Referentenentwurf

des Bundesministeriums des Innern, für Bau und Heimat

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme

(Zweites IT-Sicherheitsgesetz – IT-SiG 2.0)

A. Problem und Ziel

Die Gewährleistung der Cyber- und Informationssicherheit ist ein Schlüsselthema für Staat, Wirtschaft und Gesellschaft. Gerade mit Blick auf die zunehmende Digitalisierung aller Lebensbereiche sind sie auf funktionierende Informations- und Kommunikationstechnik angewiesen - sei es für den Informationsaustausch, die Produktion, den Konsum, Dienstleistungen oder zur Pflege privater Kontakte. Voraussetzung hierfür ist eine sichere Infrastruktur.

Cyber-Angriffe stellen für Staat, Wirtschaft und Gesellschaft daher ein großes Gefahrenpotential dar. Die Angriffe werden qualitativ immer ausgefeilter und somit für alle Betroffenen auch gefährlicher. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) beobachtet einen stetigen Anstieg von Schadprogrammen, jährlich kommen mehr als 100 Millionen neue Varianten hinzu. Die Schadsoftware Emotet dominiert bereits seit Jahren die Gefährdungslage.

Vorfälle wie die Ransomware „WannaCry“ verdeutlichen die Situation. Mittlerweile werden Daten bei Ransomwareangriffen nicht mehr nur verschlüsselt, sondern zudem vorher kopiert und ausgeleitet. Auch die Aufdeckung von Schwachstellen in Computerchips wie „Meltdown“ und „Spectre“ machen die Anfälligkeit für Sicherheitslücken besonders deutlich. Daneben hat der zu Beginn des Jahres 2018 in den Medien bekanntgewordene Angriff auf die Kommunikationsinfrastrukturen des Auswärtigen Amtes deutlich gemacht, dass der Staat seine Schutzmaßnahmen anpassen muss. Vorfälle, bei denen persönliche Daten unter anderem aus sozialen Netzwerken, Kunden- oder Patientendateien ohne Einverständnis und Wissen der Betroffenen offengelegt und weit verbreitet werden (z.B. Datenleak-Vorfall Anfang des Jahres 2019) zeigen, dass nicht nur Staat, Wirtschaft und Gesellschaft, sondern auch Individualinteressen betroffen sind.

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

Insgesamt ist Cyber-Sicherheit nicht statisch, ein aktuelles Schutzniveau ist daher kein Garant für eine erfolgreiche Abwehr der Angriffe von morgen. Daher bedarf es einer ständigen Anpassung und Weiterentwicklung der Schutzmechanismen und der Abwehrstrategien.

B. Lösung

Entsprechend dem Auftrag aus dem Koalitionsvertrag für die 19. Legislaturperiode wird der mit dem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl. I 2015 S. 1324) geschaffene Ordnungsrahmen durch das Zweite IT-Sicherheitsgesetz erweitert (IT-SiG 2.0). Schwerpunktmäßig werden folgende Änderungen vorgenommen:

ENTWURF

– Verbesserung des Schutzes der IT der Bundesverwaltung u.a. durch weitere Prüf- und Kontrollbefugnisse des BSI und Festlegung von Mindeststandards durch das BSI.

– Schaffung von Befugnissen zur Detektion von Schadprogrammen zum Schutz der Regierungsnetze.

– Abfrage von Bestandsdaten bei Anbietern von Telekommunikationsdienstleistungen, um Betroffene über Sicherheitslücken zu informieren.

– Befugnis für das BSI, Sicherheitslücken an den Schnittstellen informationstechnischer Systeme zu öffentlichen TK-Netzen zu detektieren sowie Einsatz von Systemen und Verfahren zur Analyse von Schadprogrammen und Angriffsmethoden.

– Schaffung einer Anordnungsbefugnis des BSI gegenüber Telekommunikations- und Telemedienanbietern zur Abwehr spezifischer Gefahren für die Informationssicherheit.

– Ausweitung der Pflichten für Betreiber Kritischer Infrastrukturen und weiterer Unternehmen im besonderen öffentlichen Interesse.

– Schaffung von Eingriffsbefugnissen für den Einsatz und Betrieb von kritischen Komponenten.

– Pflicht der Telemediendiensteanbieter, Fälle von rechtswidrig verbreiteten Daten an das BKA als Zentralstelle zu melden.

– Etablierung von Verbraucherschutz im Bereich der Informationssicherheit als zusätzliche Aufgabe des BSI.

– Schaffung der Voraussetzungen für ein einheitliches IT-Sicherheitskennzeichen, das die IT-Sicherheit der Produkte sichtbar macht.

– Überarbeitung des Bußgeldregimes.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

E. Erfüllungsaufwand

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Es entsteht kein Erfüllungsaufwand für die Bürgerinnen und Bürger.

E.2 Erfüllungsaufwand für die Wirtschaft

Der Wirtschaft entsteht für die Erfüllung der im Gesetz vorgesehenen zusätzlichen Aufgaben ein Aufwand von einmaligen Personalkosten in Höhe von ca. 69.654 Euro, jährlichen

ENTWURF

Personalkosten in Höhe von ca. 2.913.022 Euro und jährlichen Sachkosten in Höhe von rund 6 Millionen Euro.

Die Ermittlung des Erfüllungsaufwands für die Wirtschaft ist von deutlichen Unsicherheiten geprägt, da zu einer Reihe von Vorschriften noch untergesetzliche Ausführungen erforderlich sind und die von der Wirtschaft genutzte IT nur in Teilen bekannt ist.

E.3 Erfüllungsaufwand der Verwaltung

Der Verwaltung entsteht für die Erfüllung der im Gesetz vorgesehenen zusätzlichen Aufgaben insgesamt ein Aufwand von insgesamt 948 Panstellen/Stellen mit Personalkosten in Höhe von jährlich rund 68,6 Millionen Euro.

Davon entfallen auf:

– das Bundesamt für Sicherheit in der Informationstechnik 799 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 56,9 Millionen Euro. Darin ist bereits eine OPH-Quote enthalten. Zusätzlich entstehen Sachkosten in Höhe von einmalig 28 Mio. Euro und jährlich in Höhe von rund 47,5 Mio. Euro;

– das Bundeskriminalamt 90 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 7,3 Mio. Euro. Zusätzlich sind zur Umsetzung des Gesetzes Sachkosten in Höhe von einmalig 765.000 Euro und jährlich in Höhe von rund 9,5 Mio. Euro zu berücksichtigen;

– die Bundesnetzagentur rund 34 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von 2,4 Mio. Euro;

– die Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben 21 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von 1,7 Mio. Euro;

– das Bundesministerium des Innern, für Bau und Heimat 4 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von 284.724 Euro.

Dezentral werden bei den Ressorts für ein Ineinandergreifen des Sicherheitsmanagements und den erforderlichen Ausbau der Informationssicherheit in der Bundesverwaltung weitere Planstellen/Stellen mit Personalkosten und gegebenenfalls weitere Sachkosten erforderlich werden, die im jeweiligen Haushaltsaufstellungsverfahren geltend gemacht werden.

F. Weitere Kosten

Keine.

ENTWURF

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 BSIG vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 73 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, wird wie folgt geändert:

1. § 2 wird wie folgt geändert:

   a) Absatz 3 Satz 1 wird wie folgt gefasst:

   „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) In Absatz 3 Satz 2 werden vor den Worten „der Bundesgerichte“ die Wörter „des Bundesverfassungsgerichts“ und ein Komma eingefügt.

   c) Nach Absatz 8 wird folgender Absatz 8a eingefügt:

   „(8a) Protokollierungsdaten im Sinne dieses Gesetzes sind Aufzeichnungen über technische Ereignisse oder Zustände innerhalb informationstechnischer Systeme. Protokollierungsdaten dienen der Erkennung, Eingrenzung oder Beseitigung von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder der Erkennung, Eingrenzung oder Beseitigung von Angriffen auf die Kommunikationstechnik des Bundes.“

   d) Nach Absatz 9 werden die folgenden Absätze 9a und 9b eingefügt:

   „(9a) IT-Produkte im Sinne dieses Gesetzes sind Softwareprodukte sowie alle einzelnen oder miteinander verbundenen Hardwareprodukte.

   (9b) Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffser-

ENTWURF

kennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten."

e) In Absatz 10 Satz 1 Nummer 1 wird das Wort „sowie" durch ein Komma ersetzt und es werden nach dem Wort „Versicherungswesen" die Wörter „sowie Siedlungsabfallentsorgung" eingefügt.

f) Die folgenden Absätze 13 und 14 werden angefügt:

„(13) Kritische Komponenten im Sinne dieses Gesetzes werden für Betreiber nach § 8d Absatz 2 Nummer 1 durch den Katalog von Sicherheitsanforderungen nach § 109 Absatz 6 des Telekommunikationsgesetzes näher bestimmt. Alle übrigen kritischen Komponenten werden gesetzlich festgelegt.

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

1. die Güter nach § 60 Absatz 1 Nummer 1 bis 5 der Außenwirtschaftsverordnung in der jeweils geltenden Fassung herstellen oder entwickeln,

2. die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind oder

3. die Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung in der jeweils geltenden Fassung sind, oder nach § 1 Absatz 2 der Störfall-Verordnung diesen gleichgestellt sind.

Die Unternehmen im besonderen öffentlichen Interesse nach Nummer 2 werden durch die Rechtsverordnung nach § 10 Absatz 5 bestimmt, in der festgelegt wird, welche wirtschaftlichen Kennzahlen bei der Berechnung der inländischen Wertschöpfung heranzuziehen sind, mit welcher Methodik die Berechnung zu erfolgen hat und welche Schwellenwerte maßgeblich dafür sind, dass ein Unternehmen zu den größten Unternehmen in Deutschland im Sinne der Nummer 2 gehört."

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

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

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

„5a. Wahrnehmung der Aufgaben und Befugnisse nach Artikel 58 Absatz 7 und 8 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (ABl. L 151 vom 7.6.2019, S. 15) als nationale Behörde für die Cybersicherheitszertifizierung;".

c) Nummer 14 wird wie folgt gefasst:

„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 Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;".

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

ENTWURF

„14a. Verbraucherschutz und Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik, insbesondere durch Beratung und Warnung von Verbrauchern in Fragen der Sicherheit in der Informationstechnik und unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;“.

e) Nummer 17 wird wie folgt gefasst:

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

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

g) Die folgenden Nummern 19 und 20 werden angefügt:

„19. Empfehlungen für Identifizierungs- und Authentisierungsverfahren und Bewertung dieser Verfahren im Hinblick auf die Informationssicherheit;

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

3. Nach § 4 werden die folgenden §§ 4a und 4b eingefügt:

„§ 4a

Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte

(1) Das Bundesamt ist befugt, die Sicherheit der Kommunikationstechnik des Bundes und ihrer Komponenten, einschließlich technischer Infrastrukturen, die zu deren Betrieb erforderlich sind, zu kontrollieren. Es kann hierzu die Bereitstellung der zur Erfüllung der Aufgaben nach § 2 Absatz 1 Satz 2 Nummer 1 und 14 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 die unentgeltliche Herausgabe von Kopien davon, auch in elektronischer Form, verlangen, soweit nicht Geheimschutzinteressen oder überwiegende Sicherheitsinteressen entgegenstehen.

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

(3) Bei Einrichtungen eines Dritten, bei dem eine Schnittstelle zur Kommunikationstechnik des Bundes besteht, kann das Bundesamt auf der Schnittstellenseite der Einrichtung nur im Einvernehmen mit dem Dritten die Sicherheit der Schnittstelle kontrollieren. Es kann hierzu im Einvernehmen mit dem Dritten die zur Aufgabenerfüllung erforderlichen Informationen, insbesondere zu technischen Details, zu Strategien, Planungen und Regelungen sowie Unterlagen und Datenträger des Betreibers einsehen und unentgeltlich Kopien, auch in elektronischer Form, 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

ENTWURF

ihrer jeweiligen Rechts- und Fachaufsicht mit. Mit der Mitteilung soll es Vorschläge zur Verbesserung der Informationssicherheit, insbesondere zur Beseitigung der festgestellten Mängel, verbinden.

(5) Ausgenommen von den Befugnissen nach Absatz 1 bis 3 sind die Auslands-Informations- und Kommunikationstechnik im Sinne des § 9 Absatz 2 des Gesetzes über den Auswärtigen Dienst, soweit sie nicht ausschließlich für das Inland oder Anwender im Inland betrieben wird. Die Bestimmungen für die Schnittstellen der Kommunikationstechnik des Bundes im Inland bleiben davon unberührt. Näheres zu Satz 1 regelt eine Verwaltungsvereinbarung zwischen dem Bundesministerium des Innern, für Bau und Heimat und dem Auswärtigen Amt.

(6) Die Befugnisse nach Absatz 1 bis 3 gelten im Geschäftsbereich des Bundesministeriums der Verteidigung nicht für Informations- und Kommunikationstechnik, die für die Bundeswehr und ihre Zwecke betrieben wird. Näheres regelt eine Verwaltungsvereinbarung zwischen dem Bundesministerium des Innern, für Bau und Heimat und dem Bundesministerium der Verteidigung.

§ 4b

Allgemeine Meldestelle für die Sicherheit in der Informationstechnik

(1) Zur Wahrnehmung der Aufgaben nach § 3 nimmt das Bundesamt als zentrale Stelle für Meldungen Dritter Informationen über Sicherheitsrisiken in der Informationstechnik entgegen und wertet diese aus.

(2) Das Bundesamt kann zur Wahrnehmung der Aufgaben nach Absatz 1 Informationen zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweisen entgegennehmen. Das Bundesamt richtet hierzu geeignete Meldemöglichkeiten ein. Die Meldungen können anonym erfolgen. Soweit die Meldung nicht anonym erfolgt, kann der Meldende im Rahmen der Meldung verlangen, dass seine personenbezogenen Daten nur anonymisiert weitergegeben werden dürfen. Dies gilt nicht in den Fällen des § 5 Absatz 5 und Absatz 6 Satz 1. Eine Übermittlung der personenbezogenen Daten in den Fällen von § 5 Absatz 5 und Absatz 6 Satz 1 hat zu unterbleiben, wenn für das Bundesamt erkennbar ist, dass die schutzwürdigen Interessen des Meldenden das Allgemeininteresse an der Übermittlung überwiegen. Zu berücksichtigen ist dabei auch die Art und Weise, mittels derer der Meldende die Erkenntnisse gewonnen hat. Die Entscheidung nach Satz 6 muss dem oder der behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem oder einer weiteren Bediensteten des Bundesamts, der oder die die Befähigung zum Richteramt hat, zur vorherigen Prüfung vorgelegt werden.

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

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

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

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

ENTWURF

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

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

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

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

(5) Sonstige gesetzliche Meldepflichten, Regelungen zum Geheimschutz, Übermittlungshindernisse und Übermittlungsregelungen bleiben unberührt.“

4. § 5 wird wie folgt geändert:

a) Absatz 2 wird wie folgt gefasst:

„(2) Protokolldaten nach Absatz 1 Satz 1 Nummer 1 dürfen über den für die automatisierte Auswertung nach Absatz 1 Satz 1 Nummer 1 erforderlichen Zeitraum hinaus, längstens jedoch für 12 Monate, gespeichert werden, soweit tatsächliche Anhaltspunkte bestehen, dass diese im Falle der Bestätigung eines Verdachts nach Absatz 3 Satz 2 zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich sein können. Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Auswertung der nach diesem Absatz gespeicherten Daten nur automatisiert erfolgt und dass ein Zugriff auf Daten, die länger als drei Monate gespeichert sind, nur beim Vorliegen tatsächlicher Erkenntnisse über die Betroffenheit des Bundes mit einem Schadprogramm erfolgt. Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist. Eine nicht automatisierte Verarbeitung ist nur nach Maßgabe der nachfolgenden Absätze zulässig. Soweit hierzu die Wiederherstellung pseudonymisierter Protokolldaten erforderlich ist, muss diese durch die Präsidentin oder den Präsidenten des Bundesamtes oder der Vertretung im Amt angeordnet werden. Die Entscheidung ist zu dokumentieren.“

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

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

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

„§ 5a

Verarbeitung behördeninterner Protokollierungsdaten

Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes Protokollierungsdaten, die durch den Betrieb von Kommunikationstechnik des Bundes anfallen, verarbeiten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen

ENTWURF

von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist und Geheimschutzinteressen oder überwiegende Sicherheitsinteressen nicht entgegenstehen. Die Bundesbehörden sind verpflichtet, das Bundesamt bei Maßnahmen nach Satz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu behördeninternen Protokollierungsdaten nach Satz 1 sicherzustellen. Hierzu dürfen sie dem Bundesamt die entsprechenden Protokollierungsdaten übermitteln. § 5 Absatz 1 Satz 5, Absatz 2 bis 4, 8 und 9 gilt entsprechend. § 4a Absatz 6 gilt für die Verpflichtung nach § 5a Satz 2 entsprechend.“

6. Der bisherige § 5a wird § 5b und wie folgt geändert:

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

   b) Dem Absatz 7 wird folgender Satz angefügt:

   „Ein begründeter Einzelfall liegt in der Regel vor, wenn eine Stelle eines Landes betroffen ist.“

7. Nach § 5b wird folgender § 5c eingefügt:

„§ 5c

Bestandsdatenauskunft

(1) Das Bundesamt darf von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes) Auskunft verlangen. Die Auskunft nach Satz 1 darf nur verlangt werden, um im Einzelfall

1. weitergehende Angriffe auf die Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme Kritischer Infrastrukturen, digitaler Dienste oder von Unternehmen im besonderen öffentlichen Interesse zu verhindern oder

2. sonstige erhebliche Schäden vom betroffenen Dritten abzuwenden,

und wenn das Bundesamt im Rahmen der Erfüllung seiner gesetzlichen Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 2 oder 14 von ziel- und zweckgerichteten Beeinträchtigungen der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme Dritter Kenntnis erlangt hat und die schutzwürdigen Interessen des betroffenen Dritten eine unmittelbare Kontaktaufnahme durch das Bundesamt mit ihm als erforderlich erscheinen lassen. Die Auskunft desjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, muss für die Kontaktaufnahme erforderlich sein.

(2) Die Auskunft nach Absatz 1 darf nach Maßgabe des Absatzes 1 Satz 3 auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§§ 113 Absatz 1 Satz 3, 113c Absatz 1 Nummer 3 des Telekommunikationsgesetzes). Die rechtlichen und tatsächlichen Grundlagen des Auskunftsverlangens sind aktenkundig zu machen.

(3) Aufgrund eines Auskunftsverlangens nach den Absätzen 1 bis 2 hat derjenige, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, die zur Auskunftserteilung erforderlichen Daten unverzüglich zu übermitteln.

ENTWURF

(4) Nach erfolgter Auskunft weist das Bundesamt die betroffene Person auf die bei ihr festgestellten Beeinträchtigungen hin. Nach Möglichkeit weist das Bundesamt die betroffene Person auf technische Mittel hin, mittels derer die festgestellten Beeinträchtigungen durch die betroffene Person selbst beseitigt werden können.

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

(6) In den Fällen des Absatzes 2 ist die betroffene Person über die Auskunft zu benachrichtigen. Im Falle der Weitergabe der Information nach § 5 Absatz 5 oder wenn Tatsachen die Annahme rechtfertigen, dass die Voraussetzungen einer Weitergabe nach § 5 Absatz 5 vorliegen, ergeht darüber keine Benachrichtigung an die betroffene Person, sofern und solange überwiegende schutzwürdige Belange Dritter entgegenstehen. Wird nach Satz 4 die Benachrichtigung zurückgestellt oder von ihr abgesehen, sind die Gründe aktenkundig zu machen.

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

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

2. Übermittlungen nach Absatz 5.“

8. § 7 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) Nach der Angabe „§ 3 Absatz 1 Satz 2 Nummer 14“ werden die Wörter „und Nummer 14a“ angefügt.

bb) In Nummer 1 werden nach dem Wort „Warnungen“ die Wörter „und Informationen“ eingefügt.

cc) In Nummer 1 Buchstabe c) werden die Wörter „im Falle eines Verlustes oder eines unerlaubten Zugriffs“ durch die Wörter „bei einem Verlust oder unerlaubten Zugriff“ ersetzt.

dd) Nach Nummer 1 Buchstabe c) wird folgender Buchstabe d) angefügt:

„d) Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten.“

ee) Satz 3 und 4 werden gestrichen.

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

„(1a) Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung der Warnungen zu informieren. Diese Informationspflicht besteht nicht,

1. wenn hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks gefährdet wird oder,

2. wenn berechtigterweise davon ausgegangen werden kann, dass der Hersteller an einer vorherigen Benachrichtigung kein Interesse hat.

ENTWURF

Soweit entdeckte Sicherheitslücken oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern oder weil das Bundesamt gegenüber Dritten zur Vertraulichkeit verpflichtet ist, kann es den Kreis der zu warnenden Personen einschränken; Kriterien hierfür sind insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere Zuverlässigkeit des Empfängers."

c) Absatz 2 Satz 1 wird wie folgt gefasst:

„Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 und Nummer 14a kann das Bundesamt die Öffentlichkeit unter Nennung der Bezeichnung und des Herstellers des betroffenen Produkts vor Sicherheitslücken in informationstechnischen Produkten und Diensten und vor Schadprogrammen warnen, wenn hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik hiervon ausgehen, oder Sicherheitsmaßnahmen sowie den Einsatz bestimmter informationstechnischer Produkte und Dienste empfehlen."

9. § 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 Nummer 1, 14, 14a, 17 und 18 auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen. Es kann sich hierbei der Unterstützung Dritter bedienen, soweit berechtigte Interessen des Herstellers der betroffenen Produkte und Systeme dem nicht entgegenstehen.

(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. In dem Auskunftsverlangen gibt das Bundesamt die Rechtsgrundlage, den Zweck des Auskunftsverlangens und die benötigten Auskünfte an und legt eine angemessene Frist für die Übermittlung der Auskünfte fest. Das Auskunftsverlangen enthält ferner einen Hinweis auf die in § 14 vorgesehenen Sanktionen.

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

(4) Die Auskünfte und die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14, 14a, 17 und 18 genutzt werden. Das Bundesamt darf seine Erkenntnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14, 14a, 17 und 18 erforderlich ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben.

(5) Kommt ein Hersteller der Aufforderung des Bundesamtes nach Absatz 2 Satz 1 nicht oder nur unzureichend nach, kann das Bundesamt hierüber die Öffentlichkeit informieren. Es kann hierbei den Namen des Herstellers sowie die Bezeichnung des betroffenen Produkts oder Systems angeben, und darlegen inwieweit der Hersteller

ENTWURF

seiner Auskunftspflicht nicht nachgekommen ist. Zuvor ist dem Hersteller mit angemessener Frist Gelegenheit zur Stellungnahme zu gewähren. § 7 Absatz 2 Satz 2 gilt entsprechend.“

10. Nach § 7a werden die folgenden §§ 7b, 7c und 7d eingefügt:

„§ 7b

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

(1) Das Bundesamt kann im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 2, 14 oder 17 zur Detektion von Sicherheitslücken und anderen Sicherheitsrisiken an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen Maßnahmen (Portscans) durchführen, wenn Tatsachen die Annahme rechtfertigen, dass diese ungeschützt im Sinne des Absatzes 2 sein können und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sind. Die Maßnahmen müssen sich auf das zur Detektion von Sicherheitslücken oder anderen Sicherheitsrisiken in der Informationstechnik

1. des Bundes oder

2. Kritischer Infrastrukturen, digitaler Dienste und der Unternehmen im besonderen öffentlichen Interesse

Notwendige beschränken. Erlangt das Bundesamt dabei Informationen, die durch Artikel 10 des Grundgesetzes geschützt sind, darf es diese nur zum Zwecke der Übermittlung nach § 5 Absatz 5 und 6 verarbeiten. Sofern die Voraussetzungen des § 5 Absatz 5 und 6 nicht vorliegen, sind Informationen, die nach Artikel 10 des Grundgesetzes geschützt sind, unverzüglich zu löschen. Maßnahmen nach Satz 1 dürfen nur durch eine Bedienstete oder einen Bediensteten des Bundesamtes mit der Befähigung zum Richteramt angeordnet werden.

(2) Ein informationstechnisches System ist ungeschützt im Sinne des Absatzes 1, wenn auf diesem öffentlich bekannte Sicherheitslücken bestehen oder wenn auf Grund sonstiger offensichtlich unzureichender Sicherheitsvorkehrungen unbefugt von Dritten auf das System zugegriffen werden kann.

(3) Wird durch Maßnahmen gemäß Absatz 1 eine Sicherheitslücke oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt und stehen überwiegende Sicherheitsinteressen nicht entgegen, sind die für das informationstechnische System Verantwortlichen darüber zu informieren. Das Bundesamt soll dabei auf bestehende Abhilfemöglichkeiten hinweisen. Sind dem Bundesamt die Verantwortlichen nicht bekannt oder ist ihre Identifikation nur mit unverhältnismäßigen Aufwand möglich und stehen überwiegende Sicherheitsinteressen nicht entgegen, ist hilfsweise der betreibende Dienstleister des jeweiligen Netzes oder Systems unverzüglich zu benachrichtigen. Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Anzahl der gemäß Absatz 1 ergriffenen Maßnahmen.

(4) Das Bundesamt darf zur Erfüllung seiner Aufgaben Systeme und Verfahren einsetzen, welche einem Angreifer einen erfolgreichen Angriff vortäuschen, um den Einsatz von Schadprogrammen oder andere Angriffsmethoden zu erheben und auszuwerten. Das Bundesamt darf dabei die zur Auswertung der Funktionsweise der Schadprogramme und Angriffsmethoden erforderlichen Daten verarbeiten.

ENTWURF

§ 7c

Anordnungen des Bundesamtes gegenüber Diensteanbietern

(1) Zur Abwehr konkreter erheblicher Gefahren für die in Absatz 2 genannten Schutzziele kann das Bundesamt gegenüber einem Anbieter von Telekommunikationsdiensten im Sinne des Telekommunikationsgesetzes (Diensteanbieter) mit mehr als 100.000 Kunden anordnen, dass er

1. die in § 109a Absätze 5 oder 6 des Telekommunikationsgesetzes bezeichneten Maßnahmen trifft, oder

2. technische Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene informationstechnische Systeme verteilt,

sofern und soweit der Diensteanbieter dazu technisch in der Lage ist und es ihm wirtschaftlich zumutbar ist. Vor der Anordnung der Maßnahmen durch das Bundesamt ist Einvernehmen mit der Bundesnetzagentur herzustellen. Vor der Anordnung der Maßnahme nach Satz 1 Nummer 2 durch das Bundesamt ist zusätzlich Einvernehmen mit dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit herzustellen. Die Daten, auf die mit der Maßnahme nach Satz 1 Nummer 2 zugegriffen werden soll, sind in der Anordnung zu benennen. § 5 Absatz 7 Satz 2 bis 8 gilt entsprechend. Widerspruch und Anfechtungsklage gegen die Anordnungen nach Satz 1 haben keine aufschiebende Wirkung.

(2) Schutzziele gemäß Absatz 1 Satz 1 sind

1. die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit der Kommunikationstechnik des Bundes, eines Betreibers Kritischer Infrastrukturen, eines Unternehmens im besonderen öffentlichen Interesse, oder eines Anbieters Digitaler Dienste, oder

2. die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informations- oder Kommunikationsdiensten, oder

3. Informationen, deren Verfügbarkeit, Unversehrtheit oder Vertraulichkeit eingeschränkt wird durch unerlaubte Zugriffe auf eine erhebliche Anzahl von telekommunikations- oder informationstechnischen Systemen von Nutzern.

(3) Ordnet das Bundesamt eine Maßnahme nach Absatz 1 Satz 1 Nummer 1 an, so kann es gegenüber dem Diensteanbieter auch anordnen, den Datenverkehr an eine vom Bundesamt benannte Anschlusskennung umzuleiten.

(4) Das Bundesamt darf Daten, die von einem Diensteanbieter nach Absatz 1 Satz 1 Nummer 1 und Absatz 3 umgeleitet wurden, verarbeiten, um Informationen über Schadprogramme oder andere Sicherheitsrisiken in informationstechnischen Systemen zu erlangen. Die übermittelten Daten dürfen durch das Bundesamt so lange gespeichert werden, wie dies für die Erfüllung des in Satz 1 genannten Zwecks erforderlich ist, längstens jedoch für drei Monate. Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Gesamtzahl der empfangenen Datenumleitungen.

ENTWURF

§ 7d

Anordnungen des Bundesamtes gegenüber Anbietern von Telemediendiensten

Das Bundesamt kann in begründeten Einzelfällen zur Abwehr konkreter, erheblicher Gefahren für informationstechnische Systeme einer Vielzahl von Nutzern, die von Telemedienangeboten von Diensteanbietern im Sinne des § 2 Nummer 1 des Telemediengesetzes ausgehen, die durch ungenügende technische und organisatorische Vorkehrungen im Sinne des § 13 Absatz 7 des Telemediengesetzes dergestalt unzureichend gesichert sind, dass sie keinen hinreichenden Schutz bieten vor

1. unerlaubten Zugriffen auf die für diese Telemedienangebote genutzten technischen Einrichtungen oder

2. Störungen, auch soweit sie durch äußere Angriffe bedingt sind,

gegenüber dem jeweiligen Diensteanbieter im Sinne des § 2 Nummer 1 des Telemediengesetzes anordnen, dass dieser die jeweils zur Herstellung des ordnungsgemäßen Zustands seiner Telemedienangebote erforderlichen technischen und organisatorischen Maßnahmen ergreift, um den ordnungsgemäßen Zustand seiner Telemedienangebote herzustellen.“

11. § 8 wird wie folgt geändert:

a) Absatz 1 wird durch die folgenden Absätze 1 und 1a neu gefasst:

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

1. Stellen des Bundes,

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

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

umzusetzen sind. Abweichungen von den Mindeststandards sind nur in sachlich gerechtfertigten Fällen zulässig, sie sind zu dokumentieren und zu begründen.

(1a) Das Bundesministerium des Innern, für Bau und Heimat kann im Benehmen mit der Konferenz der IT-Beauftragten der Ressorts bei bedeutenden Mindeststandards die Überwachung und Kontrolle ihrer Einhaltung durch das Bundesamt anordnen. Das Bundesamt teilt das Ergebnis seiner Kontrolle der jeweiligen überprüften Stelle, deren zuständiger Aufsichtsbehörde sowie der Konferenz der IT-Beauftragten der Ressorts mit. Für andere öffentlich- oder privatrechtlich organisierte Stellen dürfen nur dann Schnittstellen zur Kommunikationstechnik des Bundes eingerichtet werden, soweit die für die Einrichtung verantwortliche Stelle vertraglich sicherstellt, dass die öffentlich- oder privatrechtlich organisierte Stelle sich zur Einhaltung der Mindeststandards verpflichtet. Das Bundesamt kann im Einvernehmen mit dem Dritten die Einhaltung der Mindeststandards überprüfen und kontrollieren. Das Bundesamt berät die unter Satz 1 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 Vorschrif-

ENTWURF

ten nach diesem Absatz empfehlenden Charakter. Von der Verpflichtung ausgenommen ist im Geschäftsbereich des Bundesministeriums der Verteidigung die Informations- und Kommunikationstechnik im Sinne des § 4a Absatz 6.“

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

c) Folgender Absatz 4 wird angefügt:

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

12. § 8a wird wie folgt geändert:

a) Nach Absatz 1 werden die folgenden Absätze 1a und 1b eingefügt:

„(1a) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst spätestens ein Jahr nach Inkrafttreten dieses Gesetzes auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter bzw. Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Absatz 1 Satz 2 und 3 gelten entsprechend.

(1b) Betreiber Kritischer Infrastrukturen müssen für die Angriffserkennung und -nachverfolgung relevante nicht personenbezogene Daten, die beim Betrieb einer Kritischen Infrastruktur anfallen, mindestens vier Jahre speichern.“

b) In Absatz 2 Satz 1 und 2 wird die Angabe „Absatz 1“ jeweils durch die Angabe „Absatz 1 bis 1b“ ersetzt.

c) Absatz 3 Satz 1 wird wie folgt gefasst:

„Betreiber Kritischer Infrastrukturen haben die Erfüllung der Anforderungen nach Absatz 1 bis 1b spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 und anschließend alle zwei Jahre auf geeignete Weise nachzuweisen.“

d) In Absatz 4 Satz 1 und 3 wird die Angabe „Absatz 1“ jeweils durch die Angabe „Absatz 1 bis 1b“ ersetzt.

13. § 8b wird wie folgt geändert:

a) Absatz 2 wird wie folgt geändert:

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

bb) Absatz 2 Nummer 4 Buchstabe a wird wie folgt gefasst:

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

b) Der Absatz 3 wird wie folgt gefasst:

ENTWURF

„(3) Betreiber Kritischer Infrastrukturen sind verpflichtet, die von ihnen betriebenen Kritischen Infrastrukturen beim Bundesamt zu registrieren und eine Kontaktstelle zu benennen. Die Registrierung eines Betreibers einer Kritischen Infrastruktur kann das Bundesamt auch selbst vornehmen, wenn der Betreiber seine Pflicht zur Registrierung nicht erfüllt. Die Betreiber haben sicherzustellen, dass sie über die benannte oder durch das Bundesamt festgelegte 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 der folgende Absatz 3a eingefügt:

„(3a) Rechtfertigen Tatsachen die Annahme, dass ein Betreiber seine Pflicht zur Registrierung nach Absatz 3 nicht erfüllt, so hat der Betreiber dem Bundesamt auf Verlangen die für die Bewertung aus Sicht des Bundesamtes erforderlichen Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen und Auskunft zu erteilen."

d) Nach Absatz 4 wird folgender Absatz 4a eingefügt:

„(4a) Während einer erheblichen Störung gemäß Absatz 4 Satz 1 Nummer 2, § 8f Absatz 7 Nummer 2 oder § 8f Absatz 8 Nummer 2 kann das Bundesamt im Einvernehmen mit der jeweils zuständigen Aufsichtsbehörde des Bundes von den betroffenen Betreibern Kritischer Infrastrukturen oder Unternehmen im besonderen öffentlichen Interesse die Herausgabe der zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten verlangen."

e) In Absatz 6 Satz 1 werden nach den Wörtern „Störung nach Absatz 4" ein Komma und die Wörter „oder § 8f Absatz 7 oder 8" eingefügt.

f) In Absatz 6 Satz 2 wird die Angabe „§ 8c Absatz 3" durch die Angabe „§ 8d Absatz 3" ersetzt.

