Bundesrat **Drucksache** **323/26**

29.05.26

In - DS - R - Wi

Gesetzentwurf
der Bundesregierung

Entwurf eines Gesetzes zur Stärkung der Cybersicherheit

A. Problem und Ziel

Cyberangriffe in Deutschland nehmen in Qualität und Quantität zu. Deutschland als führende Wirtschaftsnation in Europa ist verstärkt im Fokus auch hochprofessioneller Cyberangriffe mit großem Wirkpotential. Angesichts der geopolitischen Lage gewinnen auch hybride Bedrohungen zunehmend an Bedeutung.

Der Krieg in der Ukraine verdeutlicht, wie essentiell Cybersicherheit für einen modernen Staat wie Deutschland ist. Die Gewährleistung einer verlässlichen und sicheren Nutzung der Informationstechnologie und der zugrundeliegenden Kommunikationsinfrastruktur ist essentielle Voraussetzung für das Funktionieren des Gemeinwesens. Deutschlands wirtschaftlicher Erfolg und gesellschaftlicher Zusammenhalt sowie die nationale Sicherheit sind mit der Gewährleistung von Cybersicherheit untrennbar verbunden. Angriffe im Cyberraum überwinden mühelos Landes- oder Zuständigkeitsgrenzen und können sich dadurch auf sämtliche Lebensbereiche und Sektoren einschließlich der Kommunikationsinfrastruktur insgesamt auswirken. Gezielte Angriffe auf kritische Infrastrukturen und wichtige Unternehmen, Aktionen von Cyberkriminellen oder Angriffe auf bzw. Sabotage von staatlichen Strukturen sind geeignet, die Funktionsfähigkeit des Gemeinwesens, der Wirtschaft und des Staats- und Verwaltungswesens massiv und anhaltend zu beeinträchtigen.

Dieser sicherheitspolitischen Herausforderung kann nur begegnet werden, indem die Erkennung und Abwehr von Cyberangriffen ausgebaut wird und hierzu wirksame, angemessene und rechtsklare gesetzliche Grundlagen geschaffen werden. Die Aufklärung und die Detektion konkreter Angriffe und langfristig laufender Angriffskampagnen müssen verbessert und die Detektion konkreter Vorbereitungshandlungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) ausgebaut werden. Insbesondere gegen groß angelegte Cyberangriffe mit großem Schadenspotential bieten präventive Maßnahmen in den eigenen IT-Systemen alleine allerdings keinen hinreichenden Schutz. Es müssen daher für die Polizeien des Bundes und das BSI ergänzend Möglichkeiten zur Unterbindung solcher Cyberangriffe geschaffen werden, um gravierende Folgeschäden abwenden oder minimieren zu können.

B. Lösung

Mit Anpassungen im BSI-Gesetz (BSIG) wird dem BSI ermöglicht, die Resilienz der Informationstechnik der Bundesverwaltung im Cyberraum zu erhöhen und die Erkenntnis-

---

Fristablauf: 10.07.26

besonders eilbedürftige Vorlage gemäß Artikel 76 Absatz 2 Satz 4 GG

Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln
Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0720-2946

lage zu verbessern. Des Weiteren erhalten die Polizeien des Bundes im Bundeskriminalamtsgesetz (BKAG) und im Bundespolizeigesetz (BPolG) die notwendigen Befugnisse, um eine zukunftsfähige Cyberabwehr aufzubauen.

Die bestehenden Möglichkeiten des BSI, schädlichen Datenverkehr umzuleiten, werden an die geänderten Nutzungsbedingungen angepasst, indem die bestehenden Anordnungsbefugnisse auf weitere zentrale Diensteanbieter erweitert werden. Zugleich werden die Möglichkeiten verbessert, auf maliziöse Domains, die die Bundesverwaltung tangieren, zu reagieren. Zudem wird der Einsatz von Incident Response Teams zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme auch in Fällen des so genannten Prepositionings (d.h. das vorbereitende Platzieren von Hintertüren und Angriffsstrukturen in IT-Systemen) klar geregelt. Ferner wird eine Rechtsgrundlage dafür geschaffen, die für den Betrieb von Angriffserkennungssystemen und die Einschätzung der aktuellen Bedrohungslage erforderliche Datengrundlage durch entsprechende Auskunftsersuchen zu technischen Informationen zu verbessern. Komplementär hierzu soll die Ausbreitung maliziöser Infrastruktur eingedämmt werden, indem Endnutzern ein optionaler Schutz vor maliziösen Domains bereitgestellt wird und, wie bisher bereits Telekommunikationsanbieter, auch Anbieter digitaler Dienste verpflichtet werden, Informationen des BSI über konkrete Gefahren, die ihre Kunden betreffen, an diese weiterzugeben.

Für das Bundeskriminalamt (BKA) und die Bundespolizei werden klare Befugnisse geschaffen, um Cyberangriffe abzuwehren. Dazu gehören insbesondere Befugnisse zur Untersagung des Betriebs informationstechnischer Systeme, zur Umleitung, Einschränkung oder Unterbindung von Datenverkehr sowie zum Auslesen, Löschen und Verändern von gefahrgegenständlichen Daten in informationstechnischen Systemen. Diese neu geschaffenen Befugnisse werden es den Polizeien des Bundes ermöglichen, zusammen mit den bereits bestehenden polizeilichen Befugnissen wie z.B. der Sicherstellung von Servern, eine wirksame Gefahrenabwehr gegen Cyberangriffe umzusetzen.

Die neugeschaffenen Befugnisse erhält das BKA für bereits bestehende gefahrenabwehrrechtliche Aufgaben sowie für die neuen Aufgaben im Bereich der Abwehr von Gefahren durch Angriffe auf die Sicherheit in der Informationstechnik.

Die Bundespolizei erhält diese Befugnisse für alle ihre gefahrenabwehrrechtlichen Aufgaben, nicht für ihre Strafverfolgungsaufgaben.

C. Alternativen

Keine.

D. Haushaltsausgaben ohne Erfüllungsaufwand

Für das BKA entsteht ein Bedarf von 49 Beschäftigten im höheren Dienst und 215 im gehobenen Dienst und damit korrespondierend ein jährlicher finanzieller Bedarf i. H. v. 33.94 Millionen Euro. Zudem entsteht ein jährlicher Sachmittelbedarf von 5 Millionen Euro für die Beschaffung von Hard- und Softwareprodukten sowie Betriebs-, Wartungs- und Pflegekosten der technischen Umgebung.

Beim BSI entsteht für die Wahrnehmung der durch dieses Gesetz zugewiesenen Aufgaben ein jährlicher Mehrbedarf aufwachsend bis zum Jahr 2030 in Höhe von rund 3 Millionen Euro für 21 Stellen (13 hD; 7 gD; 1 mD). Davon entfallen rund 2,3 Millionen Euro auf Personalkosten und rund 0,7 Millionen Euro auf personalnahe Sachkosten.

Der Bundespolizei entsteht über die Jahre 2027 bis 2031 ein aufwachsender jährlicher finanzieller Mehrbedarf in Höhe von rund 14,6 Millionen Euro für insgesamt 90 Planstellen (25 hD; 62 gD; 3 mD). Durch die gesetzliche Änderung entstehen einmalige investive

Sachkosten in Höhe von 2,5 Millionen Euro sowie ab Anschaffung jährliche anfallende Kosten in Höhe von 2,3 Millionen. Euro für Hardware, Lizenzen, Betrieb- und Wartung.

Der mit der Aufgabenwahrnehmung verbundene Erfüllungsaufwand erfordert eine gesonderte haushälterische Vorsorge, da die herausragenden und strukturell verankerten Aufgaben im Rahmen einer reinen Priorisierung bestehender Tätigkeiten durch die Bundespolizei nicht angemessen umgesetzt werden können.

Der Mehrbedarf an Sach- und Personalmitteln sowie an Planstellen und Stellen für BSI, BKA und die BPOL soll im Einzelplan 06 ausgeglichen werden.

E. Erfüllungsaufwand

Das geplante Reglungsvorhaben dient im Wesentlichen der Abwehr erheblicher Gefahren im Bereich der IT-Sicherheit und ist daher von der „One in, one out"-Regel (sog. „Bürokratiebremse") ausgenommen.

E.1 Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

E.2 Erfüllungsaufwand für die Wirtschaft

Dem Normadressat Wirtschaft entsteht durch das geplante Regelungsvorhaben ein laufender Erfüllungsaufwand in Höhe von ca. 10 Millionen Euro und einmaliger Erfüllungsaufwand in Höhe von ca. 4,4 Millionen Euro.

Davon unterfallen 282.000 Euro auf Bürokratiekosten aus Informationspflichten.

E.3 Erfüllungsaufwand der Verwaltung

Dem Normadressaten Verwaltung entsteht durch das geplante Regelungsvorhaben ein laufender Erfüllungsaufwand in Höhe von 35 Millionen Euro sowie ein einmaliger Erfüllungsaufwand in Höhe von 19,61 Millionen Euro auf Ebene des Bundes.

F. Weitere Kosten

Durch die im Gesetz für einzelne polizeiliche Befugnisse vorgesehenen richterlichen Anordnungen entstehenden den zuständigen Amtsgerichten Erfüllungsaufwände, beispielsweise für das BKA dem Amtsgericht Wiesbaden.

Auswirkungen auf Einzelpreise und das allgemeine Preisniveau, insbesondere auf die Verbraucherpreise, sind nicht zu erwarten.

Bundesrat **Drucksache** **323/26**

29.05.26

In - DS - R - Wi

Gesetzentwurf
der Bundesregierung

Entwurf eines Gesetzes zur Stärkung der Cybersicherheit

Bundesrepublik Deutschland
Der Bundeskanzler

Berlin, 29. Mai 2026

An den
Präsidenten des Bundesrates
Herrn Bürgermeister
Dr. Andreas Bovenschulte

Sehr geehrter Herr Bundesratspräsident,

hiermit übersende ich gemäß Artikel 76 Absatz 2 Satz 4 des Grundgesetzes den von der Bundesregierung beschlossenen

Entwurf eines Gesetzes zur Stärkung der Cybersicherheit

mit Begründung und Vorblatt.

Der Gesetzentwurf ist besonders eilbedürftig, um ein zügiges Inkrafttreten des Gesetzes zu ermöglichen. Angesichts der hohen Bedrohungslage gegen gezielte (staatliche) Cyberoperationen mit großem Schadenspotenzial ist es dringend geboten, dass Sicherheitsbehörden in die Lage versetzt werden, bei schwerwiegenden Angriffen auch aktiv verhindern, stoppen oder zumindest abmildern zu können.

Federführend ist das Bundesministerium des Innern.

Fristablauf: 10.07.26
besonders eilbedürftige Vorlage gemäß Artikel 76 Absatz 2 Satz 4 GG

Die Stellungnahme des Nationalen Normenkontrollrates gemäß § 6 Absatz 1 NKRG ist als Anlage beigefügt.

Mit freundlichen Grüßen
Friedrich Merz

Entwurf eines Gesetzes zur Stärkung der Cybersicherheit[1]

Vom ...

Der Bundestag hat mit Zustimmung des Bundesrates das folgende Gesetz beschlossen:

Artikel 1

Änderung des Bundespolizeigesetzes

Das Bundespolizeigesetz vom … [Artikel 1 des Entwurfs eines Gesetzes zur Modernisierung des Bundespolizeigesetzes, Bundestagsdrucksache 21/3051], das durch … [Artikel 2 des Entwurfs des Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit, Bundesrat-Drucksache 259/26] geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach der Angabe zu § 41 die folgende Angabe eingefügt:

   „§ 41a Besondere Abwehrmaßnahmen gegen Angriffe auf die Sicherheit in der Informationstechnik“.

2. Nach § 41 wird der folgende § 41a eingefügt:

„§ 41a

Besondere Abwehrmaßnahmen gegen Angriffe auf die Sicherheit in der Informationstechnik

(1) Zur Erfüllung ihrer Aufgaben nach § 1 Absatz 3 bis 5 sowie den §§ 2 bis 8 kann die Bundespolizei folgende besondere Abwehrmaßnahmen ergreifen, um eine Gefahr durch einen Angriff auf die Sicherheit in der Informationstechnik durch Verwirklichung von Straftaten nach den §§ 202a, 202b, 202c, 202d, 263a, 303a und 303b des Strafgesetzbuchs abzuwehren:

1. die Untersagung des Betriebs eines informationstechnischen Systems, von dem eine vorgenannte Gefahr ausgeht,

2. die Umleitung von Datenverkehr, von dem eine vorgenannte Gefahr ausgeht, an eine von der Bundespolizei vorgegebene Zieladresse und dessen Aufzeichnung oder dessen Einschränkung oder Unterbindung auch ohne Wissen der Betroffenen und

3. das Auslesen, Löschen oder Verändern gefahrgegenständlicher Daten in dem informationstechnischen System, von dem eine vorgenannte Gefahr ausgeht, auch durch Eingriff mit technischen Mitteln und ohne Wissen der Betroffenen.

---

[1] Artikel 4 dieses Gesetzes notifiziert gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

Besondere Abwehrmaßnahmen nach Satz 1 Nummer 3, die ohne Einwilligung der Betroffenen durch Eingriff in private informationstechnische Systeme eine Datenerhebung ermöglichen, dürfen nur unter den Voraussetzungen der Absätze 5 bis 8 durchgeführt werden.

(2) Gefahrgegenständliche Daten im Sinne des Absatzes 1 Satz 1 Nummer 3 sind die Daten von Schadprogrammen oder sonstigen informationstechnischen Angriffswerkzeugen, einschließlich Steuerungs- oder Protokolldateien, und Spuren, die technisch mit dem Angriff verbunden sind, sowie Daten, die selbst Gegenstand eines Angriffs auf die Sicherheit in der Informationstechnik sind, insbesondere Daten, die durch diesen Angriff an ein informationstechnisches System weitergeleitet werden oder wurden.

(3) Die besonderen Abwehrmaßnahmen nach Absatz 1 Satz 1 dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden.

(4) Bei den besonderen Abwehrmaßnahmen nach Absatz 1 Satz 1 Nummer 3 ist sicherzustellen, dass

1. technische Vorkehrungen, soweit dies möglich ist, getroffen werden, damit das Auslesen, Löschen und Verändern auf gefahrgegenständliche Daten beschränkt wird,

2. die in den informationstechnischen Systemen vorgenommenen Veränderungen bei Beendigung der Maßnahme rückgängig gemacht werden, soweit dies technisch möglich ist und dem Zweck der Maßnahme nicht entgegensteht, und

3. von der Bundespolizei eingesetzte Mittel nach dem Stand der Technik gegen unbefugte Nutzung geschützt werden.

(5) Besondere Abwehrmaßnahmen nach Absatz 1 Satz 1 Nummer 3, die ohne Einwilligung der Betroffenen durch Eingriff in private informationstechnische Systeme eine Datenerhebung ermöglichen, dürfen nur durchgeführt werden zur Abwehr dringender Gefahren für

1. den Bestand oder die Sicherheit des Bundes oder eines Landes,

2. Behörden oder Einrichtungen, deren Funktionieren für das Gemeinwesen oder die Verteidigung von wesentlicher Bedeutung sind,

3. die Verfügbarkeit, Vertraulichkeit oder Integrität informationstechnischer Systeme einer großen Anzahl von Personen oder

4. Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt für das Gemeinwesen oder die Verteidigung von wesentlicher Bedeutung sind.

Privat ist ein informationstechnisches System, wenn es als eigenes privat genutzt wird und aufgrund seiner technischen Funktionalität allein oder durch technische Vernetzung Daten derart vorhalten kann, dass bei einem Zugriff auf das System Umfang, Vielfalt und Qualität der Daten einen Einblick in wesentliche Teile der Lebensgestaltung der Person oder ein aussagekräftiges Bild der Persönlichkeit ermöglichen. Bei besonderen Abwehrmaßnahmen nach Absatz 1 Satz 1 Nummer 3 gilt für den Schutz des Kernbereichs privater Lebensgestaltung § 40 Absatz 10 und 11 entsprechend.

