoweit auch einen bedeutenden Zweck im Zivilrecht, indem die Funktion eines Schutzgesetzes im Sinne von § 823 Absatz 2 BGB eingenommen und damit auch zivilrechtlich ein besserer Verbraucherschutz erreicht wird.

Auf die Beschränkung des Tatbestandes auf "fremde" informationstechnische Systeme wurde bewusst verzichtet, um auch Fälle zu erfassen, in denen z. B. ein Arbeitnehmer ein mobiles IT-System des Arbeitgebers zur alleinigen Benutzung erhält und der Arbeitgeber dieses heimlich infiltriert hat, um unbefugt in den persönlichen Lebens- und Geheimbereich des Arbeitnehmers einzudringen. Auch sollen z. B. Hotelgäste bei der Benutzung für sie fremder IT-Systeme vor Infiltration der von ihnen verarbeiteten Informationen durch den Eigentümer des Systems geschützt werden.

Die Anwendungspraxis des seit 1953 geltenden § 248b StGB zeigt, dass grundsätzliche Probleme durch die Einführung eines weiteren Falles des strafbewehrten Verbots der unbefugten Benutzung von Sachen in das Strafgesetzbuch nicht zu erwarten sind.

Das informationstechnische System ist in Absatz 6 legaldefiniert. Es sollen nur solche Geräte, Anlagen etc. geschützt sein, die objektiv eine besondere Bedeutung für den Berechtigten haben oder deren Fremdnutzung besonders gefährdungsintensiv ist und die damit in herausgehobener Weise schutzwürdig sind. Damit sind z. B. nicht vernetzte elektronische Unterhaltungsgeräte, Spielzeug oder Taschenrechner aus dem Tatbestand ausgeklammert.

Zugleich stellt die Bagatellklausel des Absatzes 1 Satz 2 eine mit derjenigen des § 201 StGB inhaltsgleiche Tatbestandseinschränkung dar. Nach dieser ist die Tathandlung nur strafbar, wenn sie geeignet ist, berechtigte Interessen eines anderen zu beeinträchtigen. Ob es sich dabei um materielle oder ideelle, private oder öffentliche Interessen handelt, ist gleichgültig, sofern sie nur vom Recht als schutzwürdig anerkannt sind oder diesem jedenfalls nicht zuwiderlaufen. Dass der Betroffene tat-sächlich in seinen Interessen beeinträchtigt wird, ist nicht erforderlich; vielmehr genügt es schon, dass die Tat dazu geeignet ist.

Durchgreifende verfassungsrechtliche Bedenken gegen die Bagatellklausel unter dem Aspekt des Bestimmtheitsgrundsatzes (Artikel 103 Absatz 2 des Grundgesetzes) bestehen nicht. Sie ist in § 201 StGB in derselben Formulierung wie in § 202e StGB-E unverändert in Kraft seit dem 26. August 1990. Obwohl das BVerfG sich bereits im Jahr 2010 mit § 201 StGB befasst hat, wurde die Bagatellklausel nicht beanstandet (Vgl. BVerfG Beschluss vom 10. Dezember 2010, 1 BvR 2020/04, NJW 2011, 1863).

Ein Datenverarbeitungsvorgang (DV-Vorgang) ist ein Arbeitsablauf, der durch eine elektronische Verarbeitung zu einem konkreten Ergebnis führt (Vgl. Lenckner/Winkelbauer CR 1986, 654, 658 f; Fischer, StGB, § 263a Rn 3). Auf Grund bestimmter Eingabedaten (Input) muss mit dem im Computer gespeicherten Pro-gramm - ggf. ergänzt durch weitere Eingaben zur Steuerung - ein Arbeitsergebnis erzielt und ausgegeben werden (Output).