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

15. In § 8d Absatz 2 werden im Satzteil vor Nummer 1 nach der Angabe „§ 8a" die Wörter „Absatz 1 bis 5" eingefügt.

16. § 8e Absatz 1 und 2 wird wie folgt gefasst:

„(1) Das Bundesamt kann Dritten auf Antrag Auskunft zu den im Rahmen von § 8a Absatz 2 und 3, § 8c Absatz 4 und § 8f erhaltenen Informationen sowie zu den Meldungen nach § 8b Absatz 4, 4a und 4b sowie § 8c Absatz 4 nur erteilen, wenn

1. schutzwürdige Interessen des betroffenen Betreibers einer Kritischen Infrastruktur, des Unternehmens im besonderen öffentlichen Interesse oder des Anbieters digitaler Dienste dem nicht entgegenstehen

2. und durch die Auskunft keine Beeinträchtigung von Sicherheitsinteressen eintreten kann. Zugang zu personenbezogenen Daten wird nicht gewährt.

(2) Zugang zu den Akten des Bundesamtes in Angelegenheiten nach den §§ 8a bis 8c und § 8f wird bei Vorliegen der Voraussetzungen des § 29 des Verwaltungsverfahrensgesetzes nur gewährt, wenn

1. schutzwürdige Interessen des betroffenen Betreibers einer Kritischen Infrastruktur, des Unternehmens im besonderen öffentlichen Interesse oder des Anbieters digitaler Dienste dem nicht entgegenstehen und

ENTWURF

2. durch den Zugang zu den Akten keine Beeinträchtigung von Sicherheitsinteressen eintreten kann.“

17. Nach § 8e wird folgender § 8f eingefügt:

„§ 8f

Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse

(1) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1 und 2 sind verpflichtet, eine Selbsterklärung zur IT-Sicherheit beim Bundesamt vorzulegen aus der hervorgeht,

1. welche Zertifizierungen im Bereich der IT-Sicherheit in den letzten zwei Jahren durchgeführt wurden und welche Prüfgrundlage und welcher Geltungsbereich hierfür festgelegt wurden,

2. welche sonstigen Sicherheitsaudits oder Prüfungen im Bereich der IT-Sicherheit in den letzten zwei Jahren durchgeführt wurden und welche Prüfgrundlage und welcher Geltungsbereich hierfür festgelegt wurden oder

3. wie sichergestellt wird, dass die für das Unternehmen besonders schützenswerten IT-Systeme, Komponenten und Prozesse angemessen geschützt werden und ob dabei der Stand der Technik eingehalten wird.

(2) Das Bundesamt kann verbindliche Formulare für die Selbsterklärung nach Absatz 1 einführen.

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

(4) Für Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1 gilt die Pflicht nach Absatz 1 erstmalig zwei Jahre nach Inkrafttreten dieses Gesetzes und danach mindestens alle zwei Jahre. Für Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 2 gilt diese Pflicht erstmalig zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 5 und danach mindestens alle zwei Jahre.

(5) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1 und 2 sind verpflichtet, sich binnen ab sechs Monate nach Inkrafttreten dieses Gesetzes beim Bundesamt zu registrieren und eine zu den üblichen Geschäftszeiten erreichbare Stelle zu benennen. Die Übermittlung von Informationen durch das Bundesamt nach § 8b Absatz 2 Nummer 4 erfolgt an diese Stelle.

(6) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 3 können eine freiwillige Registrierung beim Bundesamt und Benennung einer zu den üblichen Geschäftszeiten erreichbaren Stelle vornehmen. Die Übermittlung von Informationen durch das Bundesamt nach § 8b Absatz 2 Nummer 4 erfolgt an diese Stelle.

(7) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1 und 2 haben spätestens ab sechs Monate nach Inkrafttreten dieses Gesetzes die folgenden Störungen unverzüglich über die nach Absatz 5 benannte Stelle an das Bundesamt zu melden:

ENTWURF

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

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

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

(8) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 3 haben spätestens ab sechs Monate nach Inkrafttreten dieses Gesetzes die folgenden Störungen unverzüglich an das Bundesamt zu melden:

1. Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Störfall nach der Störfall-Verordnung in der jeweils geltenden Fassung geführt haben,

2. erhebliche Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Störfall nach der Störfall-Verordnung in der jeweils geltenden Fassung führen können.

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

(9) Rechtfertigen Tatsachen die Annahme, dass ein Unternehmen ein Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 2 ist, aber seine Pflichten nach Absatz 5 nicht erfüllt, so kann das Bundesamt verlangen:

1. eine rechnerische Darlegung, wie hoch die vom Unternehmen erbrachte inländische Wertschöpfung nach der in der Rechtsverordnung nach § 10 Absatz 5 festgelegten Berechnungsmethode ist, oder

2. eine Bestätigung einer anerkannten Wirtschaftsprüfungsgesellschaft, dass das Unternehmen nach der in der Rechtsverordnung nach § 10 Absatz 5 festgelegten Berechnungsmethode kein Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 2 ist.“

18. § 9 wird wie folgt gefasst:

a) § 9 Absatz 4 wird wie folgt gefasst:

„(4) Das Sicherheitszertifikat wird erteilt, wenn

1. informationstechnische Systeme, Komponenten, Produkte oder Schutzprofile den vom Bundesamt festgelegten Kriterien entsprechen;

2. das Bundesministerium des Innern, für Bau und Heimat die Erteilung des Zertifikats nach Absatz 4a nicht untersagt hat.

ENTWURF

Vor Erteilung des Sicherheitszertifikates legt das Bundesamt den Vorgang dem Bundesministerium des Innern, für Bau und Heimat zur Prüfung nach Absatz 4a vor.“

b) Nach § 9 Absatz 4 wird folgender Absatz 4a eingefügt:

„Das Bundesministerium des Innern, für Bau und Heimat kann eine Zertifikatserteilung nach Absatz 4 im Einzelfall untersagen, wenn überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung entgegenstehen.“

19. Nach § 9 werden folgende §§ 9a bis 9c eingefügt:

„§ 9a

Nationale Behörde für die Cybersicherheitszertifizierung

(1) Das Bundesamt ist die nationale Behörde für die Cybersicherheitszertifizierung im Sinne des Artikels 58 Absatz 1 der Verordnung (EU) 2019/881.

(2) Das Bundesamt erteilt auf Antrag Konformitätsbewertungsstellen, die im Anwendungsbereich der Verordnung (EU) 2019/881 sowie des § 9 dieses Gesetzes tätig werden, eine Befugnis, als solche tätig zu werden, wenn die Voraussetzungen des maßgeblichen europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 Verordnung (EU) 2019/881 oder des § 9 dieses Gesetzes erfüllt sind. Ohne eine Befugniserteilung durch das Bundesamt dürfen Konformitätsbewertungsstellen im Anwendungsbereich der Verordnung (EU) 2019/881 nicht tätig werden.

(3) Soweit dies zur Erfüllung seiner Aufgaben nach Artikel 58 Absatz 7 der Verordnung (EU) 2019/881 sowie des § 9 dieses Gesetzes erforderlich ist, kann das Bundesamt von Konformitätsbewertungsstellen, denen eine Befugnis nach Absatz 2 erteilt wurde, Inhabern europäischer Cybersicherheitszertifikate und Ausstellern von EU-Konformitätserklärungen im Sinne von Artikel 56 Absatz 8 der Verordnung (EU) 2019/881 die erforderlichen Auskünfte und sonstige Unterstützung, insbesondere die Vorlage von Unterlagen oder Mustern, verlangen. § 3 Absatz 1 Satz 1 und 3 des Akkreditierungsstellengesetzes gilt entsprechend.

(4) Das Bundesamt kann Untersuchungen in Form von Auditierungen nach Artikel 58 Absatz 8 Buchstabe b der Verordnung (EU) 2019/881 bei Konformitätsbewertungsstellen, denen eine Befugnis nach Absatz 2 erteilt wurde, Inhabern europäischer Cybersicherheitszertifikate und Ausstellern von EU-Konformitätserklärungen im Sinne von Artikel 56 Absatz 8 der Verordnung (EU) 2019/881 durchführen, um die Einhaltung der Bestimmungen des Titels III der Verordnung (EU) 2019/881 zu überprüfen. § 3 Absatz 1 Satz 1 bis 3 des Akkreditierungsstellengesetzes gilt entsprechend.

(5) Das Bundesamt ist befugt, Betriebsstätten, Geschäfts- und Betriebsräume von Konformitätsbewertungsstellen, denen eine Befugnis nach Absatz 2 erteilt wurde, und Inhabern europäischer Cybersicherheitszertifikate im Sinne von Artikel 56 Absatz 8 der Verordnung (EU) 2019/881 zu betreten, zu besichtigen und zu prüfen, soweit dies zur Erfüllung seiner Aufgaben nach Artikel 58 Absatz 7 der Verordnung (EU) 2019/881 sowie des § 9 dieses Gesetzes erforderlich ist. § 3 Absatz 1 Satz 1 bis 3 des Akkreditierungsstellengesetzes gilt entsprechend.

(6) Das Bundesamt kann von ihm ausgestellte Cybersicherheitszertifikate oder durch eine Konformitätsbewertungsstelle, der eine Befugnis nach Absatz 2 erteilt

ENTWURF

wurde, nach Artikel 56 Absatz 6 der Verordnung (EU) 2019/881 ausgestellte Cybersicherheitszertifikate widerrufen oder EU-Konformitätserklärungen im Sinne der Verordnung (EU) 2019/881 für ungültig erklären, sofern diese Zertifikate oder EU-Konformitätserklärungen die Anforderungen nach der Verordnung (EU) 2019/881 oder eines europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 der Verordnung (EU) 2019/881 nicht erfüllen oder wenn das Bundesamt die Erfüllung nicht feststellen kann, weil der Inhaber des europäischen Cybersicherheitszertifikats oder der Aussteller der EU-Konformitätserklärung seinen Mitwirkungspflichten nach Absatz 3 nicht nachgekommen ist oder weil dieser das Bundesamt bei der Wahrnehmung seiner Befugnisse nach Absatz 4 oder im Falle eines Inhabers eines europäischen Cybersicherheitszertifikates auch nach Absatz 5 behindert hat.

(7) Das Bundesamt kann von ihm erteilte Befugnisse nach Absatz 2 widerrufen, sofern die Voraussetzungen des maßgeblichen europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 Verordnung (EU) 2019/881 oder des § 9 dieses Gesetzes nicht erfüllt sind oder wenn das Bundesamt die Erfüllung dieser Voraussetzungen nicht feststellen kann, weil die Konformitätsbewertungsstelle ihren Mitwirkungspflichten nach Absatz 3 nicht nachgekommen ist oder weil diese das Bundesamt bei der Wahrnehmung seiner Befugnisse nach Absatz 4 und 5 behindert hat.

§ 9b

Untersagung des Einsatzes kritischer Komponenten

(1) Der Einsatz von kritischen Komponenten (§ 2 Absatz 13), für die auf Grund einer gesetzlichen Regelung eine Zertifizierungspflicht besteht, ist durch den Betreiber einer Kritischen Infrastruktur dem Bundesministerium des Innern, für Bau und Heimat vor Einsatz anzuzeigen. In der Anzeige ist die kritische Komponente und die Art ihres Einsatzes anzugeben. Die Pflicht aus Satz 1 besteht bereits dann, wenn zur Vorlage von Zertifikaten Übergangsfristen gewährt werden.

(2) Kritische Komponenten nach Absatz 1 dürfen nur eingesetzt werden, wenn der Hersteller eine Erklärung über seine Vertrauenswürdigkeit gegenüber dem Betreiber der Kritischen Infrastruktur abgeben hat (Garantieerklärung). Diese Erklärung erstreckt sich auf die gesamte Lieferkette des Herstellers. Die Garantieerklärung des Herstellers der kritischen Komponente ist der Anzeige nach Absatz 1 beizufügen. Aus der Garantieerklärung muss unter anderem hervorgehen, ob und wie der Hersteller hinreichend sicherstellen kann, dass die kritische Komponente über keine technischen Eigenschaften verfügt, die geeignet sind, missbräuchlich, insbesondere zu Zwecke von Sabotage, Spionage oder Terrorismus auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur, einwirken zu können. Das Bundesministerium des Innern, für Bau und Heimat legt die Mindestanforderungen für die Garantieerklärung im Einvernehmen mit den betroffenen Ressorts unter Berücksichtigung überwiegender öffentlicher Interessen, insbesondere sicherheitspolitischer Belange, durch Allgemeinverfügung fest, die im Bundesanzeiger bekannt zu machen ist. Die Verpflichtung in Satz 1 gilt ab der Bekanntmachung der Allgemeinverfügung nach Satz 5. Soweit Änderungen der Allgemeinverfügung erfolgen, sind diese für bereits nach Absatz 1 abgegebene Garantieerklärungen unbeachtlich.

(3) Das Bundesministerium des Innern, für Bau und Heimat kann den Einsatz einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur im Einvernehmen mit dem jeweils betroffenen Ressort bis zum Ablauf von einem Monat nach Eingang der Anzeige nach Absatz 1 untersagen oder Anordnungen erlassen, wenn überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, dem Einsatz entgegenstehen. Vor Ablauf der Frist von einem Monat nach Anzeige nach Absatz 1 ist der Einsatz nicht gestattet.

ENTWURF

(4) Das Bundesministerium des Innern, für Bau und Heimat kann den weiteren Betrieb einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur im Einvernehmen mit dem jeweils betroffenen Ressort untersagen oder Anordnungen erlassen, wenn der Hersteller der kritischen Komponente sich als nicht vertrauenswürdig erwiesen hat.

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

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

2. seine in der Garantieerklärung angegebenen Tatsachen unwahr sind,

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

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

5. die kritische Komponente über technische Eigenschaften verfügt oder verfügt hat, die geeignet sind oder waren, missbräuchlich auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können.

Ein Verstoß nach Nummer 5 liegt nicht vor, wenn der Hersteller nachweisen kann, dass er die technische Eigenschaft im Sinne von Nummer 5 nicht implementiert hat und er diese jeweils ordnungsgemäß beseitigt hat.

(6) Wurde nach Absatz 4 der Einsatz einer kritischen Komponente untersagt, kann das Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit dem betroffenen Ressort ohne erneute Prüfung eines Herstellers nach Absatz 3

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

2. die Nutzung im Einsatz befindlicher kritischer Komponenten desselben Typs und desselben Herstellers nach Ablauf einer angemessenen Frist untersagen.

(7) Bei wiederholter Feststellung nicht vorliegender Vertrauenswürdigkeit nach Absatz 5 Nummer 1 bis 3 kann das Bundesministerium des Innern, für Bau und Heimat den Einsatz aller kritischen Komponenten des Herstellers untersagen.

ENTWURF

§ 9c

Freiwilliges IT-Sicherheitskennzeichen

(1) Das Bundesamt führt zur Information von Verbrauchern über die IT-Sicherheit von Produkten bestimmter vom Bundesamt festgelegter Produktkategorien ein einheitliches IT-Sicherheitskennzeichen ein. Das IT-Sicherheitskennzeichen trifft keine Aussage über die den Datenschutz betreffenden Eigenschaften eines Produktes.

(2) Das IT-Sicherheitskennzeichen besteht aus

1. einer Zusicherung des Herstellers oder Diensteanbieters, dass das Produkt für eine festgelegte Dauer bestimmte IT-Sicherheitsanforderungen erfüllt (Herstellererklärung), und

2. einer Information des Bundesamtes über sicherheitsrelevante IT-Eigenschaften des Produktes (Sicherheitsinformation).

(3) Die IT-Sicherheitsanforderungen, auf die sich die Herstellererklärung bezieht, ergeben sich aus einer vom Bundesamt veröffentlichten Technischen Richtlinie, die die jeweilige Produktkategorie umfasst, sofern das Bundesamt eine solche Richtlinie bereits veröffentlicht hat. Wird ein Produkt von mehr als einer Technischen Richtlinie umfasst, richten sich die Anforderungen nach der jeweils spezielleren Technischen Richtlinie. Liegt für die jeweilige Produktkategorie keine Technische Richtlinie vor, ergeben sich die IT-Sicherheitsanforderungen aus branchenabgestimmten IT-Sicherheitsvorgaben, sofern das Bundesamt festgestellt hat, dass diese Vorgaben geeignet sind, ausreichende IT-Sicherheitsanforderungen für die Produktkategorie abzubilden. Ein Anspruch auf diese Feststellung besteht nicht. Die Dauer, für die der Hersteller oder Diensteanbieter die Erfüllung der IT-Sicherheitsanforderungen zusichert, wird durch Rechtsverordnung nach § 10 Absatz 3 geregelt. Die Rechtsverordnung kann vorsehen, dass die für die jeweilige Produktkategorie maßgebliche Technische Richtlinie oder die branchenabgestimmten IT-Sicherheitsvorgaben eine abweichende Dauer festlegen können.

(4) Das IT-Sicherheitskennzeichen darf für ein Produkt verwendet werden, nachdem das Bundesamt das IT-Sicherheitskennzeichen für dieses Produkt freigegeben hat. Das Bundesamt prüft die Freigabe des IT-Sicherheitskennzeichens für ein Produkt auf Antrag des Herstellers oder Diensteanbieters. Dem Antrag sind die Herstellererklärung zu dem Produkt sowie alle Unterlagen beizufügen, die die Angaben in der Herstellererklärung belegen. Das Bundesamt bestätigt den Eingang des Antrags und prüft die Plausibilität der Herstellererklärung anhand der beigefügten Unterlagen. Die Plausibilitätsprüfung kann auch durch einen vom Bundesamt beauftragten qualifizierten Dritten erfolgen. Für die Antragsbearbeitung kann das Bundesamt eine Verwaltungsgebühr erheben.

(5) Das Bundesamt erteilt die Freigabe des IT-Sicherheitskennzeichens für das jeweilige Produkt, wenn

1. das Produkt zu einer der Produktkategorien gehört, die das Bundesamt durch im Bundesanzeiger veröffentlichte Allgemeinverfügung bekannt gegeben hat,

2. die Herstellererklärung plausibel und durch die beigefügten Unterlagen ausreichend belegt ist und

3. die gegebenenfalls erhobene Verwaltungsgebühr beglichen wurde.

Die Erteilung der Freigabe erfolgt schriftlich und innerhalb einer angemessenen Frist, die in der Rechtsverordnung nach § 10 Absatz 3 bestimmt wird. Den genauen Ablauf des Antragsverfahrens und die beizufügenden Unterlagen regelt die Rechtsverordnung nach § 10 Absatz 3.

(6) Hat das Bundesamt die Freigabe erteilt, ist das Etikett des IT-Sicherheitskennzeichens auf dem jeweiligen Produkt oder auf dessen Umverpackung anzubringen, sofern dies nach der Beschaffenheit des Produktes möglich ist. Das IT-Sicherheitskennzeichen kann auch elektronisch veröffentlicht werden. Wenn nach der Beschaffenheit des Produktes das Anbringen nicht möglich ist, muss die Veröffentlichung des IT-Sicherheitskennzeichens elektronisch erfolgen. Das Etikett des IT-Sicherheitskennzeichens verweist auf eine Internetseite des Bundesamtes, auf der die Herstellererklärung

ENTWURF

und die Sicherheitsinformationen abrufbar sind. Das genaue Verfahren und die Gestaltung des Verweises sind in der Rechtsverordnung nach § 10 Absatz 3 festzulegen.

(7) Nach Ablauf der festgelegten Dauer nach Absatz 3 Satz 5 oder 6 oder Rücknahmeerklärung des Herstellers oder Diensteanbieters gegenüber dem Bundesamt erlischt die Freigabe. Das Bundesamt nimmt einen Hinweis auf das Erlöschen der Freigabe in die Sicherheitsinformation auf.

(8) Das Bundesamt kann prüfen, ob die Anforderungen an die Freigabe des IT-Sicherheitskennzeichens für ein Produkt eingehalten werden. Werden bei der Prüfung Abweichungen von der abgegebenen Herstellererklärung oder Sicherheitslücken festgestellt, kann das Bundesamt die geeigneten Maßnahmen treffen, insbesondere kann es

1. Informationen über die Abweichungen oder Sicherheitslücken in geeigneter Weise in der Sicherheitsinformation veröffentlichen oder

2. die Freigabe des IT-Sicherheitskennzeichens widerrufen.

Absatz 7 Satz 2 gilt entsprechend.

(9) Bevor das Bundesamt eine Maßnahme nach Absatz 8 trifft, räumt es dem Hersteller oder Diensteanbieter Gelegenheit ein, die festgestellten Abweichungen oder Sicherheitslücken innerhalb eines angemessenen Zeitraumes zu beseitigen, es sei denn, gewichtige Gründe der Sicherheit der Produkte erfordern eine sofortige Maßnahme. Die Befugnis des Bundesamtes zur Warnung nach § 7 bleibt davon unberührt.“

20. § 10 wird wie folgt geändert:

a) Nach Absatz 2 wird folgender Absatz 3 eingefügt:

„(3) Das Bundesministerium des Innern, für Bau und Heimat bestimmt 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, des Inhalts und der Verwendung des IT-Sicherheitskennzeichens nach § 9a Absatz 1 Satz 1, um eine einheitliche Gestaltung des Kennzeichens und eine eindeutige Erkennbarkeit der gekennzeichneten informationstechnischen Produkte zu gewährleisten. Die Einzelheiten des Verfahrens zur Feststellung der Eignung branchenabgestimmter IT-Sicherheitsvorgaben und des Antragsverfahrens auf Freigabe einschließlich der diesbezüglichen Fristen, der beizufügenden Unterlagen und der Verwaltungsgebühren sowie das Verfahren und die Gestaltung des Verweises auf Sicherheitsinformationen werden ebenfalls durch eine Rechtsverordnung geregelt.“

b) Nach Absatz 4 wird folgender Absatz 5 angefügt:

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

21. § 11 wird wie folgt gefasst:

ENTWURF

„§ 11

Einschränkung von Grundrechten

Das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) wird durch die §§ 4a, 5, 5a, 5b, 5c Absatz 2, 7b und 7c eingeschränkt. Das Grundrecht der Unverletzlichkeit der Wohnung (Artikel 13 des Grundgesetzes) wird durch § 9a Absatz 5 eingeschränkt.“

22. § 14 wird wie folgt gefasst:

„§ 14

Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. einer vollziehbaren Anordnung nach

a) § 5b Absatz 6, § 7c Absatz 1 Satz 1 Nummer 1 oder Nummer 2 oder Absatz 3, § 7d, § 8a Absatz 3 Satz 5, § 8b Absatz 6 Satz 1 in Verbindung mit Absatz 4 Satz 1 Nummer 2, § 8b Absatz 6 Satz 2 in Verbindung mit Absatz 4 Satz 1 Nummer 2, § 8c Absatz 4 Satz 1 Nummer 2, oder

b) § 7a Absatz 2 Satz 1, § 8b Absatz 6 Satz 1 in Verbindung mit Absatz 4 Satz 1 Nummer 1, § 8b Absatz 6 Satz 2 in Verbindung mit Absatz 4 Satz 1 Nummer 1, § 8c Absatz 4 Satz 1 Nummer 1

zuwiderhandelt,

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

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

4. entgegen § 8a Absatz 4 Satz 2 das Betreten eines dort genannten Raums nicht gestattet, eine dort genannte Unterlage nicht oder nicht rechtzeitig vorlegt, oder eine Auskunft nicht, nicht richtig nicht vollständig oder nicht rechtzeitig erteilt oder die sonst erforderliche Unterstützung nicht oder nicht rechtzeitig gewährt,

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

6. entgegen § 8b Absatz 3 Satz 4 nicht sicherstellt, dass er erreichbar ist,

7. einer vollziehbaren Anordnung nach § 8b Absatz 3a Satz 1 zuwiderhandelt,

8. entgegen § 8b Absatz 4 Satz 1 Nummer 1 oder 2 oder § 8c Absatz 3 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

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

10. entgegen § 8f Absatz 1 in Verbindung mit Absatz 4 eine Selbsterklärung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorlegt,

ENTWURF

11. entgegen § 8f Absatz 5 Satz 1 eine Registrierung nicht, nicht vollständig oder nicht rechtzeitig vornimmt oder eine Stelle nicht oder nicht rechtzeitig benennt,

12. entgegen § 8f Absatz 7 Satz 1 Nummer 1 oder Nummer 2 oder Absatz 8 Satz 1 Nummer 1 oder Nummer 2 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

13. entgegen § 9a Absatz 2 ohne Befugnis als Konformitätsbewertungsstelle tätig wird,

14. entgegen § 9a Absatz 6 ein nicht gültiges Cybersicherheitszertifikat verwendet,

15. entgegen § 9c Absatz 4 Satz 1 das IT-Sicherheitskennzeichen ohne Freigabe für ein Produkt verwendet,

16. entgegen Artikel 53 Absatz 2 der Verordnung (EU) 2019/881 eine EU-Konformitätserklärung für eines der in Artikel 53 Absatz 2 der Verordnung (EU) 2019/881 genannten Produkte, Dienste oder Prozesse ausstellt, das den im maßgeblichen Schema festgelegten Anforderungen nicht entspricht oder eine solche EU-Konformitätserklärung verwendet,

17. entgegen Artikel 55 Absatz 1 Buchstaben a, b, c und d der Verordnung (EU) 2019/881 die dort genannten Angaben nicht binnen eines Monats nach Ausstellung der Öffentlichkeit richtig und vollständig zugänglich macht,

18. entgegen Artikel 56 Absatz 8 Satz 1 der Verordnung (EU) 2019/881 nicht unverzüglich, richtig und vollständig informiert.

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 1 Buchstabe a, Nummern 2, 9, 13, 14, 16, 17 und 18 mit einer Geldbuße bis zu 2 Millionen Euro geahndet werden, auf § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten wird verwiesen. Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 1 Buchstabe b und Nummern 3, 5, 8, 10, 11, 12 und 15 mit einer Geldbuße bis zu 1 Million Euro geahndet werden. In den übrigen Fällen kann die Ordnungswidrigkeit mit einer Geldbuße bis zu 100.000 Euro geahndet werden.

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

(4) Gegen Körperschaften gemäß § 29 des Vierten Buches Sozialgesetzbuch, Arbeitsgemeinschaften gemäß § 94 des Zehnten Buches Sozialgesetzbuch sowie die Deutsche Post AG, soweit sie mit der Berechnung oder Auszahlung von Sozialleistungen betraut ist (Institutionen der Sozialen Sicherung), werden keine Geldbußen verhängt. Bei Ordnungswidrigkeiten nach Absatz 1 von Institutionen der Sozialen Sicherung in Trägerschaft des Bundes stellt das Bundesamt das Einvernehmen über die zu ergreifenden Maßnahmen mit der für die Institution zuständigen Aufsichtsbehörde her. Bei Ordnungswidrigkeiten nach Absatz 1 von Institutionen der Sozialen Sicherung in Trägerschaft der Länder informiert das Bundesamt die zuständige Aufsichtsbehörde und schlägt geeignete Maßnahmen vor. Die jeweils zuständige Aufsichtsbehörde informiert das Bundesamt über die Einleitung und Umsetzung von Aufsichtsmitteln und sorgt für deren Durchsetzung.“

ENTWURF

Artikel 2

Änderungen des Telekommunikationsgesetzes

Das Telekommunikationsgesetz vom 3. Mai 2013 (BGBl. I S. 1084), das zuletzt durch Artikel 319 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, wird wie folgt geändert:

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

2. § 109 wird wie folgt geändert:

   a) In der Überschrift werden nach dem Wort „technische“ die Wörter „und organisatorische“ eingefügt.

   b) Absatz 2 wird wie folgt geändert:

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

      bb) Nach Absatz 2 Satz 3 wird folgender Satz eingefügt:

      „Kritische Komponenten im Sinne des § 2 Absatz 13 BSIG dürfen nur eingesetzt werden, wenn sie von einer anerkannten Prüfstelle überprüft und von einer anerkannten Zertifizierungsstelle zertifiziert wurden.“

      cc) In dem neuen Satz 9 wird die Angabe „§ 11“ durch die Angabe „§ 62“ ersetzt.

   c) Absatz 4 Satz 1 Nummer 3 wird wie folgt gefasst:

   „3. welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der durch die Vorgaben des Katalogs von Sicherheitsanforderungen nach Absatz 6 konkretisierten Verpflichtungen aus den Absätzen 1 und 2 getroffen oder geplant sind; sofern der Katalog lediglich Sicherheitsziele vorgibt, ist darzulegen, dass mit den ergriffenen Maßnahmen das jeweilige Sicherheitsziel vollumfänglich erreicht wird.“

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

   e) Absatz 6 wird wie folgt geändert:

      aa) Satz 1 wird wie folgt gefasst:

      „Die Bundesnetzagentur legt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit durch Verfügung in einen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten fest:

ENTWURF

1. Einzelheiten der nach den Absätzen 1 und 2 zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen unter Beachtung der verschiedenen Gefährdungspotenziale der öffentlichen Telekommunikationsnetze und öffentlich zugänglichen Telekommunikationsdienste,

2. Vorgaben zur Bestimmung der kritischen Komponenten im Sinne von § 2 Absatz 13 BSIG sowie

3. wer als Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial einzustufen ist.“

bb) Nach Satz 2 wird folgender Satz eingefügt:

„Die nach den Absätzen 1, 2 und 4 Verpflichteten haben die Vorgaben des Katalogs spätestens ein Jahr nach dessen Inkrafttreten zu erfüllen, es sei denn, in dem Katalog ist eine davon abweichende Umsetzungsfrist festgelegt worden.“

f) Absatz 7 wird wie folgt geändert:

aa) Nach Satz 1 werden die folgenden Sätze eingefügt:

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

bb) In dem neuen Satz 4 wird nach der Angabe „Satz 1“ die Angabe „und 2“ eingefügt und nach dem Wort „Bundesnetzagentur“ die Wörter „und an das Bundesamt für Sicherheit in der Informationstechnik, sofern dieses die Überprüfung nicht vorgenommen hat“ und ein Komma eingefügt.

cc) Nach dem neuen Satz 5 wird folgender Satz eingefügt:

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

3. § 113 Absatz 3 wird wie folgt geändert:

a) In Nummer 3 wird der Punkt durch ein Semikolon ersetzt.

b) Der Nummer 3 wird folgende Nummer 4 angefügt:

„4. das Bundesamt für die Sicherheit in der Informationstechnik.“

ENTWURF

Artikel 3

Änderung des Telemediengesetzes

Das Telemediengesetz vom 26. Februar 2007 (BGBl. I S. 179), das zuletzt durch Artikel 11 des Gesetzes vom 11. Juli 2019 (BGBl. I S. 1066) geändert worden ist, wird wie folgt geändert:

1. Nach § 15c wird folgender § 15d eingefügt:

„§ 15d

Meldepflicht bei unrechtmäßiger Übermittlung oder unrechtmäßiger Kenntniserlangung von Daten

(1) Diensteanbieter unterrichten unverzüglich das Bundeskriminalamt als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei, wenn konkrete Anhaltspunkte die Annahme rechtfertigen, dass durch die Begehung einer Straftat nach § 202a, § 202b oder § 202c StGB oder zur Begehung einer Straftat nach § 202d StGB eine unrechtmäßige Übermittlung oder unrechtmäßige Kenntniserlangung von Daten erfolgte und eine große Zahl von Personen, einen Datenbestand von großem Ausmaß oder einen Datenbestand von Behörden oder Einrichtungen des Bundes oder deren Mitgliedern oder sicherheitsempfindlicher Stellen von lebenswichtigen Einrichtungen, bei deren Ausfall oder Zerstörung eine erhebliche Bedrohung für die Gesundheit oder das Leben von Menschen zu befürchten ist oder die für das Funktionieren des Gemeinwesens unverzichtbar sind, oder fremde Geheimnisse, namentlich Betriebs- oder Geschäftsgeheimnisse, betrifft. § 7 Absatz 2 bleibt unberührt.

(2) Die Übermittlung nach Absatz 1 an das Bundeskriminalamt muss enthalten:

1. den Inhalt,

2. sofern vorhanden, die für eine retrograde Identifizierung des jeweiligen Anschlussinhabers erforderlichen Daten, insbesondere die IP-Adresse einschließlich der Portnummer und des Zeitstempels, die genutzt wurden, um die Kenntnisnahme oder Datenübermittlung nach Absatz 1 zu veranlassen unter Angabe der zu Grunde liegenden Zeitzone.