(6) Besondere Abwehrmaßnahmen nach Absatz 1 Satz 1 Nummer 3 in Verbindung mit Absatz 5 dürfen ohne Einwilligung des Betroffenen nur auf Antrag der Präsi-

dentin oder des Präsidenten des Bundespolizeipräsidiums oder einer Bundespolizeidirektion, ihrer oder seiner Vertretung oder der Leiterin oder des Leiters einer Abteilung des Bundespolizeipräsidiums durch das Gericht angeordnet werden. Zuständig ist das Amtsgericht, in dessen Bezirk die Behörde der Antragsberechtigten nach Satz 1 ihren Sitz hat. Für das Verfahren gelten die Vorschriften des Buches 1 des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit mit Ausnahme der § 23 Absatz 2 und § 37 Absatz 2 entsprechend. Die Anordnung ergeht ohne Anhörung der betroffenen Person. Eine Bekanntgabe kann unterbleiben, soweit dies aus Gründen der Geheimhaltungsbedürftigkeit erforderlich ist. Die Anordnung wird mit Erlass wirksam. Bei Gefahr im Verzug kann die Anordnung durch die nach Satz 1 Antragsberechtigten getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit die Anordnung nach Satz 7 nicht binnen 3 Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

(7) Im Antrag sind anzugeben:

1. die Kennung des Anschlusses oder des Endgerätes des informationstechnischen Systems, in das eingegriffen werden soll,

2. soweit bekannt, der Name und die Anschrift des Inhabers des informationstechnischen Systems, in das eingegriffen werden soll,

3. Art, Umfang und Dauer der besonderen Abwehrmaßnahme,

4. der Sachverhalt sowie

5. eine Begründung.

(8) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Kennung des Anschlusses oder des Endgerätes des informationstechnischen Systems, in das eingegriffen werden soll,

2. soweit bekannt, der Name und die Anschrift des Inhabers des informationstechnischen Systems, in das eingegriffen werden soll,

3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sowie

4. die wesentlichen Gründe.

(9) Die Bundespolizei darf anordnen, dass Verpflichtete nach § 170 Absatz 1 und 2 des Telekommunikationsgesetzes sowie Anbieter digitaler Dienste nach § 1 Absatz 4 Nummer 5 des Digitale-Dienste-Gesetzes Datenverkehr, von dem eine Gefahr ausgeht, umleiten oder unterbinden. Die in Satz 1 Genannten haben auf Anordnung der Bundespolizei an den Maßnahmen nach Absatz 1 Satz 1 Nummer 2 und 3 unverzüglich mitzuwirken und die erforderlichen Auskünfte zu erteilen. Nicht in Satz 1 Genannte dürfen zur Mitwirkung und Auskunftserteilung nach Satz 2 nur unter den Voraussetzungen des § 21 Absatz 1 in Anspruch genommen werden.

(10) Im Falle einer Anordnung zur Umleitung von Datenverkehr nach Absatz 1 Satz 1 Nummer 2 setzt sich die Bundespolizei mit dem Bundesamt für Sicherheit in der Informationstechnik ins Benehmen.

(11) Bei besonderen Abwehrmaßnahmen nach Absatz 1 Satz 1 kann die Bundespolizei im Einzelfall anordnen, dass der Betreiber des informationstechnischen Systems oder der zur Umleitung, Einschränkung oder Unterbindung von Datenverkehr Ver-

pflichtete gegenüber den von der besonderen Abwehrmaßnahme Betroffenen die besondere Abwehrmaßnahme nicht offenbaren darf, solange die Offenbarung Zwecken der Gefahrenabwehr oder Strafverfolgung entgegensteht. Erfolgt die Aufhebung eines Offenbarungsverbots nicht binnen 12 Monaten nach Beendigung der Maßnahme, bedarf die weitere Aufrechterhaltung der gerichtlichen Zustimmung. Absatz 6 Satz 2 bis 5 sowie § 78 Absatz 3 Satz 2 und 3 gelten entsprechend.

(12) Für die Löschung der durch die Maßnahmen nach Absatz 1 Satz 1 Nummer 2 oder 3 erlangten personenbezogenen Daten gilt § 81 Absatz 1.

(13) Die Bundespolizei übermittelt bei tatsächlichen Anhaltspunkten, dass die Aufgaben der Verteidigung betroffen sind, Informationen, die im Zusammenhang mit der Abwehr von Angriffen auf die Sicherheit in der Informationstechnik erlangt worden sind, an die Bundeswehr. § 42 des MAD-Gesetzes bleibt unberührt.“

3. In § 77 Absatz 1 wird nach der Angabe „41,“ die Angabe „41a Absatz 1 Satz 1 Nummer 2 und 3,“ eingefügt.

4. § 78 Absatz 1 Satz 1 wird wie folgt geändert:

   a) Vor der Angabe zu Nummer 1 wird nach der Angabe „bis 37, 40, 41,“ die Angabe „41a Absatz 1 Satz 1 Nummer 3,“ eingefügt.

   b) Nach Nummer 6 wird die folgende Nummer 7 eingefügt:

      „7. des § 41a Absatz 1 Satz 1 Nummer 3 der Inhaber des informationstechnischen Systems, in das eingegriffen wurde,“.

   c) Die bisherige Nummer 7 wird zu Nummer 8.

5. § 81 wird wie folgt geändert:

   a) In Absatz 1 Satz 1 wird die Angabe „41,“ durch die Angabe „41a“ ersetzt.

   b) In Absatz 2 Nummer 2 wird die Angabe „41,“ durch die Angabe „41a“ ersetzt.

6. § 85 wird wie folgt geändert:

   a) In Absatz 1 wird vor der Angabe zu Nummer 1 nach der Angabe „41,“ die Angabe „41a Absatz 1 Satz 1 Nummer 3,“ eingefügt.

   b) Nach Absatz 2 Nummer 6 wird die folgende Nummer 7 eingefügt:

      „7. bei Maßnahmen nach § 41a Absatz 1 Satz 1 Nummer 3 Angaben zur Identifizierung des informationstechnischen Systems,“.

   c) Die bisherige Nummer 7 wird zu Nummer 8.

7. § 104 wird wie folgt geändert:

   a) Absatz 1 wird wie folgt geändert:

      aa) Vor Nummer 1 wird die folgende Nummer 1 eingefügt:

         „1. einer vollziehbaren Anordnung nach

            a) § 41a Absatz 1 Satz 1 Nummer 1 oder Absatz 9 Satz 1,

b) § 41a Absatz 11 Satz 1 oder

c) § 96 Absatz 2 Satz 1 Nummer 4

zuwiderhandelt oder“.

bb) Die bisherige Nummer 1 wird zu Nummer 2 und die Angabe „übermittelt oder“ wird durch die Angabe „übermittelt.“ ersetzt.

cc) Die bisherige Nummer 2 wird gestrichen.

b) Absatz 2 wird durch den folgenden Absatz 2 ersetzt:

„(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 1 Buchstabe a mit einer Geldbuße bis zu fünfhunderttausend Euro, in den Fällen des Absatzes 1 Nummer 1 Buchstabe b und Nummer 2 mit einer Geldbuße bis zu fünfzigtausend Euro und in den Fällen des Absatzes 1 Nummer 1 Buchstabe c mit einer Geldbuße bis zu tausend Euro geahndet werden.“

8. In § 106 Absatz 1 Satz 1 wird nach der Angabe „41“ die Angabe „41a Absatz 1 Satz 1 Nummer 2 und 3,“ eingefügt.

Artikel 2

Änderung des BSI-Gesetzes

Das BSI-Gesetz vom 2. Dezember 2025 (BGBl. 2025 I Nr. 301, S. 2), das durch Artikel 4 des Gesetzes vom 11. März 2026 (BGBl. 2026 I Nr. 66) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird nach der Angabe zu § 16 die folgende Angabe eingefügt:

„§ 16a Anordnungen des Bundesamtes gegenüber Top Level Domain Name Registries und Registraren“.

2. In § 4 Absatz 2 Nummer 2 wird nach der Angabe „Einrichtungen der Bundesverwaltung“ die Angabe „und der Bundeswehr“ eingefügt.

3. § 8 wird wie folgt geändert:

a) Die Absätze 2 und 3 werden durch die folgenden Absätze 2 und 3 ersetzt:

„(2) Protokolldaten nach Absatz 1 Satz 1 Nummer 1 und an den Schnittstellen der Kommunikationstechnik des Bundes anfallende Daten nach Absatz 1 Satz 1 Nummer 2, soweit diese aus einer Zeichenfolge bestehen, die auf eine Ressource im Internet verweist, dürfen über den für die automatisierte Auswertung erforderlichen Zeitraum hinaus, längstens jedoch für 18 Monate, gespeichert werden, soweit tatsächliche Anhaltspunkte dafür bestehen, dass sie im Fall der Bestätigung eines Verdachts nach Absatz 4 Satz 2 zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen, oder zur Erkennung und Abwehr anderer Schadprogramme oder sonstiger erheblicher Gefahren für die Kommunikationstechnik des Bundes erforderlich sein können. Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Auswertung der nach Satz 1 gespeicherten Daten nur automatisiert erfolgt und ein Zugriff auf Daten, die länger als drei Monate gespeichert sind, nur bei Vorliegen tatsächlicher Erkenntnisse darüber erfolgt, dass der Bund von einem Schadprogramm oder einer sons-

tigen erheblichen Gefahr für seine Kommunikationstechnik betroffen ist. 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 Daten erforderlich ist, muss diese durch die Präsidentin oder den Präsidenten des Bundesamtes oder durch einen von ihr oder ihm beauftragten Bediensteten, der die Befähigung zum Richteramt hat, angeordnet werden. Die Entscheidung ist zu dokumentieren.

(3) Die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten sowie Protokolldaten dürfen vor ihrer Pseudonymisierung und Speicherung nach Absatz 2 zur Sicherstellung einer fehlerfreien automatisierten Auswertung manuell verarbeitet werden. Liegen Hinweise darauf 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 3 bis 6 gilt entsprechend.“

b) Absatz 6 wird wie folgt geändert:

aa) In Satz 1 wird die Angabe „§§ 202a, 202b, 303a und § 303b“ durch die Angabe „§§ 202a, 202b, 202c, 202d, 263a, 303a und 303b“ ersetzt.

bb) Satz 2 Nummer 3 wird durch die folgenden Nummern 3 und 4 ersetzt:

„3. an den Bundesnachrichtendienst zur Unterrichtung über Tatsachen, die einen internationalen kriminellen, terroristischen oder staatlichen Angriff mittels Schadprogrammen oder vergleichbarer schädlich wirkender informationstechnischer Mittel auf die Vertraulichkeit, Integrität oder Verfügbarkeit von IT-Systemen in Fällen von erheblicher Bedeutung mit Bezug zur Bundesrepublik Deutschland erkennen lassen,

4. an die Bundeswehr zur Unterrichtung über Tatsachen, die eine Bedeutung für die Erfüllung der Aufgaben der Verteidigung erkennen lassen.“.

c) Absatz 7 wird durch den folgenden Absatz 7 ersetzt:

„(7) Für sonstige Zwecke kann das Bundesamt die Daten nach Absatz 4 Satz 1 übermitteln

1. an die Strafverfolgungsbehörden zur Verfolgung einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100a Absatz 2 der Strafprozessordnung bezeichneten Straftat,

2. an die Polizeien des Bundes und der Länder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist,

3. an die Verfassungsschutzbehörden des Bundes und der Länder sowie an den Militärischen Abschirmdienst, wenn tatsächliche Anhaltspunkte für Bestrebungen in der Bundesrepublik Deutschland vorliegen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 3 Absatz 1 des Bundesverfassungsschutzgesetzes oder § 1 Absatz 1 des MAD-Gesetzes genannten Schutzgüter gerichtet sind,

4. an den Bundesnachrichtendienst, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand Straftaten nach § 3 Absatz 1 Satz 1 Nummer

8 des Artikel 10-Gesetzes plant, begeht oder begangen hat und dies von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland ist.

Die Übermittlung nach Satz 1 Nummer 1 und 2 bedarf der vorherigen gerichtlichen Zustimmung. Für das Verfahren nach Satz 1 Nummer 1 und 2 gelten die Vorschriften des Gesetzes über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit entsprechend. Zuständig ist das Amtsgericht, in dessen Bezirk das Bundesamt seinen Sitz hat. Die Übermittlung nach Satz 1 Nummer 3 und 4 erfolgt nach Anordnung des Bundesministeriums des Innern. Die §§ 9 bis 16 des Artikel 10-Gesetzes gelten entsprechend."

4. § 11 wird wie folgt geändert:

a) Absatz 1 wird durch den folgenden Absatz 1 ersetzt:

„(1) Ist die Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Einrichtung der Bundesverwaltung oder einer besonders wichtigen Einrichtung oder einer wichtigen Einrichtung beeinträchtigt oder liegen tatsächliche Anhaltspunkte für eine solche Beeinträchtigung vor, kann das Bundesamt in herausgehobenen Fällen auf Ersuchen der betroffenen Einrichtung oder des betroffenen Betreibers oder einer anderen für die Einrichtung oder den Betreiber zuständigen Behörde die Maßnahmen treffen, die erforderlich sind

1. zur Suche und Identifikation der Beeinträchtigung der Sicherheit oder Funktionsfähigkeit ihrer informationstechnischen Systeme oder

2. zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems.

Soweit das Bundesamt erste Maßnahmen zur Schadensbegrenzung und Sicherstellung des Notbetriebes vor Ort ergreift, werden für diese Tätigkeit des Bundesamts keine Gebühren oder Auslagen erhoben. Hiervon unberührt bleiben etwaige Kosten für die Hinzuziehung qualifizierter Dritter."

b) Absatz 3 wird durch den folgenden Absatz 3 ersetzt:

„(3) Das Bundesamt darf bei Maßnahmen nach Absatz 1 personenbezogene oder dem Fernmeldegeheimnis unterliegende Daten verarbeiten, soweit dies zur Suche und Identifikation von Beeinträchtigungen oder zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich und angemessen ist. Die Daten sind unverzüglich zu löschen, sobald sie für die Suche und Identifikation von Beeinträchtigungen oder die Wiederherstellung der Sicherheit oder Funktionsfähigkeit des informationstechnischen Systems nicht mehr benötigt werden. Wenn die Daten in Fällen des Absatzes 4 an eine andere Behörde zur Erfüllung ihrer gesetzlichen Aufgaben weitergegeben worden sind, darf das Bundesamt die Daten abweichend von Satz 2 bis zur Beendigung der Unterstützung dieser Behörde weiterverarbeiten. Eine Nutzung zu anderen Zwecken ist unzulässig. § 8 Absatz 8 Satz 2 bis 8 ist entsprechend anzuwenden."

5. Nach § 15 Absatz 5 wird der folgende Absatz 6 eingefügt:

„(6) Das Bundesamt kann zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1 und 2 von einem Anbieter von öffentlich zugänglichen Telekommunikationsdiensten oder einem geschäftsmäßigen Anbieter von digitalen Diensten Auskunft über

sicherheitsrelevante technische Informationen verlangen, die Rückschlüsse erlauben auf

1. Schadaktivitäten gegenüber informationstechnischen Systemen

2. Schwachstellen oder Verwundbarkeiten informationstechnischer Systeme oder

3. aktuelle Bedrohungen für die Sicherheit informationstechnischer Systeme.

Der Anbieter hat die ihm vorliegenden Informationen nach Satz 1 bereitzustellen, sofern und soweit er dazu technisch in der Lage ist und es ihm wirtschaftlich zumutbar ist. Er darf personenbezogene Daten verarbeiten, soweit dies zur Erfüllung seiner Pflicht nach den Sätzen 1 und 2 erforderlich ist. Das Bundesamt darf die bereitgestellten Daten ausschließlich zur Erfüllung seiner in Satz 1 genannten Aufgaben verwenden. Es hat die Daten unverzüglich zu löschen, sobald sie für diese Zwecke nicht mehr erforderlich sind, spätestens jedoch nach 24 Monaten."

6. § 16 wird wie folgt geändert:

a) Nach Absatz 1 Satz 3 werden die folgenden Sätze eingefügt:

„Für Anordnungen nach Satz 1 Nummer 1 kann das Bundesamt ergänzend zur eindeutigen Bezeichnung der Störquelle auf eine Liste mit Domain-Namen oder IP-Adressen verweisen. Werden nach der Anordnung Änderungen bezüglich Domain-Namen oder IP-Adressen der Störquelle, die Gegenstand der Anordnung ist, bekannt, kann das Bundesamt die betreffenden Domain-Namen oder IP-Adressen der Liste hinzufügen oder streichen."

b) In Absatz 3 Nummer 1 wird nach der Angabe „Kommunikationstechnik des Bundes" die Angabe „und der Bundeswehr" eingefügt.

c) Absatz 5 wird wie folgt geändert:

aa) In Satz 2 wird die Angabe „drei Monate" durch die Angabe „24 Monate" ersetzt.

bb) Satz 3 wird durch den folgenden Satz ersetzt:

„§ 8 Absatz 6, 7 und 8 Satz 2 bis 8 gilt entsprechend."

d) Nach Absatz 5 werden die folgenden Absätze 6 und 7 eingefügt:

„(6) Das Bundesamt nimmt Informationen zu Domain-Namen, von denen Sicherheitsrisiken für die Informationstechnik ausgehen, entgegen, wertet diese Informationen aus und stellt geeignete Informationen hierzu öffentlich zur Verfügung. Das Bundesamt hat dem Berechtigten an einem Domain-Namen, zu der Informationen öffentlich zur Verfügung gestellt werden, eine Beschwerdemöglichkeit zu eröffnen und ihm das Ergebnis der auf eine Beschwerde folgenden Überprüfung mitzuteilen.