Da auch elektronisch fernzusteuernde Anlagen und Einrichtungen geschützt werden sollen, auf denen selbst keine DV-Vorgänge im vorbeschriebenen juristischen Sinne ablaufen (z. B. ein fernwartbares Schleusentor, das durch einen schlichten Öffnen/Schließen-Befehl reagiert, ohne dass dazu ein Computerprogramm abläuft), wurde zusätzlich der Begriff des informationstechnischen Ablaufs aufgenommen. Nach der Legaldefinition des § 2 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) ist damit jede Verarbeitung oder Übertragung von Informationen durch technische

Mittel gemeint. Dies ist weitergehend als der Begriff des DV-Vorgangs. Es soll sichergestellt werden, dass der strafrechtliche Schutz von Automatisierungs-, Prozesssteuerungs- und Prozessleitsystemen (Industrial Control Systems, ICS) gewährleistet wird, um den Rechtsrahmen für Industrie 4.0 zu verbessern.

Aus diesem Grunde erstreckt sich der Schutzbereich von § 202e StGB-E nicht lediglich auf Datenverarbeitungsanlagen oder Datenverarbeitungen wie §§ 303a StGB oder 303b StGB, sondern geht darüber hinaus.

"Zugang" ist die Möglichkeit, ohne weitere Zwischenschritte einen IT-Vorgang auszulösen oder zu beeinflussen. Gemeint ist damit sowohl der physische, unmittelbare Zugriff als auch derjenige über Datenleitungen. Der Zugang ist erlangt, wenn das System infiltriert, also eine etwaige Sperre überwunden und der Täter in der Lage ist, Eingaben unmittelbar vorzunehmen.

Es wird nicht verkannt, dass die Regelung des Absatzes 1 einen weiten Anwendungsbereich hat. Die Bagatellklausel sorgt jedoch dafür, dass nicht strafwürdige Fälle von dem Tatbestand zuverlässig ausgeschlossen werden. Ferner sorgt die Begrenzung auf bestimmte IT-Systeme in Absatz 6 dafür, dass nicht schutzwürdige Systeme wie z. B. eine Modelleisenbahn von der Norm nicht erfasst werden.

Die Anwendungspraxis des geltenden Rechts hat gezeigt, dass jede weitergehende Einschränkung des Tatbestandes dazu führt, dass ein hinreichender strafrechtlicher Schutz des Grundrechts auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme nicht erreicht werden kann. Die mangelnde Effektivität der geltenden Normen lässt sich durch die trotz der hohen Zahl betroffener Opfer auffällig niedrigen Verurteilungszahlen (Vgl. Strafverfolgungsstatistik 2013 (Statistisches Bundesamt, Fachserie 10, Reihe 3): 30 Verurteilungen wegen § 202a StGB, 32 wegen § 303a StGB und 26 wegen § 303b StGB) empirisch belegen.

Die Verhängung von Strafe als ultima ratio des Staates zur Verhütung von Sozialschäden ist dann nicht am Platze, wenn das Opfer keinen Schutz verdient und keines Schutzes bedarf, weil es von ohne weiteres verfügbaren Selbstschutzmöglichkeiten ohne triftigen Grund keinen Gebrauch gemacht hat. Genau diese Selbstschutzmöglichkeit besteht heutzutage angesichts der Komplexität von IT-Systemen einerseits und derjenigen von Schadsoftware andererseits eben nicht mehr (Vgl. BVerfG a.a.O.).

Zu Absatz 2

Bestimmte, nicht schutzwürdige IT-Systeme sollen vom Tatbestand ausgenommen werden. Die Eignung zur Verarbeitung personenbezogener Daten und die Nutzung als Steuerungskomponente für bestimmte Anwendungen begründen die Schutzwürdigkeit des Systems.

Zu Absatz 3

Durch diese Regelung soll die Strafverfolgung bei Fällen im Nähebereich begrenzt werden, um bestimmte persönliche Beziehungen durch Eingreifen von Amts wegen nicht zu stören.

Zu Nummer 4

Bisher fehlt im Bereich der Computerstraftaten Qualifikationstatbestände, die dem Unrechtsgehalt herausgehobener Fallkonstellationen gerecht werden können. Um diese Lücke zu schließen, wird mit § 202e ein abgestuftes System von Qualifikationstatbeständen geschaffen.

Nicht abgebildet werden kann insbesondere das kollusive Zusammenwirken in Banden, das ein besonderes, zusätzliches Missbrauchspotential mit sich bringt. (Bsp.: gemeinsamer Aufbau und Betrieb von Botnetzen (§§ 202a, b, c, d StGB), Durchführung von DDoS-Angriffen z. N. von Firmen und/oder kritischen Infrastrukturen (§§ 303a, b StGB)).