Die Übermittlung an das Bundeskriminalamt hat in elektronischer, weiterverwertbarer, vom Bundeskriminalamt vorgegebener Form zu erfolgen. Wer mehr als 100.000 Kunden hat, hat für die Übermittlung der Benachrichtigung an das Bundeskriminalamt eine gesicherte, elektronische Schnittstelle bereitzuhalten und zu nutzen.“

2. In § 16 Absatz 2 wird in Nummer 5 der Punkt durch ein Komma ersetzt und der Nummer 5 die folgende Nummer 6 angefügt:

„6. Entgegen § 15d das Bundeskriminalamt nicht unverzüglich von der unrechtmäßigen Übermittlung oder unrechtmäßigen Kenntniserlangung unterrichtet.“

ENTWURF

Artikel 4

Änderung des Gesetzes über die Elektrizitäts- und Gasversorgung (EnWG)

In § 11 des Gesetzes über die Elektrizitäts- und Gasversorgung vom 7. Juli 2015 (BGBl. I S. 1970, S. 3621), zuletzt geändert durch Artikel 4 des Gesetzes vom 8. August 2020 (BGBl. I S. 1818), werden nach Absatz 1c die folgenden Absätze 1d bis 1f eingefügt:

„(1d) Betreiber von Energieversorgungsnetzen und von solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, haben spätestens ein Jahr nach Inkrafttreten dieses Gesetzes in ihren informationstechnischen Systemen, Komponenten oder Prozessen, die für die Funktionsfähigkeit der von ihnen betriebenen Energieversorgungsnetze oder Energieanlagen maßgeblich sind, in angemessener Weise Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter bzw. Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Dabei soll der Stand der Technik eingehalten werden. Der Einsatz von Systemen zur Angriffserkennung ist angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den möglichen Folgen eines Ausfalls oder einer Beeinträchtigung des betroffenen Energieversorgungsnetzes oder der betroffenen Energieanlage steht.

(1e) Nach Absatz 1d Verpflichtete müssen für die Angriffserkennung und -nachverfolgung relevante nicht personenbezogene Daten, die beim Betrieb eines Energieversorgungsnetzes oder einer Energieanlage anfallen, mindestens vier Jahre speichern.

(1f) Betreiber von Energieversorgungsnetzen und Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, haben dem Bundesamt für Sicherheit in der Informationstechnik erstmalig ein Jahr nach Inkrafttreten dieses Gesetzes und danach alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1d auf geeignete Weise nachzuweisen. Das Bundesamt für Sicherheit in der Informationstechnik hat die hierfür eingereichten Nachweisdokumente unverzüglich an die Bundesnetzagentur weiterzuleiten. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben sicherzustellen, dass die unbefugte Offenbarung der ihnen nach Satz 1 zur Kenntnis gelangten Angaben ausgeschlossen wird. Das Bundesamt für Sicherheit in der Informationstechnik kann bei Mängeln in der Umsetzung der Anforderungen nach Absatz 1d oder in den Nachweisdokumenten nach Satz 1 im Einvernehmen mit der Bundesnetzagentur die Beseitigung der Mängel verlangen.“

ENTWURF

Artikel 5

Änderung der Außenwirtschaftsverordnung

§ 55 Absatz 1 der Außenwirtschaftsverordnung vom 2. August 2013 (BGBl. I S. 2865), die zuletzt durch Artikel 1 der Verordnung vom 26. Oktober 2020 (BAnz AT 28.10.2020 VI) geändert worden ist, wird wie folgt geändert:

1. Nach Nummer 1 wird folgende Nummer 2 eingefügt:

„2. kritische Komponenten im Sinne des § 2 Absatz 13 des BSI-Gesetzes entwickelt oder herstellt,“.

2. Die bisherigen Nummern 2 bis 11 werden die Nummern 3 bis 12.

Artikel 6

Änderung des Zehnten Buches Sozialgesetzbuch

In § 67c Absatz 3 Satz 1 des Zehnten Buches Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130), das zuletzt durch Artikel 8 des Gesetzes vom 12. Juni 2020 (BGBl. I S. 1248) geändert worden ist, werden nach dem Wort „Verantwortlichen“ die Wörter „oder für die Wahrung oder Wiederherstellung der Sicherheit und Funktionsfähigkeit eines informationstechnischen Systems durch das Bundesamt für Sicherheit in der Informationstechnik“ eingefügt.

Artikel 7

Evaluierung

(1) Die §§ 2 Absatz 10, 8a, 8b, 8d und 8e sowie 10 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (Artikel 1) sind zum 31. Dezember 2022 unter Einbeziehung eines wissenschaftlichen Sachverständigen, der im Einvernehmen mit dem deutschen Bundestag bestellt wird, zu evaluieren.

(2) Der Artikel 10 des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl. I S. 1324) ist aufgehoben.

Artikel 8

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

ENTWURF

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

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

Maßnahmen zur Gewährleistung von Cyber-Sicherheit können jedoch nicht statisch sein. Ein ausreichendes Schutzniveau heute ist kein Garant für adäquate Schutzmechanismen und die erfolgreiche Abwehr von Angriffen morgen. Eine ständige Anpassung und Weiterentwicklung der Abwehrstrategien ist daher erforderlich. Entsprechend dem Auftrag aus dem Koalitionsvertrag für die 19. Legislaturperiode, Zeile 1969 ff., wird daher das IT-Sicherheitsgesetz fortgeschrieben und der Ordnungsrahmen erweitert, um neuen Gefährdungen angemessen zu begegnen. Die Anpassungen bestehender Regelungen und die Schaffung neuer Regelungen dienen dem Schutz von Staat, Wirtschaft und Gesellschaft.

II. Wesentlicher Inhalt des Entwurfs

Das Gesetz basiert auf Erfahrungen mit der Anwendung der im ersten IT-Sicherheitsgesetz geregelten Befugnisse sowie weiteren Erkenntnissen, z.B. aus Cyber-Angriffen und anderen Sicherheitsvorfällen. Diese betreffen Staat, Wirtschaft und Gesellschaft gleichermaßen. Wesentlicher Inhalt des Gesetzentwurfs ist:

– Die besonders hohen Sicherheitsanforderungen an die Kommunikationstechnik der Bundesverwaltung erfordern eine effektive und schnelle Prüf- und Kontrollmöglichkeit. Zu diesem Zweck werden dem Bundesamt weitere Kontrollbefugnisse eingeräumt und die Verarbeitung von Daten ermöglicht, die für die Bewertung der Netz- und Informationssicherheit von Bedeutung sein können. Pseudonymisierte Protokolldaten können künftig über einen Zeitraum von maximal zwölf Monaten gespeichert werden, da Cyber-Vorfälle in der Vergangenheit gezeigt haben, dass sich Angriffe oft über einen mehrjährigen Zeitraum erstrecken können. Veränderte Angriffsszenarien haben es zudem erforderlich gemacht, dass der Begriff der Protokollierungsdaten aufgenommen wird. Diese helfen bei der Erkennung von Schadsoftware. Darüber hinaus werden die Verbindlichkeit der Mindeststandards und der Adressatenkreis erweitert. Neben den Stellen des Bundes gelten die Mindeststandards künftig auch für IT-Dienstleister, die Dienstleistungen für die Kommunikationstechnik des Bundes erbringen. So soll bei jeder Einrichtung des Bundes ein einheitliches IT-Sicherheitsniveau gewährleistet werden.

– Außerdem kann das BSI künftig Auskunft über Bestandsdaten verlangen, um mittels einer IP-Adresse Betreiber Kritischer Infrastrukturen, Unternehmen im besonderen öffentlichen Interesse und Anbieter Digitaler Dienste über Sicherheitslücken informieren zu können, sofern erhebliche Schäden in informationstechnischen Systemen, die aufgrund ihrer gesellschaftlichen Bedeutung besonders schutzwürdig sind, drohen.

ENTWURF

– Das BSI erhält die Befugnis, Sicherheitslücken an den Schnittstellen informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen zu detektieren (sog. Portscans). Damit soll dem BSI ermöglicht werden, unter bestimmten Voraussetzungen nach Sicherheitslücken zu suchen und die Betroffenen zu informieren, damit diese die Sicherheitslücken schließen. Darüber hinaus darf das BSI künftig Systeme und Verfahren zur Analyse von Schadprogrammen und Angriffsmethoden einsetzen (Honeypots). Wird das System von einer Schadsoftware infiziert, ist es dem BSI durch Analyse des Systems möglich, insbesondere Art, Funktionsweise und Infektionsweg nachzuvollziehen. Diese Erkenntnis kann genutzt werden, um Nutzer informationstechnischer Systeme im Rahmen der gesetzlichen Aufgaben des Bundesamtes zu warnen und Systeme Kritischer Infrastrukturen oder des Bundes geeignet zu schützen.

– Mit dem Gesetz wird zudem eine Anordnungsbefugnis des BSI gegenüber Telekommunikations- und Telemediendiensteanbietern zur Abwehr spezifischer Gefahren für die Informationssicherheit geschaffen. Diese müssen die erforderlichen technischen und organisatorischen Maßnahmen ergreifen, um einen ordnungsgemäßen Zustand ihrer Angebote wiederherzustellen, wenn diese Angebote unzureichend gesichert sind.

– Die bestehenden Meldepflichten und verpflichtenden Mindeststandards für Betreiber Kritischer Infrastruktur werden auf weitere Teile der Wirtschaft ausgeweitet. Neben Kritischen Infrastrukturen gibt es weitere Unternehmen, die von besonderem öffentlichen Interesse sind: hierzu zählen Unternehmen der Rüstungsindustrie, Unternehmen, die wegen ihrer hohen Wertschöpfung eine besondere volkswirtschaftliche Bedeutung haben sowie Unternehmen, die der Regulierung durch die Störfallanordnung unterfallen. Durch eine Rechtsverordnung wird konkretisiert werden, welche Unternehmen eine besondere volkswirtschaftliche Bedeutung haben.

– Kritische Infrastrukturen sind auf Grund der voranschreitenden Digitalisierung und der damit einhergehenden Vernetzung oft auf Komponenten angewiesen, die von hoher Kritikalität sind, weil Störungen ebendieser zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit oder Integrität der Kritischen Infrastrukturen – etwa der öffentlichen Telekommunikationsnetze – führen können. Für derartige kritische Komponenten wird die Möglichkeit geschaffen, durch eine umfassende Prüfmöglichkeit deren Einsatz ggf. auch vorab untersagen zu können, soweit überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange diesem entgegenstehen. Ferner werden über eine verpflichtende Garantieerklärung bestimmte Maßnahmen von den Herstellern der kritischen Komponenten eingefordert, welche den laufenden Betrieb der Komponenten betreffen.

– Zum Schutz der Bürgerinnen und Bürger wird der Verbraucherschutz im Bereich der Informationssicherheit als zusätzliche Aufgabe des BSI ergänzt. Das BSI wird als unabhängige und neutrale Beratungsstelle für Fragen der IT-Sicherheit etabliert; u.a. soll das BSI-Angebot um eine Verbraucherschutz-Onlineplattform ergänzt werden.

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

– Das Bußgeldregime des BSIG wird insgesamt überarbeitet. Die Bußgeldtatbestände werden überarbeitet und ergänzt und so ausgestaltet, dass sie europarechtlichen Anforderungen genügen. Der Bußgeldrahmen wurde erhöht; auf diesem Wege werden auch Wertungswidersprüche bei Verstößen gegen die DSGVO und die NIS-Richtlinie behoben.

ENTWURF

– Eingeführt wird schließlich für Telemediendiensteanbieter die Verpflichtung, Fälle von rechtswidrig verbreiteten Daten an das Bundeskriminalamt als Zentralstelle zu melden. Abgestellt wird auf ein strafbares Verhalten nach §§ 202a bis 202d des Strafgesetzbuches sowie die Betroffenheit einer großen Zahl von Personen, eines Datenbestands von großem Ausmaß oder eines Datenbestands von Behörden oder Einrichtungen des Bundes oder deren Mitgliedern oder sicherheitsempfindlicher Stellen von lebenswichtigen Einrichtungen, bei deren Ausfall oder Zerstörung ein erhebliche Bedrohung für die Gesundheit oder das Leben von Menschen zu befürchten ist oder die für das Funktionieren des Gemeinwesens unverzichtbar sind.

III. Alternativen

Keine.

IV. Gesetzgebungskompetenz

Für die Änderungen des BSIG (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) Grundgesetz (GG) sowie aus Artikel 74 Absatz 1 Nummer 11 GG (Recht der Wirtschaft, einschließlich gefahrenabwehrrechtlicher Annexkompetenz) in Verbindung mit Artikel 72 Absatz 2 GG.

Die gefahrenabwehrrechtliche Annexkompetenz besteht für die Anordnungsbefugnisse des Bundesamtes für Sicherheit in der Informationstechnik (Bundesamt) gegenüber Telekommunikations- und Telemediendiensteanbietern mit Blick auf die Notwendigkeit der näheren Überwachung der im Telekommunikationsgesetz sowie im Telemediengesetz verankerten gewerberechtlichen Pflichten dieser Anbieter. Hier ist zur Aufrechterhaltung sicherer IT-Strukturen und -anwendungen eine bundesweit einheitliche Gefahrenabwehr erforderlich.

Für Änderungen, welche die Befugnisse des Bundesamtes zum Schutz der Bundesverwaltung erweitern, hat der Bund eine Gesetzgebungskompetenz kraft Natur der Sache.

Die Zuständigkeit des Bundes für Regelungen zur bundesweiten Information einschließlich eventueller Empfehlungen und Warnungen von Verbraucherinnen und Verbrauchern auf dem Gebiet der Informationssicherheit folgt mit Blick auf die gesamtstaatliche Verantwortung der Bundesregierung ebenfalls aus der Natur der Sache (Staatsleitung), denn Fragen zur Sicherheit in der Informationstechnik haben bei stetig zunehmender Digitalisierung und Vernetzung aller Lebensbereiche regelmäßig überregionale Auswirkungen. Der Bund hat darüber hinaus die ausschließliche Gesetzgebungskompetenz nach Artikel 73 Absatz 1 Nummer 8 GG für die Rechtsverhältnisse der im Dienst des Bundes und der bundesunmittelbaren Körperschaften des öffentlichen Rechts stehenden Personen.

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

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

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

ENTWURF

Soweit die Regelungen auf Artikel 74 Absatz 1 Nummer 11 GG beruhen, ist eine bundesgesetzliche Regelung zur Wahrung der Wirtschaftseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich (vgl. Artikel 72 Absatz 2 GG). Eine Regelung durch den Landesgesetzgeber würde zu erheblichen Nachteilen für die Gesamtwirtschaft führen, die sowohl im Interesse des Bundes als auch der Länder nicht hingenommen werden können. Insbesondere wäre zu befürchten, dass unterschiedliche landesrechtliche Behandlungen gleicher Lebenssachverhalte, z. B. unterschiedliche Voraussetzungen für die Vergabe von Sicherheitszertifikaten, erhebliche Wettbewerbsverzerrungen und störende Schranken für die innerdeutsche Wirtschaftstätigkeit zur Folge hätten. Internationale Abkommen zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten setzen voraus, dass in jedem Staat nur eine hoheitliche Zertifizierungsstelle existiert.

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

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

VI. Gesetzesfolgen

1. Rechts- und Verwaltungsvereinfachung

Der Gesetzentwurf trägt zur Rechts- und Verwaltungsvereinfachung bei, indem er die Pflichten und Rechte des Bundesamtes für Sicherheit in der Informationstechnik schärft und somit dazu beiträgt die jeweiligen Verantwortungen klarzustellen. Durch einheitliche Mindeststandards für die IT der öffentlichen Bundesverwaltung wird zudem ein einheitliches Niveau an IT-Sicherheit geschaffen.

2. Nachhaltigkeitsaspekte

Der Gesetzentwurf steht im Einklang mit dem Leitprinzip der Bundesregierung zur nachhaltigen Entwicklung hinsichtlich Lebensqualität und sozialem Zusammenhalt. Der Gesetzesentwurf folgt den Leitgedanken der Bundesregierung zur Berücksichtigung der Nachhaltigkeit, indem zur Stärkung von Lebensqualität ein hohes Niveau an Cyber-Sicherheit in Deutschland geschaffen wird. Der verbesserte Schutz kritischer Infrastrukturen gewährleistet ein hohes Maß an Versorgungssicherheit der Bürgerinnen und Bürger und verbessert den sozialen Zusammenhalt und die gleichberechtigte Teilhabe an der wirtschaftlichen Entwicklung im Sinne der Deutschen Nachhaltigkeitsstrategie. Der Gesetzentwurf wurde unter Berücksichtigung der Prinzipien der nachhaltigen Entwicklung im Hinblick auf die Nachhaltigkeit geprüft. Hinsichtlich seiner Wirkungen entspricht er insbesondere den Indikatoren 2.2, 6.2 und 16.2 der Deutschen Nachhaltigkeitsstrategie, indem ein sicheres Leben für alle Menschen jeden Alters gewährleistet und ihr Wohlergehen gefördert werden.

3. Haushaltsausgaben ohne Erfüllungsaufwand

Keine.

4. Erfüllungsaufwand

a. Erfüllungsaufwand für die Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

ENTWURF

b. Erfüllungsaufwand für die Wirtschaft

Der Erfüllungsaufwand für die Wirtschaft ist nur unter hoher Unsicherheit quantifizierbar. Da die Entwicklung der IT-Strukturen sowie möglicher Bedrohungen kaum abzuschätzen sind und teilweise noch konkretisierende Rechtsnormen ausstehen, können nur grobe Anhaltspunkte für den Erfüllungsaufwand benannt werden. Zur Schätzung wurden in Ermangelung empirischer Daten in großem Umfang Annahmen getroffen. Schätzwerte, die im Wesentlichen auf Annahmen basieren, bilden den unteren Rand der Spannbreite möglicher Belastungen ab und sind somit als Mindestwerte zu verstehen.

– § 7a BSIG-E: Hersteller von informationstechnischen Produkten und Systemen müssen dem BSI auf Verlangen Informationen hierzu zur Verfügung stellen, auch zu technischen Details. Bei den Anfragen des BSI wird es in der Regel um Informationen gehen, die die Software des Produktes, den internen Programmablauf und die Schaltungsdetails der zugrundeliegenden Elektronik betreffen. Der Hersteller muss also zunächst recherchieren, wer im Unternehmen für den entsprechenden Teil des Produkts zuständig ist und ob zur Beantwortung der Fragen die selbst entwickelten, eigenen Bestandteilte oder evtl. fremde bzw. hinzugekaufte von Bedeutung sind. Anschließend müssen die Daten so aufbereitet werden, dass sie dem BSI in "lesbarer Form" zur Verfügung gestellt werden können. Vor einer Herausgabe der Informationen an das BSI muss unternehmensintern geklärt werden, ob betriebliche Gründe gegen die Weitergabe sprechen. Hierfür entstehen der Wirtschaft jährliche Personalkosten in Höhe von circa 153.328 Euro.

– § 7c BSIG-E: Umsetzung angeordneter Maßnahmen im Falle erheblicher Gefahr bei Telekommunikationsdiensten. Zur Abwehr konkreter erheblicher Gefahr kann das BSI die Umsetzung verschiedener Maßnahmen bei Anbietern von Telekommunikationsdiensten anordnen. Betreiber von Telekommunikationsdiensten, die mehr als 100.000 Kunden haben, werden z. B. auf Anordnung des BSI verpflichtet, sogenannte Malwaredomänen bzw. IP-Adressen von C&C-Servern zu sperren oder auf Sinkholes umzuleiten, um infizierte Nutzersysteme zu schützen. Bei diesem Vorgang handelt es sich um einen ständigen, tagesaktuellen Prozess. Die gelieferten Informationen können auf Anbieterseite im Wesentlichen automatisiert verarbeitet werden. Hierfür entstehen der Wirtschaft jährliche Personalkosten in Höhe von circa 92.467 Euro.

– § 8a Absatz 1a und 1b BSIG-E: Betreiber Kritischer Infrastrukturen werden verpflichtet, in Kritischen Infrastrukturen Systeme zur Angriffserkennung einzusetzen und bestimmte Daten für mindestens vier Jahre zu speichern. Eine Schätzung des Erfüllungsaufwands, im Wesentlichen die Kosten für die Systeme zur Angriffserkennung selbst sowie Personal, ist insoweit nicht möglich. Denn zum einen sind solche Systeme teilweise bereits bei Betreibern Kritischer Infrastrukturen im Einsatz, sodass für diese Betreiber durch die Neuregelung überhaupt keine zusätzlichen Kosten entstehen. Zum anderen sind die Kosten für diese Systeme sehr unterschiedlich. Der Einsatz bestimmter Systeme wird aber nicht vorgeschrieben, sodass der Erfüllungsaufwand auch von Entscheidungen der Verpflichteten abhängt.

– § 8b Absatz 3 Satz 1 BSIG-E: Registrierung als Betreiber Kritischer Infrastruktur. Betreiber Kritischer Infrastrukturen müssen sich beim BSI registrieren und eine Kontaktstelle benennen. Die Pflicht zur Benennung einer Kontaktstelle für Betreiber Kritischer Infrastrukturen wurde bereits mit dem ersten IT-Sicherheitsgesetz 2015 eingeführt, neu eingeführt wurde lediglich die Registrierung der Kritischen Infrastruktur. Dies ist jedoch für die benannten Kontaktstellen der Betreiber Kritischer Infrastrukturen im Regelfall bereits heute erfüllt, sodass hier für die bestehenden Betreiber Kritischer Infrastrukturen keine zusätzlichen Erfüllungsaufwände entstehen. Lediglich für die neu im Sektor Siedlungsabfallentsorgung hinzukommenden Betreiber Kritischer Infrastrukturen ist hier mit einem erstmaligen Erfüllungsaufwand zu rechnen. Bei einer geschätzten An-

ENTWURF

zahl von ca. 100 zusätzlichen Betreibern Kritischer Infrastrukturen im Sektor Siedlungsabfallentsorgung werden daher für die Wirtschaft einmalige Personalkosten in Höhe von 6.110 € erwartet.

– § 8b Absatz 3 Satz 2 BSIG-E: Sicherstellen der Erreichbarkeit der Kontaktstelle. Betreiber Kritischer Infrastrukturen sind verpflichtet die durchgehende Erreichbarkeit einer Kontaktstelle sicherzustellen. Diese Pflicht wurde bereits mit dem ersten IT-Sicherheitsgesetz 2015 eingeführt, sodass hier für die bestehenden Betreiber Kritischer Infrastrukturen keine zusätzlichen Erfüllungsaufwände entstehen. Lediglich für die neu im Sektor Siedlungsabfallentsorgung hinzukommenden Betreiber Kritischer Infrastrukturen im Bereich der Wirtschaft ist hier mit jährlichen Personalkosten in Höhe von ca. 28.895 € zu rechnen.

– § 8b Absatz 4a BSIG-E: Für die Pflicht von Betreibern Kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse, im Falle erheblicher Störungen gemäß § 8b Abs. 4 Nr. 2, § 8f Abs. 7 Nr. 2 oder § 8f Abs. 8 Nr. 2 BSIG-E dem BSI die zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten zu übermitteln, entstehen der Wirtschaft geschätzte Personalkosten von jährlich 49.350 €.

– § 8f Absatz 1 BSIG-E: Für die Pflicht von Unternehmen im besonderen öffentlichen Interesse nach § 2 Abs. 14 Nummer 1 und 2 BSIG-E, gegenüber dem BSI eine Selbsterklärung zur IT-Sicherheit vorzulegen entstehen den betroffenen Unternehmen bei der erstmaligen Vorlage Erfüllungsaufwände von ca. 15.886 €, danach jährliche Erfüllungsaufwände von ca. 6.110€.

– § 8f Absatz 5 BSIG-E: Für die Pflicht von Unternehmen im besonderen öffentlichen Interesse nach § 2 Abs. 14 Nummer 1 und 2 BSIG-E, sich einmalig beim BSI zu registrieren und eine zu den üblichen Geschäftszeiten erreichbare Stelle zu benennen, entstehen der Wirtschaft einmalige Erfüllungsaufwände in Höhe von 15.886 Euro.

– § 8f Absatz 7 und 8 BSIG-E: Die Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1, 2 und 3 BSIG-E sind verpflichtet, bestimmte Störungen ihrer informationstechnischen Systeme, Komponenten und Prozesse unverzüglich an das BSI zu melden. Die Anzahl der meldepflichtigen Vorfälle pro Unternehmen hierbei nur schwer im Vorhinein abschätzen. Aufgrund von Erfahrungswerten aus dem Bereich der Meldungen von Betreibern Kritischer Infrastrukturen wird ein jährlicher Erfüllungsaufwand von ca. 19.552 Euro für die Wirtschaft geschätzt.

– § 9a Absatz 2 BSIG-E: Den Konformitätsbewertungsstellen entsteht für das Antragsverfahren nach § 9 Absatz 2 BSIG-E ein jährlicher Erfüllungsaufwand in Form von Personalkosten in Höhe von 13.200 Euro.

– § 109 Absatz 2 TKG-E: Kritische Komponenten im Bereich Telekommunikationsnetze und –dienste dürfen von Betreibern Kritischer Infrastrukturen nur eingesetzt werden, wenn Sie ein Zertifizierungsverfahren durchlaufen haben. Das Zertifizierungsverfahren muss hierbei eng durch Hersteller begleitet werden. Deshalb entstehen der Wirtschaft hier jährliche Personalkosten in Höhe von circa 2.280.000 Euro und jährliche Sachkosten in Höhe von circa 6.000.000 Euro.

– Für die folgenden §§ wurden jeweils geringe Erfüllungsaufwände ermittelt, so dass diese zusammengefasst aufgeführt werden um die Darstellung nicht zu stark zu zergliedern: § 4a Absatz 1 und Absatz 3, § 4b Absatz 4, § 5c, § 7d, § 8a Absatz 1b, § 8b Absatz 4a Nr. 2, § 8f Absatz 1, § 8f Absatz 5, § 8f Abs. 7 und Absatz 8, § 8f Absatz 9, § 9b Absatz 1, § 9b Absatz 2 BSIG-E- sowie § 109 Absatz 7, § 113 Absatz 3 TKG und § 15d Absatz 1 TMG. Der Erfüllungsaufwand welcher durch die vorgenannten §§ für die Wirtschaft entsteht setzt sich zusammen aus verschiedenen Informations- und Meldungspflichten der Wirtschaft gegenüber dem BSI. Hierfür entstehen der Wirtschaft

ENTWURF

einmalige Personalkosten in Höhe von ca. 31.772 Euro und jährliche Personalkosten in Höhe von ca. 270.120 Euro.

c. Erfüllungsaufwand für die Verwaltung

Der Verwaltung entsteht für die Erfüllung der im Gesetz vorgesehenen zusätzlichen Aufgaben ein Aufwand von insgesamt 948 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 68,6 Millionen Euro.

Bundesministerium des Innern, für Bau und Heimat (BMI)

Beim BMI entsteht ein Erfüllungsaufwand in Höhe von 4 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von 284.724 Euro.

– § 9b Absatz 3 BSIG-E, Untersagen der Verwendung angezeigter kritischer Komponenten in einer kritischen Infrastruktur: Die Verwendung kritischer Komponenten ist durch den Betreiber einer kritischen Infrastruktur vor der Inbetriebnahme anzuzeigen. Die Inbetriebnahme der Komponenten ist für die Dauer von drei Monaten untersagt. Innerhalb dieser Frist entscheidet das BMI, ob die Elemente zu untersagen sind. Hierfür benötigt das Ministerium 4 Planstellen/Stellen.

Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben (BDBOS)

Die BDBOS ist verantwortlich für die Kommunikationswege des Bundes. Dort ist ein Erfüllungsaufwand in Höhe von rund 21 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von 1,7 Mio. Euro.

– §§ 4a und 4b BSIG-E, Begleitung der Kontrollen des BSI zur Feststellung der Sicherheit von Kommunikationstechnik von Bundesbehörden: Die BDBOS hat die Kontrollen und die Informationsanforderungen zu koordinieren, die Prüfungen zu begleiten, Ergebnisse zusammenzufassen und Folgemaßnahmen zu bearbeiten oder anzustoßen. Dies gilt für alle Niederlassungen und Außenstellen der Behörden. Hierfür entsteht ein Personalbedarf in Höhe von 6 Planstellen/Stellen.

– § 5 Absatz 2 und Absatz 2a i. V. m. § 5a BSIG, Verarbeitung behördeninterner Protokolldaten: Mit der Neufassung des BSIG erhält das BSI die Befugnis, zur Abwehr von Gefahren für die Kommunikationstechnik behördeninterne Protokolldaten auszuwerten. Der BDBOD entsteht dadurch schätzungsweise durch die verlängerte Speicherfrist der Daten, der für die Verarbeitung zunächst notwendigen Pseudonymisierung und den sonstigen geforderten Zuarbeiten ein zusätzlicher Stellenbedarf von 2 Planstellen/Stellen.

– § 8 Absatz 1 BSIG, Umsetzung der vom BSI vorgegebenen Mindeststandards: Durch die mit § 8 Absatz 1 BSIG geschaffenen Befugnisse des BSI, Mindeststandards vorzugeben und deren Einhaltung zu überwachen und zu kontrollieren entsteht in der BDBOS ein Mehraufwand von 10 Planstellen/Stellen.

– § 8b Absatz 4a BSIG, Einleiten von Maßnahmen zur Wiederherstellung der Sicherheit und der Funktionsfähigkeit der Systeme: Um die Sicherheit und die Funktionsfähigkeit informationstechnischer Systeme nach einer erheblichen Störung wiederherzustellen, ist ein zusätzlicher Stellenbedarf von 3 Planstellen/Stellen notwendig.

Bundesnetzagentur (BNetzA)

ENTWURF

Die BNetzA ist als oberste deutsche Regulierungsbehörde zuständig für die Aufrechterhaltung und die Förderung des Wettbewerbs in den Netzmärkten. Dort entsteht ein Erfüllungsaufwand in Höhe von rund 34 Planstellen/Stellen mit jährlichen Personalkosten in Höhe von 2,4 Mio. Euro.

– §§ 4a und 4b BSIG-E, Begleitung der Kontrollen des BSI zur Feststellung der Sicherheit von Kommunikationstechnik von Bundesbehörden: Die BNetzA hat die Kontrollen und die Informationsanforderungen zu koordinieren, die Prüfungen zu begleiten, Ergebnisse zusammenzufassen und Folgemaßnahmen zu bearbeiten oder anzustoßen. Dies gilt für alle Niederlassungen und Außenstellen der Behörden. Hierfür entsteht ein Personalbedarf in Höhe von 4,5 Planstellen/Stellen.

– § 5 Absatz 2 und Absatz 2a in Verbindung mit § 5a BSIG, Verarbeitung behördeninterner Protokolldaten: Mit der Neufassung des BSIG erhält das BSI die Befugnis, zur Abwehr von Gefahren für die Kommunikationstechnik behördeninterne Protokolldaten auszuwerten. Der BNetzA entsteht dadurch schätzungsweise durch die verlängerte Speicherfrist der Daten, der für die Verarbeitung zunächst notwendigen Pseudonymisierung und den sonstigen geforderten Zuarbeiten ein zusätzlicher Stellenbedarf von 21 Planstellen/Stellen.

– § 8 Absatz 1 BSIG, Umsetzung der vom BSI vorgegebenen Mindeststandards: Durch die mit § 8 Absatz 1 BSIG geschaffenen Befugnisse des BSI, Mindeststandards vorzugeben und deren Einhaltung zu überwachen und zu kontrollieren entsteht ein Mehraufwand von 2,7 Planstellen/Stellen.

– § 8b Absatz 4a BSIG, Einleiten von Maßnahmen zur Wiederherstellung der Sicherheit und der Funktionsfähigkeit der Systeme: Um die Sicherheit und die Funktionsfähigkeit informationstechnischer Systeme nach einer erheblichen Störung wiederherzustellen, ist ein zusätzlicher Stellenbedarf von 1 Planstellen/Stellen notwendig.

– § 109 TKG, Überprüfung und Überwachung getroffener technischer Maßnahmen durch die BNetzA: Die Aufgabenerweiterung im Rahmen der Überprüfung von Sicherheitskonzepten von Telekommunikationsnetzbetreibern oder Anbietern von Telekommunikationsdiensten, erfordert bei der Aufrechterhaltung der aktuellen Stichprobensystematik und der Frequenz der Besuche einen zusätzlichen Personalbedarf von 5 Planstellen/Stellen.

Bundeskriminalamt (BKA)

Als Konsequenz aus dem Datenleak-Vorfall, bei dem zwischen Dezember 2018 und Januar 2019 rechtswidrig erlangte persönliche Daten u.a. von Politikern, Personen des öffentlichen Lebens und Journalisten veröffentlicht wurden, soll die Pflicht für Telemediendiensteanbieter, die Verbreitung rechtswidrig erlangter persönlicher Daten dem BKA als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei zu melden, eingeführt werden.

– § 15d TMG-E: Um die dem BKA hierdurch entstehenden zusätzlichen Aufwände bewältigen zu können, müssen die erforderlichen Strukturen in den Fachbereichen sowie unterstützenden Organisationseinheiten aufgebaut werden, insbesondere zur Aufbereitung und Auswertung der Daten. Zusätzlich müssen weitere Ermittlungskapazitäten zur Bewältigung der sich aus den übermittelten Datenbeständen ergebenden Verfahren geschaffen werden. Beim BKA entsteht hierdurch ein Erfüllungsaufwand in Höhe von 90 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 7,3 Mio. Euro. Zusätzlich sind zur Umsetzung des Gesetzes Sachkosten in Höhe von einmalig 765.000 Euro und jährlich in Höhe von rund 9,5 Mio. Euro zu berücksichtigen.

Bundesamt für Sicherheit in der Informationstechnik (BSI)

ENTWURF

Beim BSI ist ein Erfüllungsaufwand in Höhe von 799 Planstellen/Stellen mit Personalkosten in Höhe von jährlich rund 56,9 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.