(7) DNS-Diensteanbieter nach § 2 Nummer 8 Buchstabe a, die mindestens 50 Mitarbeiter beschäftigen oder einen Jahresumsatz und eine Jahresbilanzsumme von jeweils über 10 Millionen Euro aufweisen, sind ab dem … [einsetzen: Datum des Tages und Monats des Inkrafttretens nach Artikel 6 dieses Gesetzes sowie Jahreszahl des auf das Inkrafttreten nach Artikel 6 dieses Gesetzes folgenden Jahres] verpflichtet, auf Grundlage der vom Bundesamt veröffentlichten Informationen nach Absatz 6 ihren Nutzern einen DNS-basierten Schutz vor Angriffen

in Verbindung mit Domain-Namen, von denen Sicherheitsrisiken für die Informationstechnik ausgehen, anzubieten. § 28 Absatz 4 gilt entsprechend.“

7. § 17 wird durch die folgenden §§ 16a und 17 ersetzt:

„§ 16a

Anordnungen des Bundesamtes gegenüber Top Level Domain Name Registries und Domain-Name-Registry-Dienstleistern

(1) Zur Abwehr erheblicher Gefahren für die in § 16 Absatz 3 genannten Schutzgüter kann das Bundesamt gegenüber einem Top-Level-Domain-Name-Registry oder einem Domain-Name-Registry-Dienstleister anordnen, dass er die Nameserver-Einträge eines vom Bundesamt benannten Domain-Namens ändert oder neue Einträge hinzufügt, soweit er dazu technisch in der Lage ist und es ihm wirtschaftlich zumutbar ist. Widerspruch und Anfechtungsklage gegen die Anordnung nach Satz 1 haben keine aufschiebende Wirkung.

(2) Ordnet das Bundesamt eine Maßnahme nach Absatz 1 Satz 1 an, so kann es gegenüber einem Top-Level-Domain-Name-Registry und Domain-Name-Registry-Dienstleistern auch anordnen, die an eine bestimmte Second-Level- oder eine auf einer Ebene darunter liegende Domain gerichteten Nameserveranfragen an einen vom Bundesamt benannten Nameserver umzuleiten. § 16 Absatz 5 gilt entsprechend.

(3) Maßnahmen nach Absatz 1 Satz 1 müssen beendet werden, wenn feststeht, dass von dem Dienst, auf den die vom Bundesamt benannten Domain-Namen verweisen, keine Gefahr nach Absatz 1 Satz 1 mehr ausgeht.

§ 17

Anordnungen von Maßnahmen des Bundesamtes gegenüber Anbietern von digitalen Diensten

(1) Das Bundesamt kann in Einzelfällen zur Abwehr erheblicher Gefahren für informationstechnische Systeme einer Vielzahl von Nutzern, die von digitalen Diensten von Anbietern von digitalen Diensten nach § 2 Absatz 2 Nummer 1 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes ausgehen, die durch ungenügende technische und organisatorische Vorkehrungen nach § 19 Absatz 4 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes unzureichend gesichert sind und dadurch keinen hinreichenden Schutz bieten vor

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

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

gegenüber dem jeweiligen Anbieter von digitalen Diensten nach § 2 Absatz 2 Nummer 1 des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes anordnen, dass dieser die jeweils zur Herstellung des ordnungsgemäßen Zustands seiner digitalen Dienste erforderlichen technischen und organisatorischen Maßnahmen ergreift, um den ordnungsgemäßen Zustand seiner digitalen Dienste herzustellen. Die Zuständigkeit der Aufsichtsbehörden der Länder bleibt im Übrigen unberührt.

(2) Zur Abwehr erheblicher Gefahren für die in § 16 Absatz 3 genannten Schutzgüter kann das Bundesamt gegenüber einem Anbieter nach § 2 Nummer 4, 5, 25, 26 oder 35 anordnen, den Datenverkehr an einen vom Bundesamt benannten Domain-Namen oder eine vom Bundesamt benannte Anschlusskennung umzuleiten oder zu unterbinden, soweit der Anbieter dazu technisch in der Lage ist und es ihm wirtschaftlich zumutbar ist. § 16 Absatz 5 gilt entsprechend."

8. § 31 Absatz 2 wird durch die folgenden Absätze 2 bis 6 ersetzt:

„(2) Betreiber kritischer Anlagen sind verpflichtet, für die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, vom Bundesamt bereitgestellte Angriffsindikatoren und Informationen über Schwachstellen empfangen und verarbeiten zu können, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen.

(3) Betreiber kritischer Anlagen sind verpflichtet, innerhalb von zwölf Monaten, nachdem sie erstmals oder erneut als Betreiber kritischer Anlagen gelten, jedoch nicht früher als zwölf Monate nach der Veröffentlichung der Anforderungen gemäß Absatz 6, Folgendes an das Bundesamt automatisiert zu übermitteln:

1. kontinuierlich Verfügbarkeitsindikatoren der informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, und

2. Indikatoren zu tatsächlichen und potentiellen Angriffen sowie Informationen zu Schwachstellen, die in Systemen zur Angriffserkennung nach Absatz 2 zu erheblichen Bedrohungen, Störungen oder Beeinträchtigungen der Sicherheit in der Informationstechnik anfallen,

Das Bundesamt kann gegenüber dem Betreiber der kritischen Anlage auf eine Anbindung und Übermittlung der in Satz 1 genannten Informationen verzichten.

(4) Betreiber kritischer Anlagen dürfen personenbezogene Daten verarbeiten, soweit dies zur Erfüllung der Pflichten nach Absatz 3 Satz 1 erforderlich ist. Das Bundesamt darf die ausgeleiteten Daten zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 2, 22, 24 und 25 verarbeiten.

(5) Bei der Erfüllung der Pflichten nach den Absätzen 2 und 3 soll der Stand der Technik eingehalten werden. Der hierfür erforderliche Aufwand soll nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage stehen.

(6) Das Bundesamt legt die Anforderungen an die Anbindung und Ausleitung gemäß den Absätzen 2, 3 und 5 nach Anhörung der betroffenen Betreiber und der betroffenen Wirtschaftsverbände fest und veröffentlicht sie auf seiner Internetseite."

9. In § 39 Absatz 1 Satz 1 wird nach der Angabe „§ 31 Absatz 1" die Angabe „und 2 Satz 1" gestrichen.

10. § 50 Absatz 1 wird durch den folgenden Absatz 1 ersetzt:

„(1) Ein Top Level Domain Name Registry oder Domain-Name-Registry-Dienstleister hat einem berechtigten Zugangsnachfrager nach § 2 Nummer 2 auf Antrag un-

ter Angabe der Bestimmung, die ihm die Erhebung erlaubt, soweit dies für die Erfüllung seiner Aufgaben erforderlich ist, unverzüglich und in jedem Fall 72 Stunden nach Eingang des Antrags Zugang zu den Domain-Namen-Registrierungsdaten zu gewähren. Liegen die angefragten Informationen nicht vor, so ist dies dem berechtigten Zugangsnachfrager innerhalb von 24 Stunden nach Eingang des Antrags mitzuteilen. Die Verantwortung für die Zulässigkeit des Antrags tragen die ersuchenden Zugangsnachfrager.“

11. § 57 wird durch den folgenden § 57 ersetzt:

„§ 57

Einschränkung eines Grundrechts

Das Fernmeldegeheimnis (Artikel 10 Absatz 1 des Grundgesetzes) wird durch die §§ 7, 8, 9, 11, 12, 15, 16, 16a, 17 und 31 eingeschränkt.“

12. § 65 wird wie folgt geändert:

a) Absatz 2 wird wie folgt geändert:

aa) Nummer 1 wird wie folgt geändert:

aaa) In Buchstabe a wird die Angabe „, § 16 Absatz 1 Satz 1 Nummer 1, auch in Verbindung mit Absatz 3, Nummer 2, § 17 Satz 1“ gestrichen.

bbb) In Buchstabe c wird die Angabe „den §§ 18, 40“ durch die Angabe „§ 16 Absatz 1 Satz 1 Nummer 1, auch in Verbindung mit Absatz 3, nach § 16 Absatz 1 Satz 1 Nummer 2, § 16a Absatz 1 Satz 1, auch in Verbindung mit Absatz 2 Satz 1, nach § 17 Absatz 1 Satz 1 oder Absatz 2 Satz 1, § 18, § 40“ ersetzt.

bb) Nach Nummer 3 werden die folgenden Nummern 3a und 3b eingefügt:

„3a. entgegen § 31 Absatz 2 Satz 1 ein dort genanntes System nicht einsetzt,

3b. entgegen § 31 Absatz 3 Satz 1 einen dort genannten Indikator oder eine dort genannte Information nicht, nicht richtig, nicht vollständig, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig übermittelt,“.

b) In Absatz 5 Satz 1 Nummer 4 wird die Angabe „Nummer 10“ durch die Angabe „Nummer 3a, 3b und 10“ ersetzt.

Artikel 3

Änderung des Bundeskriminalamtgesetzes

Das Bundeskriminalamtgesetz vom 1. Juni 2017 (BGBl. I S. 1354; 2019 I S. 400), das zuletzt durch … [Artikel 1 des Entwurfs des Gesetzes zur Stärkung digitaler Ermittlungsbefugnisse in der Polizeiarbeit, Bundesratsdrucksache 259/26] geändert worden ist, wird wie folgt geändert:

1. Die Inhaltsübersicht wird wie folgt geändert:

a) Nach der Angabe zu § 3 wird die folgende Angabe eingefügt:

„§ 3a Abwehr von Gefahren durch Angriffe auf die Sicherheit in der Informationstechnik“.

b) Die Angabe zu § 59 wird durch die folgende Angabe ersetzt:

„§ 59 Durchsuchung von Gegenständen“.

c) Nach der Angabe zu § 60 wird die folgende Angabe eingefügt:

„§ 60a Zurückstellung der Benachrichtigung; Offenbarungsverbot“.

d) Nach der Angabe zu § 68 wird die folgende Angabe eingefügt:

„Abschnitt 8a

Befugnisse zur Abwehr von Angriffen auf die Sicherheit in der Informationstechnik

§ 68a Befugnisse

§ 68b Untersagung des Betriebs informationstechnischer Systeme

§ 68c Einschränkung, Unterbindung und Umleitung von Datenverkehr

§ 68d Auslesen, Löschen und Verändern von Daten in informationstechnischen Systemen

§ 68e Besondere Bestimmungen für Eingriffe in private informationstechnische Systeme

§ 68f Offenbarungsverbot“.

2. § 2 Absatz 5 Satz 1 wird wie folgt geändert:

a) In Nummer 3 wird die Angabe „unterstützen sowie“ durch die Angabe „unterstützen,“ ersetzt.

b) In Nummer 4 wird die Angabe „unterstützen.“ durch die Angabe „unterstützen sowie“ ersetzt.

c) Nach Nummer 4 wird die folgende Nummer 5 eingefügt:

„5. auf Ersuchen bei der Durchführung technischer Maßnahmen der Abwehr von Angriffen auf die Sicherheit in der Informationstechnik unterstützen.“

3. Nach § 3 wird der folgende § 3a eingefügt:

„§ 3a

Abwehr von Gefahren durch Angriffe auf die Sicherheit in der Informationstechnik

(1) Das Bundeskriminalamt nimmt die Aufgabe der Abwehr von Gefahren durch Angriffe auf die Sicherheit in der Informationstechnik wahr, wenn

1. die Gefahren schwerwiegend sind und die Abwehr nur in gemeinsamer Ausführung mit öffentlichen Stellen anderer Staaten oder zwischen- und überstaatlichen Stellen erfolgen kann,

2. sich die Gefahren gegen die Funktionsfähigkeit von Behörden oder Einrichtungen des Bundes richten oder

3. sich die Gefahren ihrer Art nach oder wegen der zur Abwehr erforderlichen Maßnahmen auf die Stellung der Bundesrepublik Deutschland in der Staatengemeinschaft oder die Verteidigung auswirken können.

(2) Gefahren durch Angriffe auf die Sicherheit in der Informationstechnik sind Gefahren der Verwirklichung von Straftaten, die in den §§ 202a, 202b, 202c, 202d, 263a, 303a und 303b des Strafgesetzbuchs bezeichnet sind.

(3) Schwerwiegend im Sinne des Absatzes 1 Nummer 1 sind Gefahren durch Angriffe auf die Sicherheit in der Informationstechnik, die sich richten gegen

1. die innere oder äußere Sicherheit der Bundesrepublik Deutschland,

2. Behörden oder Einrichtungen des Bundes oder sicherheitsempfindliche 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

3. die Verfügbarkeit, Vertraulichkeit und oder Integrität informationstechnischer Systeme einer großen Anzahl von Personen und eine gemeine Gefahr darstellen.

(4) Die Aufgaben und Befugnisse anderer Bundesbehörden bleiben unberührt. Das Bundeskriminalamt benachrichtigt die für die Polizeien zuständigen obersten Landesbehörden der betroffenen Länder, wenn das Bundeskriminalamt die Aufgabe nach Absatz 1 wahrnimmt.“

4. In § 4 Absatz 1 Satz 1 Nummer 5 wird vor der Angabe zu Buchstabe a nach der Angabe „202c,“ die Angabe „202d,“ eingefügt.

5. § 59 wird durch den folgenden § 59 ersetzt:

„§ 59

Durchsuchung von Gegenständen

(1) Das Bundeskriminalamt kann einen Gegenstand durchsuchen, wenn

1. er von einer Person mitgeführt wird, die nach § 58 durchsucht werden darf,

2. Tatsachen die Annahme rechtfertigen, dass sich in ihm ein anderer Gegenstand befindet, der sichergestellt werden darf,

3. Tatsachen die Annahme rechtfertigen, dass sich in ihm eine Person befindet, die in Gewahrsam genommen werden darf,

4. er sich an einem der in § 42 Absatz 1 Nummer 2 genannten Orte befindet,

5. er sich an einem der in § 42 Absatz 1 Nummer 3 genannten Orte befindet und Tatsachen die Annahme rechtfertigen, dass dort Straftaten nach § 5 Absatz 1 Satz 2 begangen werden sollen, oder

6. er sich in unmittelbarer Nähe einer Person befindet, die aufgrund bestimmter Tatsachen durch die Begehung von Straftaten nach § 5 Absatz 1 Satz 2 gefährdet ist

und die Durchsuchung aufgrund von auf den Gegenstand bezogenen Anhaltspunkten erforderlich ist. § 42 Absatz 1 bleibt unberührt.

(2) § 67 Absatz 4 des Bundespolizeigesetzes gilt entsprechend.“

6. § 60 Absatz 1 wird wie folgt geändert:

a) In der Angabe vor Nummer 1 wird die Angabe „eine Sache“ durch die Angabe „einen Gegenstand“ ersetzt.

b) Nummer 2 wird wie folgt geändert:

aa) In der Angabe vor Buchstabe a wird die Angabe „sie“ durch die Angabe „er“ und die Angabe „die Sache“ durch die Angabe „den Gegenstand“ ersetzt.

bb) In Buchstabe c wird die Angabe „Sachen“ durch die Angabe „Gegenstände“ ersetzt.

c) In Absatz 2 wird die Angabe „§§ 48 bis 50“ durch die Angabe „§§ 72 bis 75“ ersetzt.

d) Nach Absatz 2 wird folgender Absatz 3 eingefügt:

„(3) Sofern die nach Absatz 1 zu ergreifende Maßnahme in ihrer Wirkung mit Maßnahmen nach den §§ 49 bis 51 vergleichbar ist, darf sie nur unten den dort jeweils genannten Voraussetzungen erfolgen.“

7. Nach § 60 wird der folgende § 60a eingefügt:

„§ 60a

Zurückstellung der Benachrichtigung; Offenbarungsverbot

(1) Bei der Sicherstellung eines Gegenstandes, den eine Person im Gewahrsam hat (Gewahrsamsinhaber), kann die Benachrichtigung des Eigentümers oder des rechtmäßigen Inhabers der tatsächlichen Gewalt nach § 60 Absatz 2 in Verbindung mit § 72 Absatz 2 Satz 3 des Bundespolizeigesetzes zurückgestellt werden, solange die Benachrichtigung den Zweck der Sicherstellung gefährden würde. § 74 Absatz 1 Satz 2 bis 4 gilt entsprechend.

(2) Wird die Benachrichtigung zurückgestellt, kann unter Würdigung aller Umstände und nach Abwägung der Interessen der Beteiligten im Einzelfall angeordnet werden, dass der Gewahrsamsinhaber für die Dauer der Zurückstellung gegenüber dem Eigentümer, dem rechtmäßigen Inhaber der tatsächlichen Gewalt und dritten Personen die Sicherstellung nicht offenbaren darf.