Aufgrund dessen geht den Normen des Computerstrafrechts eine Eignung zur Generalprävention weitgehend ab. Selbst schwerste Angriffe können de lege lata unter Anwendung der Regeln der Strafzumessung fast immer nur mit Geld- oder Bewährungsstrafen geahndet werden.

Der unzutreffend niedrige Strafrahmen führt überdies dazu, dass zur Täteridentifizierung notwendige Ermittlungsmaßnahmen, wie z.B. die Telekommunikationsüberwachung oder eine Erhebung von Verkehrsdaten – jedenfalls in Form von sog. Vorratsdaten gem. § 100g Abs. 2 StPO - mangels Katalogtatenschwelle ausnahmslos nicht durchgeführt werden können.

Hinzu kommt – vor dem Hintergrund immer größer werdender gesellschaftlicher Vernetzung – ein erhebliches und stets anwachsendes Gefahrenpotential, das in den Strafnormen adäquat abgebildet werden muss. Dies gilt insbesondere da, wo Daten, die den Kernbereich der privaten Lebensgestaltung betreffen, in einer Wiese veröffentlicht werden, die dem Opfer nachhaltig Schaden zufügen kann.

Die Norm führt deshalb abgestufte Qualifikationstatbestände entsprechend der bekannten Systematik für den Bereich der Computerstraftaten ein.

ARTIKEL 5 (Änderung der Strafprozessordnung)

Zu Nummer 1

Mit der Einführung von Qualifikationstatbeständen mit entsprechend angehobenem Strafmaß (s.o.) wird die Voraussetzung geschaffen, diese Tatbestände nun auch in die Kataloge des § 100a Abs. 2 und § 100g Abs. 2 StPO aufzunehmen.

Die Qualifikationstatbestände erreichen die vom Bundesverfassungsgericht geforderte Schwere, der Strafrahmen entspricht mit einer Mindesthöchststrafe von fünf Jahren den vom Bundesverfassungsgericht gestellten Anforderungen [BVerfG. Beschluss vom 12. Oktober 2011, 2 BvR 236, 237, 422/08, BVerfGE 129, 208]. Auch im Übrigen fügen sich die Qualifikationstatbestände in die Systematik des § 100a Abs. 2 StPO und § 100g Abs. 2 StPO ein. Es handelt sich auch um Straftaten, die eine erforderliche Nähe zur Telekommunikationsüberwachung und Verkehrsdatenerhebung aufweisen und bei denen die Telekommunikationsüberwachung und Verkehrsdatenerhebung ein besonders geeignetes Ermittlungsinstrument darstellt.

Zu Nummer 2

Die in § 100a Abs. 2 vorgenommenen Änderungen werden auch auf § 100g Abs. 2 übertragen. Weil der Katalog des § 100g Abs. 2 StPO enger ausgelegt ist, als der des § 100a Abs. 2, wurden nur die besonders schwere Qualifikationstatbestände übertragen.

Zu Nummer 3

Täter, die im Darknet ihren kriminellen Aktivitäten nachgehen, handeln häufig streng abgeschirmt. „Vertrauen“ in die Geschäftspartner, mit denen in der Regel ausschließlich pseudonym und verschlüsselt kommuniziert wird, ist eine zentrale Währung auf Darknet-Handelsplattformen und auf Plattformen zur Verbreitung von Kinderpornografie. Solange es den Ermittlungsbehörden nicht möglich ist, mittels vorhandener Accounts in diese Kommunikationsbeziehungen einzudringen, ist ein erfolgversprechendes Vorgehen kaum

möglich. Viele Straftaten, insbesondere im Bereich des illegalen Handels im Darknet und der Kinderpornografie, bleiben deshalb unaufgeklärt.

Die Übernahme und Weiterführung von digitalen Identitäten der identifizierten Beschuldigten durch Ermittler ist deshalb eine der wichtigsten Ermittlungsmethoden. Sie ist gleichwohl bisher unzureichend geregelt.