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

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

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

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

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

– § 4b BSIG-E, Meldestelle: Die Sammlung von Informationen über Sicherheitslücken, Schadprogramme und IT-Sicherheitsvorfälle ist für ein Gesamtlagebild von besonderer Bedeutung. Um eine zentrale Sammlung und systematische Auswertung der an das Bundesamt gerichteten Hinweise auch angesichts der Vielzahl mit dem IT-SiG 2.0 hinzukommender Regelungsbereiche in angemessener Weise sicherzustellen, ist der

ENTWURF

Ausbau der Meldestelle beim BSI zwingend erforderlich. Der organisatorische und technische Ausbau sowie die kontinuierliche Beobachtung, Entgegennahme sowie Auswertung und Analyse der Meldungen führt zu einem zusätzlichen Personalbedarf von 14 Planstellen/Stellen.

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

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

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

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

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

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

ENTWURF

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

– § 8b Absatz 4a BSIG-E: Kommt es bei Betreibern Kritischer Infrastrukturen oder bei Unternehmen im besonderen öffentlichen Interesse zu größeren (IT-) Störungen, hat dies sehr schnell negative Auswirkungen auf große Teile der Bevölkerung. Zur Aufrechterhaltung oder Wiederherstellung von IT-Systemen im Falle einer erheblichen Störung ist es notwendig, dass das Bundesamt die Herausgabe der zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten verlangen kann. Dafür sind beim BSI 19 Planstellen/Stellen erforderlich.

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

– § 9a BSIG-E: Als Nationale Behörde für die Cybersicherheitszertifizierung im Sinne des Artikels 58 Absatz 1 der Verordnung (EU) 2019/881 führt das Bundesamt Zertifizierungen und Auditierungen durch und überwacht Konformitätsbewertungsstellen. Ebenso müssen die europäischen Schemata überprüft, angewendet und durchgesetzt sowie Prüfstellen für die Cybersicherheitszertifizierung überwacht werden Dafür entsteht für das BSI ein personeller Mehrbedarf von 120 Planstellen/Stellen.

– § 9b BSIG-E: Die in § 9b eingefügte Garantieerklärung für kritische Komponenten führt zu einem erhöhten Personalbedarf von 4 Planstellen/Stellen.

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

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

– § 109 TKG-E: Durch die Standardisierung und die Sicherstellung der Qualität der Sicherheitskonzepte der Betreiber sowie der Prüfung und Zertifizierung kritischer Komponenten entsteht dem Bundesamt zudem ein Personalbedarf von 119 Planstellen/Stellen.

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

ENTWURF

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, sondern 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 Evaluierung ist vorgesehen (Artikel 7).

B. Besonderer Teil

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

Zu Nummer 1

Zu Buchstabe a

Der derzeitige Wortlaut des § 2 Absatz 3 BSIG zur Definition der Kommunikationstechnik des Bundes umfasst bisher nicht die behördeninterne Kommunikation oder den behördeninternen Datenaustausch. Zudem werden allgemeine Datenverarbeitungsvorgänge nicht erfasst. Diese Bereiche sind jedoch, genauso wie die Informationstechnik zur Kommunikation und der Datenaustausch der Behörden untereinander oder mit Dritten, gleichermaßen Angriffsziele. Durch die Einbeziehung dieser Bereiche steigt das Sicherheitsniveau insgesamt, da mehr Detektionsmöglichkeiten geschaffen werden. Somit wird insbesondere die Detektion von zielgerichteten und nachrichtendienstlichen Angriffen verbessert. Der Begriff der Datenverarbeitung ist hierbei im Sinne der Datenschutzgrundverordnung (DSGVO) weit zu verstehen. Der Datenaustausch bleibt weiterhin umfasst. Regelungen über den Geheimschutz bleiben unberührt.

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

Zu Buchstabe b

Das Bundesverfassungsgericht wurde in § 2 Absatz 3 Satz 2 BSIG bisher unter den Begriff der „Bundesgerichte“ gefasst und nicht namentlich genannt. Der besonderen verfassungsrechtlichen Stellung des Bundesverfassungsgerichts wird durch die Aufnahme in die Aufzählung der Verfassungsorgane Rechnung getragen. Die Änderung dient der Klarstellung

ENTWURF

der vollständigen Gleichstellung mit den übrigen genannten Verfassungsorganen für die Zwecke dieser Norm.

Zu Buchstabe c

Aufgrund veränderter Angriffsszenarien wird der Begriff der Protokollierungsdaten eingeführt und in § 2 Absatz 8a legaldefiniert.

Protokollierungsdaten dokumentieren technische Ereignisse und Zustände innerhalb eines IT-Systems, die tatsächliche Anhaltspunkte für die Erkennung und Analyse laufender und die Rekonstruktion vergangener Angriffe auf die Informations- und Kommunikationstechnik des Bundes liefern können. Protokollierungsdaten von IT-Systemen werden auch als Log-Daten bezeichnet. Sie entstehen automatisiert durch die auf dem IT-System laufenden Prozesse. Inhaltsdaten sind daher regelmäßig keine Protokollierungsdaten.

Protokollierungsdaten umfassen insbesondere die Protokollierung auf Ebene des Betriebssystems, also Zustände von Prozessen, Veränderungen an Konfigurationen sowie Verbindungsaufbauten zu anderen Systemen. Zudem sind es Daten von Systemprozessen und Programmen.

Der überwiegende Teil der Protokollierungsdaten weist keinen Personenbezug auf. Zu den typischen personenbezogenen Protokollierungsdaten, die für die Analyse von technischen Ereignissen wie Start und Ende eines Programms von Bedeutung sind, gehören etwa Benutzerkennung, Hostname/Name des Endsystems, Anschlusskennungen des Endsystems und die Geräteadresse (MAC-Adresse).

Aliase wie die Benutzerkennung oder behördeninterne IP-Adressen sind für das Bundesamt grundsätzlich pseudonym, da die Auflösungen dem Bundesamt nicht bekannt sind.

Mit der Verarbeitung von Protokollierungsdaten lassen sich unter anderem weit verbreitete Trojaner wie etwa die Schadsoftware „Emotet“ besser erkennen. Durch diesen wird dem Opfer per E-Mail ein manipuliertes Word-Dokument zugestellt, das bei seinem Öffnen den Prozess Powershell ausführt, welcher wiederum weitere Schadfunktionen nachlädt und startet. Anhand der Protokollierungsdaten wird etwa sichtbar, dass eine Datei in Word geöffnet wird. Word wiederum startet den Prozess Powershell, der seinerseits Aktionen durchführt. Allein die Tatsache, dass Powershell von Word gestartet wird, ist bereits ein verdächtiges Verhalten, das auf ein Schadprogramm hindeutet. Die Inhalte des Dokuments werden nicht erhoben.

Die Nutzung von Protokollierungsdaten ist zudem das zweckmäßigsten Mittel bei der Erkennung sogenannter Advanced Persistent Threats (APT). Hier handelt es sich um komplex Angriffe (oftmals von fremden Nachrichtendiensten), deren Spuren regelmäßig nur in den Protokollierungsdaten zu finden sind.

Protokollierungsdaten werden u.a. näher in der Protokollierungsrichtlinie Bund beschrieben, die Bestandteil des auf § 8 beruhenden Mindeststandards „Protokollierung und Detektion“ ist.

Zu Buchstabe d

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

ENTWURF

Zu Buchstabe e

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

Zu Buchstabe f

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

§ 2 Absatz 13 definiert kritische Komponenten. Diese sind IT-Produkte, die in Kritischen Infrastrukturen eingesetzt werden und die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit dieser IT-Produkte zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können. Die kritischen Komponenten der Kritischen Infrastrukturen, die ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, werden durch den Katalog von Sicherheitsanforderungen nach § 109 Absatz 6 des Telekommunikationsgesetzes näher bestimmt. Für die übrigen kritischen Komponenten kann eine Festlegung künftig gesetzlich erfolgen.

§ 2 Absatz 14 regelt Unternehmen im besonderen öffentlichen Interesse. Zu diesen gehören nach Nummer 1 Rüstungshersteller sowie Hersteller von IT-Produkten für die Verarbeitung staatlicher Verschlusssachen. Grund dafür ist, dass ein Ausfall der Herstellungs- und Entwicklungstätigkeiten dieser Unternehmen wesentliche Sicherheitsinteressen der Bundesrepublik Deutschland gefährden könnte. Erhebliche Störungen der IT-Systeme dieser Unternehmen sollten dem Bundesamt daher mitgeteilt werden. Zu den Unternehmen nach Nummer 2 gehören solche, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind. Grund dafür ist, dass auch Ausfall und Störung der Geschäftstätigkeit einzelner Unternehmen, die nicht Betreiber Kritischer Infrastrukturen im Sinne dieses Gesetzes sind, von gesamtgesellschaftlicher Bedeutung sein können. Das ist zum Beispiel dann der Fall, wenn die IT-Systeme eines der größten Unternehmen Deutschlands nach inländischer Wertschöpfung durch einen Cyberangriff oder durch anderweitige IT-Störung derart gestört werden, dass das Unternehmen seiner Geschäftstätigkeit für einen längeren Zeitraum nicht nachgehen kann. Die Berechnung der inländischen Wertschöpfung wird dabei in einer Rechtsverordnung im Einzelnen festgelegt. In der Rechtsverordnung werden dafür abstrakt-generelle Kriterien verbindlich vorgegeben, nach denen Unternehmen selbst feststellen können, ob sie Unternehmen im besonderen öffentlichen Interesse im Sinne von § 2 Absatz 14 Nummer 2 sind. Die Berechnungsmethodik und auch die erfassten Unternehmen sollen sich dabei an dem Gutachten der Monopolkommission nach § 44 Absatz 1 GWB (sog. Hauptgutachten) orientieren. Darin werden derzeit alle zwei Jahre die einhundert größten Unternehmend Deutschlands nach inländischer Wertschöpfung ermittelt, wobei die Berechnung mithilfe der „direkten Wertschöpfungsstaffel“ erfolgt. Demnach wird die inländische Wertschöpfung anhand bestimmter Unternehmenskennzahlen ermittelt und ein Schwellenwert für eine nach dieser Methodik ermittelte inländische Wertschöpfung in der Rechtsverordnung ausgewiesen, bei dessen Überschreitung das entsprechende Unternehmen ein Unternehmen im besonderen öffentlichen Interesse darstellt. Unternehmen können selbst anhand der Berechnungsmethodik und des Schwellenwerts bei Kenntnis der entsprechenden Unternehmenskennzahlen ermitteln, ob sie von der Regelung betroffen sind.

ENTWURF

Die neue Kategorie der Unternehmen im besonderen öffentlichen Interesse haben zwar eine große Bedeutung in Bezug auf die IT-Sicherheit in Deutschland, jedoch ist diese im direkten Vergleich zu Betreibern Kritischer Infrastrukturen deutlich abgestuft. Sowohl die hier neu eingeführte Definition für Unternehmen im besonderen öffentlichen Interesse als auch die sich daraus ergebenden Rechtsfolgen für die betroffenen Unternehmen sind nicht mit denen von Betreibern Kritischer Infrastrukturen vergleichbar. Die neu eingeführten Verpflichtungen für diese Unternehmen bleiben dementsprechend weit hinter den Pflichten für die Betreiber Kritischer Infrastrukturen nach diesem Gesetz zurück. Um Unternehmen, die wegen ihrer Eigenschaft als Betreiber einer Kritischen Infrastruktur bereits höheren Schutzanforderungen unterliegen, nicht unnötig zu belasten, gilt ein Unternehmen nicht als Unternehmen im besonderen öffentlichen Interesse im Sinne dieses Gesetzes, wenn es Betreiber einer Kritischen Infrastruktur ist (vgl. § 2 Absatz 14). Zu den Unternehmen nach Nummer 3 gehören die Betreiber von Betriebsbereichen der oberen Klasse im Sinne der Zwölften Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes (Störfallverordnung). Diese Verordnung dient dem Schutz von Mensch und Umwelt vor den Folgen plötzlich auftretender Störfälle bei technischen Anlagen durch Austritt gefährlicher Stoffe. Da betroffene Unternehmen nach der Störfallverordnung ohnehin bereits nach § 9 der Störfallverordnung einen Sicherheitsbericht vorlegen müssen, sieht dieses Gesetz für diese Unternehmen noch weniger Verpflichtungen vor als für Unternehmen im besonderen öffentlichen Interesse nach den Nummern 1 und 2.

Zu Nummer 2

Zu Buchstabe a

Es handelt sich lediglich um eine redaktionelle Anpassung.

Zu Buchstabe b

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

Zu Buchstabe c

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

Zu Buchstabe d

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

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

ENTWURF

Bereits nach geltendem Recht ist es Aufgabe des BSI, die Anwender, also auch Verbraucherinnen und Verbraucher, nach § 3 Absatz 1 Satz 2 Nummer 14 BSIG in Fragen der Sicherheit in der Informationstechnik zu beraten, zu warnen und zu sensibilisieren. Hierzu stehen dem BSI insbesondere die Befugnisse der §§ 7, 7a BSIG zur Warnung, Empfehlung und Untersuchung auf dem Markt bereitgestellter oder zur Bereitstellung vorgesehener informationstechnischer Produkte und Systeme zur Verfügung.

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

Ein ganzheitlicher Verbraucherschutz im Bereich der Sicherheit in der Informationstechnik beschränkt sich jedoch nicht auf Maßnahmen, die sich unmittelbar an Verbraucherinnen und Verbraucher richten und auf die Vermittlung von Risikobewusstsein, Beurteilungsfähigkeit und Lösungskompetenz gerichtet sind, sondern umfasst u.a. auch das Eintreten für die Verbraucherbelange und die Sicherstellung der IT-Sicherheit gegenüber Herstellern oder die Förderung von Forschungsvorhaben mit Verbraucherschutzbezug. Insbesondere das Eintreten gegenüber den Herstellern von IT-Produkten hinsichtlich IT-Sicherheit und das konsequente Mitdenken der Hersteller der IT-Sicherheit bei Entwicklung und Gestaltung der Produkte und Dienste („security by design“) bietet einen guten Verbraucherschutz. Im Gegensatz zu Verbraucherschutzverbänden ist das BSI jedoch keine Organisation zur ausschließlichen Vertretung und Durchsetzung von Verbraucherinteressen, sondern hat als nationale Cybersicherheitsbehörde die Interessen aller Stakeholder aus Staat, Wirtschaft und Zivilgesellschaft zu berücksichtigen.

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

– Beratung und Information von Herstellern von Verbraucherprodukten, um bereits bei der Entwicklung und Gestaltung der Produkte und Dienste das konsequente Mitdenken der IT-Sicherheit ("security by design") zu erreichen.

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

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

ENTWURF

– Sicherheitstests und -analysen mit dem Schwerpunkt „IT-Sicherheitsrisiken für Verbraucherinnen und Verbraucher“. Durch Sicherheitstests und -analysen von auf dem Markt bereitgestellten IT-Produkten und Systemen kann das BSI aktuelle IT-Sicherheitsrisiken für Verbraucherinnen und Verbraucher identifizieren. Zum anderen können Sicherheitstests und -analysen zur stichprobenartigen Überprüfung bezüglich der Einhaltung der Anforderungen nach dem zuvor definierten Stand der Technik dienen.

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

– Ergänzung des BSI-Bürger-Angebots um eine Verbraucherschutz-Online-Plattform, auf der Verbraucherinnen und Verbraucher auf Empfehlungen, Warnungen und Informationen des BSI zugreifen und sich umfassend zu den für sie relevanten Themen der Cyber-Sicherheit informieren können. Die Plattform dient zudem als Kommunikationsschnittstelle zu den Verbraucherinnen und Verbrauchern. Es soll darauf geachtet werden, dass auch bereits vorhandene Strukturen und Plattformen zur Verbraucherinformation genutzt beziehungsweise mit einbezogen werden.

– Aufnahme eines kontinuierlichen Verbraucherschutzdialogs zwischen BSI, Herstellern und Diensteanbietern, um einen frühzeitigen und steten Austausch zur Realisierung eines höchstmöglichen Schutzniveaus der IT-Sicherheit bei Verbraucherprodukten zu erreichen. Hierzu nutzt das BSI seine Erfahrungen aus der Marktbeobachtung, den Sicherheitstests und -analysen sowie dem Dialog mit den Übrigen im Verbraucherschutz tätigen Akteuren.

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

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

ENTWURF

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

Zu Buchstabe e

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

Zu Buchstabe f

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

Zu Buchstabe g

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

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

Zu Nummer 3

Zu § 4a (Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte)

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

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

ENTWURF

Sofern sich die Kommunikationstechnik des Bundes nicht in Stellen des Bundes befindet, kann das Bundesamt die Befugnisse nur im Einvernehmen mit den Dritten ausüben.

Das Bundesamt wird neben der jeweils überprüften Stelle und der eigenen Fachaufsicht das Ergebnis auch der jeweiligen Rechts- und Fachaufsicht der geprüften Stelle entsprechend dem Ressortprinzip mitteilen. Sofern das Bundesamt Vorschläge zur Verbesserung der Informationssicherheit unterbreiten kann, soll es diese mit der Mitteilung des Ergebnisses verbinden.

Die Vorschrift ermöglicht die Verarbeitung von Daten, die für die Bewertung der Netz- und Informationssicherheit von Bedeutung sein können. Nicht Gegenstand der Befugnis ist die Verarbeitung von Inhaltsdaten. Die Vorschriften zur Verarbeitung besonderer Daten, insbesondere von Sozialdaten, Daten, die dem Steuergeheimnis unterliegen und personenbezogene Daten, bleiben von § 4a unberührt.

Die Vorgaben für die Verwaltung der Ergebnisse der Kontrolle, insbesondere zur Dauer der Aufbewahrung und Vernichtung, ergeben sich aus den jeweils anwendbaren Vorschriften (Registraturrichtlinie).

Um den besonderen Anforderungen an die im Ausland belegene Informations- und Kommunikationstechnik des Auswärtigen Amtes Rechnung zu tragen, sind dafür gemäß Absatz 5 die Befugnisse nach Absatz 1 bis 3 ausgenommen.

Ausgenommen gemäß Absatz 6 ist auch die Informations- und Kommunikationstechnik der Streitkräfte im Geschäftsbereich des Bundesministeriums der Verteidigung. Um ihren verfassungsmäßigen Auftrag zur Landes- und Bündnisverteidigung zu erfüllen, müssen die Streitkräfte in Krisensituationen einsatzbereit sein. Das Verteidigungsressort muss seinen verfassungsmäßigen Auftrag auch dann sicherstellen können, wenn zivile Einrichtungen, wie zum Beispiel das Bundesamt, durch die Sicherheitslage beeinträchtigt sind. Vor diesem Hintergrund müssen die erforderlichen Informations- und Kommunikationssysteme, die im Geschäftsbereich des Bundesministeriums der Verteidigung für die Streitkräfte und ihre Zwecke betrieben werden, mit eigenen Kräften kontrolliert und überprüft werden können und das Verteidigungsressort muss über entsprechende eigene Kompetenzen und Zuständigkeiten für die Informations- und Kommunikationssysteme der Streitkräfte verfügen. Um die Einsatzbereitschaft in Krisensituationen sicherzustellen und die Kontrolle der hierfür erforderlichen Informations- und Kommunikationssysteme, insbesondere auch Waffensysteme, sicherzustellen, wird zwischen dem Bundesministerium des Innern, für Bau und Heimat und dem Bundesministerium der Verteidigung eine entsprechende Verwaltungsvereinbarung geschlossen. Nicht ausgenommen von den Befugnissen des Bundesamtes ist dabei die nichtmilitärische Informations- und Kommunikationstechnik der Bundeswehrverwaltung (Art. 87b Grundgesetz), der IT-Dienstleister der Bundeswehr und die nichtmilitärische Informations- und Kommunikationstechnik der Streitkräfte (etwa Führungsakademie der Bundeswehr).

Zu § 4b (Allgemeine Meldestelle für die Sicherheit in der Informationstechnik)

Die Vorschrift ergänzt die Regelungen des § 4 BSIG (Zentrale Meldestelle für die Sicherheit in der Informationstechnik des Bundes) und des § 8b BSIG (Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen). Im Rahmen seiner Aufgabe als zentrale Meldestelle für Informationstechnik soll das BSI auch als allgemeine Meldestelle umfassend Informationen zu Sicherheitslücken, Schadprogrammen und IT-Sicherheitsvorfällen zentral sammeln und auswerten können. 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.

ENTWURF

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

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

§ 4b Absatz 3 eröffnet die Möglichkeit, dass das Bundesamt andere Bundesbehörden, Dritte und die Öffentlichkeit über mögliche Gefahren der Cyber- und Informationssicherheit informieren kann, beispielsweise zu Zwecken der Schadensverhinderung oder -verringerung.

§ 4b Absatz 2 führt Schutzrechte der Meldenden ein. Nach Absatz 5 bleiben jedoch bestehende gesetzliche Meldepflichten, Regelungen zum Geheimschutz, Übermittlungshindernisse und Übermittlungsregelungen, die auch den Aufgaben anderer Behörden dienen, hiervon unberührt. Für eine Übermittlung personenbezogener Daten nach § 5 Absatz 5 und Absatz 6 Satz 1 BSIG trifft Absatz 2 Satz 6 eine Regelung, nach der eine Abwägung unter Berücksichtigung der schutzwürdigen Interessen des Meldenden zu erfolgen hat.

Zu Nummer 4

Auf Grund von Erfahrungen mit verschiedenen Angriffen in der Vergangenheit ist zum Schutz der Regierungsnetze eine Anpassung des § 5 BSIG erforderlich. Das Bundesamt nimmt dabei weiterhin sonderordnungsbehördliche Funktionen beim Schutz von Kommunikationstechnik des Bundes wahr und nicht Aufgaben der allgemeinen Gefahrenabwehr. Die Zuständigkeit für die allgemeine Gefahrenabwehr, welche grundsätzlich im Rahmen der den Gefahrenabwehrbehörden gesetzlich zugewiesenen Aufgaben auch die Abwehr von Angriffen aus dem Cyberraum umfassen kann, liegt weiterhin bei den zuständigen Polizeibehörden.

Zu Buchstabe a

Mit der Änderung wird die Möglichkeit zur Speicherung pseudonymisierter Protokolldaten im Sinne des § 2 Absatz 8 BSIG von drei auf maximal 12 Monate erhöht. Wie Cyber-Vorfälle in der Vergangenheit innerhalb der Bundesverwaltung zeigen, erstrecken sich insbesondere spezialisierte Cyberangriffe, so genannte Advanced Persistent Threats (APTs), über einen mehrjährigen Zeitraum. Persistenz bezeichnet dabei das Bemühen der Angreifer, sich nachhaltig und unbemerkt in der Kommunikationstechnik des Bundes einzunisten. Eine wesentliche Eigenschaft eines APT-Angriffs ist dessen unterschwellige Vorgehensweise, durch die er lange unerkannt im System bleiben kann. Kennzeichnend ist, dass Angreifer vorsichtig und verdeckt vorgehen, so dass zwischen der initialen Infektion der Kommunikationstechnik des Bundes und der Aufdeckung des Angriffs in der Regel große Zeiträume

ENTWURF

liegen. Um durch APT hervorgerufene Kompromittierungen erkennen und entfernen zu können, muss die Speicherdauer der Protokolldaten den Zeitraum des APT-Angriffs einschließen. Nur wenn das Vorgehen des Angreifers – auch im Nachhinein – aufgeklärt werden kann, kann die Kommunikationstechnik des Bundes vor gleichartigen zukünftigen Bedrohungen geschützt werden. Die Zeitspanne zwischen Infektion und Entdeckung eines APT-Angriffs beträgt Monate, fortlaufende APTs bleiben in der Praxis zum Teil über Jahre unentdeckt. Um bei einem Vorfall die durch den APT hervorgerufenen Kompromittierungen zeitnah und besser erkennen und entfernen zu können, sollte daher die Speicherdauer der Protokolldaten den Zeitraum der gesamten Wirkdauer eines APTs möglichst einschließen. Eine Speicherdauer von 12 Monaten verbessert die Möglichkeit der Reaktion auf Angriffe wesentlich und gewährleistet zugleich einen angemessenen Schutz von personenbezogenen Daten.

Satz 2 stellt eine Einschränkung des Zugriffs auf die Daten dar, um diesen Zugriff auf das fachlich gebotene Maß zu beschränken. Ein Zugriff auf Daten, die älter als 3 Monate sind, ist nur dann zulässig, wenn tatsächliche Anhaltspunkte für einen Angriff vorliegen. Hierfür sind sowohl technische als auch organisatorische Vorkehrungen zu treffen.

Zu Buchstabe b

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

Bei der Verarbeitung von Protokolldaten ist eine regelmäßige automatisierte Qualitätssicherung der verarbeiteten Daten im Klartext erforderlich, um semantische und grammatikalische Fehler in den Daten aufzudecken, bevor diese das Gesamtsystem in seiner fehlerfreien Funktion stören. Eine Fehlfunktion des Prüfsystems kann i.d.R. nur so aufgedeckt werden. Eine effektive Qualitätssicherung der Protokolldaten kann nur erfolgen, wenn hierbei einzelne Datensätze auch nicht pseudonymisiert manuell ausgewertet werden könnten. Eine regelmäßige Qualitätssicherung wurde durch die bisherigen Regelungen des § 5 BSIG nicht ermöglicht.

Zu Nummer 5

§ 5a regelt die Verarbeitung von Protokollierungsdaten durch das Bundesamt. Die Bedeutung und Funktion der Protokollierungsdaten findet sich in der Begründung zu § 2 Absatz 8a.

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

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

ENTWURF

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

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.

Satz 3 stellt klar, dass die Bundesbehörden auch berechtigt sind, dem Bundesamt die Protokollierungsdaten für die Erkennung und Abwehr von Gefahren für die Kommunikationstechnik zu übermitteln.

Mit dem Verweis auf die Absätze 1 Satz 5, 2 und 4 von § 5 BSIG wird klargestellt, dass für die Verarbeitung der Protokollierungsdaten dieselben Beschränkungen gelten.

Der Datenschutz wird nach Maßgabe der strengen Voraussetzungen des § 5 BSIG, auf den § 5a BSIG verweist, gewährleistet. Nach § 5 Absatz 8 BSIG hat das Bundesamt vor Erhebung der Datenerhebung und -verwendung ein Konzept zu erstellen und für Kontrollen durch den Bundesbeauftragten für den Datenschutz und Informationsfreiheit bereitzuhalten. Auch die für die automatisierte Auswertung verwendeten Kriterien sind zu dokumentieren. Weitere Anforderungen an die Informationssicherheit folgen aus dem auf § 8 Absatz 1 Satz 1 BSIG beruhenden Mindeststandard zur Protokollierung und Detektion von Cyber-Angriffen.

Der Verweis in Satz 5 auf die Ausnahme in § 4a Absatz 6 stellt klar, dass die für die Streitkräfte und ihre Zwecke betriebene Informations- und Kommunikationstechnik im Geschäftsbereich des Bundesministeriums der Verteidigung keine Mitwirkungs- und Unterstützungspflicht besteht. Eine Verpflichtung zur Übermittlung von Daten besteht daher nicht. Gegenüber den die Informations- und Kommunikationstechnik der Streitkräfte betreibenden Stellen kommt dem BSI damit keine Anordnungsbefugnis zu. Davon unbenommen bleibt die Möglichkeit zur Mitwirkung und Unterstützung des Bundesministeriums der Verteidigung und seines Geschäftsbereichs auf Ersuchen hinsichtlich der Erkennung, Eingrenzung oder Beseitigung von Störungen oder Fehlern.

Zu Nummer 6

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

Zu Nummer 7

Zu § 5c (Bestandsdatenauskunft)

§ 5c regelt die Möglichkeit des Bundesamtes zur Bestandsdatenauskunft. Die Möglichkeit des Bundesamtes, diese Auskunft zu verlangen, ist erforderlich, um Opfer vor Cyber-Angriffen, die erhebliche Schäden zur Folge haben können, zu warnen und bei der Angriffsabwehr zu unterstützen. Mit der Bestandsdatenauskunft soll das Bundesamt IP-Adressen einer (juristischen) Person zuordnen können. Insbesondere soll das Bundesamt anhand der Bestandsdatenauskunft mittels einer IP-Adresse Betreiber Kritischer Infrastrukturen, Unternehmen im besonderen öffentlichen Interesse und Anbieter digitaler Dienste über Cyber-Angriffe informieren können. Die Bestandsdatenauskunft dient damit der Information und somit letztlich dem Schutz der Betroffenen.

ENTWURF

Zu Absatz 1

Das Bundesamt kann unter den Voraussetzungen des Absatzes 1 von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, Bestandsdaten im Sinne von §§ 95 und 11 des Telekommunikationsgesetzes verlangen.

Satz 2 stellt hohe Anforderungen an das Auskunftsverlangen. Auskunft darf im Einzelfall nur verlangt werden, um Angriffe auf informationstechnische Systeme herausragender Infrastrukturen, Dienste und Unternehmen, die aufgrund ihrer gesellschaftlichen Bedeutung besonders schutzwürdig sind, zu verhindern oder sonstige erhebliche Schäden vom betroffenen Dritten abzuwenden. Die Befugnis setzt voraus, dass das Bundesamt Kenntnis von ziel- oder zweckgerichteten Beeinträchtigungen im Rahmen seiner Aufgaben zur Abwehr von Gefahren für die Sicherheit in der Informationstechnik des Bundes, die Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen sowie die Beratung und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik erlangt hat.

Satz 3 stellt klar, dass die Auskunft für die Kontaktaufnahme mit dem Betroffenen erforderlich sein muss.

Zu Absatz 2

Absatz 2 lässt den Abruf von Bestandsdaten nach dem Telekommunikationsgesetz anhand einer IP-Adresse zu. Die Auskunft kann nur nach Maßgabe des Absatzes 1 Satz 3 erfolgen. Die Bestandsdatenauskunft anhand einer IP-Adresse kann daher nur zum Zweck der Kontaktaufnahme und der Information des Betroffenen erfolgen. Nicht umfasst von der Befugnis sind Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt sind (Daten im Sinne des § 113 Absatz 1 Satz 2 TKG).

Absatz 3 Satz 2 regelt eine Dokumentationspflicht, wodurch eine aufsichtliche Kontrolle durch die Datenschutzbeauftragten ermöglicht sowie die verwaltungsgerichtliche Kontrolle erleichtert werden.

Zu Absatz 3

Aufgrund der in der Regel gegebenen Eilbedürftigkeit sind die zur Auskunftserteilung erforderlichen Daten unverzüglich zu übermitteln.

Zu Absatz 4

Aus Absatz 4 ergibt sich, dass die Bestandsdatenauskunft der Information und somit letztlich dem Schutz der Betroffenen dient. Absatz 4 regelt, dass das Bundesamt nach erfolgter Auskunft den Betroffenen nicht nur auf festgestellte Beeinträchtigungen hinweist, sondern nach Möglichkeit auch auf Abhilfemöglichkeiten hinweist. Insgesamt ist die Eingriffstiefe einer Bestandsdatenauskunft nach § 5c aufgrund des präventiven Zwecks und der Betroffenheit von Unternehmen bzw. juristischen Personen geringer als im Kontext der Bestandsdatenauskunft durch Sicherheitsbehörden.

Zu Absatz 5

Aus Absatz 5 ergibt sich, dass personenbezogene Daten nur unter den strengen Voraussetzungen des § 5 Absatz 5 und 6 an andere Stellen übermittelt werden dürfen.

Zu Absatz 6

Absatz 6 regelt die Benachrichtigung des Betroffenen über die Bestandsdatenauskunft anhand einer IP-Adresse. Für die Benachrichtigung des Betroffenen über die Weitergabe nach

ENTWURF

§ 5 Absatz 5 BSIG trifft Absatz 6 Satz 2 eine besondere Regelung. Diese schließt die Benachrichtigung durch die in § 5 Absatz 5 BSIG genannten Stellen nicht aus.

Zu Absatz 7

Durch die jährliche Berichtspflicht in Absatz 7 wird eine transparente Umsetzung der Regelung sichergestellt. Die gemäß Absatz 7 Nummer 1 und 2 notwendigen Angaben werden in den jährlichen Bericht nach § 5 Absatz 9 BSIG des Bundesamtes an die Beauftragte oder den Beauftragten für den Datenschutz und die Informationsfreiheit (BfDI) aufgenommen.

Zu Nummer 8

Zu Buchstabe a

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

Zu Buchstabe b

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

Zu Buchstabe c

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

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

Zudem wurde der Absatz 2 Satz 1 neu gefasst, um die Voraussetzungen für Warnungen nach § 7 Absatz 2 klarzustellen.

ENTWURF

Zu Nummer 9

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

Zu Absatz 1

Das BSI kann zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14, 14a, 17 und 18 Produkte und Systeme untersuchen. Dies ist insbesondere für die umfassende Auswertung von Informationen über bestehende Sicherheitsrisiken von Bedeutung.

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

Zu Absatz 2

§ 7a Absatz 2 ermöglicht dem Bundesamt, für Untersuchungen nach § 7a 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 IT-Produkten und IT-Systemen zu gewährleisten. Daher ist die Befugnis Auskünfte zu verlangen, ein notwendiger Schritt in Richtung von mehr Sicherheit in der Informationstechnik.

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

Im Rahmen der zunehmenden Digitalisierung haben die Sicherheit und die Vertrauenswürdigkeit von IT-Systemen, von Hard- und Software eine für den Einzelnen ebenso große Bedeutung. Es muss sichergestellt sein, dass IT-Produkte nur die herstellerseitig zugesagten Funktionalitäten haben und der Hersteller eingebaute Wartungskanäle, Backdoors etc. offenlegt und unbekannte - sogar dem Hersteller unbekannte - Sicherheitslücken nicht zu einer Gefahr für die IT-Sicherheit werden.