(3) Die Zurückstellung der Benachrichtigung nach Absatz 1 sowie das Offenbarungsverbot nach Absatz 2 dürfen nur auf Antrag der zuständigen Abteilungsleitung des Bundeskriminalamtes oder deren Vertretung durch das Gericht angeordnet werden.

(4) Bei Gefahr im Verzug kann die Anordnung durch die zuständige Abteilungsleitung des Bundeskriminalamtes oder deren Vertretung getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit die Anordnung nach Satz 1 nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

(5) In dem Antrag nach Absatz 3 sind anzugeben:

1. Angaben zur Identifizierung des Gegenstands, der sichergestellt wird,
2. Name und die Anschrift des Gewahrsamsinhabers,
3. soweit bekannt, Name und Anschrift des Eigentümers oder rechtmäßigen Inhabers, dessen Benachrichtigung zurückgestellt werden soll,
4. Art, Umfang und Dauer der Zurückstellung der Benachrichtigung sowie für den Fall, dass ein Offenbarungsverbot erlassen werden soll, Art, Umfang und Dauer des Offenbarungsverbots,
5. der Sachverhalt sowie
6. eine Begründung.

(6) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. Angaben zur Identifizierung des Gegenstands, der sichergestellt wird,
2. Name und die Anschrift des Gewahrsamsinhabers,
3. soweit bekannt, Name und Anschrift des Eigentümers oder rechtmäßigen Inhabers, dessen Benachrichtigung zurückgestellt werden soll,
4. Art, Umfang und Dauer der Zurückstellung der Benachrichtigung sowie für den Fall, dass ein Offenbarungsverbot erlassen werden soll, Art, Umfang und Dauer des Offenbarungsverbots sowie
5. die wesentlichen Gründe.“

8. § 63 wird wie folgt geändert:

a) In Absatz 2 Nummer 3 wird die Angabe „eine Sache“ durch die Angabe „einen Gegenstand“ und die Angabe „oder Sache“ durch die Angabe „oder den Gegenstand“ ersetzt.

b) In Absatz 6 Satz 1 wird die Angabe „eine Sache“ durch die Angabe „einen Gegenstand“ ersetzt.

9. Nach Abschnitt 8 wird der folgende Abschnitt 8a eingefügt:

„Abschnitt 8a

Befugnisse zur Abwehr von Angriffen auf die Sicherheit in der Informationstechnik

§ 68a

Befugnisse

(1) Zur Erfüllung seiner Aufgaben nach den §§ 3a und 5 bis 8 kann das Bundeskriminalamt, um eine Gefahr nach Absatz 2 abzuwehren,

1. die notwendigen Maßnahmen treffen, soweit nicht dieses Gesetz die Befugnisse des Bundeskriminalamtes besonders regelt,

2. Maßnahmen entsprechend den §§ 39 Absatz 1 und 3, 40 bis 46, 49 bis 53, 54 und 58 bis 62 treffen sowie

3. Maßnahmen nach den §§ 68b bis 68d treffen.

(2) Gefahr im Sinne dieses Abschnitts ist eine im Einzelfall bestehende Gefahr im Sinne des § 3a Absatz 2.

(3) Die §§ 16 bis 21 des Bundespolizeigesetzes gelten entsprechend für Maßnahmen nach Absatz 1.

(4) Das Bundeskriminalamt übermittelt bei tatsächlichen Anhaltspunkten, dass die Aufgaben der Verteidigung betroffen sind, Informationen, die im Zusammenhang mit der Abwehr von Angriffen auf die Sicherheit in der Informationstechnik erlangt worden sind, unverzüglich an die Bundeswehr. § 42 des MAD-Gesetzes bleibt unberührt.

§ 68b

Untersagung des Betriebs informationstechnischer Systeme

Das Bundeskriminalamt darf zur Abwehr einer Gefahr den Betrieb eines informationstechnischen Systems, von dem diese Gefahr ausgeht, untersagen.

§ 68c

Einschränkung, Unterbindung und Umleitung von Datenverkehr

(1) Das Bundeskriminalamt darf zur Abwehr einer Gefahr Datenverkehr, von dem diese Gefahr ausgeht, einschränken, unterbinden oder auf eine vom Bundeskriminalamt vorgegebene Zieladresse umleiten und aufzeichnen, auch ohne Wissen der Betroffenen.

(2) Das Bundeskriminalamt darf anordnen, dass die Verpflichteten nach § 170 Absatz 1 und 2 des Telekommunikationsgesetzes sowie Anbieter digitaler Dienste nach § 1 Absatz 4 Nummer 5 des Digitale-Dienste-Gesetzes Datenverkehr von dem eine Gefahr ausgeht, umleiten oder unterbinden. Die in Satz 1 Genannten haben auf Anordnung des Bundeskriminalamtes an den Maßnahmen nach Absatz 1 unverzüglich mitzuwirken und die erforderlichen Auskünfte zu erteilen. Nicht in Satz 1 Genannte dürfen zur Mitwirkung und Auskunftserteilung nach Satz 2 nur unter den Voraussetzungen des § 21 Absatz 1 des Bundespolizeigesetzes in Anspruch genommen werden.

(3) Im Falle einer Anordnung zur Umleitung von Datenverkehr setzt sich das Bundeskriminalamt mit dem Bundesamt für Sicherheit in der Informationstechnik ins Benehmen.

(4) Für die Löschung nach Absatz 1 erlangter personenbezogener Daten gilt § 79.

§ 68d

Auslesen, Löschen und Verändern gefahrgegenständlicher Daten in informationstechnischen Systemen

(1) Das Bundeskriminalamt darf zur Abwehr einer Gefahr gefahrgegenständliche Daten in dem informationstechnischen System, von dem die Gefahr ausgeht, auch durch Eingriff mit technischen Mitteln und ohne Wissen des Betroffenen, auslesen, löschen oder verändern.

(2) Gefahrgegenständliche Daten sind die Daten von Schadprogrammen oder sonstigen informationstechnischen Angriffswerkzeugen, einschließlich Steuerungs- oder Protokolldateien, und Spuren, die technisch mit dem Angriff verbunden sind, sowie Daten, die selbst Gegenstand eines Angriffs auf die Sicherheit in der Informationstechnik sind, insbesondere Daten, die durch diesen Angriff an ein informationstechnisches System weitergeleitet werden oder wurden

(3) Bei Maßnahmen nach Absatz 1 ist sicherzustellen, dass, soweit möglich, technische Vorkehrungen getroffen werden, damit das Auslesen, Löschen oder Verändern auf gefahrgegenständliche Daten beschränkt wird. In den informationstechnischen Systemen vorgenommene Veränderungen sind bei Beendigung der Maßnahme rückgängig zu machen, soweit dies technisch möglich ist und dem Zweck der Maßnahme nicht entgegensteht. Vom Bundeskriminalamt eingesetzte Mittel sind nach dem Stand der Technik gegen unbefugte Nutzung zu schützen.

(4) Die Maßnahmen nach Absatz 1 dürfen auch durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. § 68c Absatz 2 Satz 2 und 3 gilt entsprechend.

(5) Für die Löschung nach Absatz 1 erlangter personenbezogener Daten gilt § 79.

§ 68e

Besondere Bestimmungen für Eingriffe in private informationstechnische Systeme

(1) Maßnahmen nach § 68d, die ohne Einwilligung des Betroffenen durch Eingriff in private informationstechnische Systeme eine Datenerhebung ermöglichen, dürfen abweichend von § 68d Absatz 1 nur angeordnet werden

1. zur Abwehr dringender Gefahren für

   a) den Bestand oder die Sicherheit des Bundes oder eines Landes,

   b) Behörden oder Einrichtungen, deren Funktionieren für das Gemeinwesen oder die Verteidigung von wesentlicher Bedeutung ist,

   c) die Verfügbarkeit, Vertraulichkeit oder Integrität informationstechnischer Systeme einer großen Anzahl von Personen oder

   d) Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt für das Gemeinwesen oder die Verteidigung von wesentlicher Bedeutung ist.

(2) Privat ist ein informationstechnisches System, wenn es als eigenes privat genutzt wird und aufgrund seiner technischen Funktionalität allein oder durch technische Vernetzung Daten derart vorhalten kann, dass bei einem Zugriff auf das System Um-

fang, Vielfalt und Qualität der Daten einen Einblick in wesentliche Teile der Lebensgestaltung der Person oder ein aussagekräftiges Bild der Persönlichkeit ermöglichen.

(3) Die Anordnung nach Absatz 1 erfolgt auf Antrag der zuständigen Abteilungsleitung des Bundeskriminalamtes oder deren Vertretung durch das Gericht.

(4) Bei Gefahr im Verzug kann die Anordnung durch die zuständige Abteilungsleitung des Bundeskriminalamtes oder deren Vertretung getroffen werden. In diesem Fall ist die gerichtliche Entscheidung unverzüglich nachzuholen. Soweit die Anordnung nach Satz 1 nicht binnen drei Tagen durch das Gericht bestätigt wird, tritt sie außer Kraft.

(5) In dem Antrag nach Absatz 3 sind anzugeben:

1. die Kennung des Anschlusses oder des Endgerätes des informationstechnischen Systems, in das eingegriffen werden soll,

2. soweit bekannt, der Name und die Anschrift des Inhabers des informationstechnischen Systems, in das eingegriffen werden soll,

3. Art, Umfang und Dauer der Maßnahme,

4. der Sachverhalt sowie

5. eine Begründung.

(6) Die Anordnung ergeht schriftlich. In ihr sind anzugeben:

1. die Kennung des Anschlusses oder des Endgerätes des informationstechnischen Systems, in das eingegriffen werden soll,

2. soweit bekannt, der Name und die Anschrift des Inhabers des informationstechnischen Systems, in das eingegriffen werden soll,

3. Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sowie

4. die wesentlichen Gründe.

(7) Für den Schutz des Kernbereichs privater Lebensgestaltung gilt § 51 Absatz 7 und 8 entsprechend.

§ 68f

Offenbarungsverbot

(1) Bei den Maßnahmen nach den §§ 68b bis 68d kann das Bundeskriminalamt im Einzelfall anordnen, dass der Betreiber des informationstechnischen Systems oder der zur Umleitung, Einschränkung, oder Unterbindung von Datenverkehr Verpflichtete gegenüber den von der Maßnahme Betroffenen die Maßnahme nicht offenbaren darf, solange die Offenbarung Zwecken der Gefahrenabwehr oder Strafverfolgung entgegensteht.

(2) Erfolgt die Aufhebung eines Offenbarungsverbots nicht binnen 12 Monaten bedarf die weitere Aufrechterhaltung der gerichtlichen Zustimmung. § 74 Absatz 3 Satz 5 und 6 gilt entsprechend.“

10. In § 69 Absatz 1 Satz 1 wird die Angabe „Abschnitt 5“ durch die Angabe „den Abschnitten 5 und 8a“ ersetzt.

11. § 74 Absatz 1 Satz 1 wird wie folgt geändert:

    a) In der Angabe vor Nummer 1 wird die Angabe „bis 53 und 64“ durch die Angabe „bis 53, 64 und 68d“ ersetzt.

    b) In Nummer 11 wird die Angabe „Zielperson.“ durch die Angabe „Zielperson,“ ersetzt.

    c) Nach Nummer 11 wird die folgende Nummer 12 eingefügt:

    „12. des § 68d (Auslesen, Löschen und Verändern von Daten in informationstechnischen Systemen) der Inhaber des informationstechnischen Systems in das eingegriffen wurde.“

12. In § 79 Absatz 1 Satz 1 wird die Angabe „Abschnitt 5“ durch die Angabe „den Abschnitten 5 oder 8a“ ersetzt.

13. § 82 wird wie folgt geändert:

    a) In Absatz 1 wird vor der Angabe zu Nummer 1 die Angabe „53 und 64“ durch die Angabe „53, 64 und 68d in Verbindung mit 68e“ ersetzt.

    b) Absatz 2 wird wie folgt geändert:

    aa) In Nummer 11 wird die Angabe „Zielperson.“ durch die Angabe „Zielperson,“ ersetzt.

    bb) Nach Nummer 11 wird die folgende Nummer 12 eingefügt:

    „12. bei Maßnahmen nach § 68d (Auslesen, Löschen und Verändern von Daten in informationstechnischen Systemen) die Angaben zur Identifizierung des informationstechnischen Systems.“

14. § 87a Absatz 1 und 2 wird durch die folgenden Absätze 1 und 2 ersetzt:

„(1) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. entgegen § 10b Absatz 5 Satz 1 oder § 52 Absatz 8 Satz 1 die dort genannten Daten nicht, nicht vollständig oder nicht rechtzeitig sichert oder

2. einer vollziehbaren Anordnung nach

    a) § 60a Absatz 2 oder § 68f Absatz 1 oder

    b) § 68b oder § 68c Absatz 2 Satz 1,

zuwiderhandelt.

(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 1 und Nummer 2 Buchstabe b mit einer Geldbuße bis zu fünfhunderttausend Euro und in den Fällen des Absatzes 1 Nummer 2 Buchstabe a mit einer Geldbuße bis zu fünfzigtausend Euro geahndet werden.“

Artikel 4

Änderungen des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes

Das Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz vom 23. Juni 2021 (BGBl. I S. 1982; 2022 I S. 1045), das zuletzt durch Artikel 3 des Gesetzes vom 10. März 2026 (BGBl. 2026 I Nr. 64) geändert worden ist, wird wie folgt geändert:

Nach § 19 Absatz 4 werden die folgenden Absätze 5 bis 6 eingefügt:

„(5) Wird einem Anbieter von digitalen Diensten eine Störung bekannt, die im Zuge der Inanspruchnahme durch einen Nutzer von einem seiner Dienste ausgeht, hat er den Nutzer, soweit ihm dieser bekannt ist, unverzüglich darüber zu benachrichtigen. Soweit technisch möglich und wirtschaftlich zumutbar, hat der Anbieter den Nutzer im Rahmen seiner jeweiligen Verantwortlichkeit für geschäftsmäßig angebotene digitale Dienste auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen er die Störung erkennen und beseitigen kann. Wurde dem Anbieter die Störung durch das Bundesamt für Sicherheit in der Informationstechnik mitgeteilt, hat der Anbieter dabei alle in der Störungsmeldung mitgelieferten Informationen, mit denen die Störung erkannt und beseitigt werden kann, an den Nutzer weiterzuleiten. Der Anbieter darf die Teile des Datenverkehrs von und zu einem in Anspruch genommenen Dienst, von dem eine Störung ausgeht, umleiten, soweit dies erforderlich ist, um den Nutzer über die Störung benachrichtigen zu können.

(6) Wird ein Anbieter von digitalen Diensten vom Bundesamt für Sicherheit in der Informationstechnik über konkrete Gefahren für die Sicherheit in der Informationstechnik informiert, die im Zuge der Inanspruchnahme durch einen Nutzer von einem seiner Dienste ausgehen oder diese betreffen, hat er den Nutzer, soweit ihm dieser bekannt ist, unverzüglich darüber zu benachrichtigen. Dabei hat der Anbieter insbesondere alle in der Mitteilung des Bundesamts für Sicherheit in der Informationstechnik nach Satz 1 enthaltenen Informationen, mit denen die Gefahren erkannt und ihnen vorgebeugt werden können, an den Nutzer weiterzuleiten. Werden einem Anbieter digitaler Dienste Gefahren für die Sicherheit in der Informationstechnik bekannt, die im Zuge der Inanspruchnahme durch einen Nutzer von einem seiner Dienste ausgehen oder diese betreffen, kann er den Nutzer darüber benachrichtigen. Soweit technisch möglich und wirtschaftlich zumutbar, kann er den Nutzer auf angemessene, wirksame und zugängliche technische Mittel hinweisen, mit denen er diese Gefahren erkennen und ihnen vorbeugen kann.“

Artikel 5

Änderung des Energiewirtschaftsgesetzes

Das Energiewirtschaftsgesetz vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch … [Artikel 1 des Entwurfs eines Gesetzes zur Änderung des Energiewirtschaftsgesetzes und weiterer energierechtlicher Vorschriften zur Umsetzung des Europäischen Gas- und Wasserstoff-Binnenmarktpakets, Bundestagsdrucksache 21/5440] geändert worden ist, wird wie folgt geändert:

1. Nach § 5c Absatz 6 werden die folgenden Absätze 7 bis 11 eingefügt:

„(7) Der Betreiber nach Absatz 1 Satz 1 Nummer 1 bis 3 ist verpflichtet, spätestens zwölf Monate, nachdem er erstmals oder erneut als Betreiber kritischer Anlagen gilt,

jedoch nicht früher als zwölf Monate nach der Veröffentlichung der Anforderungen nach Absatz 10 Satz 1, Folgendes an das Bundesamt für Sicherheit in der Informationstechnik automatisiert zu übermitteln:

1. kontinuierlich Verfügbarkeitsindikatoren in Bezug auf kritische Komponenten oder kritische Funktionen gemäß der Festlegung nach Absatz 6 oder der Rechtsverordnung nach § 56 Absatz 6 des BSI-Gesetzes und

2. Indikatoren zu potenziellen und tatsächlichen Angriffen sowie Informationen zu Schwachstellen, die in Systemen zur Angriffserkennung nach Absatz 4 Nummer 11 zu erheblichen Bedrohungen, Störungen oder Beeinträchtigungen der Sicherheit in der Informationstechnik anfallen.