Mit der Übernahme von Accounts kann die Kommunikation unter den in der Szene bekannten Nicknamen der identifizierten Beschuldigten verdeckt fortgeführt werden. Dies ist deshalb so wichtig, weil in den entsprechenden Szenen den langjährig aktiven Accounts ein großes Vertrauen entgegen gebracht wird, während neu angelegten Accounts eher Misstrauen entgegenschlägt.

Derzeit ist die Übernahme von digitalen Identitäten des identifizierten Beschuldigten nach überwiegender Auffassung mangels expliziter Rechtsgrundlage nur mit freiwilliger und ausdrücklicher Zustimmung des Beschuldigten möglich. Weder über eine Beschlagnahme gemäß § 94 StPO noch über die Vorschriften zur vorläufigen Sicherstellung von dem Verfall oder der Einziehung unterliegender Gegenstände gemäß § 111b ff. StPO werden die Strafverfolgungsbehörden ermächtigt, einem Beschuldigten die Nutzungs- bzw. Eigentumsrechte an Kennungen bei Telemediendiensten oder Telekommunikationsdiensten endgültig zu entziehen.

Bisher existieren lediglich Behelfslösungen, die es an erforderlicher Rechtssicherheit und Durchsetzbarkeit vermissen lassen: Die Beschuldigten müssen in den entsprechenden Ermittlungsverfahren etwa auf positive Folgen der Hilfe zur Aufklärung oder Verhinderung von schweren Straftaten gem. § 46b StGB hingewiesen und um die freiwillige Übergabe von Zugangsdaten und Passwörtern gebeten werden. Dies hat zur Folge, dass nur in den wenigsten Fällen die Beschuldigten mit einer Übernahme von digitalen Identitäten einverstanden sind, denn es besteht ein erhebliches Risiko der Selbstbelastung.

Es bedarf deshalb einer ausdrücklichen Ermächtigung für die Übernahme von digitalen Identitäten, auch gegen den Willen der Beschuldigten. Die anschließende Nutzung entsprechender übernommener Accounts hat gegenüber den Kommunikationspartnern keinen Eingriffscharakter, so dass diesbezüglich keine spezielle Ermächtigungsgrundlage erforderlich ist. Nach der Rechtsprechung des BVerfG schützt das Fernmeldegeheimnis des Art. 10 GG das Vertrauen des Einzelnen darin, dass eine Fernkommunikation, an der er beteiligt ist, nicht von Dritten zur Kenntnis genommen wird, nicht aber die Enttäuschung des personengebundenen Vertrauens in den Kommunikationspartner. Auch ein Eingriff in das Recht auf informationelle Selbstbestimmung (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) liegt nicht schon dann vor, wenn eine staatliche Stelle sich unter einer Legende in eine Kommunikationsbeziehung zu einem Grundrechtsträger begibt. Das Vertrauen eines Kommunikationsteilnehmers in die Identität und Wahrhaftigkeit seiner Kommunikationspartner ist dann nicht schutzwürdig, wenn hierfür wie bei anonymer Internetkommunikation über Nicknames keinerlei Überprüfungsmechanismen bereitstehen. Das Vertrauen darauf, jedenfalls nicht mit einer staatlichen Stelle zu kommunizieren, ist nicht schutzwürdig. Dies gilt auch dann, wenn durch die staatliche Stelle gerade das deliktische Vertrauen dem Kommunikationspartner gegenüber ausgenutzt wird, wonach das Gegenüber ebenfalls ein Straftäter sei. Das deliktische Vertrauen, beim Kommunikationspartner handele es sich ebenfalls um einen Straftäter, ist nicht schutzwürdig.

Dabei ist auch ein weiterer Aspekt zu beachten: Eine Übernahme der Identität kann in der Regel erfolgen, wenn der Nutzer die Zugangsdaten preisgibt. Der Nutzer läuft dabei aber möglicherweise Gefahr, sich einer Verfolgung wegen weiterer Straftaten auszusetzen, die erst durch den polizeilichen Einblick in den Account offenbar werden. Deswegen ist es erforderlich, den Nutzer gegen diese erzwungene Selbstbelastung zu schützen. Darüber hinaus können in der Regel durch die Weiterführung des Accounts deutlich mehr Rechtsgüter geschützt und Straftaten aufgeklärt werden, als durch das Verbot der Selbstbelas-

tung möglicherweise nicht verfolgt werden können. Das Insolvenzrecht hält hier mit § 97 Abs. 1 InsO ein erfolgreiches Beispiel bereit: Der Nutzer wird davor geschützt, aufgrund von durch den Mitwirkungsakt ggf. aufgedeckter weiterer Straftaten verfolgt zu werden. Dies kann – in Verbindung mit den Strafzumessungsregeln – ein entscheidendes Anreizkriterium sein, um den Nutzer zu einer Übergabe der Zugangsdaten zu bewegen und so die Verfolgung von Darknet-Kriminalität entscheidend zu erleichtern.