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

Zu Absatz 3

§ 7a Absatz 3 (§ 7a Absatz 2 BSIG alt) enthält eine Zweckbindung für die aus der Untersuchung nach § 7a 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

ENTWURF

die Wahrnehmung der Öffentlichkeit in Fragen der sicheren Informationstechnik und ermöglichen ein hohes Maß an Transparenz. Des Weiteren hat der Staat auch eine Schutzpflicht gegenüber den Bürgerinnen und Bürgern, indem er diese vor jeglichen Gefahren warnen und schützen muss. Sofern es zu einer Veröffentlichung von Informationen kommen sollte, die Geschäfts- oder Betriebsgeheimnisse beinhalten, ist sicherzustellen, dass diese vertraulichen Informationen unkenntlich gemacht werden. Das BSI kann sich dafür auch der Hilfe des entsprechenden Herstellers bedienen.

Zu Absatz 4

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

Zu Absatz 5

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

Zu Nummer 10

Zu § 7b (Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden)

Zu Absatz 1

Mit § 7b Absatz 1 wird die Befugnis zur Durchführung von sogenannten Portscans geschaffen, um das Bestehen von Sicherheitslücken und andere Sicherheitsrisiken in der Informationstechnik des Bundes und in der Informationstechnik Kritischer Infrastrukturen, digitaler Dienste und der Unternehmen im besonderen öffentlichen Interesse zu prüfen.

Kommunizieren informationstechnische Systeme über das Internet, so nutzen diese regelmäßig das TCP/IP-Protokoll. Dieses Protokoll sieht als Teil der Adressierung eine Portnummer vor. Wird ein informationstechnisches System über das Internet angesprochen, so wird neben der IP-Adresse eine Portnummer übermittelt, die spezifisch für den angefragten Dienst ist. Systemseitig verbirgt sich hinter jedem Port eine Applikation, die die Portkommunikation durchführt. Ein bekanntes Beispiel ist der Port 80 als Standard für einen Webserver. Typischerweise sendet der Browser eine Anfrage (Request) an den gewünschten Webserver, der durch seine URL bzw. IP-Adresse und Portnummer (z. B. 123.123.123:80) gekennzeichnet ist. Das angesprochene System antwortet in der Regel mit der dort hinterlegten Startseite im html- oder xml-Format, die auf dem aufrufenden System dann angezeigt wird.

Grundsätzlich können beliebige Applikationen mit einem Port verknüpft werden. Sender und Empfänger müssen dann allerdings das applikationsspezifische Protokoll bedienen können. Typischerweise gibt es daneben eine Reihe von Standarddiensten auf festgelegten Portnummern (ftp, telnet, smtp, rsh, ssh usw.).

Hat eine mit einem Port verknüpfte Applikation eine Sicherheitslücke, so funktioniert die Kommunikation zwischen Sender und Empfänger nicht wie vorgesehen. Fehlt z. B. bei einem Remote Shell-Dienst das Passwort, können sich Unbefugte über das Internet an dem

ENTWURF

betroffenen System ohne Zugangsbeschränkung anmelden. Dies kann erhebliche Gefahren für das informationstechnische System und ggf. die davon abhängigen Prozesssteuerungen bergen.

Sicherheitslücken im Bereich der Portkommunikation durch Software- und Konfigurationsfehler sind häufig. Eine besondere Gefahr geht von diesen Lücken insbesondere dann aus, wenn diese in Industriesteueranlagen (SCADA), informationstechnischen Systemen von KRITIS-Unternehmen oder IoT-Geräten (Internet der Dinge) auftreten und nicht unverzüglich geschlossen werden. Derartige Lücken werden regelmäßig auf allgemein zugänglichen Plattformen im Internet veröffentlicht und sind somit im Sinne des Absatzes 2 öffentlich bekannt. Da die Zahl der Sicherheitslücken insgesamt steigt und damit auch die Zahl der veröffentlichten Sicherheitslücken, besteht ein dringender Handlungsbedarf zur Prüfung, ob die IT-Systeme der in Absatz 1 Ziffern 1 und 2 genannten Einrichtungen diese Sicherheitslücken aufweisen.

Bei einem Portscan werden IP-Adressen und Ports aufgezählt und eine Anfrage an die so gebildete Adresse gesendet. Der Raum aller IP-Adressen ist unterteilt. So sind den Staaten regelmäßig IP-Adresskontingente zugeteilt. Innerhalb von Staaten teilen sich diese dann weiter auf Organisationen auf. Insbesondere haben die in Deutschland tätigen Internet-Zugangsanbieter eigene IP-Adresskontingente, die sie ihren in der Regel privaten Kunden dynamisch zuteilen. Demgegenüber stehen statische IP-Adressen, die in der Regel den in Absatz 1 Ziffern 1 und 2 in Bezug genommenen IT-Systemen zugewiesen sind.

Das Bundesamt ist bei Portscans schon allein aus technischen Gründen regelmäßig auf statische IP-Adressen beschränkt. Private Endnutzer, denen in der Regel dynamische IP-Adressen zugewiesen werden, werden daher grundsätzlich nicht von Portscans erfass. Aufgrund der hohen Dynamik bei der Zuordnung von IP-Adressen und dem stetigen technischen Wandel der IT-Landschaft, ist dabei allerdings nicht auszuschließen, dass ausnahmsweise in Einzelfällen auch Ports privater Anwender detektiert werden.

Die Portscans dienen der Suche nach öffentlich bekannten Sicherheitslücken und -risiken in Kommunikationsnetzen als auch informationstechnischen Systemen, die vollständig ohne Schutzmechanismen arbeiten. Daneben werden von der Definition auch die Kommunikationsnetze und informationstechnische Systeme erfasst, die zwar Schutzmechanismen verwenden, die aber faktisch wirkungslos sind. Dies ist der Fall, wenn das Netz oder System bzw. der jeweils zum Schutz verwendete Mechanismus eine bereits bekannte Sicherheitslücke besitzt. Es ist auch der Fall in Kommunikationsnetzen und informationstechnischen Systemen, deren Schutzmechanismen wirkungslos sind. Dies wäre zum Beispiel dann der Fall, wenn für ein System herstellerseitig stets ein identisches Passwort („0000“ oder „admin“) vergeben würde.

Technisch sendet das Bundesamt zum Zweck der Detektion öffentlich bekannter Sicherheitslücken ein oder mehrere Anfragen an einen oder mehrere Ports der Betreiber eines informationstechnischen Systems und wertet die von dem System gelieferte Antwort aus. Absatz 1 Satz 2 stellt klar, dass das Bundesamt keine tiefergehenden Untersuchungen oder Eingriffe in den fremden Systemen vornehmen darf. Zulässig ist alleine das Testen, ob die Systeme tatsächlich ungeschützt sind, um die Betroffenen dann informieren zu können. Eine darüberhinausgehende Ausforschung der fremden informationstechnischen Systeme ist unzulässig.

Das bedeutet, dass das Bundesamt nicht in das System eindringt, sondern nur die von dem System gewissermaßen an jedermann gelieferte Antwort nutzt. Somit erfolgt weder ein Eingriff in die Integrität des informationstechnischen Systems noch werden aktiv die auf dem System gespeicherten Informationen erhoben. Es handelt sich vielmehr um eine vom jeweiligen System im Grundzustand vorgesehene nach außen angebotene Kommunikation für jedermann. Auch Straftäter suchen diese Sicherheitslücken, um sie auszunutzen. Mit der Norm wird dem Bundesamt die Möglichkeit gegeben, Sicherheitslücken zu identifizieren

ENTWURF

und die Betroffenen über den Fund zu informieren, damit die Betroffenen die Sicherheitslücke schließen können, bevor sie durch Straftäter ausgenutzt werden können.

Durch die Beschränkung der vom Bundesamt angesteuerten IP-Adressen auf statische IP-Adressen des deutschen Adressraums wird sichergestellt, dass sich die gescannten Systeme regelmäßig in Deutschland befinden. Da privaten Endnutzern in der Regel dynamische IP-Adressen zugewiesen sind, werden diese daher nicht erfasst. Je nach Typ der Sicherheitslücke (des Systemfehlers) kann das gescannte informationstechnische System gegebenenfalls auch ungewollt gespeicherte Daten zurückliefern. Diese sind, wenn sie nicht an Strafverfolgungsbehörden gemäß § 5 Absatz 5 und 6 BSIG weitergegeben werden müssen, unverzüglich zu löschen. Absatz 1 Satz 3 verweist daher auf einen möglichen Eingriff in den Schutzbereich des Artikel 10 des Grundgesetzes. Da zu den kritischen Infrastrukturen auch Telekommunikationsnetze gehören, ist – wie bereits dargestellt – der Fall vorstellbar, dass Daten aus informationstechnischen Systemen von Telekommunikationsnetzen bei einem Portscan zurückgeliefert werden, die ohne die bestehende Fehlersituation nicht zurückgeliefert worden wären. Da es sich um einen Fehler im informationstechnischen System handelt, ist nicht vorhersehbar, ob in den zurückgelieferten Daten auch solche sind, die vom Schutzbereich des Artikels 10 des Grundgesetzes erfasst sind. Dies kann zum Beispiel der Fall sein, wenn ein IT-System von Telekommunikationsdiensteanbietern, die zu den kritischen Infrastrukturen gehören, eine Sicherheitslücke der gesuchten Art aufweisen. Die durch das Fehlverhalten eines Systems ungewollt zurückgelieferten Daten sind abhängig vom Systemtyp und den damit verarbeiteten Daten. Beispielsweise könnte ein fehlerhafter Router nach Anfrage IP-Adressen zurückliefern. Daher wird § 7b Absatz 1 in § 11 angeführt und die Übermittlung solcher Daten an andere Stellen ist nur unter den Voraussetzungen von § 5 Absatz 5 und 6 für die Strafverfolgung zulässig. Dies kann z. B. der Fall sein, wenn sich aus den Daten Hinweise ergeben, dass die Sicherheitslücke bereits zur Begehung von Straftaten genutzt wird, so dass die zuständigen Strafverfolgungsbehörden informiert werden müssen. Ansonsten sind solche Daten unverzüglich zu löschen.

Zu Absatz 2

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

Dies ist der Fall, wenn das Netz oder System bzw. der jeweils zum Schutz verwendete Mechanismus eine bereits bekannte Sicherheitslücke besitzt. Es ist auch der Fall in Kommunikationsnetzen und informationstechnischen Systemen, deren Schutzmechanismen wirkungslos sind. Dies wäre zum Beispiel dann der Fall, wenn für ein System herstellerseitig stets ein identisches Passwort („0000“ oder „admin“) vergeben würde.

Zu Absatz 3

§ 7b Absatz 3 regelt die Informationspflichten des Bundesamtes. Ist ein Sicherheitsproblem identifiziert worden, so sollen in erster Linie die Betriebsverantwortlichen informiert werden. Die Provider sollen zum einen hilfsweise in Anspruch genommen werden, wenn ein Sicherheitsproblem bei einer Vielzahl von Betroffenen detektiert wurde. Die hilfsweise Inanspruchnahme der Provider kommt zum anderen vor allem dann in Betracht, wenn dem Bundesamt die Verantwortlichen oder betreibenden Dienstleister unbekannt sind, wie dies bei privaten Endnutzern der Fall wäre, denen derzeit eine dynamische IP-Adresse zugewiesen wird. Bei den Betreibern kritischer Infrastrukturen ist dem BSI entweder aus der vorherigen Erfüllung seiner Aufgaben oder aus öffentlich zugänglichen Registern (z.B. der Internetdienst „Whois“) bekannt, wem eine bestimmte statische IP-Adresse dauerhaft zugewiesen ist. In

ENTWURF

diesen Fällen kann das BSI auch direkt an den Betreiber des informationstechnischen Systems herantreten, damit dieser möglichst schnell die Sicherheitslücke schließen kann. Anbieter von Telekommunikationsdiensten können Nutzer nach § 109a TKG benachrichtigen.

Zu Absatz 4

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

Der Analyse von Schadsoftware mittels Honeypots kommt durch die Verbreitung von Internet of Things-Geräten (IoT-Geräte) eine zunehmende Bedeutung zu, insbesondere, weil diese Geräte ihre eigentliche Funktion beibehalten und dennoch von Schadsoftware infiziert sein können. Für die Nutzenden gestaltet es sich somit häufig schwierig, infizierte IoT-Geräte zu erkennen. Durch die Analyse des Bundesamtes der beim Honeypot genutzten Angriffsmuster kann das erforderliche Wissen generiert und den Nutzenden über allgemein zugängliche Informationsquellen zum Schutz und zur Bereinigung ihrer informationstechnischen Systeme zur Verfügung gestellt werden.

Zu § 7c (Anordnungen des Bundesamtes gegenüber Diensteanbietern)

Die Gesetzgebungskompetenz des Bundes für die Anordnungsbefugnisse des neuen § 7c folgt aus Artikel 74 Absatz 1 Nummer 11 des Grundgesetzes (GG) – Recht der Wirtschaft, einschließlich gefahrenabwehrrechtlicher Annexkompetenz – in Verbindung mit Artikel 72 Absatz 2 GG. Die gefahrenabwehrrechtliche Annexkompetenz ergibt sich aus der Notwendigkeit eines bundeseinheitlichen Niveaus von Cyber-Sicherheit der Diensteanbieter nach § 109a Absatz 5 und 6 des Telekommunikationsgesetzes (TKG) durch das Bundesamt zum Schutz der in Absatz 1 Satz 1 aufgeführten gefährdeten Bereiche. Das Ergreifen von Maßnahmen nach § 109a Absatz 5 und 6 TKG steht im Ermessen der Diensteanbieter. Zur Abwehr besonderer Gefahrenlagen bedarf es zusätzlich der Regelung der Anordnungsbefugnis für das Bundesamt, da zur Aufrechterhaltung betriebsfähiger, sicherer IT-Strukturen und -anwendungen eine bundesweit einheitliche Gefahrenabwehr erforderlich ist. Die Anordnungsbefugnis dient der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung im Bereich des Rechts der Wirtschaft aus Artikel 74 Absatz 1 Nummer 11 GG als einer dem Bund zugewiesenen Sachmaterie und ist für eine wirksame Gefahrenabwehr hinsichtlich der in der Zuständigkeit des Bundes liegenden Bestimmungen aus § 109a Absätze 5 und 6 TKG erforderlich. Im Interesse der Gewährleistung einer bundesweit einheitlichen IT-Sicherheit darf es in den in § 7c geregelten Fällen nicht mehr allein im Ermessen des Anbieters liegen, ob er die genannten Maßnahmen ergreift, sondern das Bundesamt muss die Möglichkeit haben, diese im Gefahrenabwehrfalle bundesweit einheitlich vorzugeben. Es wird auf die Ausführungen zur koordinierenden Stellung des Bundesamtes in der Begründung zu § 7d verwiesen. Eine solche koordinierende Rolle wird auch für Cyber-Gefahren benötigt, die sich über Telekommunikationsdienste realisieren. Gerade bei DDoS-Attacken werden Telekommunikationsdienste verschiedener Anbieter genutzt. Eine erfolgreiche Abwehr derartiger Angriffe bedingt ein zeitnahes konzertiertes Vorgehen aller betroffenen Diensteanbieter, was nur durch Anordnung durch eine zentrale Stelle gewährleistet werden kann.

Die neugeschaffene Norm hat die Abwehr solcher Gefahren zum Gegenstand, die derart weit verbreitet sind, dass eine Einzelabwehr nicht zielführend ist. In solchen Fällen muss für eine effektive Gefahrenabwehr bereits bei den Telekommunikationsdiensten angesetzt

E-NTWURF

werden. Ein konkreter Fall dieses Gefahrenszenarios sind Botnetze. Eine konkrete erhebliche Gefahr, die sich beispielsweise aus dem Betrieb eines Botnetzes ergibt, muss im jeweiligen Einzelfall bewertet und abgewogen werden. Dabei bemisst sich die Erheblichkeit beispielsweise an der Bedeutung des angegriffenen Ziels, der durch den Angriff eintretenden Gefahr für die öffentliche Sicherheit und Ordnung oder der Beeinträchtigung eines anderen Rechtsgutes von erheblicher Bedeutung.

Botnetze entstehen durch die zumeist durch den Nutzer unbemerkte Installation einer Schadsoftware (häufig auch unter Ausnutzung einer Schwachstelle) auf dem Datenverarbeitungssystem des Nutzers. Durch diese Schadsoftware hat der Täter einen nahezu vollständigen Zugriff auf die kompromittierten Systeme. Die zahlreichen kompromittierten Systeme (sog. Bots) werden ohne Wissen der Nutzer mittels sog. „Command-and-Control-Server“ (sog. C&C-Server) durch den Täter kontrolliert und gesteuert. Dieses Netz aus C&C-Server und Bots nennt man Botnetz. Der Täter ist regelmäßig auch in der Lage, Daten der Nutzer von den Bots auszuleiten und das Botnetz für DDoS-Angriffe einzusetzen. Bei Distributed Denial of Service (DDoS)-Angriffen wird durch gezielt herbeigeführte Überlastung versucht, die Verfügbarkeit eines Internetdienstes oder eines Zielsystems zu stören. Laut Bundeslagebild Cybercrime 2019 des Bundeskriminalamts vom 30. September 2020 hat sich die Angriffsbandbreite für DDoS-Angriffe im Vergleich zum Vorjahr in etwa verdoppelt.

Botnetze betreffen die Integrität der kompromittierten Systeme, die dadurch in einen Bot verwandelt werden. Sie betreffen ferner die Vertraulichkeit, da in aller Regel Nutzerdaten ausgeleitet werden. Außerdem betreffen Sie die Verfügbarkeit diejenigen Systeme und Internetdienste, gegen die sie zum Zweck von DDoS-Angriffen kollektiv genutzt werden.

Zu Absatz 1

Zu Satz 1

Während Absatz 2 Nummer 1 bis 3 die Schutzziele nennt, ergeben sich aus Absatz 1 Satz 1 Nummer 1 und 2 die dann dem Bundesamt zur Verfügung stehenden Gefahrenabwehrmaßnahmen.

Die Anordnungsbefugnis beschränkt sich auf solche Diensteanbieter, die mehr als 100.000 Kunden haben, da sie regelmäßig bereits technische und organisatorische Vorkehrungen getroffen haben, um die Verpflichtungen aus § 109a Absatz 5 und 6 TKG zu erfüllen und im Falle der Bereinigung von informationstechnischen Systemen eine große Anzahl von Nutzern erreichen. Die gewählte Kundenanzahl orientiert sich an § 113 Absatz 5 Satz 2 TKG. Die Diensteanbieter können zudem nur verpflichtet werden, wenn sie dazu technisch in der Lage sind und es ihnen wirtschaftlich zumutbar ist.

Zu Nummer 1

Absatz 1 Satz 1 Nummer 1 betrifft die Anordnung des Treffens von Maßnahmen, wie sie in § 109a Absatz 5 und 6 bezeichnet sind. Für Diensteanbieter bestehen nach § 109a Absatz 5 oder 6 TKG Möglichkeiten, um bestimmte Schutzmaßnahmen zum Schutz der Netz- und Informationssicherheit zu ergreifen. Die Maßnahmen einzelner Diensteanbieter sind jedoch in besonderen Gefahrenlagen nicht ausreichend. Vielmehr bedarf es zur Aufrechterhaltung betriebsfähiger, sicherer IT-Strukturen und -anwendungen in diesen Fällen bundesweit einheitlicher Maßnahmen. Das Bundesamt hat derzeit keine Befugnis, gegenüber den Diensteanbietern anzuordnen, dass sie die in § 109a Absatz 5 oder 6 TKG genannten Maßnahmen treffen. Damit fehlt dem Bundesamt die Ermächtigung, insbesondere bei den folgenden Problemen effektiv zu reagieren und schnell Schutzmaßnahmen einzuleiten:

Sind IP-Adresse oder Domänennamen von Internet-Systemen bekannt, die von Kriminellen zur Steuerung infizierter Nutzersysteme (z. B. Bots) genutzt werden, beispielsweise von C&C-Server, kann nach derzeitiger Rechtslage gegenüber Diensteanbietern nicht angeordnet werden, den Datenverkehr zu diesen Systemen zu sperren oder umzuleiten. Eine

ENTWURF

schnelle Entscheidung über eine solche Sperrung oder Umleitung kann insbesondere wichtig sein, um bei Botnetzinfektionen Nutzer zu schützen, damit deren Rechner nicht ferngesteuert werden oder einen flächendeckenden Angriff auf wichtige Infrastrukturen (z.B. Geldautomaten) abzuwehren. Für das Bundesamt besteht derzeit nur die Möglichkeit, die Diensteanbieter über das Computer-Emergency-Response-Team des Bundes zu bitten, erkannte C&C-Server abzuschalten, über den Domain Name Service die entsprechenden Domänen zu blockieren oder auf Sinkholes umzuleiten, was in der Regel die Rechtshilfe des zuständigen Staates, in dem der Domänenname registriert ist, erfordert. Dies ist sehr zeitaufwändig und nicht mit allen Staaten möglich.

Eine effektivere Reaktion ist es, gegenüber den deutschen Diensteanbietern anzuordnen, die Malwaredomänen bei den eigenen DNS-Resolvern/DNS-Nameservern zu sperren oder auf Sinkholes umzuleiten, also keine Auflösung des DNS-Namens 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 Bundesamt vorgegebene IP-Adresse des „Sinkhole“ erfolgen, um Nutzer der dabei erkannten infizierten Systeme über die zuständigen Provider benachrichtigen zu können.

Diese Maßnahme bei den Diensteanbietern greift zwar nur dann, wenn die Systeme des Nutzers die DNS-Resolver bzw. DNS-Nameserver des betreffenden Diensteanbieters 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 sonst 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 Bundesamt bereits vorhanden. Im Rahmen seiner Tätigkeit hat das Bundesamt 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 Bundesamt angesiedelt werden.

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

Die Diensteanbieter selbst haben bereits die Befugnis gemäß § 109a Absatz 5 und 6 TKG, bei Störungen die Nutzung des Telekommunikationsdienstes bis zur Beendigung der Störung einzuschränken, umzuleiten oder zu unterbinden. Gemäß § 109a Absatz 6 TKG dürfen Diensteanbieter Datenverkehr zu Störungsquellen auch einschränken oder unterbinden, soweit dies zur Vermeidung von Störungen in den Telekommunikations- oder informationstechnischen Systemen der Nutzer erforderlich ist.

ENTWURF

Durch die Anordnungsbefugnis des Bundesamtes entfällt eine gegebenenfalls erforderliche Einzelfallprüfung bei den Diensteanbietern. Auch kann so ein zeitnahes und koordiniertes Vorgehen gegen die Gefahr gewährleistet werden, wenn verschiedene Anbieter betroffen sind.

Zu Nummer 2

Darüber hinaus ist in Absatz 1 Satz 1 Nummer 2 die Anordnungsbefugnis zur Mitwirkung des Diensteanbieters bei Bereinigung betroffener Datenverarbeitungssysteme von einem konkret benannten Schadprogramm enthalten. Eine solche Befugnis, die sich in der Regel auf die Verteilung von lückenschließender Software (Patches) oder auf die Übersendung von Befehlen zur Löschung von Schadsoftware beschränkt, wird insbesondere zum Zwecke einer effektiven Bekämpfung der Gefahren durch Botnetze (auch gegen die Bedrohung durch „Ransomware of Things“) benötigt. Hier obliegt es regelmäßig dem Bundesamt die technischen Möglichkeiten zur Bereinigung zu analysieren und technische Befehle dem Diensteanbieter zuzuliefern, so dass dieser sie an seine Kunden verteilen kann. Bei den technischen Befehlen handelt es sich beispielsweise um Programme, die dazu dienen eine Sicherheitslücke zu schließen oder um Schlüsselwörter, die die Funktion der Schadsoftware modifizieren. So gab es in der Vergangenheit Fälle, in denen sich die Schadsoftware nach Übersendung eines Schlüsselwortes selbstständig deinstallierte. Während andere Staaten von dieser Möglichkeit Gebrauch machten, unterblieb dieses in Deutschland mangels klarer Rechtslage. Dies wird mit der hier vorliegenden Regelung nun getroffen.

Für bestimmte technische Einrichtungen (z.B. Router, IoT-Geräte) übernimmt der Diensteanbieter bereits heute auch die Verantwortung, dass diese von Sicherheitslücken oder Schadprogrammen bereinigt werden. Hierbei handelt es sich allerdings um Fälle in denen die Überlassung der technischen Einrichtung Gegenstand eines Vertragsverhältnisses zwischen Nutzer und Diensteanbieter ist (z.B. Mietrouter). Mit dieser Vorschrift wird zukünftig auch ermöglicht, dass ein Diensteanbieter technische Einrichtungen für die Erbringung seiner Dienste auch dann bereinigt, wenn ein solches, unmittelbares Vertragsverhältnis nicht besteht (z.B. Kaufrouter).

Diese Befugnis soll vor allem im Rahmen der internationalen Kooperation bei der Bekämpfung von Botnetzen genutzt werden können und jeweils nur, soweit dies erforderlich und verhältnismäßig ist. Bei solchen Zugriffen geht es nicht etwa um ausforschendes Eindringen des Bundesamtes in informationstechnische Systeme, sondern um das Problem, dass im Zusammenhang mit der Stilllegung bzw. Übernahme von Botnetzen die meisten IT-Nutzer nicht wissen (können), dass z. B. ihr IoT-Gerät Teil eines Botnetzes ist und sie die dadurch bestehende Gefahr für andere in aller Regel gar nicht selbst bereinigen (können). Auch in solchen Situationen muss eine Bereinigung möglich sein.

Zu Satz 2 bis 5

Die Regelung enthält neben den engen Tatbestandsvoraussetzungen weitere Einschränkungen. Vor der Anordnung der Maßnahmen durch das Bundesamt ist Einvernehmen mit der Bundesnetzagentur herzustellen. Die Anordnungsbefugnis nach Absatz 1 Satz 1 Nummer 2 wird noch weiter eingeschränkt. Es ist zusätzlich Einvernehmen mit dem oder der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit herzustellen. Die Daten, auf die mit der Maßnahme zugegriffen werden soll, sind in der Anordnung zu benennen. Von der Maßnahme darf der Kernbereich privater Lebensführung nicht betroffen sein. § 5 Absatz 7 Satz 2 bis 8 BSIG gilt entsprechend. Diese Voraussetzungen sichern die Wahrung der Verhältnismäßigkeit sowie das Verfahren.

Zu Absatz 2

In Absatz 2 Satz 1 Nummer 1, 2 und 3 werden die Ziele der konkreten erheblichen Gefahr definiert, die sogenannten Schutzziele. Es werden die im § 2 Absatz 2 genannten Eigenschaften der Verfügbarkeit, Unversehrtheit und Vertraulichkeit einbezogen. Grundsätzlich

ENTWURF

kann ein Botnetz eine Gefahr für alle Telekommunikationsdienste darstellen. Das Bundesamt kann zur Abwehr konkreter erheblicher Gefahren für die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit der Kommunikationstechnik des Bundes, eines Betreibers kritischer Infrastrukturen, eines Unternehmens im besonderen öffentlichen Interesse oder Anbieter digitaler Dienste (Nummer 1), oder für die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informations- oder Kommunikationsdiensten (Nummer 2), oder für die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen, soweit diese durch unerlaubte Zugriffe, auf eine erhebliche Anzahl von Telekommunikations- oder informationstechnischen Systemen von Nutzern, eingeschränkt werden (Nummer 3), die Anbieter von Telekommunikationsdiensten im Sinne des § 3 Nummer 6 des TKG mit mehr als 100.000 Kunden zur Durchführung von Schutzmaßnahmen verpflichten.

Zu Nummer 1 und 2

Durch einen Botnetz-gestützten DDoS-Angriff kann die Verfügbarkeit der in Nummer 1 und 2 genannten Ziele zeitweise oder dauerhaft eingeschränkt oder gänzlich beseitigt werden.

Zu Nummer 3

Es werden die im § 2 Absatz 2 genannten Eigenschaften der Verfügbarkeit, Unversehrtheit und Vertraulichkeit einbezogen. Durch die Erheblichkeitsschwelle im Hinblick auf die Anzahl der betroffenen Nutzer wird sichergestellt, dass Maßnahmen nur getroffen werden, wenn nicht lediglich eine unbedeutende Anzahl von Nutzern betroffen ist.

Zu Absatz 3 und 4

Nach Absatz 3 kann das Bundesamt gegenüber dem Diensteanbieter auch anordnen, den Datenverkehr an eine vom Bundesamt benannte Anschlusskennung umzuleiten, wenn es eine Maßnahme nach Absatz 1 Satz 1 Nummer 1 anordnet. Dies ermöglicht dem Bundesamt den Betrieb sog. Sinkhole-Server, welche eine effektive Maßnahme zur Minderung von Gefahren, die von Botnetzen ausgehen, darstellen.

Mittels der mit „Sinkhole“ bezeichneten Maßnahmen werden die an ein Zielsystem gerichteten Daten zum einen umgeleitet und zum anderen zu Auswertungszwecken gespeichert. Die Umleitung kann entweder durch direkte Umleitung des IP-Datenverkehrs vom ursprünglichen Ziel (C&C-Server) zum Sinkhole-Server oder durch Änderung der im DNS-System gespeicherten IP-Adresse zu einer von einem Botnetz genutzten Domain erfolgen. Dies versetzt den Sinkhole-Betreiber insbesondere in die Lage, die Kommunikation zwischen sog. Bots und dem C&C-Server zu unterbinden. Je nachdem, ob Kennungen für C&C-Server oder Bots verwendet werden, wird jeweils eine der Kommunikationsrichtungen unterbunden und der Datenverkehr erhoben. Durch die Umleitung der Kommunikation wird der Betrieb des Botnetzes in wesentlichen Teilen unterbunden. Zugleich ermöglicht die Auswertung der gespeicherten Kommunikation die Analyse der Funktionsweise des Botnetzes und die Identifikation betroffener informationstechnischer Systeme. Damit wird das Bundesamt in die Lage versetzt, Informationen über die genutzten Schadprogramme und andere über das Netz genutzte Angriffsmethoden zu erlangen. Für die Anordnung nach Absatz 1 Satz 1 Nummer 2 sind die so erlangten Hinweise von zentraler Bedeutung, um in Zusammenarbeit mit dem Diensteanbieter die Bereinigung betroffener Datenverarbeitungssysteme von einem konkret benannten Schadprogramm vorzunehmen.

Absatz 3 umfasst daher die Befugnis des Bundesamtes, von dem Anbieter die Umleitung des „schadhaften“ Datenstroms an eine vom Bundesamt benannte Anschlusskennung (in der Regel IP-Adresse) zu verlangen. Da das Bundesamt die umgeleiteten Daten analysieren muss, benötigt es Zugriff auf diese Daten. Würde der Diensteanbieter verpflichtet, den Datenstrom selbst zu speichern, müsste er die dafür erforderlichen technischen Maßnahmen treffen und die bei ihm gespeicherten Daten regelmäßig an das BSI übermitteln. Um den Aufwand für den Diensteanbieter so weit wie technisch möglich zu minimieren, ist die Ausleitung des Datenstroms an das Bundesamt erforderlich. Es handelt sich dabei nicht um

ENTWURF

eine Befugniserweiterung für das Bundesamt, da es nach Absatz 4 ohnehin berechtigt ist, die umgeleiteten Daten zu verarbeiten, sondern nur um eine technische Vereinfachung der Datenübermittlung zwischen Diensteanbieter und Bundesamt.

Durch Umleitung und Sperrung von Datenströmen werden bereits heute Botnetz-Angriffe erfolgreich abgewehrt, da die Daten auf den angegriffenen Systemen nicht mehr ankommen und so beispielsweise eine Überlastung vermieden wird. Für die Analyse der technischen Abläufe ist es allerdings notwendig, die Daten nicht nur umzuleiten oder zu sperren, sondern diese zu Analysezwecken auch verarbeiten zu können. Das Bundesamt erhält dadurch Kenntnisse, die der Vermeidung und Abwehr künftiger Angriffe dienen und kann die Daten unter der Voraussetzung des § 5 BSIG auch an Strafverfolgungsbehörden übermitteln. Bei den vom Bundesamt zu analysierenden Daten handelt es sich in der Regel um Steuerungsinformationen der Schadprogramme oder sinnlose Daten, um Überlastungen hervorzurufen. Umfasst sind regelmäßig auch IP-Adressen oder andere Internetkennungen der informationstechnischen Systeme, die zu einem Schadverbund zusammengeschlossen sind. Je nach Schadprogramm ist nicht ausgeschlossen, dass auch andere auf den betroffenen Systemen gespeicherte Informationen in den Daten enthalten sind. Es ist beispielsweise vorstellbar, dass Trojaner Zahlungsdaten von den befallenen Rechnern an die C&C-Server übertragen. Aufgrund der Zweckbindung der Datenverarbeitung in Absatz 4 darf das Bundesamt solche Informationen jedoch nur verwenden, wenn diese Teildaten Informationen über Schadprogramme oder andere Sicherheitsrisiken in informationstechnischen Systemen enthalten.