Der Umfang der zu übermittelnden Daten soll dabei in einem angemessenen Verhältnis zum Nutzen für die Erkennung und Abwehr von Gefahren für die Betreiber kritischer Anlagen nach der BSI-Kritisverordnung vom 22. April 2016 (BGBl. I S. 958), die zuletzt durch Artikel 9 des Gesetzes vom 11. März 2026 (BGBl. 2026 I Nr. 66) geändert worden ist, stehen.

(8) Der Betreiber nach Absatz 1 Satz 1 Nummer 1 bis 3 darf personenbezogene Daten verarbeiten, soweit dies zur Erfüllung der Pflichten nach Absatz 7 Satz 1 erforderlich ist. Das Bundesamt für Sicherheit in der Informationstechnik darf die übermittelten Daten zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 2, 22, 24 und 25 des BSI-Gesetzes verarbeiten.

(9) Die Übermittlung an das Bundesamt für Sicherheit in der Informationstechnik nach Absatz 7 muss unidirektional und rückwirkungsfrei erfolgen. Dabei soll der Stand der Technik eingehalten werden. Der hierfür erforderliche Aufwand soll nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage stehen.

(10) Die Anforderungen an die Übermittlung und die hierfür erforderliche technische Anbindung werden von der Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik durch Festlegung nach § 29 Absatz 1 bestimmt. Die Bundesnetzagentur beteiligt die Betreiber nach Absatz 1 Satz 1 Nummer 1 bis 3 und deren Branchenverbände entsprechend ihrer Betroffenheit. Im Rahmen der Festlegung können bestimmte Betreibergruppen von der Verpflichtung nach Absatz 7 ausgenommen werden. Die Festlegung kann als Teil des IT-Sicherheitskatalog nach Absatz 2 erfolgen.

(11) Durch die Absätze 7 und 8 wird das Fernmeldegeheimnis (Artikel 10 Absatz 1 des Grundgesetzes) eingeschränkt."

2. In § 43k Satz 2 wird die Angabe „Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz" durch die Angabe „BSI-Kritisverordnung" ersetzt.

3. § 95 wird wie folgt geändert:

   a) Absatz 1 wird wie folgt geändert:

      aa) Nach Nummer 3b wird die folgende Nummer 3c eingefügt:

         „3c. entgegen § 5c Absatz 7 Satz 1 einen dort genannten Indikator oder eine dort genannte Information nicht, nicht richtig, nicht vollständig, nicht in der vorgeschriebenen Weise oder nicht rechtzeitig übermittelt,".

      bb) Die bisherigen Nummern 3c bis 3j werden zu den Nummern 3d bis 3k.

b) Absatz 2 wird wie folgt geändert:

aa) In Nummer 1 wird die Angabe „Nummer 3b bis 3e“ durch die Angabe „Nummer 3b, 3d bis 3f“ ersetzt.

bb) In Nummer 2 Buchstabe a wird die Angabe „Nummer 3g bis 3j“ durch die Angabe „Nummer 3h bis 3k“ ersetzt.

cc) In Nummer 3 Buchstabe a wird die Angabe „Nummer 4“ durch die Angabe „Nummer 3c, 4“ ersetzt.

Artikel 6

Einschränkung eines Grundrechts

Durch Artikel 1 Nummer 2 (§ 41a des Bundespolizeigesetzes), Artikel 2 Nummer 3 bis 8 (§§ 8, 11, 15, 16, 16a, 17 und 31 des BSI-Gesetzes) sowie Artikel 3 Nummer 6, 7 und 9 (§§ 60, 60a und 68a bis 68e des Bundeskriminalamtgesetzes) und Artikel 5 Nummer 1 (§ 5c des Energiewirtschaftsgesetzes) wird das Fernmeldegeheimnis (Artikel 10 Absatz 1 des Grundgesetzes) eingeschränkt.

Artikel 7

Inkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Zielsetzung und Notwendigkeit der Regelungen

Cyberangriffe in Deutschland nehmen in Qualität und Quantität zu. Deutschland als führende Wirtschaftsnation in Europa ist verstärkt im Fokus auch hochprofessioneller Cyberangriffe mit großem Wirkpotential. Angesichts der geopolitischen Lage gewinnen auch hybride Bedrohungen zunehmend an Bedeutung.

Der Krieg in der Ukraine verdeutlicht, wie essentiell Cybersicherheit für einen modernen Staat wie Deutschland ist. Die Gewährleistung einer verlässlichen und sicheren Nutzung der Informationstechnologie und der zugrundeliegenden Kommunikationsinfrastruktur ist essentielle Voraussetzung für das Funktionieren des Gemeinwesens. Deutschlands wirtschaftlicher Erfolg und gesellschaftlicher Zusammenhalt sowie die nationale Sicherheit sind mit der Gewährleistung von Cybersicherheit untrennbar verbunden. Angriffe im Cyberraum überwinden mühelos Landes- oder Zuständigkeitsgrenzen und können sich dadurch auf sämtliche Lebensbereiche und Sektoren einschließlich der Kommunikationsinfrastruktur insgesamt auswirken. Gezielte Angriffe auf kritische Infrastrukturen und wichtige Unternehmen, Aktionen von Cyberkriminellen oder Angriffe auf bzw. Sabotage von staatlichen Strukturen sind geeignet, die Funktionsfähigkeit des Gemeinwesens, der Wirtschaft und des Staats- und Verwaltungswesens massiv und anhaltend zu beeinträchtigen.

Dieser sicherheitspolitischen Herausforderung kann nur begegnet werden, indem die Erkennung und Abwehr von Cyberangriffen ausgebaut wird und hierzu wirksame, angemessene und rechtsklare gesetzliche Grundlagen geschaffen werden. Die Aufklärung und die Detektion konkreter Angriffe und langfristig laufender Angriffskampagnen müssen verbessert und die Detektion konkreter Vorbereitungshandlungen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) ausgebaut werden. Insbesondere gegen groß angelegte Cyberangriffe mit großem Schadenspotential bieten präventive Maßnahmen in den eigenen IT-Systemen alleine allerdings keinen hinreichenden Schutz. Es müssen daher für die Polizeien des Bundes und das BSI ergänzend Möglichkeiten zur Unterbindung solcher Cyberangriffe geschaffen werden, um gravierende Folgeschäden abwenden oder minimieren zu können.

II. Wesentlicher Inhalt des Entwurfs

Der Entwurf sieht Anpassungen im BSI-Gesetz (BSIG) vor, mit denen dem BSI ermöglicht wird, die Resilienz der Informationstechnik der Bundesverwaltung im Cyberraum zu erhöhen und die Erkenntnislage zu verbessern. Des Weiteren erhalten die Polizeien des Bundes im Bundeskriminalamtsgesetz (BKAG) und im Bundespolizeigesetz (BPolG) die notwendigen Befugnisse, um eine zukunftsfähige Cyberabwehr aufzubauen.

Die bestehenden Möglichkeiten des BSI, schädlichen Datenverkehr umzuleiten, werden an die geänderten Nutzungsbedingungen angepasst, indem die bestehenden Anordnungsbefugnisse auf weitere zentrale Diensteanbieter erweitert werden. Zugleich werden die Möglichkeiten verbessert, auf maliziöse Domains, die die Bundesverwaltung tangieren, zu reagieren. Zudem wird der Einsatz von Incident Response Teams zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme auch in Fällen des so genannten Prepositionings (d.h. das vorbereitende Platzieren von Hintertüren und Angriffsstrukturen in IT-Systemen) klar geregelt. Ferner wird eine Rechtsgrundlage dafür geschaf-

fen, die für den Betrieb von Angriffserkennungssystemen und die Einschätzung der aktuellen Bedrohungslage erforderliche Datengrundlage durch entsprechende Auskunftsersuchen zu technischen Informationen zu verbessern. Komplementär hierzu soll die Ausbreitung maliziöser Infrastruktur eingedämmt werden, indem Endnutzern ein optionaler Schutz vor maliziösen Domains bereitgestellt wird und, wie bisher bereits Telekommunikationsanbieter, auch Anbieter digitaler Dienste verpflichtet werden, Informationen des BSI über konkrete Gefahren, die ihre Kunden betreffen, an diese weiterzugeben.

Für das Bundeskriminalamt (BKA) und die Bundespolizei werden klare Befugnisse geschaffen, um Cyberangriffe abzuwehren. Dazu gehören insbesondere Befugnisse zur Untersagung des Betriebs informationstechnischer Systeme, zur Umleitung, Einschränkung oder Unterbindung von Datenverkehr, sowie zum Auslesen, Löschen und Verändern von gefahrgegenständlichen Daten in informationstechnischen Systemen. Diese neu geschaffenen Befugnisse werden es den Polizeien des Bundes ermöglichen, zusammen mit den bereits bestehenden polizeilichen Befugnissen wie z.B. der Sicherstellung von Servern, eine wirksame Gefahrenabwehr gegen Cyberangriffe umzusetzen.

Die neugeschaffenen Befugnisse erhält das BKA für bereits bestehende gefahrenabwehrrechtliche Aufgaben sowie für die neuen Aufgaben im Bereich der Abwehr von Gefahren durch Angriffe auf die Sicherheit in der Informationstechnik. Die Bundespolizei erhält diese Befugnisse für alle ihre gefahrenabwehrrechtlichen Aufgaben.

III. Alternativen

Keine.

IV. Gesetzgebungskompetenz

Für die Änderung des Bundespolizeigesetzes in Artikel 1 folgt die Gesetzgebungskompetenz des Bundes aus Artikel 73 Absatz 1 Nummer 5 (Grenzschutz), 6 (Luftverkehr) und 6a (Eisenbahnen) des Grundgesetzes (GG) sowie aus der Natur der Sache (u.a. Schutz von Bundesorganen).

Für die Änderungen des BSI-Gesetzes in Artikel 2, die den rein technischen Schutz der Informationstechnik von und für Unternehmen und sonstige Einrichtungen im besonderen öffentlichen Interesse betreffen, folgt die Gesetzgebungskompetenz des Bundes aus Artikel 73 Absatz 1 Nummer 7 GG (Telekommunikation) 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 BSI gegenüber Anbietern von Telekommunikations- und Digitalen Diensten (einschließlich den Anbietern von Domainname-Diensten) mit Blick auf die Notwendigkeit eines bundeseinheitlichen Niveaus von Cybersicherheit der Diensteanbieter bezüglich im Telekommunikationsgesetz verankerter gewerblicher Pflichten dieser Anbieter sowie mit Blick auf die Notwendigkeit der näheren Überwachung der im Digitale Dienste Gesetz verankerten gewerberechtlichen Pflichten der Digitale Diensteanbieter. Hier ist zur Aufrechterhaltung sicherer IT-Strukturen und -anwendungen eine bundesweit einheitliche Gefahrenabwehr erforderlich.

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

Die Regelungen in Artikel 3 zur Änderung des Bundeskriminalamtgesetzes beruhen auf Artikel 73 Absatz 1 Nummer 1 (auswärtige Angelegenheiten sowie Verteidigung einschließlich des Schutzes der Zivilbevölkerung), Artikel 73 Absatz 1 Nummer 9a GG (Abwehr von Gefahren des internationalen Terrorismus), Artikel 73 Absatz 1 Nummer 10 GG (internatio-

nale Verbrechensbekämpfung) in Verbindung mit der Gesetzgebungskompetenz des Bundes aus der Natur der Sache sowie auf der Gesetzgebungskompetenz aus der Natur der Sache (insbesondere Schutz von Mitgliedern von Verfassungsorganen des Bundes, Schutz der Funktionsfähigkeit der Einrichtungen und Behörden des Bundes).

Die Gesetzgebungskompetenz des Bundes für die Regelungen zum gerichtlichen Verfahren in den Artikeln 1, 2 und 3 sowie für die Regelungen zu den Bußgeldvorschriften in den Artikeln 1, 2, 3 und 5 folgt aus Artikel 74 Absatz 1 Nummer 1 GG (gerichtliches Verfahren, Strafrecht).

Die Änderungen des Telekommunikation-Digitale-Dienste-Datenschutzgesetzes (TDDDG) in Artikel 4 beruht auf Artikel 74 Absatz 1 Nummer 11 GG (Recht der Wirtschaft) in Verbindung mit Artikel 72 Absatz 2 GG. Eine bundesgesetzliche Regelung dieser Materie ist zur Wahrung der Wirtschaftseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich. Eine Regelung durch den Landesgesetzgeber würde zu erheblichen Nachteilen für die Gesamtwirtschaft führen, die sowohl im Interesse des Bundes als auch der Länder nicht hingenommen werden können. Insbesondere wäre zu befürchten, dass unterschiedliche landesrechtliche Behandlungen gleicher Lebenssachverhalte erhebliche Wettbewerbsverzerrungen und störende Schranken für die länderübergreifende Wirtschaftstätigkeit zur Folge hätten. Gerade Telemedienangebote sind typischerweise bundesweit zugänglich. Unterschiedliche technik-bezogene Ausgestaltungsregelungen in den Ländern wären praktisch nicht umsetzbar. Im Interesse des Bundes und der Länder muss die Teilhabe an einer sich stetig weiterentwickelnden Informationsgesellschaft, der eine wesentliche wirtschaftslenkende Bedeutung zukommt, gewahrt bleiben.

Die Änderungen des Energiewirtschaftsgesetzes beruhen auf Art. 74 Absatz 1 Nummer 11 GG (Recht der Wirtschaft) in Verbindung mit Art. 72 Absatz 2 GG. Eine bundesgesetzliche Regelung dieser Materie ist zur Wahrung der Wirtschaftseinheit im Bundesgebiet im gesamtstaatlichen Interesse erforderlich. Eine Regelung durch den Landesgesetzgeber würde zu erheblichen Nachteilen für die Gesamtwirtschaft führen, die sowohl im Interesse des Bundes als auch der Länder nicht hingenommen werden können. Insbesondere wäre zu befürchten, dass unterschiedliche landesrechtliche Anforderungen an die von den Betreibern Kritischer Infrastrukturen zu treffenden Sicherheitsvorkehrungen erhebliche Wettbewerbsverzerrungen und störende Schranken für die länderübergreifende Wirtschaftstätigkeit zur Folge hätten.

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

Der Gesetzentwurf steht mit dem Recht der Europäischen Union und den für die Bundesrepublik Deutschland verbindlichen völkerrechtlichen Verträgen im Einklang. Er berührt weder die Regelungen des primären noch des sekundären Unionsrecht in einer Weise, die einer Umsetzung oder Anwendung entgegensteht.

Der Gesetzentwurf ist ferner mit den von der Bundesrepublik Deutschland abgeschlossenen völkerrechtlichen Verträgen vereinbar. Insbesondere stehen seine Regelungen im Einklang mit den Verpflichtungen aus der Europäischen Menschenrechtskonvention sowie weiteren einschlägigen internationalen Übereinkommen.

VI. Gesetzesfolgen

1. Rechts- und Verwaltungsvereinfachung

Der Gesetzentwurf trägt zur Rechts- und Verwaltungsvereinfachung bei, indem er die Pflichten und Rechte des BSI schärft und somit dazu beiträgt, die jeweiligen Verantwortungen klarzustellen.

2. Nachhaltigkeitsaspekte

Der Gesetzentwurf steht im Einklang mit dem Leitgedanken der Bundesregierung zur nachhaltigen Entwicklung im Sinne der Deutschen Nachhaltigkeitsstrategie, die der Umsetzung der UN-Agenda 2030 für nachhaltige Entwicklung der Vereinten Nationen dient.

Die Schaffung von Befugnissen im Bereich der Cyberabwehr beim BKA, der Bundespolizei und dem BSI zur Abwehr schwerwiegender Gefahren für die Sicherheit in der Informationstechnik und entsprechenden Befugnissen macht Deutschland im Cyberraum handlungsfähiger und resilienter. Cyberangriffen und sonstigen damit verbundenen Formen der Cyberkriminalität wird so zielgerichtet entgegengewirkt und schwerwiegende Schadenseintritte werden abgewendet oder minimiert.