Im Übrigen ist nach der Regelung die Übernahme von Accounts nicht nur dann möglich, wenn der ursprüngliche Inhaber die Zugangsdaten preisgibt. Accounts können auch dann übernommen und genutzt werden, wenn die staatliche Stelle die Zugangsdaten auf andere Weise erlangt, etwa durch verdeckte Ermittlungsmaßnahmen oder im Rahmen einer Durchsuchung.

Zu Artikel 6 (Änderung des Gesetzes über die internationale Rechtshilfe in Strafsachen)

Aufgrund der teilweise sehr langen Bearbeitungszeiten von Rechtshilfeersuchen besteht häufig die Gefahr, dass Daten bereits gelöscht oder verschoben worden sind, wenn das Ersuchen abschließend bearbeitet ist.

Deshalb ist es erforderlich, ein Vorabsicherungsverfahren im nationalen Recht zu verankern. Art. 16, 17, 29 der Cybercrime-Konvention (CCC) sehen vor, dass der Vertragsstaat Vorkehrungen treffen muss, um Daten - die in der Regel flüchtig sind, schnell gelöscht oder verschoben werden können - in Erwartung eines noch zu stellenden Rechtshilfeersuchens unverzüglich sichern zu können. Aktuell existieren keine entsprechenden Regelungen in DEU(ohne Herausgabe, sondern reine Vorabsicherung beim Provider).

Maßnahmen der Verfahrensbeschleunigung auf EU-Ebene, wie etwa die Vorschläge im Rahmen des Dossiers „e-evidence“, lassen die Erforderlichkeit dabei nicht entfallen: So werden die Regelungen im Rahmen „e-evidence“, wenn/falls sie in Kraft treten, nur für innereuropäische Maßnahmen gelten; Maßnahmen in Drittstaaten sind nur möglich, wenn kein Konflikt mit dem nationalen Recht besteht.

Es ist aber gerade auch zur Unterstützung von Cybercrime-Ermittlungsverfahren in Drittstaaten außerhalb der EU erforderlich, durch eine rasche Vorabsicherung von Daten die in Deutschland vorhandenen Beweise zu sichern. Diese Unterstützung für Ermittlungsmaßnahmen in anderen Vertragsstaaten der CCC wird auch die Cybersicherheit in Deutschland stärken, weil viele Cyberstraftaten, die sich in Deutschland auswirken, vom Ausland aus begangen werden. Deutschland macht sich unglaubhaft, wenn es einerseits von diesen Drittstaaten ein effektives Vorgehen gegen Cyberkriminelle fordert, aber gleichzeitig nicht die innerstaatlichen Voraussetzung für eine effektive und zielgerichtete Unterstützung von Ermittlungen schafft.

Deutschland kann aufgrund der fehlenden Regelungen anfragende Drittstaaten derzeit nicht effektiv unterstützen. Solange eine explizite Regelung zur Vorabsicherung nicht existiert, müssen die betroffenen Behörden – wenn eine Unterstützung überhaupt möglich ist – mit rechtlich komplexen Behelfslösungen arbeiten, die in der Regel keine unverzügliche Vorabsicherung ermöglichen. Eine tatsächliche „Vorabsicherung“ (Sicherung und Verbleib der Daten beim Provider bis zum Eintreffen des Rechtshilfeersuchens) findet somit in Deutschland nicht statt.

§ 67 IRG in seiner derzeitigen Fassung ist nicht einschlägig, da die Norm nur von einer Beschlagnahme oder Sicherstellung von Gegenständen oder Daten spricht.