Zu § 7d (Anordnungen des Bundesamtes gegenüber Anbietern von Telemediendiensten)

Die Gesetzgebungskompetenz des Bundes für diese Anordnungsbefugnis folgt aus Artikel 74 Absatz 1 Nummer 11 GG (Recht der Wirtschaft, einschließlich gefahrenabwehrrechtlicher Annexkompetenz) in Verbindung mit Artikel 72 Absatz 2 GG. Die gefahrenabwehrrechtliche Annexkompetenz ergibt sich aus der Notwendigkeit der näheren Überwachung der gewerberechtlichen Maßnahmen der Telemediendiensteanbieter aus § 13 Absatz 7 des Telemediengesetzes (TMG) durch das Bundesamt zum Schutz informationstechnischer Systeme einer Vielzahl von Nutzern. Die Einhaltung dieser Maßnahmen durch die Telekommunikationsdiensteanbieter muss verpflichtend geregelt werden und es bedarf der Regelung einer Durchsetzungsmöglichkeit für das Bundesamt, da zur Aufrechterhaltung sicherer IT-Strukturen und -anwendungen eine bundesweit einheitliche Gefahrenabwehr erforderlich ist. Die Anordnungsbefugnis dient der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung im Bereich des Rechts der Wirtschaft aus Artikel 74 Absatz 1 Nummer 11 GG als einer dem Bund zugewiesenen Sachmaterie und ist für den wirksamen Vollzug der in der Zuständigkeit des Bundes liegenden Bestimmungen aus § 13 Absatz 7 des TMG erforderlich. Im Interesse der Gewährleistung einer bundesweit einheitlichen IT-Sicherheit muss das Bundesamt in den in § 7d geregelten Fällen die Möglichkeit haben, die Ergreifung erforderlicher Maßnahmen im Gefahrenabwehrfalle bundesweit einheitlich vorgeben zu können. Bei Cyber-Angriffen, die von Telemedienangeboten ausgehen, ist des Öfteren zu beobachten, dass diese für den einzelnen Telemedienanbieter jeweils keine Störung darstellen, zu dessen Behebung er verpflichtet wäre. Dies trifft u.a. regelmäßig auf Host-Provider zu, deren originärer Dienst von einer mittels Telemedienangeboten wirkenden Schadsoftware nicht beeinträchtigt ist. Ein Anbieter von Web-Diensten kann ebenfalls zum Verbreiter von Schadsoftware werden, wenn er in seinen Dienst Angebote Dritter (z. B. Analytics) eingebunden hat, von denen die Schadsoftware auswirkt. Auch hier ist das Vorliegen einer vom Telemediendiensteanbieter ausgehenden Störung, die er zu beseitigen hat, vom jeweiligen Einzelfall abhängig. Es bedarf deshalb einer zentralen Stelle, die die Gefahr die von einem Telemedienangebot ausgeht, feststellt und auf die Abstellung dieser hinwirkt. Durch die Anordnungsbefugnis, ist derjenige Anbieter zur Mitwirkung verpflichtet, auf dessen System die Störung wirksam wird, unabhängig davon, ob diese ggf. von Unterauftragnehmern ausgeht. Dem Bundesamt kommt mit der Anordnungsbefugnis somit zugleich eine koordinierende Stellung zu, um die Gefahr abzustellen.

ENTWURF

Das Bundesamt hat gemäß § 3 Absatz 1 Satz 2 Nummer 2 BSIG bereits 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.

Im Hinblick auf Anbieter von Telemedienangeboten hat das Bundesamt derzeit keine Befugnis, diese zu Maßnahmen anzuweisen, um 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 – durch unzureichende Sicherung eine konkrete, erhebliche Gefahr ausgeht.

Nach der bisherigen Rechtslage sind Diensteanbieter nur nach § 13 Absatz 7 TMG zu technischen und organisatorischen Vorkehrungen verpflichtet. Diensteanbieter sind gemäß § 2 Nummer 1 TMG erfasst, soweit diese ihre Dienste „geschäftsmäßig“ anbieten. Erfasst sind auch Hostingunternehmen, die z. B. sog. „Webbaukästen“ oder vorkonfigurierte Webshop- bzw. CMS-Systeme anbieten. Diese sind dann ihren Kunden gegenüber verpflichtet, Maßnahmen zu treffen, um die Schutzgüter des § 13 Absatz 7 TMG zu sichern.

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 ein Schaden bei den Nutzern also bereits realisiert.

Im Hinblick auf die nachfolgenden Beispielszenarien für konkrete, erhebliche Gefahren 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 Bundesamt 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, gegenüber den Shopbetreibern anzuordnen, konkrete Absicherungsmaßnahmen durchzuführen, besteht seitens des Bundesamtes nicht.

b) Einer der häufigsten Infektionswege für Schadsoftware ist die vom Anwender unbemerkte Infektion über "Phishing" und "Drive-by-Downloads", beispielsweise durch schadhafte Online-Werbung. Des Weiteren kommt es immer wieder zu Sicherheitsvorfällen, bei denen sogenanntes "Cryptocurrency“ bzw. „Bitcoin Mining" in schadhaften Werbebannern versteckt und im Browser der Anwender ausgeführt wird. In allen Fällen handelt es sich um Schadsoftware, die (oftmals vom Webseitenbetreiber unbemerkt) Anwender beim Aufrufen einer Webseite infiziert.

Bereits im Jahr 2013 hat das Bundesamt vor einer breitflächigen Verteilung von Schadsoftware über Werbebanner gewarnt. Kriminelle haben dabei Server, die zur Auslieferung von Weberbannern genutzt werden, kompromittiert. Die Schadsoftware wurde sodann über bekannte und viel besuchte deutsche Online-Angebote von Nachrichten-, Politik-, Lifestyle- und Fachmagazinen, Tageszeitungen, Jobbörsen und Städteportalen an die Besucher – von diesen unbemerkt – verteilt.

In dem vorgenannten Fall waren es sog. OpenX-Ad-Server, die gravierende Sicherheitslücken enthielten. Gleichwohl lässt sich das grundsätzliche Problem auch auf Server (z.B. Web- oder Fileserver) übertragen, die Kunden bei Hostinganbietern betreiben. Auch diese

ENTWURF

Server können, wenn keine ausreichenden technischen oder organisatorischen Vorkehrungen getroffen werden, durch Angreifer auf unterschiedlichste Weisen kompromittiert werden – und dies unbemerkt vom Kunden und von eventuellen Nutzern des Kunden.

Fehlerhaft konfigurierte bzw. ungepatchte Server stellen – wie auch zahlreiche Beispiele aus der jüngsten Vergangenheit belegen – ein nicht zu unterschätzendes Risiko für Anbieter und Nutzer dar. So wurden im Jahr 2019 die Update-Server eines großen taiwanesischen Hardwareherstellers unbemerkt übernommen, um mit Schadsoftware versehene Updates an Endkunden auszuliefern. Die weltweit eingesetzten CMS-Systeme WordPress und Joomla wurden im Jahr 2019 über den Troldesh-Verschlüsselungstrojaner angegriffen, die im "/.well-known/"-Verzeichnis auf den Servern hinterlassen wurde. Gleichzeitig wurden auf diesen kompromittierten Websevern Phishing-Webseiten bekannter Unternehmen hinterlegt. Im August 2020 wurde eine Sicherheitslücke im CMS WordPress bekannt, die rund 700.000 Websites betrifft. In all diesen Fallkonstellationen besteht für das Bundesamt aber lediglich die Möglichkeit der Warnung unter gleichzeitiger Information der jeweils zuständigen Telemedienanbieter. Es besteht allerdings – wie im vorgenannten Fall auch – keine zielgerichtete Möglichkeit des Bundesamtes, die Webseitenbetreiber oder auch Hostinganbieter zur Absicherung ihrer Hardware und/oder Software sowie zur Beseitigung der Infektion zu verpflichten bzw. eine entsprechende Anordnung auszusprechen.

Es wird daher eine Anordnungsbefugnis des Bundesamtes im BSIG selbst benötigt, um Diensteanbieter zur Umsetzung konkreter Maßnahmen zu verpflichten, wenn ihre Telemedienangebote durch ungenügende technische und organisatorische Vorkehrungen im Sinne des § 13 Absatz 7 TMG dergestalt unzureichend gesichert sind, dass sie keinen hinreichenden Schutz vor unerlaubten Zugriffen auf die für diese Telemedienangebote genutzten technischen Einrichtungen und vor Störungen, auch soweit sie durch äußere Angriffe bedingt sind, bieten. Dabei überlässt das Bundesamt es dem Diensteanbieter, welche technischen und organisatorischen Maßnahmen im Einzelfall jeweils erforderlich sind, um den ordnungsgemäßen Zustand seiner Telemedienangebote herzustellen.

Die Regelung ist verhältnismäßig, da dem Bundesamt eine Anordnung nur dann möglich sein soll, wenn die konkrete, erhebliche Gefahr für Datenverarbeitungssysteme nicht nur weniger, sondern einer Vielzahl von Nutzern besteht. Die Betroffenheit einer Vielzahl von Nutzern ist regelmäßig anzunehmen, wenn sich das Telemedienangebot an ein breite Öffentlichkeit wendet, wie es z. B. insbesondere bei Web-Shops und Web-Seiten (Jedermann-Dienst) der Fall ist.

Zu Nummer 11

Zu Buchstabe a

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

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

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

ENTWURF

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

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

Aufgrund der Besonderheiten der für die Streitkräfte betriebenen Informations- und Kommunikationstechnik im Sinne des § 4a Absatz 6 und der einsatzspezifischen Anforderungen an sie, ist diese von der Verpflichtung zur Umsetzung von Mindeststandards ausgenommen (siehe Begründung zu § 4a). Die Informations- und Kommunikationstechnik im Geschäftsbereich des Bundesministeriums der Verteidigung unterliegt jedoch regelmäßig höheren Standards.

Zu Buchstabe b

Gemäß § 3 Absatz 1 Satz 2 Nummer 1 BSIG gehört es zu den Aufgaben des Bundesamtes, 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 Bundesamtes zugreifen können.

Zu Buchstabe c

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

Um sicherzustellen, dass die Belange der Cyber- und Informationssicherheit ausreichend und umfassend berücksichtigt werden, soll das Bundesamt bei der Planung und Umsetzung von Digitalisierungsvorhaben von der jeweils zuständigen Stelle des Bundes stets frühzeitig beteiligt werden. Das Bundesamt ist danach insbesondere bei wesentlichen Digitalisierungsvorhaben zu beteiligen. Dem Bundesamt ist insoweit die Gelegenheit zur Stellungnahme einzuräumen.

Zu Nummer 12

Zu Buchstabe a, b, und d

§ 8a Absatz 1a ergänzt 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, nun auch ausdrücklich um Systeme zur Angriffserkennung. Diese Systeme stellen eine effektive Maßnahme zur Begegnung von Cyber-Angriffen dar und unterstützen insbesondere die Schadensreduktion.

ENTWURF

Bereits heute ist eine große Anzahl von Systemen zur Angriffserkennung verfügbar. Diese unterscheiden sich u.a. in den Verfahren zur Detektion und sind für unterschiedliche Einsatzszenarien optimiert. Unterschiede liegen z.B. in den jeweils untersuchten Daten, die beispielsweise an den Übergängen zu öffentlichen Netzen, vom netzwerkinternen Datenverkehr oder auch von internen Daten der IT-Systeme erhoben werden. Ebenso unterscheidet sich die Methodik zur Erkennung von Cyber-Angriffen. Hierbei gibt es beispielsweise den Abgleich mit statischen Mustern zu Software und Kommunikationen, von denen bekannt ist, dass sie im Zusammenhang mit Cyber-Angriffen stehen. Es werden auch generische Muster sowie Verfahren der künstlichen Intelligenz eingesetzt, um Hinweise auf Cyber-Angriffe zu erhalten. Eine weitere Methode ist es, den störungsfreien Betrieb zu erfassen und dann Abweichungen von diesem Zustand zur Detektion zu verwenden (so genannte Anomaliedetektion).

Die Systeme zur Angriffserkennung sollen die Kommunikationstechnik der Betreiber Kritischer Infrastrukturen möglichst umfassend schützen. Gleichzeitig können Systeme zur Angriffserkennung zum Beispiel im Falle falscher Warnmeldungen auch zu Schäden führen. Gefordert wird daher – entsprechend Absatz 1 – nur ein angemessener Einsatz, dem eine Abwägung der Interessen an einem umfassenden Schutz mit bestehenden Risiken vorgeht.

Unternehmen benötigen für den Einsatz von Systemen zur Angriffserkennung Informationen, die sich als Erkennungsmuster zu Cyber-Angriffen einsetzen lassen. Der Einsatz der Systeme zur Angriffserkennung erfordert, dass die eingesetzten Erkennungsmuster ständig aktuell gehalten werden. Das Bundesamt wird dabei weiterhin, wie in der Vergangenheit geschehen (§ 8b Absatz 2 Nummer 4a), die Betreiber unterstützen. Hierzu wird eigens der Austausch über die Malware Information Sharing Plattform (MISP) des Bundesamtes bereitgestellt. Für einen möglichst reibungslosen und effizienten Austausch sind definierte Prozesse, Formate und Werkzeuge zum Austausch von technischen Merkmalen zu Cyber-Angriffen notwendig. Das Bundesamt wird hierzu Vorgaben veröffentlichen.

Bereits heute werden auf einer Vielzahl von IT-Systemen Systeme zur Angriffserkennung genutzt. Diese Systeme untersuchen automatisiert Daten aus den IT-Systemen, zu dessen Schutz sie eingesetzt werden. Unter diesen können sich auch personenbezogene Daten befinden. Soweit die Verarbeitung personenbezogener Daten für die Angriffserkennung erforderlich ist, sind Betreiber Kritischer Infrastrukturen nach § 8a Absatz 1a nun auch ausdrücklich dazu verpflichtet. Die Regelung enthält daher eine rechtliche Verpflichtung im Sinne von Artikel 6 Absatz 1 Buchstabe c DSGVO zur Verarbeitung personenbezogener Daten. Die Grundlage für die Verarbeitung der notwendigen Daten des IT-Systems kann sich im Einzelfall aber auch aus § 100 TKG ergeben.

Durch die Einräumung einer Jahresfrist ab Inkrafttreten dieses Gesetzes haben die Betreiber hinreichend Zeit, die Verpflichtung zum Einsatz von Systemen zur Angriffserkennung zu erfüllen.

Wie Cyber-Vorfälle der Vergangenheit zeigen, erstrecken sich insbesondere spezialisierte Cyber-Angriffe, so genannte Advanced Persistent Threats (APTs), über einen mehrjährigen Zeitraum. Persistenz bezeichnet dabei das Bemühen der Angreifer, sich nachhaltig und unbemerkt in den informationstechnischen Systemen einzunisten. Hierfür muss der Angreifer vorsichtig und verdeckt vorgehen, so dass zwischen der initialen Infektion und der Aufdeckung des Angriffs in der Regel große Zeiträume liegen. Diese Vorgehensweise war bisher vor allem staatlich assoziierten Akteuren vorbehalten, die über die entsprechenden Ressourcen zur Durchführung von Cyber-Angriffen verfügen. Aufgrund der zunehmenden Automatisierung und Professionalisierung von Cyber-Angriffen werden Unternehmen nun aber auch verstärkt durch kriminelle Akteure bedroht, die sich der Mittel von APT-Angriffen bedienen. Um durch APT hervorgerufene Kompromittierungen zu erkennen und zu bereinigen, muss die Dauer der Speicherung von Daten, die eine nachträgliche Analyse und Detektion zu lassen, den Zeitraum des APT-Angriffs einschließen. Nur wenn das Vorgehen

ENTWURF

des Angreifers – auch im Nachhinein – aufgeklärt werden kann, kann die Kommunikationstechnik der Betreiber Kritischer Infrastrukturen vor ähnlichen und gleichartigen Bedrohungen geschützt werden. Zudem gestattet das Vorhalten dieser Daten eine Feststellung des Umfangs der Kompromittierung und damit eine zielgerichtete und somit weniger aufwändige Bereinigung der informationstechnischen Systeme.

Zu Buchstabe c

Die Anpassung des § 8 Absatz 3 erfolgt zur Klarstellung, dass die Nachweise nach Absatz 3 erstmalig zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 vorzulegen sind.

Zu Nummer 13

Zu Buchstabe a und b

Die Änderung ist erforderlich wegen der Erweiterung des Anwendungsbereichs auf weitere Unternehmen 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. 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 künftig unmittelbar verankert werden. Die Pflicht zur Registrierung für KRITIS-Betreiber ist auch erforderlich, damit das BSI seinen Aufgaben nach § 3 und § 8b Absatz 2 Nummer 4 BSIG nachkommen kann. Insbesondere soll das Bundesamt die meldepflichtigen Unternehmen im Gegenzug auch über sie betreffende Informationen unverzüglich in Kenntnis setzen. Dies können von anderen Unternehmen gemeldete Vorfälle sein, oder auch Informationen, die das Bundesamt über andere Quellen erlangt, z.B. Schwachstellen in bestimmten IT-Produkten oder neue Methoden oder Angriffsvektoren für Cyberangriffe. Damit das Bundesamt diese Informationen zielgenau an die Unternehmen weiterleiten kann, ist es erforderlich, dass das BSI die entsprechenden Unternehmen kennt, und somit einschätzen kann, welche Informationen für diese Unternehmen relevant sind. Die bisherige reine Benennung von Kontaktstellen ist hier nicht ausreichend, da das Bundesamt ausreichende Informationen darüber benötigt, welche Informationen für diese Unternehmen relevant sind. Zudem kann das Bundesamt eine Anlage im Wege der Ersatzvornahme selbst als Kritische Infrastruktur registrieren, wenn der Betreiber seiner Pflicht nicht nachkommt. Gilt eine registrierte Anlage – zum Beispiel, weil ein maßgeblicher Schwellenwert unterschritten wird – nicht oder nicht mehr als Kritische Infrastruktur, löscht das Bundesamt die entsprechende Registrierung.

Zu Buchstabe c

§ 8b Absatz 3a regelt die Befugnis des Bundesamtes, die Herausgabe der für eine Bewertung erforderlichen Unterlagen zu verlangen. Das BSIG beinhaltet derzeit keine eigenständige Rechtsgrundlage, um von Betreibern Kritischer Infrastrukturen Auskünfte zu Kennzahlen bezüglich der jeweiligen Schwellwerte zu verlangen. Das Bundesamt 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 in Verbindung mit der BSI-KritisV sind oder Angaben unvollständig oder erläuterungsbedürftig sind.

Das Bundesamt erhält daher die Befugnis zur Abfrage von schwellwertrelevanten Kennzahlen der Betreiber. Betreiber werden verpflichtet, dem Auskunftsersuchen unverzüglich nachzukommen.

ENTWURF

Zu Buchstabe d

In Absatz 4a werden Befugnisse des BSI im Falle des Eintritts einer erheblichen Störung geregelt. Diese sind erforderlich, um im Einzelfall die Bewältigung der Störung zu gewährleisten. Das Bundesamt trifft Maßnahmen im Einvernehmen mit der jeweils zuständigen Aufsichtsbehörde des Bundes, soweit es eine solche gibt.

Zu Buchstabe e und f

Es handelt sich um eine Folgeanpassung sowie eine redaktionelle Korrektur.

Zu Nummer 14

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

Zu Nummer 15

Es handelt sich um eine Folgeanpassung.

Zu Nummer 16

Es handelt sich um eine Folgeanpassung.

Zu Nummer 17

Zu § 8f (Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse)

§ 8f regelt die Pflichten für Unternehmen von besonderem öffentlichem Interesse. Die Pflichten gelten für die Unternehmen in diesem Bereich zwei Jahre nach Inkrafttreten dieses Gesetzes bzw. der Rechtsverordnung nach § 10 Absatz 5.

Das besondere öffentliche Interesse bei Unternehmen nach § 2 Absatz 14 Nummer 1 besteht dahingehend, dass diese Unternehmen wichtige Güter und Produkte im Bereich der Rüstung sowie für IT-Produkte für die Verarbeitung von Verschlusssachen herstellen. Das besondere öffentliche Interesse bei Unternehmen nach § 2 Absatz 14 Nummer 2 besteht dahingehend, dass bei diesen volkswirtschaftlich besonders wichtigen Unternehmen vermieden werden soll, dass Cyber-Angriffe oder anderweitige IT-Störungen zu Schäden führen können z.B. durch Produktionsausfälle, Datenverlust, Sabotage, Schäden an IT-Systemen oder Anlagen. Diese Unternehmen sind somit entweder in sicherheitsrelevanten Branchen aktiv, oder haben aufgrund ihrer Größe und entsprechender wirtschaftlicher Leistungsfähigkeit ein inhärentes Interesse daran, bestmöglich sicherzustellen, dass Cyber-Angriffe oder sonstige IT-Störungen nicht zu länger andauernden Produktionsausfällen oder anderweitigen Schäden führen können. Daher werden diese Unternehmen verpflichtet, mittels einer Selbsterklärung gegenüber dem Bundesamt darzulegen, welche Maßnahmen zur Verbesserung ihrer IT-Sicherheit dort vorgesehen sind und durchgeführt werden. Aus technischer Sicht besonders geeignet wären hierbei beispielsweise Zertifizierungen, Audits oder Prüfungen nach nationalen oder internationalen Standards, beispielsweise dem BSI-Grundschutz oder der ISO/IEC 27001, oder auch nach anderen branchenspezifischen Normen oder Standards. Jedoch zeichnen sich die Unternehmen im besonderen öffentlichen Interesse in diesen Bereichen auch dadurch aus, dass sie in Art und Größe der Unternehmen sehr heterogen zusammengesetzt sind, und zudem zumeist in sehr unterschiedlichen Branchen tätig sind. Zudem besteht bei diesen Unternehmen zwar wie vorher dargelegt ein Schutzinteresse von staatlicher Seite, jedoch ist dieses beispielsweise im Vergleich zu Kritischen Infrastrukturen, welche eine unmittelbare Versorgung der Bevölkerung mit lebenswichtigen Gütern erbringen, deutlich abgestuft. Daher wird davon abgesehen, für Unternehmen im besonderen öffentlichen Interesse ein vergleichbar striktes Nachweisregime wie bei

ENTWURF

Kritischen Infrastrukturen beispielsweise durch verpflichtende Zertifizierungen nach nationalen oder internationalen Normen oder nach Sicherheitskatalogen einzuführen. Im Gegenzug für die durch die Unternehmen einzureichenden Selbsterklärungen erhält das Bundesamt jedoch hiermit die Möglichkeit, den Unternehmen passgenaue Hinweise und Empfehlungen zur weiteren Verbesserung ihrer IT-Sicherheit zu geben.

Weiterhin werden diese Unternehmen verpflichtet, bestimmte Vorfälle wie beispielsweise Cyberangriffe oder anderweitige IT-Störungen zu melden, wenn diese die Produktion bzw. die Erbringung der Wertschöpfung beeinträchtigt haben oder beeinträchtigen können. Hierbei kann durch die Unternehmen nur die eigene Erbringung der Wertschöpfung betrachtet werden, da etwaige Störungen der vorgelagerten Wertschöpfungskette für die Unternehmen im Regelfall nicht direkt ersichtlich sind. Entsprechende Meldungen an das Bundesamt - auch im Vorfeld konkreter Schadenseintritte - sind notwendig, um eine möglichst umfassende und frühzeitige Warnung möglicherweise ebenfalls betroffener Unternehmen im besonderen öffentlichen Interesse oder auch Betreiber Kritischer Infrastrukturen zu gewährleisten und darüber hinaus fundierte Aussagen zur IT-Sicherheitslage in Deutschland treffen zu können.

Hierbei wird bewusst nicht allein auf Cyber-Angriffe, sondern allgemein auf (erhebliche) Störungen, die die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse betreffen, abgestellt. Der Begriff der „Störung“ ist dabei entsprechend der höchstrichterlichen Rechtsprechung zu § 100 Absatz 1 TKG funktional zu verstehen. Eine Störung im Sinne des BSIG liegt daher vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken. Dazu zählen insbesondere Fälle von Sicherheitslücken, Schadprogrammen und erfolgten, versuchten oder erfolgreich abgewehrten Angriffen auf die Sicherheit in der Informationstechnik sowie außergewöhnliche und unerwartete technische Defekte mit IT-Bezug (zum Beispiel nach Softwareupdates oder ein Ausfall der Serverkühlung).

Solche Vorfälle können entweder durch gezielte Cyber-Angriffe oder auch durch Software- oder Konfigurationsfehler in besonders wichtigen IT-Systemen mitunter zu schwerwiegenden Schäden oder Ausfällen führen, wie auch der presseöffentlich bekannte Fall eines deutschen Automobilherstellers zeigte, dessen Produktion im Oktober 2019 infolge einer IT-Störung mehrere Stunden komplett stillstand. Durch die Meldepflicht an das Bundesamt können Erkenntnisse gewonnen werden, wie solche Störungen erkannt, behoben und vermieden werden können. Gemäß § 8f Absatz 7 besteht eine Meldepflicht, für Störungen die zu einem Ausfall der Wertschöpfung oder einer erheblichen Beeinträchtigung der Wertschöpfung geführt haben sowie für erhebliche Störungen, die zu einem Ausfall der Wertschöpfung oder einer erheblichen Beeinträchtigung der Wertschöpfung führen können. Ein Ausfall der Wertschöpfung wäre unbestritten meldepflichtig, da hierbei ein entsprechend bedeutendes Unternehmen faktisch stillgelegt wäre. Da die Frage, ob es sich bei einer Beeinträchtigung der Wertschöpfung eines Unternehmens (z.B. Ausfall einiger, aber nicht aller Produktionsstrecken) auch um eine erhebliche Beeinträchtigung handelt, vom Unternehmen abhängt, ist dies im Einzelfall zu entscheiden. Beispielsweise kann ein kurzfristiger Teilausfall ggf. durch ausreichende Lagerkapazitäten oder alternative Produktionsstrecken kompensiert werden. Die Kriterien der „erheblichen Störung“ sowie der „erheblichen Beeinträchtigung“ wurden bereits im ersten IT-Sicherheitsgesetz aus dem Jahr 2015 mit der Meldepflicht nach § 8b Absatz 4 BSIG für Betreiber Kritischer Infrastrukturen eingeführt und haben sich in der Umsetzungspraxis seitdem bewährt. Diese Erkenntnisse wiederum können mit anderen Unternehmen geteilt werden, und das IT-Sicherheitsniveau in Deutschland somit erhöht werden, ohne dass das meldende Unternehmen selbst an die Öffentlichkeit gehen muss, um andere Unternehmen zu warnen oder zu informieren. Ähnlich wie bei Kritischen Infrastrukturen soll daher hier ein vertrauensvoller Austausch zwischen Bundesamt und meldenden Unternehmen aufgebaut werden.

ENTWURF

Für die Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 3 besteht laut der Störfallverordnung bereits die Pflicht, ein Störfallkonzept vorlegen. Von zusätzlichen verpflichtenden Nachweisen im Bereich der IT-Sicherheit wird daher hier abgesehen. Gleichwohl haben Unternehmen nach Nummer 3 IT-Störungen an das Bundesamt zu melden, die zu einem Störfall nach der Störfall-Verordnung in der jeweils geltenden Fassung geführt haben oder führen können. Hierzu zählen nach der vorgenannten Verordnung insbesondere Ereignisse, die zu ernsten Gefahren führen, welche das Leben von Menschen bedrohen oder bei denen schwerwiegende Gesundheitsbeeinträchtigungen von Menschen zu befürchten sind oder die Gesundheit einer großen Zahl von Menschen beeinträchtigt werden kann.

Zu Tatsachen nach Absatz 7 zählt insbesondere, wenn Unternehmen laut dem letzten Hauptgutachten der Monopolkommission der Bundesregierung im Betrachtungszeitraum eine inländische Wertschöpfung erbracht haben, aufgrund dessen sie gemäß der Rechtsverordnung nach § 10 Absatz 5 als Unternehmen im besonderen öffentlichen Interesse gelten. Das hierbei betrachtete Gutachten soll hierbei nicht älter als zwei Jahre sein.

Die Pflicht zur Registrierung von Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1 und 2 ist erforderlich, damit das Bundesamt seinen Aufgaben nach § 3 und § 8b Absatz 2 Nummer 4 BSIG nachkommen kann. Insbesondere soll das Bundesamt die meldepflichtigen Unternehmen im Gegenzug auch über sie betreffende Informationen unverzüglich in Kenntnis setzen. Dies können von anderen Unternehmen gemeldete Vorfälle sein, die auch für dieses Unternehmen relevant sind, oder auch Informationen, die das Bundesamt über andere Quellen erlangt, z.B. Schwachstellen in bestimmten IT-Produkten oder neue Methoden oder Angriffsvektoren für Cyber-Angriffe. Damit das Bundesamt diese Informationen zielgenau an die Unternehmen weiterleiten kann, ist es erforderlich, dass es die entsprechenden Unternehmen kennt, und somit einschätzen kann, welche Informationen für diese Unternehmen relevant sind.

Für Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 3 besteht die Möglichkeit für eine freiwillige Registrierung beim Bundesamt, um ebenfalls von einem vertrauensvollen Austausch profitieren zu können.

Zu Nummer 18

Zu Buchstabe a und b

Die Änderung wurde vorgenommen, um klarzustellen, dass es sich bei der Untersagung eines Zertifikats nach Nummer 4a um eine Ermessensvorschrift handelt.

Zu Nummer 19

Zu § 9a (Nationale Behörde für die Cybersicherheitszertifizierung)

Die Regelung dient der Ergänzung der unmittelbar geltenden Vorschriften zur Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik der Verordnung (EU) 2019/881 des europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nummer 526/2013 (Rechtsakt zur Cybersicherheit).

Zu Absatz 1

Absatz 1 legt fest, dass das Bundesamt die nationale Behörde für die Cybersicherheitszertifizierung im Sinne des Artikels 58 Absatz 1 der Verordnung (EU) 2019/881 ist. Das Bundesamt nimmt dementsprechend die in der Verordnung (EU) 2019/881 genannten Aufgaben wahr und verfügt über die dort geregelten Befugnisse.

ENTWURF

Zu Absatz 2

Um sicherzustellen, dass Konformitätsbewertungsstellen im Anwendungsbereich der Verordnung (EU) 2019/881 nur dann tätig werden, wenn diese die in der Verordnung dafür vorgesehenen Anforderungen erfüllen, dürfen Konformitätsbewertungsstellen dort erst dann tätig werden, wenn das Bundesamt dafür eine Befugnis erteilt hat. Dabei handelt es sich um die Zuständigkeit einer Behörde, Stellen die Befugnis zu erteilen, als Konformitätsbewertungsstelle tätig zu werden im Sinne des § 1 Absatz 2 Satz 1 Gesetz über die Akkreditierungsstelle. Dadurch wird auch klargestellt, dass das Tätigwerden einer Konformitätsbewertungsstelle im Anwendungsbereich außerhalb der Verordnung (EU) 2019/881 oder des BSIG außerhalb des Verantwortungsbereichs des Bundesamtes liegen.

Zu Absatz 3, **4, 5, 6 und 7**

Diese Absätze dienen der Umsetzung der Verordnung (EU) 2019/881 durch Ergänzung der dort geregelten Befugnisse und Pflichten.

Zu § 9b (Untersagung des Einsatzes kritischer Komponenten)

Kritische Infrastrukturen sind auf Grund der voranschreitenden Digitalisierung und auch Vernetzung zur Aufrechterhaltung des Betriebs oft auf Komponenten angewiesen, die von hoher Kritikalität sind, weil Störungen dieser IT-Produkte zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit oder Integrität der Kritischen Infrastrukturen und zu Gefährdungen für die öffentliche Sicherheit führen können.

Für derartige kritische Komponenten sind neben der technischen Qualität und der Art des Einsatzes gleichsam auch die Organisationsstruktur und mögliche – den Schutzzielen dieses Gesetzes widersprechende – tatsächliche Mitwirkungen, Handlungen und unter Umständen auch sonstigen rechtlichen Verpflichtungen des Herstellers der Komponenten relevant. § 9b BSIG adressiert diese möglichen Gefahren und auch Verstöße gegen bestimmte Handlungspflichten.

Zu Absatz 1 und 2

Neben den bestehenden 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 auch eine Erklärung des Herstellers der kritischen Komponenten eingeholt werden, dass dieser in der Lage ist, die gesetzlich geforderten Bestimmungen, sowie auch weitergehende flankierende Pflichten selbst einzuhalten (Pflichten der Garantieerklärung). Dies gilt nur für solche kritischen Komponenten, für die eine gesetzliche Zertifizierungspflicht besteht, da die Zertifizierungspflicht die erhöhte technische Komplexität und Sicherheitsrelevanz der Komponente wiederspiegelt, welche sodann die zusätzlichen Maßnahmen erforderlich machen.

Die Anzeige des Einsatzes durch den KRITIS Betreiber ist notwendig, um dem Bundesministerium des Innern, für Bau und Heimat Kenntnis von dem geplanten Einsatz der Komponenten zu verschaffen, da nur so eine mögliche Durchführung der Maßnahmen der Absätze 3 bis 6 möglich wird. Die Anzeigepflicht besteht ab Inkrafttreten der Regelung, unabhängig davon, ob es sich um den erstmaligen Einsatz handelt. Soweit mehrere Komponenten desgleichen Typs eingesetzt werden (was je nach Art der Komponente der Regelfall sein kann), bezieht sich die Anzeige generell auf diesen Komponententyp. Es ist in diesen Fällen nicht notwendig, für jede einzelne Komponente eine separate Anzeige vorzunehmen. Dennoch muss die Art des Einsatzes (Absatz 1 Satz 2) dargestellt werden, was unter Umständen bei gleichen Komponententypen und unterschiedlicher Art des Einsatzes eine differenzierte Anzeige erfordert. Unter Art des Einsatzes ist die Funktion und Verortung (etwa Lokalisierung, Sicherheitsrelevanz, insbesondere mögliche Auswirkungen auf die Sicherheit der Kri-

ENTWURF

tischen Infrastrukturen, Funktionalität, Quantität des Einsatzes usw.) in der Kritischen Infrastruktur anzugeben. Die Anzeige hat durch den Betreiber zu erfolgen, da nur er Kenntnis über diese Tatsachen hat (zum Beispiel aufgrund der Schutzbedarfsanalyse bestimmter Teile eines Kommunikationsnetzes nach TKG).