3. Haushaltsausgaben ohne Erfüllungsaufwand

a) Bundeskriminalamt

Mit der neuen Aufgabe der Abwehr von Gefahren durch Angriffe auf die Sicherheit in der Informationstechnik sowie mit der Einführung der cyberspezifischen Befugnisse wird das BKA befähigt, Maßnahmen der Cyberabwehr für eigene originäre Aufgaben (§§ 5, 6, 7 und 8 BKAG) zu bearbeiten. Mit dieser Erweiterung der Aufgaben und Befugnisse ergeben sich beim BKA zusätzliche Personal- und Sachausgaben. Die Cyberabwehr unterteilt sich in drei wesentliche Prozesse: Die unmittelbare Abwehr von Gefahren durch Angriffe auf die Informationstechnik, die Auswertung und Bewertung vorliegender Informationen zu (drohenden) Cyberangriffen sowie die Aufklärung und technische Bereitstellung von Daten und Informationen im Rahmen der polizeilichen Zentralstellenaufgabe. Die unmittelbare Abwehr von Gefahren durch Angriffe auf die Sicherheit in der Informationstechnik umfasst hierbei alle Arbeitsprozesse, die erforderlich sind, um eine erkannte, bereits bestehende polizeiliche Gefahrenlage national und international koordiniert abzuwehren.

Das Erfordernis, gefahrenreduzierende Maßnahmen im Vorgriff oder in Ergänzung von Strafverfolgungsmaßnahmen operativ umzusetzen, ist dabei stark einzelfallabhängig und kann qualitativ und quantitativ stark variieren, von einfachen Cyberabwehrmaßnahmen bis hin zu einem komplexen und technisch herausragenden Maßnahmenbündel.

Vor dem Hintergrund möglicher Fallkonstellationen aufgrund der verschiedenen gesetzlichen Aufgaben des BKA, die eine Umsetzung operativer Maßnahmen zur Gefahrenabwehr erforderlich machen, und der besonderen, spezifischen Herausforderungen der Gefahrenabwehr, ist angesichts der bestehenden Bedrohungslage mit einer signifikanten Anzahl gefahrenreduzierender Maßnahmen zu rechnen. Zudem ist mit einer zusätzlichen Wechselwirkung von Gefahrenabwehrmaßnahmen und sich anschließenden, strafverfolgenden Maßnahmen zu rechnen, welche durch das BKA aus einer Hand durchgeführt werden.

Die Umsetzung der gesetzlichen Aufgabe erzeugt im BKA den nachstehenden Aufwand:

- Umleitung von maliziösem Datenverkehr
- Untersagung des Betriebs von informationstechnischen Systemen

- Eingriff in informationstechnische Systeme zum Zweck des Auslesens, der Löschung und der Änderung von Daten
- Takedown und Sinkholing einer professionellen und leistungsfähigen Störer-Infrastruktur
- Monitoring von Foren und Marktplätzen im Darknet
- Analyse von Schadsoftware und deren Verbreitung
- Bewertung von Cyber-Bedrohungen und deren Auswirkungen auf die öffentliche Sicherheit
- Erstellung von Lagebildern und Prognosen zu Cyber-Bedrohungen
- Erfassung und Analyse von Daten zu Cyberangriffen
- Entwicklung von technischen Tools zur Unterstützung der Cyber-Abwehr
- Bereitstellung von Daten und Informationen zu Cyber-Bedrohungen für andere Behörden und Organisationen

Die Personalkosten fallen dabei jährlich aufwachsend wie folgt an:

Jahr	**2027**	**2028**	**2029**	**2030**	**2031**
Personal	19 hD / 86 gD	14 hD / 81 gD	6 hD / 38 gD	5 hD / 7 gD	5 hD / 3 gD
Personalkosten*	9.885.984 €	8.831.173 €	4.073.034 €	1.230.265 €	879.358 €
Personalnahe Sacheinzelkosten*	3.596.250 €	3.253.750 €	1.507.000 €	411.000 €	274.000 €

*Die Kosten fallen im jeweiligen Haushalt zusätzlich an und sind in den Folgejahren kumulierend zu berücksichtigen.

Durch die gesetzliche Änderung entstehen jährliche Kosten in Höhe von 5.000.000 Euro für Hardware, Lizenzen, Betrieb- und Wartung.

b) Bundesamt für Sicherheit in der Informationstechnik

Die Umsetzung der Gefahrenabwehr im digitalen Raum in den originären Aufgabenbereichen neben den gesetzlichen Änderungen auch die Fortentwicklung der Organisation mit Personal und Technik. Notwendig ist insbesondere die personelle und technische Erweiterung der bestehenden Fähigkeiten des BSI, da u.a. die von den Angreifern genutzte Technik komplex und hochgradig gesichert ist.

Derzeit betreut das BSI die Betreiber kritischer Anlagen bei der Etablierung und dem Betrieb von Systemen zur Angriffserkennung i. S. d. § 2 Nummer 41 BSIG. Diese Systeme sollen durch die zukünftige Anbindung an das BSI neben den bisherigen geeigneten Parametern und Merkmalen aus dem laufenden Betrieb auch regelmäßige Verfügbarkeitsindikatoren der kritischen Anlage kontinuierlich und automatisch erfassen und diese an das BSI übertragen. Die Erstellung der konkreten inhaltlichen Anforderungen an die Datenerhebung und Übertragung obliegt dem BSI, welches die Anforderungen zudem auf die fortlaufende Ver-

änderung der technischen IT-Sicherheitsbedrohungslage regelmäßig anpassen soll. Diese inhaltliche Ausgestaltung erfordert einerseits eine wiederholte Auseinandersetzung mit der beabsichtigten weiteren Datenverarbeitung, der Datenweiterverwertung und dem derzeitigen Stand der Technik. Weiterhin muss sie sich an der technischen Funktionalität der Schnittstelle zwischen dem BSI und den referenzierten Systemen zur Angriffserkennung orientieren, damit die inhaltliche Spezifikation auch im Rahmen der Möglichkeiten der technischen Ausgestaltung abgebildet wird.

Eingehende Meldungen müssen kontinuierlich ausgewertet und für eine Lagedarstellung aufbereitet werden. Bei Störungen müssen reaktive Maßnahmen daraus abgeleitet werden.

Durch die weitergehende Verwendung und dadurch gesteigerte Bedeutung der Systeme zur Angriffserkennung – unter dem gleichzeitigen Wegfall der Nachweispflicht über ihre Verwendung aus dem bisherigen Geltungsbereich des Nachweises kritischer Anlagen – rückt die Aufsicht über den ordnungsgemäßen Einsatz in den verstärkten Fokus des BSI. Eine Sanktionierung des nicht ordnungsgemäßen Einsatzes war in der bisherigen Fassung des § 65 BSIG nicht vorgesehen. Mit ihrer Aufnahme obliegt den betreuenden Fachreferaten die Prüfung der Systemverwendung, die Abfrage und Mahnung des Betreibers, die fachseitige Ermittlung der Gründe für die zunächst festgestellte Nichtnutzung und die Vorbereitung zur Übergabe für ein eventuell notwendiges Sanktionsverfahren im BSI. Gerade zu Beginn der Umstellung hin zu einer Anbindung wird dabei ein etwas höheres Aufkommen an notwendigen Prüfungen, Betreiberkommunikation und, soweit nötig, Verfahren erwartet.

Durch die Erweiterung des Verpflichtetenkreises in Bezug auf Anordnungen nach § 16 BSIG wächst der Umsetzungsaufwand, da zusätzliche Schnittstellen zu weiteren Verpflichteten etabliert und dauerhaft aufrechterhalten werden müssen.

Wechselnde maliziöse Internet-Domänen nehmen bei der Verbreitung von Schadsoftware eine tragende Rolle ein. § 15 BSIG ermöglicht dem BSI ein Vorgehen gegen solche Domänen. Hierzu müssen Meldewege etabliert, eine Datenbank geschaffen und Rückkanäle zu DNS-Diensteanbietern aufgebaut und dauerhaft betreut werden.

Derzeit unterstützt das BSI bereits auf Ersuchen einer betroffenen Institution bei der Wiederherstellung der Sicherheit und Funktionsfähigkeit der informationstechnischen Systeme (also bei konkreten IT-Sicherheitsvorfällen). Durch die Gesetzesänderung erhält das BSI auch das Recht, auf Ersuchen einer Institution in deren informationstechnischen Systemen nach vorbereitenden Maßnahmen von Angreifern (sog. Prepositioning) zu suchen und diese zu identifizieren (sog. Threat Hunting). Das BSI plant vorerst, pro Jahr drei solcher Threat Hunting-Untersuchungen durchzuführen; eine Steigerung der Anzahl ist durchaus vorgesehen. Da beim Threat Hunting dieselben technischen Methoden und Werkzeuge wie bei der seit Jahren praktizierten Vorfallsbearbeitung angewendet werden, ist der für das Threat Hunting veranschlagte Personalbedarf eher gering.

Durch die Erweiterung der Befugnisse entstehen neue Aufwände für die rechtliche Begleitung der technischen Aufgaben, insbesondere im Bereich der Durchsetzung von einzelnen technischen Maßnahmen. Zudem entstehen neue rechtliche Aufwände durch die Erweiterung der Sanktionsverfahren auf den nicht ordnungsgemäßen Einsatz von Systemen zur Angriffserkennung. Die Rechtsreferate beraten die Abteilungen des Hauses bei der rechtmäßigen Ausübung ihrer Befugnisse. Hierbei handelt es sich um eine Daueraufgabe. Durch die erhebliche Befugniserweiterung werden die Beratungsanfragen, insbesondere bei den Abteilungen I (z.B. für § 8 BSIG-neu), Abteilung C (z.B. für § 11 BSIG-neu), Abteilung S (z.B. für § 15 BSIG-neu) sowie Abteilung W (z.B. für § 31 BSIG-neu) des BSI, ansteigen. Durch die Ausweitung und Veränderung der Systematik des BSIG werden zahlreiche Auslegungsfragen erwartet sowie die rechtliche Beratung in der operativ-technischen Umset-

zung. Der Schwerpunkt der Rechtsberatung wird hier auf der verhältnismäßigen Ausübung der Befugnisse liegen.

Die Personalkosten fallen dabei jährlich aufwachsend wie folgt an:

Jahr	**2027**	**2028**	**2029**	**2030**
Personal	7 hD / 3 gD	1 hD / 2 gD / 1 mD	4 hD / 2 gD	1 hD
Personalkosten*	1.125.829 €	366.000 €	668.395 €	123.235 €
Personalnahe* Sacheinzelkosten	342.500 €	137.000 €	205.500 €	34.250 €

*Die Kosten fallen im jeweiligen Haushalt zusätzlich an und sind in den Folgejahren kumulierend zu berücksichtigen.

c) Bundespolizei

Die Umsetzung der Gefahrenabwehr im digitalen Raum in den originären Aufgabenbereichen der Bundespolizei erfordert neben den gesetzlichen Änderungen auch die Fortentwicklung der Organisation mit Personal und Technik. Notwendig ist insbesondere die personelle und technische Erweiterung der bestehenden Fähigkeiten der Bundespolizei, da u.a. die von den Angreifern genutzte Technik komplex und hochgradig gesichert ist. Zur Abwehr von Cyberangriffen analysiert die Bundespolizei unter anderem Datenströme, Codierungsverfahren, Protokollstrukturen sowie kryptographische und steganographische Techniken. Darüber hinaus gehören technische Verwundbarkeitsprüfungen und Penetrationstests zur Identifikation und Bewertung sicherheitsrelevanter Schwachstellen in den IT-Systemen der Bundespolizei zum Aufgabenbereich. Die informationstechnischen Ansatzpunkte für die gefahrenabwehrenden Behörden sind vielfältig. Die für die Angriffe genutzten Steuerungssysteme sind in der Regel weltweit verteilt und die Angreifer selbst agieren häufig aus dem Ausland. Botnetze verdeutlichen, wie komplex die zu erkennenden Strukturen sein können: Sie werden von international agierenden Angreifern mithilfe weit verbreiteter Schadsoftware in verschiedenste Systeme eingeschleust. Ihre Auswertung ist entscheidend, um die Angriffsstrategie und mögliche Hinweise auf die Störer zu identifizieren. Angreifer, die in der Lage wären, erfolgreiche Angriffe gegen Behörden und Unternehmen aus dem Aufgabenkontext der Bundespolizei vorzubereiten bzw. ausführen, sind weitestgehend staatlich organisiert oder beauftragt. Hybride Bedrohungen gewinnen in diesem Zusammenhang zunehmend an Bedeutung, da Angreifer staatlich instrumentalisiert und gesteuert werden können. Eine Aufklärung derartiger Infrastruktur erfordert in der Regel eine mittel- bis langfristige Befassung und damit eine Konzentration und Professionalisierung des eingesetzten Personals je spezifischem Akteur.

Eine erfolgreiche Abwehr von Gefahren für die Sicherheit in der Informationstechnik muss sich daher auf zwei Bereiche fokussieren: auf die operative fallbezogene und auf die technische Abwehr von Gefahren für die Sicherheit in der Informationstechnik. Das Aufgabenfeld der Bundespolizei im Bereich der Cyberabwehr umfasst die Abwehr, Aufklärung und Reaktion auf Cyberangriffe und fremdgesteuerte Cyberkampagnen. Dazu zählen insbesondere die Bearbeitung von IKT-bezogenen Sicherheitsvorfällen, die revisionssichere Sicherung und Auswertung digitaler Spuren, die Durchführung forensischer Analysen, technische Unterstützungsleistungen sowie die Ableitung von Handlungsempfehlungen zur Stärkung der IT-Sicherheit. So sind neben klassischen technischen Fähigkeiten, wie der beweissi-

cheren Erfassung aller relevanten Spuren (digitale Forensik), im gefahrenabwehrenden Handeln auch polizeiliche Cyberermittlerkompetenzen auszubauen. Einsätze im Rahmen der aktiven Abwehr von Gefahren für die Sicherheit in der Informationstechnik müssen unter qualitativ höchsten Maßstäben vorbereitet, durchgeführt und dokumentiert werden. Insbesondere sind hier Datenschutz- und Persönlichkeitsrechte betreffende Vorgaben umzusetzen, welche unter Umständen die Aufwände für einen erfolgreichen risikominimierten Einsatz erhöhen.

Die Personalkosten fallen dabei jährlich aufwachsend wie folgt an:

Jahr	**2027**	**2028**	**2029**	**2030**	**2031**
Personal	5 hD / 9 gD /	5 hD / 17 gD / 3 mD /	5 hD / 16 gD	5 hD / 10 gD	5 hD / 10 gD
Personal-kosten*	1.819.006 €	2.988.458 €	2.613.639 €	1.932.525 €	1.932.525 €
Personal-nahe Sachein-zelkosten*	534.788 €	878.607 €	768.410 €	568.162 €	568.162 €

*Die Kosten fallen im jeweiligen Haushalt zusätzlich an und sind in den Folgejahren kumulierend zu berücksichtigen.

Durch die gesetzliche Änderung entstehen einmalige investive Sachkosten in Höhe von 2,5 Millionen Euro sowie ab Anschaffung jährliche Kosten in Höhe von 2,3 Millionen Euro für Hardware, Lizenzen, Betrieb- und Wartung.

Der Mehrbedarf an Sach- und Personalmitteln sowie an Planstellen und Stellen für BSI, BKA und BPOL soll im Einzelplan 06 ausgeglichen werden.

4. Erfüllungsaufwand

Das geplante Regelungsvorhaben dient im Wesentlich der Abwehr von erheblichen Gefahren im Bereich der IT-Sicherheit und ist daher von der One in, one out-Regel (sog. „Bürokratiebremse“) ausgenommen.