Dies kommt aber für Telekommunikationsverkehrsdatenerhebung nach § 100g Abs. 1 StPO, Daten aus der Speicherpflicht nach § 100g Abs. 2 StPO, Bestandsdaten nach § 100j StPO, Auskunftsersuchen nach Bestands- und Nutzungsdaten von Telemedien (§§

161, 163 StPO, 14, 15 TMG) nicht in Betracht, weil die jeweils einschlägigen Spezialnormen weitere oder andere Voraussetzungen vorsehen.

Hinzu kommt, dass § 67 IRG eine Sicherstellung und Beschlagnahme - also einen Übergang der Daten in staatliche Verfügungsgewalt - bereits vor Stellung des Rechtshilfeersuchens vorsieht. Dies ist auch aus grundrechtlicher Sicht problematisch, weil die Daten auf diesem Wege bereits vor Stellung des Rechtshilfeersuchens (und damit noch vor dem Vorliegen eines Grundes für die Sicherstellung und Beschlagnahme) in staatliche Verfügung gelangen könnten. Grundrechtsschonender wäre es demgegenüber, eine bloße Sicherung beim Provider anordnen zu können. Die Daten würden erst dann in staatliche Gewalt übergehen, wenn das Rechtshilfeersuchen tatsächlich gestellt und für valide befunden wurde.

Die Norm sieht deshalb vor, dass die Behörden und Beamten des Polizeidienstes anordnen können, dass bestimmte Daten für höchstens 180 Tage vor Veränderungen geschützt beim Provider gespeichert und verwahrt werden müssen. Die Zuständigkeit der Polizei begründet sich aus der besonderen Eilbedürftigkeit der Maßnahme. Gleichzeitig ist von einer eher geringen Grundrechtsrelevanz der Maßnahme auszugehen, weil die Daten noch nicht in staatliche Verfügung übergehen.

Eine Verlängerung dieses Vorabsicherungs-Zeitraums ist möglich, so dass sich eine maximale Dauer der Vorabsicherung von 360 Tagen ergibt. Dieser Zeitrahmen erlaubt die sachgerechte Bearbeitung von Rechtshilfeersuchen zur Herausgabe der Daten. So ist sichergestellt, dass diese nur dann in staatliche Gewalt gelangen oder im Rahmen von Rechtshilfe herausgegeben werden, wenn alle Voraussetzungen sorgfältig geprüft wurden.

Die Norm stellt dabei klar, dass die Daten nur dann erhoben werden dürfen - also von der Vorab-Speicherung in staatliche Verfügung übertragen werden - wenn die Voraussetzungen der allgemeinen Vorschriften - also etwa § 100g StPO - vorliegen.

Ebenso richtet sich die Benachrichtigung nach den allgemeinen Vorschriften. Wenn eine Vorschrift die Benachrichtigung des Nutzers untersagt, darf der Nutzer auch nicht über die Vorabsicherung informiert werden.

Zu Artikel 7 (Änderung des Justizvergütungs- und entschädigungsgesetzes)

Es handelt sich um eine Folgeänderung, mit der ein Entschädigungsanspruch der Provider für Maßnahmen der Vorabsicherung einführt wird. Der Entschädigungsanspruch betrifft dabei nur die Vorabsicherung selbst. Für die - ggf. erfolgende - anschließende Erhebung der Daten durch die Behörde kann davon unabhängig eine Entschädigung nach den dafür geltenden Vorschriften verlangt werden.

Zu Artikel 8 (Änderung des Artikel 10-Gesetzes)

Es handelt sich um eine Folgeänderung zur Einführung des neuen § 202f StGB.

Zu Artikel 9 (Änderung des Bundeskriminalamtsgesetzes)

Es handelt sich um eine Folgeänderung zur Einführung der neuen §§ 202e und 202f StGB.

Zu Artikel 10 (Änderung der Außenwirtschaftsverordnung)

Zu Nummer 1 und Nummer 2

Die Änderung trägt der Aufnahme der KRITIS-Kernkomponentenbranchenspezifischen IT-Produkte, die bisher als branchenspezifische Software rechtsunsystematisch lediglich in der Außenwirtschaftsverordnung definiert waren, Rechnung und ist ein Folgeänderung.

Zu Artikel 11 (Inkrafttreten)

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