Soweit für gesetzliche Zertifizierungspflichten Übergangsfristen zur Vorlage der Sicherheitszertifikate gewährt werden, ist dies sowohl für die Anzeige nach Absatz 1, als auch für die übrigen Regelungen des § 9b BSIG unbeachtlich. Gesetzliche Übergangsfristen für Sicherheitszertifikate sind der Tatsache geschuldet, dass die Hersteller bei neuen Zertifizierungspflichten in der Regel Zeit brauchen, bis alle Anforderungen erfüllt sind und auch Zertifikate vorgelegt werden können. Teils können die Vorgaben der Zertifizierung selbst (Schemata) auch erst sukzessive bereitgestellt werden. Diese Übergangsfristen sind bei den Maßnahmen nach §9b nicht zu beachten, da der Anknüpfungspunkt der Regelung des § 9b nicht in dem Abprüfen bestimmter sicherheitstechnischer Vorgaben liegt, sondern Gefahren im Mittelpunkt stehen, die selbst durch eine Zertifizierung nicht ausgeräumt werden könnten. Vor diesem Hintergrund ist die Prüfung und Bewertung der Einhaltung der Garantieerklärung der Hersteller nicht im Rahmen der Zertifizierung selbst durchzuführen. Durch die systematische Trennung der Prüfung der technischen Sicherheitsanforderungen (z.B. Einhaltung des Sicherheitskataloges nach § 109 Absatz 6 TKG) von der Schaffung eines Verfahrens zur Prüfung der Einhaltung der Aussagen der Garantieerklärung wird gewährleistet, dass die Sicherheitsaussagen der technischen Zertifizierung und Evaluierung systematisch nicht mit einer Bewertung der Vertrauenswürdigkeit vermischt werden.

Die Inhalte der Garantieerklärung werden mittels einer Allgemeinverfügung vorgegeben. Dies ist notwendig, da sich die Garantieerklärung perspektivisch auf verschiedene KRITIS-Sektoren erstrecken kann und für diese jeweils spezifische Inhalte vorgegeben werden müssen. Die Garantieerklärung ist vorzulegen, wenn für den KRITIS Sektor kritische Komponenten festgelegt wurden, für die zusätzlich eine gesetzliche Zertifizierungspflicht besteht. Um überwiegenden öffentlichen Interessen, insbesondere sicherheitspolitischen Belangen, angemessen Rechnung zu tragen, muss die Garantieerklärung auch mögliche Gefahren und Verstöße gegen bestimme Handlungspflichten abdecken, die sich aus den Organisationsstrukturen oder möglichen sonstige rechtlichen Verpflichtungen des Herstellers ergeben. Diese Zielvorgaben werden durch die Inhalte der Garantierklärung konkretisiert. Die Inhalte der Garantieerklärung legt das Bundesministerium des Innern, für Bau und Heimat (BMI) mittels Allgemeinverfügung fest. Um alle relevanten Belange der Ressorts ausreichend berücksichtigen zu können, bindet das BMI die betroffenen Ressorts zur späteren Herstellung des Einvernehmens frühzeitig in die Erstellung ein. Die Betroffenheit richtet sich u.a. nach dem Sektor der Kritischen Infrastruktur und den daraus folgenden Ressortzuständigkeiten. So ist etwa das Bundesministerium für Wirtschaft und Energie (BMWi) im Sektor Telekommunikation betroffen. Das Auswärtige Amt (AA) ist dann als Ressort betroffen, wenn durch die mögliche Entscheidung nach Absatz 4 öffentliche Interessen aufgrund außen- und sicherheitspolitischer Belange berührt sind.

Zu Absatz 3

Nach Absatz 3 kann das BMI im Einvernehmen mit den jeweils betroffenen Ressorts den nach Absatz 1 angezeigten geplanten Einsatz von kritischen Komponenten gegenüber dem Betreiber der Kritischen Infrastruktur innerhalb von einem Monat untersagen oder sonstige Anordnungen erlassen, wenn entgegenstehende überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange dem Einsatz entgegenstehen. Die Betreiber müssen eine entsprechende Entscheidung abwarten, bevor der Einsatz gestattet ist (Untersagungsvorbehalt).

Die Notwendigkeit einer derartigen Möglichkeit ist der Tatsache geschuldet, dass mit zunehmender informationstechnischer Komplexität der eingesetzten kritischen Komponenten ein wesentlicher Teil der Beherrschbarkeit der Technologie im Rahmen der Produktpflege (Softwareupdates, Firmware-Updates, Schließen von Sicherheitslücken) beim Hersteller

ENTWURF

selbst oder auch der weiteren Lieferkette verbleibt. Auf Grund der hohen Komplexität der kritischen Komponenten und der zu erwartenden stetigen Software/Firmware-Updates bieten etwa weder eine Komponentenzertifizierung, noch hohe technische Sicherheitsanforderungen eine ausreichende Sicherheit dahingehend, dass die Hersteller keine missbräuchlichen Zugriffmöglichkeiten auf Hard- und Software implementieren, oder sonstige Handlungen vornehmen, die Sabotage oder Spionage ermöglichen. Geeignete technische Maßnahmen können derartige Risiken zwar minimieren bzw. in den möglichen Auswirkungen abschwächen, die letztlich im Raum stehende Frage der – in diesem Sinne - Vertrauenswürdigkeit von Herstellern kann hierdurch jedoch nicht umfassend adressiert werden.

Die umfassende Prüfung derartiger Restrisiken muss über eine objektive Risikobewertung der Hersteller der kritischen Komponenten erfolgen, was Absatz 3 durch den weiten Prüfungsrahmen und durch das Tatbestandsmerkmal der überwiegenden öffentlichen Interessen, insb. sicherheitspolitischer Belange, ermöglicht. Absatz 3 dient damit auch der Umsetzung der Empfehlungen der sog. EU-5G Toolbox („Cybersecurity of 5G Networks – EU Toolbox of risk mitigating measures“, dort „strategic measure“ SM03), welche die Bewertung von Risikoprofilen der Hersteller und mögliche Restriktionen als eine der Schlüsselmaßnahmen zur Absicherung der 5G Netze – welche als Telekommunikations-Netze dem Regelungsbereich des § 9b grundsätzlich auch unterfallen können – herausgestellt.

Die Entscheidung kann nur im Einvernehmen mit den jeweils betroffenen Ressorts erfolgen. Die Betroffenheit richtet sich u.a. nach dem Sektor der Kritischen Infrastruktur und den daraus folgenden Ressortzuständigkeiten. So ist bspw. das BMWi im Sektor Telekommunikation betroffen. Das Auswärtige Amt ist dann als Ressort betroffen, wenn durch die mögliche Entscheidung nach Absatz 3 (und auch Absatz 4) außen- und sicherheitspolitische Belange berührt sind. Dies ermöglicht die notwendige Einbeziehung aller relevanten Belange der in die Entscheidung.

Um eine mögliche Entscheidung im Einvernehmen mit den betroffenen Ressorts zu unterstützen und vorzubereiten, ist ein fortlaufender und regelmäßiger, Austausch der in der Regel betroffenen Ressorts zu Entscheidungen nach Absatz 3 in Form eines „interministeriellen Jour Fixes“ aufzunehmen (BMI, BMWi, AA, Bundeskanzleramt auf Ebene Referatsleitung). Der strukturierte Austausch ist notwendig, um eine umfassende Sachverhaltsaufklärung und Sachverhaltsvorbereitung – als Voraussetzung für eine Entscheidung nach Absatz 3 – in den knappen Entscheidungsfristen (ein Monat nach Anzeige) zu ermöglichen.

Da das Einvernehmen mit den betroffenen Ressorts zwingende Voraussetzung für eine Entscheidung nach Absatz 3 ist, muss durch die Ressorts proaktiv ein geeigneter Eskalationsmechanismus vorgehalten werden. Dies ist notwendig für Fälle, in welchen auf Arbeitsebene Einvernehmen bezüglich einer Untersagung oder Anordnung nach Absatz 3 nicht erzielt werden kann. Da es sich bei der Untersagungsentscheidung nach Absatz 3 um das Ergebnis eines Verwaltungsverfahrens auf ministerieller Ebene handelt, muss der Eskalationsmechanismus auch die Ministerebene einschließen, auf der Einvernehmen herzustellen ist, wenn dies auf Arbeitsebene nicht gelingt. Soweit auch auf Ministerebene ein Dissens bestehen bleibt, ist zeitnah durch die Bundesregierung nach den Vorgaben der Gemeinsamen Geschäftsordnung der Bundesregierung (GOBReg) über den Streit zu beraten mit dem Ziel, eine einvernehmliche Entscheidung voranzutreiben (§ 15 Absatz 1 f. GOBReg). Die formale Erteilung des Einvernehmens verbleibt bei den betroffenen Ressorts.

Zu Absatz 4

Absatz 4 regelt im Gegensatz zu Absatz 3 die Prüfung der Einhaltung der Vorgaben der Garantieerklärung im laufenden Betrieb. Bei festgestellten Verstößen kann der weitere Betrieb einer Komponente untersagt werden (Rückbau). Die Pflichten aus der Garantieerklärung beziehen sich damit nicht allein auf den Zeitpunkt des Einbaus, sondern müssen fortwährend, also gerade im Betrieb der Komponenten, eingehalten werden. Dies erfordert eine fortlaufende Bewertung der Vertrauenswürdigkeit, mithin vorliegender Erkenntnisse von

ENTWURF

Verstößen gegen die Garantieerklärung. Für Entscheidungen nach Absatz 4 ist gleichsam das Einvernehmen mit den betroffenen Ressorts – wie in Absatz 3 dargestellt – notwendig. Die fortlaufende Bewertung der Vertrauenswürdigkeit von Herstellern ist auch Gegenstand des in der Gesetzesbegründung zu Absatz 3 erläuterten „interministeriellen Jour Fixe“. Alle betroffenen Ressorts können die erneute Überprüfung einer bestimmten Garantierklärung anregen.

Zu Absatz 5

Absatz 5 listet alternativ die Gründe auf, welche zu einer mangelnden Vertrauenswürdigkeit eines Herstellers führen können.

Zu Absatz 6 und 7

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

Zu § 9c (Freiwilliges IT-Sicherheitskennzeichen)

Zu Absatz 1

Das Bundesamt hat nach § 7 Absatz 1 Nummer 1a in Verbindung mit § 3 Absatz 1 Satz 2 Nummer 14 BSIG die Aufgabe, Anwender von Produkten im Bereich der Sicherheit der Informationstechnik zu warnen und zu beraten. Dieser Auftrag soll gemäß dem Koalitionsvertrag der 19. Legislaturperiode (Ziffer 1987-1997) und dem Auftrag des Bundestages vom März 2017 (BT-Drucksache 18/11808) im Sinne eines einheitlichen „IT-Gütesiegels“ konkretisiert und umgesetzt werden. Das „IT-Gütesiegel“ wird im Rahmen der Neuregelung des § 9a BSIG als einheitliches IT-Sicherheitskennzeichen umgesetzt. Das IT-Sicherheitskennzeichen 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 Sicherheitsinformation zum Produkt. Die hybride Ausgestaltung bedeutet, dass neben der reinen Herstellererklärung gegen eine technische Vorschrift (bspw. eine Technische Richtlinie) 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

ENTWURF

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 daher nicht geeignet, die genannten Zielvorgaben aus dem Koalitionsvertrag zu erfüllen.

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

Durch die Verwendung des Begriffes Diensteanbieter ermöglicht die Vorschrift die Verwendung des IT-Sicherheitskennzeichens künftig auch für digitale Dienstleistungen. Mit dem Begriff Diensteanbieter sind nicht ausschließlich die im Gesetz bereits definierten Anbieter digitaler Dienste gemeint. Es kommen daher grundsätzlich auch andere als die digitalen Dienste im Sinne des § 2 Absatz 11 in Betracht.

Die Einführung des IT-Sicherheitskennzeichens erfolgt schrittweise für verschiedene Produktkategorien. Die Auswahl der relevanten Produktkategorien im Verbraucherbereich obliegt dem Ermessen des Bundesamtes.

Zu Absatz 2

Das IT-Sicherheitskennzeichen setzt sich zur Verwirklichung des Zwecks des Absatzes 1 aus zwei Komponenten zusammen, der Herstellererklärung und den 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 das jeweilige Produkt die in den maßgeblichen IT-Sicherheitsanforderungen festgelegten Vorgaben erfüllt und für die jeweils maßgebliche Dauer der Herstellererklärung auch weiterhin erfüllen wird. Dies kann z.B. beinhalten, dass der Hersteller das Produkt durch Softwareupdates anpasst. Die IT-Sicherheitsanforderungen, 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. Das IT-Sicherheitskennzeichen stellt dabei keine Zertifizierung dar. Die dem IT-Sicherheitskennzeichen zugrundeliegenden IT-Sicherheitsvorgaben dienen hierbei als Grundlage für die Herstellererklärung nach Nummer 1. Die Sicherheitsinformation bildet den dynamischen Anteil des IT-Sicherheitskennzeichens. Die durch das Bundesamt zu veröffentlichenden Informationen werden hierbei in geeigneter Weise, angelehnt an das „Responsible Disclosure-Verfahren“, dem Hersteller mit der Gelegenheit zur Rückäußerung zur Kenntnis gegeben.

Zu Absatz 3

Die einzuhaltenden IT-Sicherheitsanforderungen für das jeweilige Produkt werden durch die zugrundeliegende Technische Richtlinie bzw. branchenabgestimmte Sicherheitsvorgaben bestimmt. Diese Technischen Richtlinien bzw. branchenabgestimmten Sicherheitsvorgaben sollen internationale und europäische Normen und Standards berücksichtigen und zur Anwendung bringen. Es werden dabei nur Aspekte der IT-Sicherheit betrachtet. Vorgaben an die Einhaltung des Datenschutzes werden durch das IT-Sicherheitskennzeichen nicht erfasst bzw. dargestellt. Da Produkte auch von mehreren Technischen Richtlinien erfasst sein können, stellt Absatz 2 klar, dass es jeweils auf die speziellen, in der Regel höheren, Anforderungen ankommt. Wird ein Produkt sowohl von einer Technischen Richtlinie als auch von branchenabgestimmten Sicherheitsvorgaben erfasst, ist nur die Technische

ENTWURF

Richtlinie maßgeblich. Näheres regelt die Rechtsverordnung. Der maßgebliche Zeitraum, für den die Hersteller mit den IT-Sicherheitskennzeichen eine Erklärung über die IT-Sicherheit ihrer Produkte abgeben, kann je nach Produktkategorie unterschiedlich lang sein, da auch die gewöhnlichen Lebenszyklen der Produkte verschiedener Kategorien unterschiedlich ausfallen. Deshalb wird die Dauer der Herstellererklärung wie auch der maßgebliche Zeitpunkt für den Beginn nicht pauschal im Gesetz festgelegt, sondern der Regelung in der Rechtsverordnung, beziehungsweise in den Technischen Richtlinien oder branchenabgestimmten IT-Sicherheitsvorgaben überlassen. So kann für jede Produktkategorie unter Berücksichtigung der spezifischen Eigenarten der jeweiligen Produkte ein angemessener Zeitraum bestimmt werden.

Zu Absatz 4 und Absatz 5

Das IT-Sicherheitskennzeichen darf erst nach Freigabe durch das Bundesamt verwendet werden. Die Freigabe wird auf Antrag des Herstellers erteilt, erfolgt aber nur für Produkte der Kategorien, für die das Bundesamt das IT-Sicherheitskennzeichen durch öffentliche Bekanntmachung bereits eingeführt hat. Dies ist erforderlich, da Technische Richtlinien auch abstrakt verschiedenste Produktkategorien erfassen können und daher zur Begrenzung der Produktkategorien, für die das IT-Sicherheitskennzeichen verfügbar sein soll, nicht geeignet sind. Die Freigabe eines IT-Sicherheitskennzeichens für ein Produkt ist keine Zertifizierung im Sinne des § 9. Die Freigabe des IT-Sicherheitskennzeichens wird in Absatz 5 nur grundlegend geregelt

Zu Absatz 6

Das IT-Sicherheitskennzeichen kann nur dann die gewünschte Wirkung im Rahmen der Kaufentscheidung entfalten, wenn dieses 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. Auch für Produkte, an denen aufgrund ihrer Beschaffenheit kein Zeichen angebracht werden kann, ist die elektronische Veröffentlichung vorgesehen. Herstellererklärung und die Sicherheitsinformation bilden gemeinsam einen „elektronischen Beipackzettel“, welcher auf einer Webseite des Bundesamtes abrufbar gemacht wird. Das genaue Verfahren und die Inhalte der Herstellererklärung werden in der Rechtsverordnung nach § 10 Absatz 3 festgelegt.

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

Zu Absatz 7

Nach Ablauf der in der Rechtsverordnung für die jeweilige Produktkategorie festgelegten Dauer, auf die sich die Herstellererklärung bezieht, erlischt die Freigabeerklärung. Dasselbe gilt, wenn der Hersteller gegenüber dem Bundesamt erklärt, dass er seinen Antrag zurücknimmt. Das Bundesamt fügt einen Hinweis in die Sicherheitsinformation ein, dass die Freigabe des IT-Sicherheitskennzeichens erloschen ist.

Zu Absatz 8 und Absatz 9

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. Anlass zur Prüfung können beispielsweise bekanntgewordene Schwachstellen zum betreffenden Gerät, der verwendeten Technologie oder aber ähnliche Geräte des gleichen Herstellers sein, die noch kein IT-Sicherheitskennzeichen tragen. Dieses Recht ist notwendig, um die Validität des IT-Sicherheitskennzeichens aufrechterhalten zu können.

ENTWURF

Wenn und soweit bei dieser Prüfung Abweichungen oder Sicherheitslücken auffallen, kann das BSI diese auch im Rahmen der Sicherheitsinformationen zum Produkt aufführen. In Ausübung des pflichtgemäßen Ermessens kann das BSI alternativ auch die Freigabe des IT-Sicherheitskennzeichens widerrufen und damit die weitere Verwendung untersagen.

Zum Schutz der Interessen des Herstellers, ist diesem vor dem Treffen einer Maßnahme nach Absatz 8 Gelegenheit einzuräumen, die festgestellten Abweichungen oder Sicherheitslücken innerhalb eines angemessenen Zeitraumes zu beseitigen. Dies gilt zum Schutz der Verbraucherinnen und Verbraucher dann nicht, wenn gewichtige Gründe der Sicherheit der Produkte eine sofortige Maßnahme erfordern.

Zu Nummer 20

Zu Buchstabe a

Die Verordnungsermächtigung ist notwendig, um das Verwaltungsverfahren zur Freigabe und die genauen Inhalte des IT-Sicherheitskennzeichens im Detail abbilden zu können. Daneben werden in der Verordnung die Details der Ausgestaltung (grafische Darstellung, Aufbau des „elektronischen Beipackzettels“ usw.) festgelegt. Die Verordnung soll des Weiteren die Einzelheiten der Gestaltung des Verfahrens zur Feststellung der Eignung branchenabgestimmter IT-Sicherheitsvorgaben regeln sowie das Verfahren auf Freigabe, insbesondere die Frist, innerhalb derer das Bundesamt über eine Freigabe zu entscheiden hat, der vom jeweiligen Hersteller dem Antrag beizufügenden Unterlagen sowie der Verwaltungsgebühren, die das Bundesamt für die Bearbeitung des Antrags auf Freigabe erheben kann. Zudem ist dort das genaue Verfahren und die Gestaltung des Verweises auf Sicherheitsinformationen, der Teil des Etiketts des IT-Sicherheitskennzeichens sein soll, zu regeln.

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 Teilen davon ein besonderes öffentliches Interesse im Sinne des § 2 Absatz 14 Nummer 2 und 3 besteht. Bei der Bestimmung der Anlagen oder Teilen davon ist die Systematik zur Bestimmung Kritischer Infrastrukturen nach § 10 Absatz 1 in Verbindung mit 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 des Grundgesetzes Genüge getan.

Die Nennung der § 4a und § 5a in § 11 liegt darin begründet, dass bei Inanspruchnahme der dort geregelten Befugnisse im Einzelfall nicht ausgeschlossen werden kann, dass Daten betroffen werden, die durch Artikel 10 Grundgesetz geschützt sind. Das betrifft namentlich Daten, die Aufschluss über Umstände der von Beschäftigten und anderen Nutzern über die Kommunikationstechnik des Bundes abgewickelten Kommunikation zulassen, z.B. IP-Adressen.

Im Rahmen einer Detektionsmaßnahme nach § 7b kann ein Eingriff in das Fernmeldegeheimnis vorliegen, wenn ein System, das fehlerhaft arbeitet oder in anderer Weise dergestalt reagiert, dass es Daten zurücksendet (etwa Statusinformationen der jeweiligen Portapplikation oder Logdaten wie IP-Adressen), die vom Schutzbereich des Artikel 10 des Grundgesetzes erfasst sind.

ENTWURF

Bei der Anwendung von § 7c kommt es zu einem Eingriff in das Fernmeldegeheimnis, wenn laufende Kommunikationsvorgänge bzw. deren Verkehrsdaten auf einen vom Bundesamt bestimmten Anschluss umgeleitet und dann verarbeitet werden.

Das Grundrecht der Unverletzlichkeit der Wohnung (Artikel 13 Grundgesetz) kann durch § 9a Absatz 5 eingeschränkt werden, wenn das Bundesamt zur Erfüllung der ihm zugewiesenen Aufgaben, Prüfungen in Betriebsstätten, Geschäfts- oder Betriebsräumen von Konformitätsbewertungsstellen oder Inhabern europäischer Cybersicherheitszertifikate durchführt.

Zu Nummer 22

Zu § 14 (Bußgeldvorschriften)

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

Die bisherigen Sanktionen haben nur einen Teil der Pflichten aus dem BSIG abgedeckt und in ihrer Höhe nicht den europarechtlichen und tatsächlichen Anforderungen entsprochen. Es war daher erforderlich, den Katalog der Tatbestände zur Wahrnehmung der übertragenen Aufgaben insbesondere im Bereich kritischer Infrastrukturen zu präzisieren und zu erweitern. Außerdem wird Wertungswidersprüchen der Bußgeldhöhen zu Verstößen gegen die DSGVO sowie die NIS-RL (EU) 2016/1148 begegnet. Zur besseren Differenzierung wurde zudem eine zusätzliche Stufe für weniger schwere Verstöße hinzugefügt.

Zu Absatz 1

Zu Nummer 1

Mit § 14 Absatz 1 Nummer 1 Buchstaben a und b werden Fälle von Zuwiderhandlungen gegen vollziehbare Anordnungen erfasst. Die getrennte Aufzählung in den Buchstaben a und b ermöglicht es, aufgrund unterschiedlicher Schwere der Zuwiderhandlungen erforderliche Bußgeldbewehrungen in unterschiedlicher Höhe vorzunehmen.

In Nummer 1 Buchstabe a ist insbesondere eine erstmalige Bußgeldbewehrung einer Zuwiderhandlung gegen eine vollziehbare Anordnung nach § 5b Absatz 6 vorgesehen, wenn Hersteller eines informationstechnischen Systems, entgegen dem Verlangen des Bundesamtes, nicht oder in unzureichender Form an der Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen Systems mitwirken.

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

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

Die von § 5b BSIG erfassten Betroffenen haben gemein, dass sie sich einem erhöhten Bedrohungspotential ausgesetzt sehen, dem ein herausragendes öffentliches Interesse an der Sicherheit eben dieser erfassten Betroffenen gegenübersteht. Daher sind initiale Maßnahmen des MIRT stets von Eilbedürftigkeit geprägt, um Maßnahmen zur Schadensbegrenzung zu treffen, einen Notbetrieb sicherzustellen und um alsbald wieder einen Normalbetrieb zu ermöglichen. Hierzu kann es erforderlich sein, dass - wenn die IT-Sicherheit durch eine Sicherheitslücke in der verwendeten Hard- oder Software gefährdet wird - der

ENTWURF

Hersteller des betroffenen Produktes schnell und nachhaltig zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit beiträgt – etwa durch das zeitnahe Bereitstellen eines Sicherheitspatches. Mittels Verwaltungszwang sind diese vom Hersteller zu erbringenden Leistungen nicht durchsetzbar, denn sie setzen das betriebsinterne Know-how des Herstellers voraus. Hinzu tritt die besondere Eilbedürftigkeit in diesen Fällen, die einer Durchsetzung durch Verwaltungszwang ebenfalls entgegensteht, da durch § 5b Absatz 6 BSIG ein beschleunigtes Tätigwerden des Herstellers ermöglicht werden soll, um die im herausragenden öffentlichen Interesse stehende Beeinträchtigung schnellstmöglich und effektiv beseitigen zu können.

Die Bußgeldbewehrung einer Zuwiderhandlung gegen eine vollziehbare Anordnung nach § 7c Absatz 1 Satz 1 erfolgt, um die neu eingeführten Anordnungsbefugnisse des BSI gegenüber Anbietern von Telekommunikationsdiensten auch wirksam durchsetzen zu können.

Dasselbe gilt für die Sanktionierung einer Zuwiderhandlung gegen eine vollziehbare Anordnung nach § 7d BSIG zur Durchsetzung der neu eingeführten Anordnungsbefugnisse des BSI gegenüber Anbietern von Telemediendiensten.

Die Bußgeldbewehrung einer Zuwiderhandlung gegen eine vollziehbare Anordnung nach § 8a Absatz 3 Satz 5 soll sicherstellen, dass die Beseitigung von Sicherheitsmängeln bei Betreibern Kritischer Infrastrukturen wirksam durchgesetzt werden kann. Die Weigerung zur Beseitigung des Sicherheitsmangels auch nach einer erfolgten Anordnung stellt nicht nur eine potentielle Gefahr für die von dem Betreiber versorgten Adressaten im In- und Ausland dar, sondern auch für die weiteren Betreiber in der Branche, wenn sich aus der Ausnutzung des Sicherheitsmangels weitere Kenntnisse und Angriffsvektoren in den Sektor ergeben. Gerade im Bereich der Betreiber Kritischer Infrastrukturen können Sicherheitsmängel schwerwiegende Folgen haben und müssen umgehend beseitigt werden.

Durch die Sanktionierung einer Zuwiderhandlung gegen eine vollziehbare Anordnung nach § 8b Absatz 6 Satz 1 wird die fehlende Mitwirkung bei der Bekämpfung einer IT-Bedrohungslage mit einem Bußgeld bewehrt. Dies soll die Betreiber dazu anhalten, in Krisenfällen das Erforderliche zu unternehmen, um die Gefahrenlage zu beenden.

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

Weiterhin wird der Fall einer Zuwiderhandlung gegen eine vollziehbare Anordnung auf Schließung einer bereits erfassten Sicherheitslücke sanktioniert.

Erstmalig bußgeldbewehrt wird sowohl in § 14 Absatz 1 Nummer 1 Buchstabe a als auch Buchstabe b eine Zuwiderhandlung gegen eine vollziehbare Anordnung nach § 8b Absatz 6 Satz 1 oder Satz 2, jeweils in Verbindung mit Absatz 4 Satz 1. Dabei wird Absatz 4 Satz 1 nach Nummern 1 und 2 aufgeteilt und unterschiedliche Bußgeldhöhen vorgesehen, da es für die Bußgeldhöhe relevant ist, ob es sich um eine Störung oder um eine erhebliche Störung handelt. Das Bundesamt ist auf die Mitwirkung des Herstellers der betroffenen informationstechnischen Produkte und Systeme an der Beseitigung oder Vermeidung einer dort genannten Störung angewiesen, da nur dieser das entsprechende betriebsinterne Know-how besitzt und gegebenenfalls eine besondere Eilbedürftigkeit hinzutreten kann.

Aufgrund unterschiedlicher Schwere der Zuwiderhandlungen wird auch eine getrennte Bußgeldbewehrung für § 8c Absatz 4 Satz 1 Nummern 1 und 2 vorgesehen.

ENTWURF

Zu Nummer 2

Mit § 14 Absatz 1 Nummer 2 wird erstmals eine Sanktionsmöglichkeit dafür geschaffen, dass entgegen § 8a Absatz 1 Satz 1, Absatz 1a oder Absatz 1b eine dort genannte Vorkehrung oder Maßnahme nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig getroffen wird. Eine nicht sichergestellte Funktionsfähigkeit der Kritischen Infrastrukturen hätte schwerwiegende Folgen und muss vermieden werden.

Zu Nummer 3

Der § 14 Absatz 1 Nummer 3 ermöglicht es, ein Bußgeld für den Fall zu verhängen, dass die von den Betreibern zu erbringenden Nachweise, Nachforderungen, Auskünfte und Kennzahlen nicht, nicht rechtzeitig oder nicht geeignet erbracht werden. Dies ist erforderlich, da ansonsten die hierauf aufbauenden Aufsichts- und Unterstützungsaufgaben des Bundesamtes nicht oder nur kaum umsetzbarem Aufwand durchsetzbar sind. Für die Wahrnehmung der aufsichtsbehördlichen Aufgaben des BSI ist es unabdingbar, dass der die Nachweise der Betreiber ordnungsgemäß und fristgerecht erbracht werden. Denn der tagesaktuelle Überblick über den Stand des deutschlandweiten IT-Sicherheitsniveaus einerseits und über die Entwicklung der laufenden IT-Vorfälle andererseits sind Kernaufgaben des BSI und gerade bei Kritischen Infrastrukturen von höchstem öffentlichen Interesse für die Prävention, Detektion, und Angriffsbewältigung dieses Landes. Diese Aufsicht über die teils hochkomplexen Sicherheitssysteme kann nur sichergestellt werden, wenn das Bundesamt auch die nach § 8a Absatz 3 Satz 1 BSIG zu erbringenden Nachweise von den Betreibern zugeliefert bekommt. Andernfalls müsste eine regelmäßige Überprüfung der Anlagen durch das Bundesamt oder von ihm beauftragte Dritte erfolgen.

Zu Nummer 4

Wie mit § 14 Absatz 1 Nummer 3 BSIG soll mit der erstmaligen Bußgeldbewehrung mit der neuen Nummer 4 (§ 8a Absatz 4 Satz 2 BSIG) gewährleistet werden, dass Auskunftsverlangen besser durchgesetzt werden können, wobei sich Nummer 4 insbesondere auf Auskünfte bei Vor-Ort-Kontrollen bezieht. Auch die Verweigerung des Zurverfügungstellens der erforderlichen Unterlagen und des Betretens der Geschäftsräume ist durch Anordnungen nicht ausreichend sanktionierbar. Wiederum kann sich der Betreiber nach anfänglicher Verweigerung darauf berufen, dass er – erlangt das Bundesamt nachträglich doch Kenntnis von den erforderlichen Dokumenten – jetzt zur angeordneten Handlung nicht mehr gezwungen, die Beugungswirkung des Zwangsgeldes also nicht erforderlich sei. Die Begehung und Prüfung der Anlagen vor Ort ist mit erheblichen personellen Aufwänden verbunden und ganz ursprünglich als Ausnahme für das In-Zweifel-Ziehen unklarer Nachweise und Audits gedacht. Ohne eine auch nachträgliche Sanktionierungsmöglichkeit ist bei Verweigerung nur eine unzureichende Durchsetzung gewährleistet.

Zu Nummer 5

Nach § 14 Absatz 1 Nummer 5 handelt ordnungswidrig, wer die eigene Anlage nicht oder nicht rechtzeitig benennt oder eine Registrierung nicht oder nicht rechtzeitig vornimmt (§ 8b Absatz 3 Satz 1). Dies ist erforderlich, um alle Anlagen zu erfassen und die unverzügliche Weiterleitung wichtiger Sicherheitsinformationen an betroffene Betreiber sicherzustellen. So kann bei Störungen und sonstigen IT-Sicherheitsinformationen, die für die Verfügbarkeit und Funktionsfähigkeit der Betreiber maßgeblich sind, ein verlässlicher, beständiger und schneller Informationsfluss gewährleistet werden. Auch kann der Betreiber hierüber unverzüglich das Lagezentrum des BSI und darüber andere Betreiber Kritischer Infrastrukturen in seiner Branche unabhängig informieren. Die Kontaktstelle ist dabei Anknüpfungspunkt für Meldungen an das Bundesamt einerseits und adressatenspezifische Informationen und Warnungen an die Unternehmen andererseits. Die Sanktionierung ist erforderlich, um im

ENTWURF

Fall eines bundesweiten Störfalls unmittelbar alle potentiell betroffenen Kritischen Infrastrukturen vorzubereiten und etwaige notwendige Schutzmaßnahmen unverzüglich in Gang zu setzen.

Zu Nummer 6

Nach § 14 Absatz 1 Nummer 6 handelt ordnungswidrig, wer nicht sicherstellt, dass die einzurichtende Kontaktstelle jederzeit erreichbar ist. Es handelt sich um eine erstmalige Bußgeldbewehrung einer bereits im BSIG vorhandenen Norm. Diese 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“ im Sinne des § 8b Absatz 3 Satz 4 BSIG, dass Betreiber Kritischer Infrastrukturen über die registrierte Kontaktstelle in der Lage sein müssen, Informationen (Cyber- Sicherheitswarnungen, Lageinformationen etc.) entgegenzunehmen und diese unverzüglich auszuwerten (Bearbeitung der Informationen auf Zuruf). In der Regel werden Informationen während der üblichen Geschäftszeiten versendet. Es ist jedoch nicht auszuschließen, dass in Ausnahmefällen dringende Warnungen auch außerhalb der üblichen Geschäftszeiten (an Feiertagen, Wochenenden oder nachts) versendet werden. Für diese Fälle können bereits existierende dauerhaft erreichbare Stellen in der Organisation, z. B. Pforte, Werkschutz oder sonstige Bereitschaftsdienste, akuten Handlungsbedarf erkennen und ggf. eine Alarmierung bzw. Weiterleitung vornehmen, um die Erreichbarkeit zu gewährleisten.