4.1. Erfüllungsaufwand für Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

4.2. Erfüllungsaufwand für die Wirtschaft

lfd. Nr.	Norm; Bezeichnung der Vorgabe	IP	Fallzahl	Jährlicher Aufwand pro Fall (Minuten * Lohnkosten pro Stunde (Wirtschaftszweig)	Jährlicher Erfüllungsaufwand (in Tsd. Euro)	Einmalige Fallzahl	Einmaliger Aufwand pro Fall in Euro	Einmaliger Erfüllungsaufwand in Tsd. Euro
4.2.1	§ 41a Abs. 2 Nummer 1 i. V. m § 41a Abs. 1 BPolG-E Mitwirkung an Abwehrmaßnahmen gegen Angriffe auf die IT-Sicherheit		30	5.280 Euro = (6.000 / 60 * 52,80 Euro/h (WZ: J))	158			
4.2.2	§ 41a Abs. 2 Nr. 2 i. V. m § 41a Abs. 1 BPolG-E Mitwirkung an Abwehrmaßnahmen gegen Angriffe auf die IT-Sicherheit		10	5.280 Euro = (6.000 / 60 * 52,80 Euro/h (WZ: J))	53			
4.2.3	§ 15, Abs. 6 BSIG-E	ja	1.000	105,6 Euro = (120 / 60 *	106			

lfd. Nr.	Norm; Bezeichnung der Vorgabe	IP	Fallzahl	Jährlicher Aufwand pro Fall (Minuten * Lohnkosten pro Stunde (Wirtschaftszweig)	Jährlicher Erfüllungsaufwand (in Tsd. Euro)	Einmalige Fallzahl	Einmaliger Aufwand pro Fall in Euro	Einmaliger Erfüllungsaufwand in Tsd. Euro
	Bereitstellung von Informationen durch Anbieter von Telekommunikationsdiensten und digitalen Anbietern			52,80 Euro/h (WZ: J))				
4.2.4	§ 16 Abs. 6 BSIG-E Auf Grundlage der vom BSI veröffentlichten Informationen Kunden einen DNS-basierten Schutz vor Angriffen im Zusammenhang mit sicherheitsriskanten Domains anzubieten		5	52.800 Euro = (60.000 / 60 * 52,80 Euro/h (WZ: J))	264			

lfd. Nr.	Norm; Bezeichnung der Vorgabe	IP	Fallzahl	Jährlicher Aufwand pro Fall (Minuten * Lohnkosten pro Stunde (Wirtschaftszweig)	Jährlicher Erfüllungsaufwand (in Tsd. Euro)	Einmalige Fallzahl	Einmaliger Aufwand pro Fall in Euro	Einmaliger Erfüllungsaufwand in Tsd. Euro
4.2.5	§ 16a BSIG-E Umsetzung der Anordnungsbefugnis gegenüber Top Level Registries und Registraren		40	264 Euro = (300 / 60 * 52,80 Euro/h (WZ: J))	11			
4.2.6	§ 17 Abs. 2 BSIG-E Bei Anordnung des BSI Datenverkehr an eine benannte Domain oder Anschlusskennung umzuleiten oder zu unterbinden		40	2.640 Euro = (3.000 / 60 * 52,80 Euro/h (WZ: J))	106			
4.2.7	§ 31 Abs. 2 BSIG-E Anbindung von Systemen zur Angriffserkennung bei		2.100	2.112 Euro = (2.400 / 60 * 52,80 Euro/h (WZ: J))	4.435	2.100	2.112 Euro = (2.400 / 60 * 52,80 Euro/h (WZ: J))	4.435

lfd. Nr.	Norm; Bezeichnung der Vorgabe	IP	Fallzahl	Jährlicher Aufwand pro Fall (Minuten * Lohnkosten pro Stunde (Wirtschaftszweig)	Jährlicher Erfüllungsaufwand (in Tsd. Euro)	Einmalige Fallzahl	Einmaliger Aufwand pro Fall in Euro	Einmaliger Erfüllungsaufwand in Tsd. Euro
	Betreibern kritischer Anlagen an das BSI							
4.2.8	§ 50 Abs. 1 BSIG-E Zugang zu Domain-Namen-Registrierungsdaten gewähren		50	422,4 Euro = (480 / 60 * 52,80 Euro/h (WZ: J))	21			
4.2.9	§ 19 Abs. 5 und 6 TDDDG-E Benachrichtigungen durch Dienstanbieter	ja	402.000	0,44 Euro = (0,5 / 60 * 52,80 Euro/h (WZ: J))	177			
4.2.10	§ 68b BKAG-E Untersagung des Betriebs eines informationstechnischen Systems		300	5.280 Euro = (6.000 / 60 * 52,80 Euro/h (WZ: J))	1.584			
4.2.11	§ 68c Abs. 2 BKAG-E		600	5.280 Euro = (6.000	3.168			

lfd. Nr.	Norm; Bezeichnung der Vorgabe	IP	Fallzahl	Jährlicher Aufwand pro Fall (Minuten * Lohnkosten pro Stunde (Wirtschaftszweig)	Jährlicher Erfüllungsaufwand (in Tsd. Euro)	Einmalige Fallzahl	Einmaliger Aufwand pro Fall in Euro	Einmaliger Erfüllungsaufwand in Tsd. Euro
	Mitwirkung an Abwehrmaßnahmen gegen Angriffe auf die IT-Sicherheit			/ 60 * 52,80 Euro/h (WZ: J))				
	Summe (in Tsd. Euro)				**10.082**			**4.435**
	davon aus Informationspflichten (IP)				**282**			**0**

Lfd. Nr. 4.2.1: Mitwirkung an Abwehrmaßnahmen gegen Angriffe auf die IT-Sicherheit; § 41a Absatz 2 Nummer 1 i.V.m § 41a Absatz 1 BPolG-E

Durch die gesetzliche Änderung wird die Bundespolizei ermächtigt, zur Abwehr von Angriffen auf die IT-Sicherheit den Betrieb eines informationstechnischen Systems durch ein Unternehmen zu untersagen. Die betroffenen Unternehmen unterliegen dabei einer Mitwirkungspflicht. Es wird angenommen, dass ca. 30 Unternehmen pro Jahr betroffen sind. Unter Berücksichtigung des durchschnittlichen Lohnsatzes für den Wirtschaftszweig J (Information und Kommunikation) von 52,80 Euro und einem Zeitaufwand von 100 Stunden pro Fall ergibt sich ein laufender Erfüllungsaufwand in Höhe von ca. 158.000 Euro.

Lfd. Nr. 4.2.2: Mitwirkung an Abwehrmaßnahmen gegen Angriffe auf die IT-Sicherheit; § 41a Absatz 2 Nummer 2 i.V.m § 41a Absatz 1 BPolG-E

Durch die gesetzliche Änderung wird die Bundespolizei ermächtigt, zur Abwehr von Angriffen auf die IT-Sicherheit den Datenverkehr an eine vorgegebene Zieladresse umzuleiten. Die betroffenen Unternehmen unterliegen dabei einer Mitwirkungspflicht. Es wird angenommen, dass ca. 10 Unternehmen pro Jahr betroffen sind. Unter Berücksichtigung des durchschnittlichen Lohnsatzes für den Wirtschaftszweig J (Information und Kommunikation) von 52,80 Euro und einem Zeitaufwand von 100 Stunden pro Fall ergibt sich ein laufender Erfüllungsaufwand in Höhe von ca. 53.000 Euro.

Lfd. Nr. 4.2.3: Bereitstellung von Informationen durch Anbieter von Telekommunikationsdiensten und digitalen Anbietern; § 15 Absatz 6 BSIG-E (Informationspflicht)

Die neue gesetzliche Regelung sieht vor, dass Anbieter von öffentlich zugänglichen Telekommunikationsdiensten und geschäftsmäßige Anbieter von digitalen Diensten bekannte sicherheitsrelevante technische Informationen, die Rückschlüsse auf Schadaktivitäten, Schwachstellen, Verwundbarkeiten oder aktuelle Bedrohungen geben, auf Anforderung dem BSI bereitzustellen haben. Es wird angenommen, dass pro Jahr ca. 1.000 Meldungen notwendig sind. Unter der Berücksichtigung des durchschnittlichen Lohnsatzes für diesen Wirtschaftszweig J (Information und Kommunikation) von 52,80 Euro und einem Zeitaufwand von 2 Stunden pro Fall, ergibt sich ein laufender Erfüllungsaufwand in Höhe von ca. 106.000 Euro.

Lfd. Nr. 4.2.4: **Auf Grundlage der vom BSI veröffentlichten Informationen Kunden einen DNS-basierten Schutz vor Angriffen im Zusammenhang mit sicherheitsriskanten Domains anzubieten; §16 Absatz 6 BSIG-E**

Die neue gesetzliche Regelung sieht vor, dass DNS-Anbieter ab einer relevanten Größe ihren Kunden auf Grundlage von Informationen des BSI einen Schutz vor Angriffen im Zusammenhang mit sicherheitsriskanten Domains anzubieten haben. Es wird angenommen, dass fünf Unternehmen bzw. DNS-Anbieter betroffen sind. Unter der Berücksichtigung des durchschnittlichen Lohnsatzes für den Wirtschaftszweig J (Information und Kommunikation) von 52,80 Euro und einem Zeitaufwand von 1.000 Stunden pro DNS-Anbieter ergibt sich ein laufender Erfüllungsaufwand in Höhe von ca. 264.000 Euro.

Lfd. Nr. 4.2.5: Umsetzung der Anordnungsbefugnis gegenüber Top Level Registries und Registrare; §16a BSIG-E

Das BSI kann zur Abwehr erheblicher Gefahren für die benannten Schutzgüter gegenüber Anbieter von Top Level Domain Name Registries und Domain-Name-Registry-Dienstleistern anordnen, dass sie die Namenseinträge einer Domain ändern oder neue Einträge hinzufügen. Dies umfasst auch die Dekonnektierung einer Domain, so dass diese nicht mehr erreichbar ist. Es wird angenommen, dass ca. 40 Anwendungsfälle pro Jahr auftreten. Unter Berücksichtigung des durchschnittlichen Lohnsatzes für den Wirtschaftszweig J (Information und Kommunikation) von 52,80 Euro und einem Zeitaufwand von 5 Stunden pro Anordnung ergibt sich ein laufender Erfüllungsaufwand in Höhe von ca. 11.000 Euro.

Lfd. Nr. 4.2.6: Bei Anordnung des BSI Datenverkehr an eine benannte Domain oder Anschlusskennung umzuleiten oder zu unterbinden; § 17 Absatz 2 BSIG-E

Das BSI kann zur Abwehr erheblicher Gefahren für die genannten Schutzgüter gegenüber Telekommunikationsanbietern anordnen, den Datenverkehr an eine vom BSI benannte Domain oder Anschlusskennung umzuleiten oder zu unterbinden. Es wird angenommen, dass ca. 40 Anwendungsfälle pro Jahr auftreten. Unter der Berücksichtigung des durchschnittlichen Lohnsatzes für den Wirtschaftszweig J (Information und Kommunikation) von 52,80 Euro, und einem Zeitaufwand von 50 Stunden pro Fall ergibt sich ein laufender Erfüllungsaufwand in Höhe von ca. 106.000 Euro.

Lfd. Nr. 4.2.7: Anbindung von Systemen zur Angriffserkennung bei Betreibern kritischer Anlagen an das BSI; § 31 Absatz 2 BSIG-E

Betreiber kritischer Anlagen sind verpflichtet Systeme zur Angriffserkennung einzusetzen und an das BSI anzubinden. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter, Merkmale aus dem laufenden Betrieb sowie regelmäßige Verfügbarkeitsindikatoren der kritischen Anlage kontinuierlich und automatisch erfassen, auswerten und an das BSI ausgeleitet werden. Es wird angenommen, dass pro Jahr ca. 2.100 kritische

Anlagen laufend angebunden sind. Unter Berücksichtigung des durchschnittlichen Lohnsatzes für den Wirtschaftszweig J (Information und Kommunikation) von 52,80 Euro und einem Zeitaufwand von 40 Stunden pro Fall ergibt sich ein laufender Erfüllungsaufwand in Höhe von ca. 4.435.000 Euro. Zudem wird angenommen, dass für die einmalige Anbindung der betreffenden kritischen Anlagen Kosten in gleicher Höhe einmalig anfallen (40 Stunden pro Fall * 52,80 Euro * 2.100 Anlagen = 4.435.000 Euro).

Lfd. Nr. 4.2.8: Zugang zu Domain-Namen-Registrierungsdaten gewähren; § 50 Absatz 1 BSIG-E

Auf Anfrage des BSI müssen Top-Level-Domain-Registries und Domain-Registry-Dienstleister einen Zugang auf Domain-Registrierungsdaten gewähren. Es wird angenommen, dass 50 Zugangsanfragen pro Jahr gewährt werden müssen. Unter Berücksichtigung des durchschnittlichen Lohnsatzes für den Wirtschaftszweig J (Information und Kommunikation) in Höhe von 52,80 Euro und einem angenommenen Zeitaufwand pro Fall von 8 Stunden ergibt sich ein laufender Erfüllungsaufwand in Höhe von ca. 21.000 Euro.

Lfd. Nr. 4.2.9: Benachrichtigungen durch Dienstanbieter, § 19 Absatz 5 und 6 TDDDG-E (Informationspflicht)

Anbieter digitaler Dienste sind künftig dazu verpflichtet, Informationen des BSI über konkrete Gefahren, die Kunden der Anbieter betreffen, an ihre Nutzer weiterzugeben. Es wird angenommen, dass pro Jahr ca. 402.000 Kundenbenachrichtigungen notwendig sind, welche aber hochautomatisiert sind. Als Zeitansatz werden daher vereinfacht 0,5 Minuten pro Fall angesetzt. Unter Berücksichtigung des durchschnittlichen Lohnsatzes für den Wirtschaftszweig J (Information und Kommunikation) in Höhe von 52,80 Euro und einem Zeitaufwand pro Fall ergibt sich ein laufender Erfüllungsaufwand in Höhe von ca. 177.000 Euro.

Lfd. Nr. 4.2.10: Untersagung des Betriebs eines informationstechnischen Systems; § 68b BKAG-E

Um Cyberbedrohungen abzuwenden und einzudämmen, kann das BKA den Betrieb eines informationstechnischen Systems untersagen. Dies kann zum Beispiel durch die Deaktivierung infizierter Server von Unternehmen erreicht werden. Eine Abstimmung mit betroffenen Unternehmen ist in diesen Fällen notwendig. Es wird angenommen, dass ca. 300 Anwendungsfälle auftreten. Als zeitlicher Aufwand pro Fall werden 100 Stunden angesetzt. Bei einem durchschnittlichen Lohnsatz von 52,80 Euro (Wirtschaftszweig J „Information und Kommunikation“) entsteht ein laufender Erfüllungsaufwand in Höhe von ca. 1.584.000 Euro.

Lfd. Nr. 4.2.11: Mitwirkung an Abwehrmaßnahmen gegen Angriffe auf die IT-Sicherheit; § 68c Absatz 2 BKAG-E

Durch die gesetzliche Änderung wird das BKA ermächtigt, zur Abwehr von Angriffen auf die IT-Sicherheit den Datenverkehr an eine vorgegebene Zieladresse umzuleiten. Die betroffenen Unternehmen unterliegen dabei einer Mitwirkungspflicht. Es wird angenommen, dass ca. 600 Unternehmen pro Jahr betroffen sind. Unter Berücksichtigung des durchschnittlichen Lohnsatzes für den Wirtschaftszweig J (Information und Kommunikation) von 52,80 Euro und einem Zeitaufwand von 100 Stunden pro Fall ergibt sich ein laufender Erfüllungsaufwand in Höhe von ca. 3.168.000 Euro.