Zu Nummer 7

Nach § 14 Absatz 1 Nummer 7 kann sanktioniert werden, wenn einem Auskunftsverlangen (§ 8b Absatz 3a Satz 1 BSIG) nicht nachgekommen wird. Dadurch wird die fehlende Mitwirkung bei der Identifizierung als Kritische Infrastruktur mit einem Bußgeld bewehrt. Dies soll die Betreiber dazu anhalten, sich rechtzeitig zu melden und eine lückenlose und nachvollziehbare Erfassung aller deutschen Kritischen Infrastrukturen sicherstellen.

Zu Nummer 8

Durch § 14 Absatz 1 Nummer 8 wird zusätzlich neben § 8b Absatz 4 Satz 1 Nummer 2 erstmalig auch die Nummer 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. Die Meldung aktueller Störfälle ist neben den Nachweisen über den Stand der IT-Sicherungsmaßnahmen in den einzelnen Kritischen Infrastrukturen die zweite kritische Voraussetzung für den Überblick über die IT-Sicherheitslage in Deutschland. Das Bundesamt ist erste unabhängige Anlauf- und Meldestelle für IT-Störungen und -Angriffe und stellt durch deren Vernetzung Bedrohungen für ganze Branchen oder Bereiche in Deutschland fest, um unmittelbar reagieren und bedrohte Betreiber zeitnah warnen zu können. Die Sanktionierung nicht ordnungsgemäßen, insbesondere fehlenden oder verspäteten Meldeverhaltens ist grundlegend für die schnelle und umfassende Reaktionsmöglichkeit auf bundesweite Angriffe oder Störfälle. Nur so kann sichergestellt werden, dass wichtige Meldungen nicht aus wirtschaftlichen oder außenwirkungsbezogenen Erwägungen zurückgehalten oder unterlassen werden. Sie ist auch als Bußgeld erforderlich, um die notwendige Meldemotivation der Betreiber auch durch nachträgliche Sanktionierbarkeit herzustellen, der Verwaltungszwang liefe hier aufgrund der zentralen Bedeutung der Aktualität der Informationen leer.

Zu Nummer 9

Die erstmalige Bußgeldbewehrung des § 8c Absatz 1 Satz 1 durch § 14 Absatz 1 Nummer 9 ergibt sich parallel zu § 8a Absatz 1 Satz 1 BSIG für Anbieter digitaler Dienste.

ENTWURF

Zu Nummer 10

Mit § 14 Absatz 1 Nummer 10 wird die neue Pflicht für Unternehmen im besonderen öffentlichen Interesse aus § 8f Absatz 1 oder 2 in Verbindung mit Absatz 4 BSIG erfasst, dem BSI eine Selbsterklärung ordnungsgemäß vorzulegen. Damit trifft diese abgestuft eine Anzeige und Vorlagepflicht wie die Betreiber Kritischer Infrastrukturen, die entsprechend sanktioniert werden kann.

Zu Nummer 11

Nach § 14 Absatz 1 Nummer 11 handelt ordnungswidrig, wer eine Registrierung eines Unternehmens im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1 und 2 beim Bundesamt nicht oder nicht rechtzeitig vornimmt (§ 8f Absatz 5 Satz 1 Variante 1). Dies ist erforderlich, um alle Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1 und 2 zu erfassen und die unverzügliche Weiterleitung wichtiger Sicherheitsinformationen an die betroffenen Unternehmen sicherzustellen. Außerdem handelt nach § 14 Absatz 1 Nummer 11 ordnungswidrig, wer nicht sicherstellt, dass die nach § 8f Absatz 5 Variante 2 benannte Stelle zu üblichen Geschäftszeiten erreichbar ist. Dies ist erforderlich, um die unverzügliche Weiterleitung wichtiger Sicherheitsinformationen an betroffene Unternehmen sicherzustellen. Die Ordnungsvorschrift hält Unternehmen zur Einhaltung dieser Verpflichtung an. Dabei heißt „zu üblichen Geschäftszeiten erreichbar“ im Sinne des § 8f Absatz 5 Satz 1 BSIG-E, dass Unternehmen im besonderen öffentlichen Interesse werktags zwischen 8 Uhr und 17 Uhr in der Lage sein müssen, Informationen (Cyber-Sicherheitswarnungen, Lageinformationen etc.) entgegenzunehmen und diese unverzüglich auszuwerten (Bearbeitung der Informationen auf Zuruf).

Somit stellt § 14 Absatz 1 Nummer 11 durch die Sanktionierung die verpflichtende Anbindung der Unternehmen im besonderen öffentlichen Interesse an die für Kritische Infrastrukturen bereits bestehenden Warn- und Alarmierungsmechanismen sicher. So kann bei Störungen, die für die Verfügbarkeit und Funktionsfähigkeit dieser Unternehmen maßgeblich sind, ein schneller Informationsfluss gewährleistet und das Lagezentrum des BSI sowie andere potentiell Betroffene unabhängig und unverzüglich informiert werden. Die Kontaktstelle ist dabei Anknüpfungspunkt für Meldungen an das Bundesamt und adressatenspezifische Informationen und Warnungen an die Unternehmen.

Zu Nummer 12

Nach § 14 Absatz 1 Nummer 13 handelt ordnungswidrig, wer nach § 8f Absatz 7 Satz 1 Nummer 1 oder Nummer 2 oder Absatz 8 Satz 1 Nummer 1 oder Nummer 2 meldepflichtige Störungen nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig meldet. Die Vorschrift ist erforderlich, um die zügige und vollständige Meldung von Störungen an das Bundesamt zu gewährleisten, damit dieses im Gegenzug seinen Aufgaben nach § 2 BSIG nachkommen kann sowie andere Unternehmen über sie betreffende Informationen hierzu informieren kann.

Zu Nummer 13

Die Vorschrift dient der Umsetzung der europäischen Vorgaben zu Konformitätsbewertungsstellen, die im Anwendungsbereich des Rechtsakts zur Cybersicherheit, Verordnung (EU) 2019/881 (Cyber Security Act – CSA), sowie des § 9 BSIG tätig werden. Die Sanktionierungsmöglichkeit muss bestehen, um die Tätigkeit von Stellen ohne die erforderliche Befugniserteilung durch das Bundesamt zu unterbinden; das gilt sowohl für nicht erteilte, als auch durch das Bundesamt widerrufene Befugniserteilungen. Die Erforderlichkeit der Sanktionierung ergibt sich im Übrigen aus Artikel 65 der Verordnung (EU) 2019/881.

ENTWURF

Zu Nummer 14

Der § 14 Absatz 1 Nummer 14 ist erforderlich zur Sicherung der Glaubwürdigkeit und Integrität der nach Artikel 56 Absatz 6 der Verordnung (EU) 2019/881 ausgestellten Cybersicherheitszertifikate, indem die Verwendung oder Werbung mit einem nicht bestehenden oder nicht mehr gültigen – z.B. aufgrund Widerruf – Cybersicherheitszertifikat mit dem hier normierten Bußgeld belegt wird. Damit wird gleichermaßen sichergestellt, dass der Widerruf des Zertifikates aufgrund des Nichtvorliegens oder Wegfalls der Voraussetzungen aus den § 9a Absätzen 3 bis 5 dieses Gesetzes effektiv die Weiterverwendung des Zertifikates unterbindet. Die Erforderlichkeit der Sanktionierung ergibt sich im Übrigen aus Artikel 65 der Verordnung (EU) 2019/881.

Zu Nummer 15

Zur Abwendung des Missbrauchs des freiwilligen IT-Sicherheitskennzeichens nach § 9c wird durch § 14 Absatz 1 Nummer 15 sanktioniert, wenn das IT-Sicherheitskennzeichen ohne Freigabe für ein Produkt verwendet wird.

Zu Nummer 16, 17 und 18

Zur Verhinderung, dass EU-Konformitätserklärungen nur entsprechend den Vorgaben der Verordnung (EU) 2019/881 abgegeben und verwendet werden, kann das Bundesamt Verstöße gegen die entsprechenden Vorgaben sanktionieren.

Zur Sicherherstellung der tatsächlich erfolgten Veröffentlichung der Informationen, die sich aus Artikel 55 Absatz 1 Buchstaben a, b, c und d der Verordnung (EU) 2019/881 ergeben, kann das BSI aufgrund § 14 Absatz 1 Nummer 16 im Rahmen seiner Aufsichtsfunktion sanktionieren.

Zur Abwendung der Unterlassung der Informationspflicht, die sich aus Artikel 56 Absatz 8 Satz 1 der Verordnung (EU) 2019/881 ergibt, wird durch §14 Absatz 1 Nummer 17 sanktioniert.

Die Erforderlichkeit der Sanktionierungen ergibt sich im Übrigen aus Artikel 65 der Verordnung (EU) 2019/881.

Zu Absatz 2 und 3

§ 14 Absatz 2 BSIG regelt die Höhe der jeweiligen Bußgelder und entspricht so den europarechtlichen und tatsächlichen Anforderungen. Die Höchstwerte betragen regelmäßig 100.000 Euro, 1 Mio. Euro beziehungsweise 2 Mio. Euro.

Die Androhung des Bußgeldrahmens in Höhe von bis zu 2 Mio. Euro gilt für Verstöße mit unmittelbarer Beeinträchtigung der IT-Sicherheit in Deutschland. Sie soll auch dem erhöhten Unwertgehalt einer Missachtung behördlich angeordneter Maßnahmen gerecht werden. Sie folgt damit den Anforderungen der RL (EU) 2016/1148 (NIS-Richtlinie), wonach die vorgesehenen Sanktionen wirksam, angemessen und abschreckend sein müssen und orientiert sich an den gleichlautenden Vorgaben der DSGVO. Darüber hinaus gilt die Androhung des Bußgeldrahmens in Höhe von bis zu 2 Mio. Euro auch für Sanktionen gegen gewisse Verstöße gegen die Verordnung (EU) 2019/881 und diese begleitenden Vorschriften. Die Androhung des allgemeinen Bußgeldrahmens in Höhe von bis zu 1 Mio. Euro gilt für Pflichten, deren Missachtung zu mittelbaren Beeinträchtigungen der IT-Sicherheit führt. Sie sind zwingende Voraussetzung für die ordnungsgemäße Wahrnehmung der Aufgaben des Bundesamtes zur unabhängigen Prävention und Detektion von Gefahren und die Sicherstellung eines homogenen IT-Sicherheitsniveaus in Deutschland. Der zusätzliche minder schwere Bußgeldrahmen in Höhe von bis zu 100.000 Euro umfasst Verstöße gegen die formalen Voraussetzungen zur Durchführung der übertragenen Aufgaben.

ENTWURF

Die vorgesehenen Bußgeldhöhen müssen sich an dem europarechtlichen Rahmen der NIS-Richtlinie, der Verordnung (EU) 2019/881 sowie der DSGVO messen lassen. Die in § 14 geregelten Bußgelder beziehen sich auch auf die Wahrnehmung der Aufsichtsaufgabe des Bundesamtes über die Betreiber Kritischer Infrastrukturen und Anbieter Digitaler Dienste. Diese Aufgabe folgt aus unmittelbar der Umsetzung der NIS-RL-Richtlinie. Nach Artikel 21 der NIS-RL sind die Mitgliedstaaten dazu verpflichtet, sicherzustellen, dass die Bestimmungen der Richtlinie Anwendung finden. Dafür haben sie Sanktionen vorzusehen, die "wirksam, angemessen und abschreckend" sind. Welcher Rahmen EU-rechtlich für eine solche Wirkung als passend angesehen wird, hat der europäische Gesetzgeber explizit in Artikel 83 DSGVO zum Ausdruck gebracht. Danach müssen in gleichem Wortlaut Geldbußen, so sie denn für dieselben Adressaten "wirksam, verhältnismäßig und abschreckend" sein sollen, nach Artikel 83 Absätze 4 und 5 bis zum Rahmen von 10 beziehungsweise 20 Mio. Euro ermöglicht werden. Den Höchstrahmen in Höhe von 20 Mio. Euro erreichen zu können, ist insbesondere erforderlich im Hinblick auf die im Bereich der KRITIS-Betreibern umsatzstarken Konzerne, die nur mit hohen Bußgeldandrohungen zu ordnungsgemäßem Verhalten angehalten werden können. Dies wird für den Rahmen bis 2 Mio. Euro mittels des Verweises auf § 30 Absatz 2 Satz 3 OWiG gewährleistet. Dadurch verzehnfacht sich der regelmäßige Höchstrahmen, wenn sich die Geldbuße gemäß § 30 Absatz 1 OWiG gegen juristische Personen und Personenvereinigungen richtet, auf 20 Mio. Euro. Dadurch kann auf nationaler Ebene eine hinreichend effektive Motivationswirkung zur Befolgung der gesetzlichen Vorschriften erreicht und der europarechtlichen Wertung entsprochen werden.

Die Bußgelder orientieren sich an der Wirtschaftskraft der Adressaten und werden entsprechend angepasst. Nur so können die Sanktionen generalpräventiv wirken. Andernfalls besteht die Gefahr und Praxis, dass einzelne Unternehmen sich wegen einer nur geringen Bußgeldhöhe gegen die Erfüllung ihrer gesetzlichen Pflicht entscheiden, weil die Zahlung eines Bußgeldes nach Abwägung der möglichen Aufwände für das Unternehmen für sie finanziell attraktiver ist. Da sich die Verpflichtungen nur auf die Betreiber und Anbieter Digitaler Dienste entsprechend kritischer Größe oder deren Hersteller beziehen, sind die bisherigen Bußgelder verglichen zur Wirtschaftskraft zu gering, um eine lenkende Wirkung erzielen zu können.

Ein Verstoß gegen die funktionelle Absicherung der für Deutschland essentiellen Infrastrukturen, Dienste und Unternehmen muss zudem ebenso schwerwiegend sanktioniert werden können, wie ein datenschutzrechtlicher Verstoß, z. B. durch den Versand von Spam-E-Mails. Andernfalls droht ein Wertungswiderspruch.

Zu Absatz 4

Die Sonderregelung schließt aus, dass gegen die für das BSIG legaldefinierten Institutionen der Sozialen Sicherung Bußgelder verhängt werden, sofern diese nach der Rechtsverordnung in § 10 Absatz 1 BSIG als Kritische Infrastruktur eingestuft sind. Diese Institutionen der Sozialen Sicherung unterliegen als KRITIS-Betreiber der gesetzlichen Pflicht, angemessene technische und organisatorische Maßnahmen zur IT-Sicherheit umzusetzen, (§ 8a Absatz 1), alle zwei Jahre entsprechende Nachweise zu erbringen (§ 8a Absatz 3), sich beim Bundesamt zu registrieren und eine Kontaktstelle zu benennen (§ 8b Absatz 3) und Störungen an das BSI zu melden (§ 8b Absatz 4). Für die Institutionen der Sozialen Sicherung stehen mit unmittelbaren Aufsichtsmaßnahmen der Aufsichtsbehörde geeignetere Durchsetzungsmittel zur Verfügung (vgl. § 89 Viertes Buch Sozialgesetzbuch).

Für Institutionen der Sozialen Sicherung in Trägerschaft des Bundes gilt nach Satz 2 eine Einvernehmensregelung. Das Einvernehmen bezieht sich auf das „ob“ der geeigneten Maßnahme, vorbereitend legt das Bundesamt der zuständigen Aufsichtsbehörde die Ordnungswidrigkeit dar und gibt Informationen zu Abhilfemöglichkeit oder Schwere des Verstoßes. Die Auswahl des Aufsichtsmittels (das „wie“) verbleibt bei der zuständigen Aufsichtsbehörde. Im Unterschied zu Satz 2 gilt für Institutionen der Sozialen Sicherung in Trägerschaft der Länder nach Satz 3 eine Benehmensregelung. Zur Gewährleistung einer effektiven

ENTWURF

Sanktionierung ist in Satz 4 für beide Fälle eine Information des Bundesamtes durch die zuständige Aufsichtsbehörde vorgesehen.

Zu Artikel 2 (Änderungen des Telekommunikationsgesetzes)

Zu Nummer 1

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

Zu Nummer 2

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

Zu Buchstabe a

Entsprechend der Inhaltsübersicht ist auch die Überschrift der Regelung anzupassen.

Zu Buchstabe b

Zu Doppelbuchstabe aa

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

Zu Doppelbuchstabe bb

Bislang unterliegen Netz- und Systemkomponenten keinerlei Zertifizierungsverpflichtungen. Künftig sind kritische Komponenten im Sinne des § 2 Absatz 13 BSIG zu überprüfen und zu zertifizieren. Nach § 2 Absatz 13 Satz 2 BSIG werden die kritischen Komponenten für Betreiber Kritischer Infrastrukturen, die ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, durch den Katalog von Sicherheitsanforderungen nach § 109 Absatz 6 TKG näher bestimmt. Die Ermächtigungsgrundlage für die Festlegung des Katalogs wird insofern angepasst. Einzelheiten zum Zertifizierungsverfahren werden – wie bisher – im BSIG geregelt.

Zu Doppelbuchstabe cc

Anpassung an die aktuelle Rechtslage.

Zu Buchstabe c

Die Neufassung der Nummer 3 konkretisiert die im Sicherheitskonzept vorzunehmenden Darstellungen der Netzbetreiber und Diensteerbringer. Dabei sind künftig bei der Erstellung des Sicherheitskonzepts deutliche Bezüge zu den Vorgaben des Sicherheitskatalogs nach

ENTWURF

Absatz 6, die die Verpflichtungen aus den Absätzen 1 und 2 näher ausgestalten, aufzunehmen. In Fällen, in denen der Sicherheitskatalog lediglich ein Sicherheitsziel vorgibt, ohne eine konkrete Schutzmaßnahme vorzuschreiben ist darzulegen, dass durch die jeweils gewählte Maßnahme das vorgegebene Sicherheitsziel vollumfänglich erreicht wird. Dies führt zu mehr Transparenz hinsichtlich der getroffenen technischen und organisatorischen Schutzmaßnahmen und stellt eine Erleichterung bei der Überprüfung der Sicherheitskonzepte dar.

Zu Buchstabe d

Es erfolgt die Anpassung der offiziellen Bezeichnung der Europäischen Agentur für Cyber-Sicherheit (ENISA). Diese hat seit Juli 2019 eine neue Bezeichnung.

Zu Buchstabe e

Zu Doppelbuchstabe aa

Absatz 6 Satz 1 bildet die Ermächtigungsgrundlage für den Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten. Dieser konkretisiert die nach den Absätzen 1 und 2 zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen und bildet gleichzeitig die Grundlage für die von den Verpflichteten zu erstellenden Sicherheitskonzepte. Vor dem Hintergrund der fortschreitenden Technik und der Weiterentwicklung der Netze, die zu einer zunehmenden Kritikalität führt, ist es angezeigt, die Ermächtigungsgrundlage für den Sicherheitskatalog anzupassen und so den von den zuständigen Behörden festzulegenden Inhalt ausdrücklich im Gesetz zu verankern. Wie bislang auch sind die Einzelheiten der nach den Absätzen 1 und 2 zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen festzulegen. Dabei stellt die Regelung erstmals darauf ab, dass differenzierte Vorgaben in Anbetracht verschiedener Gefährdungspotenziale aufzustellen sind. Der Umfang der zu ergreifenden Schutzmaßnahmen nimmt mit steigendem Gefährdungspotenzial zu.

Darüber hinaus sind im Sicherheitskatalog künftig Vorgaben zur Bestimmung der kritischen Komponenten im Sinne von § 2 Absatz 13 BSIG festzulegen. Diese Regelung flankiert die in Absatz 2 neu geschaffene Zertifizierungspflicht für kritische Komponenten.

In Anbetracht der Weiterentwicklung der öffentlichen Telekommunikationsnetze und dem überragenden Stellenwert, den diese Netze für Gesellschaft, Wirtschaft und Verwaltung einnehmen, müssen für Netze mit erhöhtem Gefährdungspotenzial höchste Sicherheitsanforderungen gelten. Zur Schaffung von Rechtssicherheit und zur Beseitigung von Abgrenzungsschwierigkeiten ist künftig im Sicherheitskatalog festzulegen, wer als Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial einzustufen ist. Dabei ist eine Benennung konkreter Unternehmen möglich, jedoch nicht zwingend. Die Festlegung kann auch anhand von abstrakten technischen Parametern erfolgen, so dass Unternehmen, die diese Parameter erfüllen als Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial einzustufen sind.

Zu Doppelbuchstabe bb

Bislang bestand keine gesetzliche Regelung zur Umsetzungsfrist der Vorgaben des Sicherheitskatalogs. Zur Klarstellung wird in Absatz 6 aufgenommen, dass die Vorgaben des Katalogs spätestens ein Jahr nach dessen Inkrafttreten zu erfüllen sind. Es handelt sich dabei um eine übliche technische Umsetzungsfrist. Abweichende Umsetzungsfristen können im Katalog selbst festgelegt werden.

ENTWURF

Zu Buchstabe f

Zu Doppelbuchstabe aa

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

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

Zu Doppelbuchstabe bb

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

Zu Doppelbuchstabe cc

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

Zu Nummer 3

Es handelt sich um eine Folgeänderung zu Artikel 1 Nummer 7 (§ 5c).

Zu Artikel 3 (Änderung des Telemediengesetzes)

Zu Nummer 1

Zu § 15d (Meldepflicht bei unrechtmäßiger Übermittlung oder unrechtmäßiger Kenntniserlangung von Daten)

Zu Absatz 1

Die Regelung bezieht sich auf eine unrechtmäßige Übermittlung oder unrechtmäßige Kenntniserlangung von Daten beim Diensteanbieter. Abgestellt wird wiederum auf ein strafbares Verhalten nach §§ 202a bis 202d des Strafgesetzbuches sowie die Betroffenheit einer großen Zahl von Personen, eines Datenbestands von großem Ausmaß oder eines Datenbestands von Behörden oder Einrichtungen des Bundes oder deren Mitgliedern oder sicherheitsempfindlicher Stellen von lebenswichtigen Einrichtungen, bei deren Ausfall oder Zerstörung ein erhebliche Bedrohung für die Gesundheit oder das Leben von Menschen zu befürchten ist oder die für das Funktionieren des Gemeinwesens unverzichtbar sind. Konkrete tatsächliche Anhaltspunkte für eine unrechtmäßige Übermittlung oder unrechtmäßige Kenntniserlangung von Daten beim Diensteanbieter sind ausreichend. Die Norm knüpft die Verpflichtung zur Unterrichtung des Bundeskriminalamts an eine positive Kenntniserlangung des Providers. Auf welche Weise diese Kenntniserlangung erfolgt, ist unerheblich (zum Beispiel eigene Recherche oder Hinweise von Nutzern). Zudem wird klargestellt, dass den Diensteanbieter keine allgemeine Überwachungs- oder Nachforschungspflicht trifft; § 7 Absatz 2 TMG bleibt unberührt.

ENTWURF

Eine große Zahl von Personen liegt regelmäßig vor, wenn 1000 Personen oder mehr betroffen sind. Dem Diensteanbieter steht es jedoch frei, auch bei einer geringeren Anzahl von Betroffenen eine Meldung an das Bundeskriminalamt zu übersenden. Dies bezieht sich jedoch nur auf Daten des Telemediendiensteanbieters. Bei Daten, die unrechtmäßig an den Telemediendiensteanbieter übermittelt wurden, liegt eine große Zahl von Personen regelmäßig vor, wenn 100.000 Personen oder mehr betroffen sind. Nach kriminalpolizeilicher Erfahrung liegen qualitative Unterschiede in der unrechtmäßigen Kenntniserlangung bzw. unrechtmäßigen Übermittlung von Daten des Diensteanbieters zu der unrechtmäßigen Übermittlung von Daten an den Diensteanbieter. Im letzteren Fall handelt es sich in der Regel um Daten, die aus bereits bekannten Beständen erneut zusammengestellt wurden bzw. Doppelungen oder um Daten, die nicht valide sind.

Welches Ausmaß an Datenmengen als groß beziffert wird, kann sich in den nächsten Jahren erheblich verändern. Die Mengen von Daten wachsen typischerweise exponentiell an. Laut einer IDC-Studie zum Datenwachstum verdoppelt sich das Datenvolumen alle zwei Jahre (Quelle: Klaus Manhart: IDC-Studie zum Datenwachstum in CIO, 12.07.2011, abgerufen am 09.09.2020, 16:15 Uhr). Ein im Jahr 2020 als ein „großes Datenvolumen“ bezeichneter Datenbestand kann möglicherweise im Jahr 2025 als „durchschnittlich“ angesehen werden. Für das Jahr 2020 lässt sich jedoch festhalten, dass ein „Datenbestand von großem Ausmaß“ üblicherweise mit 10 Gigabyte zu beziffern ist.

Die Meldepflicht der Diensteanbieter nach Absatz 1 schließt Fälle, bei denen eine unrechtmäßige Übermittlung oder unrechtmäßige Kenntniserlangung von Daten über den Diensteanbieter stattgefunden hat, ein. Absatz 1 bezieht sich auf die Aufgabenwahrnehmung des Bundeskriminalamtes als Zentralstelle nach § 2 Absatz 1 BKAG.

Regelungsadressat der Norm sind Diensteanbieter, bei denen die Daten gespeichert, zwischengespeichert, übertragen, veröffentlicht oder weitergegeben werden.

Durch Absatz 1 sowie die Anknüpfung an die Straftatbestände des §§ 202a bis 202d des Strafgesetzbuches wird klargestellt, dass der gewählte Datenbegriff weit ist und sämtliche Daten, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar sind, erhält, umfasst. Geschützt werden damit nicht nur die personenbezogenen Daten gemäß Artikel 4 Nummer 1 Datenschutz-Grundverordnung. Daneben sind auch Betriebs- und Geschäftsgeheimnisse umfasst (§ 2 Ziffer 1 Geschäftsgeheimnisgesetz).

Das Bundeskriminalamt erhält die Daten als Zentralstelle und kann die erlangten Hinweise schnell bewerten und erforderliche Folgemaßnahmen, etwa die Information zuständiger Dienststellen bei den Ländern, einleiten.

Die Meldepflicht für die Diensteanbieter genügt den Verhältnismäßigkeitsanforderungen, da sie sich auf die in der Regelung bestimmten Fälle beschränkt. Diese Fälle sind durch eine große Anzahl der möglicherweise betroffenen Personen, der Art der Daten oder des Schädigungspotentials etwa für die Sicherheit und den Bestand des Staates gekennzeichnet.

Zu Absatz 2

Das Bundeskriminalamt benötigt sämtliche relevante Daten, die für die Beurteilung des jeweiligen Einzelfalls und davon abhängigen Folgemaßnahmen der jeweils zuständigen Behörden auf dem Gebiet der Strafverfolgung und Gefahrenabwehr maßgeblich sind. Eine genaue Definition bzw. Eingrenzung der Art der Daten ist nicht möglich. Das Bundeskriminalamt muss vielmehr aufgrund der übermittelten Daten in die Lage versetzt werden, den Sachverhalt ausreichend anzureichern und den zuständigen Strafverfolgungs- bzw. Gefahrenabwehrbehörden abverfügen zu können. Falls vorhanden sind alle Daten zu übermitteln, die zum Tatgeschehen gehören und damit Hinweise über die „Spuren des Eindringens“ und

ENTWURF

„Spuren des Abfließens“ der Daten liefern können. Es ist wichtig beurteilen zu können, welche Motivation hinter dem Abfluss steckt, um gegebenenfalls gefahrenabwehrrechtlich tätig werden zu können.

Im Zusammenhang mit Daten des Telemediendiensteanbieters, von denen unrechtmäßig Kenntnis erlangt wurde bzw. die unrechtmäßig übermittelt wurden, betreffen diese Daten regelmäßig die Bestandsdaten, wie IP-Adressen, E-Mail-Adressen, Namen und Anschriften der Geschädigten bzw. Tatverdächtigen, Passwörter, etc.

Die Meldung an das Bundeskriminalamt erfolgt über eine elektronische Schnittstelle. Eine solche besteht bereits für Meldungen nach dem Netzwerkdurchsetzungsgesetz und kann daher auf die Meldungen erweitert werden.

Zu Nummer 2

Die Bußgeldbewehrung dient der Sicherstellung der unverzüglichen Unterrichtung des Bundeskriminalamtes von der unrechtmäßigen Kenntniserlangung durch den Diensteanbieter zur Ermöglichung der Koordinierung der Ermittlungstätigkeiten und der Strafverfolgung durch die zuständigen Ermittlungs- und Justizbehörden der Länder.

Zu Artikel 4 (Änderung des Gesetzes über die Elektrizitäts- und Gasversorgung (EnWG))

Durch die Änderung wird die in § 8a Absatz 1a BSIG neu eingeführte Pflicht für Betreiber Kritischer Infrastrukturen, Systeme zur Angriffserkennung einzusetzen, auch analog für Betreiber von Energieversorgungsnetzen und solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 BSIG als Kritische Infrastruktur bestimmt wurden, eingeführt.

In § 11 Absatz 1f wird für Betreiber Kritischer Infrastrukturen, die Energieversorgungsnetze oder Energieanlagen betreiben, eine Pflicht zum Nachweis der Anforderungen aus § 11 Absatz 1d EnWG an das BSI eingeführt. Im Falle von Mängeln in der Umsetzung der Anforderungen oder Mängeln in den Nachweisdokumenten wird das BSI befugt, im Einvernehmen mit der Bundesnetzagentur die Beseitigung der Mängel zu verlangen.

Zu Artikel 5 (Änderung der Außenwirtschaftsverordnung)

Zu Nummer 1 und 2

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

Zu Artikel 5 (Änderung des Zehnten Buches Sozialgesetzbuch)

Mit der Ergänzung wird klargestellt, dass nicht nur für die Kontrollaufgaben des Bundesamtes Sozialdaten gespeichert und genutzt und in Verbindung mit § 69 Absatz 5 des Zehnten Buches Sozialgesetzbuch übermittelt werden können, sondern auch soweit dies für die Wahrung sowie unter Umständen für die Wiederherstellung der Sicherheit und Funktionsfähigkeit eines informationstechnischen Systems erforderlich ist. Damit wird gewährleistet, dass die Sozialleistungsträger, wenn sie Betreiber einer Kritischen Infrastruktur sind, sich bei der Wiederherstellung der Sicherheit oder Funktionsfähigkeit ihres informationstechnischen Systems in herausgehobenen Fällen zur Unterstützung an das Bundesamt wenden können. Soweit sich aus dem BSIG Pflichten zur Mitwirkung für Sozialleistungsträger ergeben, bei denen es auch zur Übermittlung von Sozialdaten an das BSI kommen kann, folgt die sozialdatenschutzrechtliche Übermittlungsbefugnis aus § 69 Absatz 5 des Zehnten Buches Sozialgesetzbuch. Die dem Bundesamt übermittelten Sozialdaten unterliegen gemäß § 35 Absatz 1 des Ersten Buches Sozialgesetzbuch dem Sozialgeheimnis.

ENTWURF

Zu Artikel 6 (Evaluierung)

Gemäß Artikel 10 des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17. Juli 2015 wären die §§ 2 Absatz 10, 8a bis 8c und § 8e sowie § 10 BSIG vier Jahre nach Inkrafttreten der Verordnung zur Bestimmung Kritischer Infrastrukturen zu evaluieren gewesen. Diese Rechtsverordnung lag mit Inkrafttreten des zweiten Korbs (in dem Regelungen für die Sektoren Finanzen, Transport und Verkehr sowie Gesundheit getroffen wurden) am 30. Juni 2017 erstmals vollständig vor. Eine Evaluierung hätte demnach im Juni 2021 zu erfolgen. Bereits vor Durchführung dieser Evaluierung haben Erfahrungen aus der Praxis jedoch bereits umfangreichen Änderungsbedarf am BSIG angezeigt, der sich teilweise auch direkt auf die zu evaluierenden Vorschriften bezieht. Dieser Änderungsbedarf wird mit dem vorliegenden Gesetz umgesetzt und die zu evaluierenden Vorschriften werden dabei teilweise angepasst. Zudem tritt zu den Sektoren der Kritischen Infrastrukturen der Sektor Siedlungsabfallentsorgung hinzu. Diese Änderungen könnten im Rahmen einer Evaluierung im Sommer 2021 noch nicht mit ausreichender Erfahrungsgrundlage evaluiert werden, sodass es zu einer unnötigen und unwirtschaftlichen Doppelevaluierung käme. Zudem würde eine Evaluierung nach Art. 10 des IT-Sicherheitsgesetzes von 2015 auch Vorschriften evaluieren, die in der damals eingeführten Form dann nicht mehr der aktuellen Rechtslage entsprächen. Damit könnte der Evaluierungszweck, Verbesserungsmöglichkeiten der geltenden Rechtslage aufzuzeigen, nicht mehr erreicht werden. Die in Artikel 10 IT-Sicherheitsgesetz vorgesehene Evaluierung wird daher mit diesem Gesetz auf einen Zeitpunkt verschoben, zu dem bereits eine ausreichende Erfahrungsgrundlage für eine Evaluierung besteht und zudem entsprechend der Neufassung des BSIG aktualisiert.

Zu Artikel 7 (Inkrafttreten)

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

ENTWURF