4.3. Erfüllungsaufwand der Verwaltung

lfd. Nr.	Norm; Bezeichnung der Vorgabe	Bund/ Land	Fallzahl	Jährlicher Aufwand pro Fall	Jährlicher Erfüllungsaufwand in Tsd. Euro	Einmalige Fallzahl	Einmaliger Aufwand pro Fall in Euro	Einmaliger Erfüllungsaufwand in Tsd. Euro
4.3.1	§ 41a Abs. 1 BPolG-E Besondere Abwehrmaßnahmen gegen Angriffe auf die Sicherheit in der Informationstechnik	Bund	1	64.000	64	1	19.400.000	19.400,00
4.3.2	§ 41a Abs. 2, Nr. 1 BPolG-E Umleitung von Datenverkehr auf eine vorgegebene Zieladresse	Bund	1	2.967.240	2.967			
4.3.3	§ 41a Abs. 2, Nr. 2 BPolG-E Eingriff in ein informationstechnisches System	Bund	1	1.901.640	1.902			
4.3.4	§ 41a Abs. 2 Nr. 3 BPolG-E	Bund	1	3.819.720	3.820			

lfd. Nr.	Norm; Bezeichnung der Vorgabe	Bund/ Land	Fallzahl	Jährlicher Aufwand pro Fall	Jährlicher Erfüllungsaufwand in Tsd. Euro	Einmalige Fallzahl	Einmaliger Aufwand pro Fall in Euro	Einmaliger Erfüllungsaufwand in Tsd. Euro
	Untersagung des Betriebs eines informationstechnischen Systems							
4.3.5	§ 11 Abs. 1 und Abs. 3 BSIG-E Maßnahmen zur Abwehr und Eindämmung von Angriffen einschließlich der systematischen Suche nach Angriffspuren (Threat Hunting)	Bund	1	595.200	595			
4.3.6	§ 16 Abs. 6 BSIG-E Datenverarbeitung und Information zur Bekämpfung von Domainphishing	Bund	1	213.300	213			

lfd. Nr.	Norm; Bezeichnung der Vorgabe	Bund/ Land	Fallzahl	Jährlicher Aufwand pro Fall	Jährlicher Erfüllungsaufwand in Tsd. Euro	Einmalige Fallzahl	Einmaliger Aufwand pro Fall in Euro	Einmaliger Erfüllungsaufwand in Tsd. Euro
4.3.7	§ 16a Abs. 1 BSIG-E Anordnung gegenüber Top Level Domains	Bund	1	35.520	36			
4.3.8	§ 16a Abs. 2 BSIG-E Verarbeitung und Auswertung umgeleiteter Daten	Bund	1	213.120	213			
4.3.9	§ 31 Abs. 2 BSIG-E Anbindung von Systemen zur Angriffserkennung bei Betreibern kritischer Anlagen an das BSI	Bund	1	1.119.360	1.119	1	211.080	211,00
4.3.10	§ 65 Abs. 2, Nummer 3a BSIG-E Bußgeldverfahren und Sanktionierung	Bund	1	106.560	107			

lfd. Nr.	Norm; Bezeichnung der Vorgabe	Bund/ Land	Fallzahl	Jährlicher Aufwand pro Fall	Jährlicher Erfüllungsaufwand in Tsd. Euro	Einmalige Fallzahl	Einmaliger Aufwand pro Fall in Euro	Einmaliger Erfüllungsaufwand in Tsd. Euro
	bei Fehlen eines geeigneten Systems zur Angriffserkennung							
4.3.11	§ 2 Abs. 5 Satz 1 Nr. 5 BKAG-E Unterstützung bei der Durchführung technischer Maßnahmen der Abwehr von Angriffen auf die Sicherheit in der Informationstechnik	Bund	1	710.000	710			
4.3.12	§ 3a BKAG-E Abwehr von Gefahren durch Angriffe auf die Sicherheit in der Informationstechnik	Bund	1	9.437.000	9.437			
4.3.13	§ 68a Abs. 1	Bund	1	995.000	995			

lfd. Nr.	Norm; Bezeichnung der Vorgabe	Bund/ Land	Fallzahl	Jährlicher Aufwand pro Fall	Jährlicher Erfüllungsaufwand in Tsd. Euro	Einmalige Fallzahl	Einmaliger Aufwand pro Fall in Euro	Einmaliger Erfüllungsaufwand in Tsd. Euro
	Nr.2 d i.V.m § 8 BKAG Eigenschutz der Liegenschaften, sonstigen Einrichtungen und Veranstaltungen des BKA							
4.3.14	§ 68b BKAG-E Untersagung des Betriebs informationstechnischer Systeme	Bund	1	3.426.000	3.426			
4.3.15	§ 68c BKAG-Einschränkung, Unterbindung und Umleitung von Datenverkehr	Bund	1	2.021.000	2.021			
4.3.16	§ 68d BKAG-E Auslesen, Löschen und Veränderung von Daten in	Bund	1	7.273.000	7.273			

lfd. Nr.	Norm; Bezeichnung der Vorgabe	Bund/ Land	Fallzahl	Jährlicher Aufwand pro Fall	Jährlicher Erfüllungsaufwand in Tsd. Euro	Einmalige Fallzahl	Einmaliger Aufwand pro Fall in Euro	Einmaliger Erfüllungsaufwand in Tsd. Euro
	informationstechnischen Systemen							
	Summe (in Tsd. Euro)				**34.898**			**19.611**
	davon Bund				**34.898**			**19.611**
	davon Land (inklusive Kommunen)				**0**			**0**

Lfd. Nr. 4.3.1: Besondere Abwehrmaßnahmen gegen Angriffe auf die Sicherheit in der Informationstechnik; § 41a Absatz 1 BPolG-E

Die Bundespolizei ist darauf angewiesen, vorbeugende Maßnahmen zu ergreifen, um Bedrohungen aus dem Cyberraum entgegenzuwirken, die ihre Einsatzfähigkeit beeinträchtigen könnten. Darüber hinaus setzt die Bundespolizei Cyberfähigkeiten erfolgreich zur Strafverfolgung, zur Sicherung ihrer eigenen Einrichtungen und zur Unterstützung anderer Behörden ein. Künftig kann die Bundespolizei zur Erfüllung ihrer Aufgaben besondere Abwehrmaßnahmen ergreifen, um Angriffe auf die Sicherheit in der Informationstechnik abzuwehren. Zur Sicherstellung der besonderen Abwehrmaßnahmen werden einmalige Sachkosten in Höhe von ca. 19,4 Millionen Euro notwendig. Zudem erweitern sich die datenschutzrechtlichen Aufsichtsmaßnahmen des BfDI. Es wird angenommen, dass dafür jährlich ca. 1.440 Stunden (0,9 MAK) notwendig sind. Unter der Berücksichtigung des durchschnittlichen Lohnsatzes für die Bundesverwaltung in Höhe von 44,40 Euro pro Stunde ergibt sich ein laufender Erfüllungsaufwand in Höhe von ca. 64.000 Euro auf Ebene des Bundes.

Lfd. Nr. 4.3.2: Umleitung von Datenverkehr auf eine vorgegebene Zieladresse; § 41a Absatz 2, Nummer 1 BPolG-E

Mit der gesetzlichen Anpassung wird der Bundespolizei die Möglichkeit gegeben, Datenverkehr zur Gefahrenabwehr an eine von der Bundespolizei vorgegebene Zieladresse umzuleiten und den umgeleiteten Datenverkehr aufzuzeichnen. Die Maßnahme zielt dabei auch auf die Aufzeichnung und Auswertung des Datenverkehrs zwischen Angreifer und bedrohtem IT-System ab. Es wird angenommen, dass zur jährliche Aufgabenerfüllung ca. 49.600 Stunden (31 MAK) notwendig sind. Unter der Berücksichtigung des durchschnittlichen Lohnsatzes für die Bundesverwaltung in Höhe von 44,40 Euro pro Stunde sowie jährlichen Sachkosten in Höhe von 765.000 Euro ergibt sich ein laufender Erfüllungsaufwand in Höhe von ca. 2.967.000 Euro auf Ebene des Bundes.

Lfd. Nr. 4.3.3: Eingriff in ein informationstechnisches System; § 41a Absatz 2, Nummer 2 BPolG-E

Mit der gesetzlichen Anpassung wird der Bundespolizei die Befugnis eingeräumt, in ein informationstechnisches System einzugreifen, um Daten auszulesen, zu löschen oder zu verändern. Diese Befugnis zielt sowohl auf informationstechnische Systeme von Angreifern wie auch von Geschädigten. Es wird angenommen, dass zur jährlichen Aufgabenerfüllung ca. 25.600 Stunden (16 MAK) notwendig sind. Unter der Berücksichtigung des durchschnittlichen Lohnsatzes für die Bundesverwaltung in Höhe von 44,40 Euro pro Stunde sowie jährlichen Sachkosten in Höhe von 765.000 Euro ergibt sich ein laufender Erfüllungsaufwand in Höhe von ca. 1.902.000 Euro auf Ebene des Bundes.

Lfd. Nr. 4.3.4: Untersagung des Betriebs eines informationstechnischen Systems; § 41a Absatz 2 Nummer 3 BPolG-E

Mit der gesetzlichen Anpassung wird die Bundespolizei ermächtigt zur Abwehr eines Angriffs auf die Sicherheit in der Informationstechnik, den Betrieb eines informationstechnischen Systems zu untersagen. Dadurch wird sichergestellt, dass störende Infrastrukturen sowie infizierte Systeme abgeschaltet werden. Es wird angenommen, dass zur jährliche Aufgabenerfüllung ca. 68.800 Stunden (43 MAK) notwendig sind. Unter der Berücksichtigung des durchschnittlichen Lohnsatzes für die Bundesverwaltung in Höhe von 44,40 Euro pro Stunde sowie jährlichen Sachkosten in Höhe von 765.000 Euro ergibt sich ein laufender Erfüllungsaufwand in Höhe von ca. 3.820.000 Euro auf Ebene des Bundes.

Lfd. Nr. 4.3.5: Maßnahmen zur Abwehr und Eindämmung von Angriffen einschließlich der systematischen Suche nach Angriffspuren (Threat Hunting); § 11 Absatz 1 und 3 BSIG-E

Mit der gesetzlichen Änderung in § 11 Absatz 1 und 3 des BSIG wird das BSI ermächtigt nicht nur auf Angriffe reagieren zu können, sondern im Voraus nach potenziellen Angreifern aufzuklären, die eine zukünftige Bedrohung darstellen könnten (sog. Threat Hunting). Es wird angenommen, dass zur jährlichen Aufgabenerfüllung ca. 8.000 Stunden (5 MAK) notwendig sind. Zudem sind jährliche Sachkosten in Höhe von ca. 240.000 Euro anzusetzen. Unter der Berücksichtigung des durchschnittlichen Lohnsatzes für die Bundesverwaltung in Höhe von 44,40 Euro pro Stunde ergibt sich ein laufender Erfüllungsaufwand in Höhe von ca. 595.000 Euro auf Ebene des Bundes.

Lfd. Nr. 4.3.6: Datenverarbeitung und Information zur Bekämpfung von Domainphishing; § 16 Absatz 6 BSIG-E

Mit der gesetzlichen Änderung zur Datenverarbeitung und Bereitstellung relevanter Informationen wird ein Beitrag zur Bekämpfung der zunehmend wachsenden Bedrohung durch Domain-Phishing geleistet. Zudem erweitern sich die datenschutzrechtlichen Aufsichtsmaßnahmen des BfDI. Es wird angenommen, dass zur jährlichen Aufgabenerfüllung (einschließlich der erweiterten datenschutzrechtlichen Aufsichtsmaßnahmen) ca. 4.800 Stunden (3 MAK) notwendig sind. Unter der Berücksichtigung des durchschnittlichen Lohnsatzes für die Bundesverwaltung in Höhe von 44,40 Euro pro Stunde ergibt sich ein laufender Erfüllungsaufwand in Höhe von ca. 213.00 Euro auf Ebene des Bundes.

Lfd. Nr. 4.3.7: Anordnung gegenüber Top Level Domains; § 16a Absatz 1 BSIG-E

Durch die gesetzliche Änderung wird das BSI ermächtigt Anordnungen gegenüber Anbietern von Top Level Domain Name Registries und Domain-Name-Registry-Dienstleistern anzuordnen. Zum Beispiel, dass Einträge auf einer vom BSI benannten Domain hinzugefügt oder geändert werden. Es wird angenommen, dass zur jährlichen Aufgabenerfüllung ca. 800 Stunden (0,5 MAK) notwendig sind. Unter der Berücksichtigung des durchschnittlichen

Lohnsatzes für die Bundesverwaltung in Höhe von 44,40 Euro pro Stunde ergibt sich ein laufender Erfüllungsaufwand in Höhe von ca. 36.000 Euro auf Ebene des Bundes.

Lfd. Nr. 4.3.8: Verarbeitung und Auswertung umgeleiteter Daten; § 16a Absatz 2 BSIG-E

Durch die gesetzliche Änderung darf das BSI Daten, die von Top Level Name Registries und Domain Name Registries-Dienstleister umgeleitet wurden, verarbeiten und auswerten. Es wird angenommen, dass zur jährlichen Aufgabenerfüllung ca. 4.800 Stunden (3 MAK) notwendig sind. Unter der Berücksichtigung des durchschnittlichen Lohnsatzes für die Bundesverwaltung in Höhe von 44,40 Euro ergibt sich ein laufender Erfüllungsaufwand in Höhe von ca. 213.000 Euro auf Ebene des Bundes.

Lfd. Nr. 4.3.9: Anbindung von Systemen zur Angriffserkennung bei Betreibern kritischer Anlagen an das BSI; § 31 Absatz 2 BSIG-E

Die gesetzliche Änderung sieht vor, dass Systeme zur Angriffserkennung, welche bei Betreibern kritischer Anlagen eingesetzt wurden, an das BSI angebunden werden. Dies bedeutet, die verschiedenen Parameter und Merkmale aus dem laufenden Betrieb sowie regelmäßige Verfügbarkeitsindikatoren zu erfassen, auszuwerten und über eine Anbindung an das BSI weiterzuleiten. Das BSI ist für die Festlegung der Anforderungen verantwortlich und veröffentlicht diese.

Dem BSI entsteht dadurch zunächst einmaliger Erfüllungsaufwand in Höhe von ca. 211.000 Euro, welcher sich aus einmaligen Personalkosten in Höhe von ca. 142.000 Euro und einmaligen Sachkosten in Höhe von 69.000 Euro zusammensetzt.

Zudem wird angenommen, dass zur jährlichen Aufgabenerfüllung ca. 14.400 Stunden (9 MAK) und jährliche Sachkosten in Höhe von 480.000 Euro notwendig sind. Unter Berücksichtigung des durchschnittlichen Lohnsatzes für die Bundesverwaltung in Höhe von 44,40 Euro ergibt sich in Summe ein laufender Erfüllungsaufwand in Höhe von ca. 1.119.000 Euro auf Ebene des Bundes.

Lfd. Nr. 4.3.10: Bußgeldverfahren und Sanktionierung bei Fehlen eines geeigneten Systems zur Angriffserkennung; § 65 Absatz 2, Nummer 3a BSIG-E

Die gesetzliche Änderung ermöglicht Bußgeldverfahren durch das BSI bei Unterlassung des Einsatzes von Systemen zur Angriffserkennung und ihrer Anbindung an das BSI einzuleiten. Es wird angenommen, dass zur jährlichen Aufgabenerfüllung ca. 2.400 Stunden (1,5 MAK) notwendig sind. Unter Berücksichtigung des durchschnittlichen Lohnsatzes für die Bundesverwaltung in Höhe von 44,40 Euro ergibt sich in Summe ein laufender Erfüllungsaufwand in Höhe von ca. 107.000 Euro auf Ebene des Bundes.

Lfd. Nr. 4.3.11: Unterstützung bei der Durchführung technischer Maßnahmen der Abwehr von Angriffen auf die Sicherheit in der Informationstechnik; § 2 Absatz 5 Satz 1 Nummer 5 BKAG-E

Mit der neuen gesetzlichen Änderung wird das BKA ermächtigt, Unterstützungsmaßnahmen auf Ersuchen der Polizeien des Bundes und der Länder zu ergreifen. Bisher kann das BKA als Zentralstelle bei den kriminaltechnischen Untersuchungen sowie bei der Datenverarbeitung unterstützen. Künftig kann das BKA nach der neu eingefügten Nummer 5 die Bundes- und Landespolizeien im Einzelfall und auf deren Ersuchen direkt bei der Durchführung von Maßnahmen im Bereich der Cyberabwehr unterstützen. Es wird angenommen, dass zur jährlichen Aufgabenerfüllung ca. 16.000 Stunden (10 MAK) notwendig sind. Unter Berücksichtigung des durchschnittlichen Lohnsatzes für die Bundesverwaltung in Höhe von 44,40 Euro ergibt sich in Summe ein laufender Erfüllungsaufwand in Höhe von ca. 710.000 Euro auf Ebene des Bundes.

Lfd. Nr. 4.3.12: Abwehr von Gefahren durch Angriffe auf die Sicherheit in der Informationstechnik; u.a. § 3a BKAG-E

Die neue gesetzliche Regelung sieht zusätzliche Aufgaben und Befugnisse des BKA bei Angriffen auf die Sicherheit in der Informationstechnik vor, wenn u. a. eine internationale Tragweite bzw. außenpolitische Belange des Bundes betroffen sind. Zudem erweitern sich die datenschutzrechtlichen Aufsichtsmaßnahmen des BfDI. Es wird angenommen, dass zur jährlichen Aufgabenerfüllung (einschließlich der erweiterten datenschutzrechtlichen Aufsichtsmaßnahmen) ca. 172.000 Stunden (107,5 MAK) notwendig sind. Unter Berücksichtigung des durchschnittlichen Lohnsatzes für die Bundesverwaltung in Höhe von 44,40 Euro sowie jährlichen Sachkosten in Höhe von 1.800.000 Euro ergibt sich in Summe ein laufender Erfüllungsaufwand in Höhe von ca. 9.437.000 Euro auf Ebene des Bundes.

Lfd. Nr. 4.3.13: Eigenschutz der Liegenschaften, sonstigen Einrichtungen und Veranstaltungen des BKA; § 68a Absatz 1 Nummer 2 Buchstabe d i.V.m § 8 BKAG

Die neue gesetzliche Regelung erweitert den bestehenden Eigenschutz des BKA. Das BKA muss in der Lage sein, nicht nur seinen Personenschutzauftrag nach § 6 BKAG im digitalen Raum zu erfüllen, sondern auch sich selbst gegen Cyberangriffe (auf seine eigenen Anlagen z. B. Zugangs- und Kontrollsysteme, Energieinfrastruktur) verteidigen zu können. Es wird angenommen, dass zur jährlichen Aufgabenerfüllung 22.400 Stunden (14 MAK) notwendig sind. Unter Berücksichtigung des durchschnittlichen Lohnsatzes für die Bundesverwaltung in Höhe von 44,40 Euro ergibt sich in Summe ein laufender Erfüllungsaufwand in Höhe von ca. 995.000 Euro auf Ebene des Bundes.

Lfd. Nr. 4.3.14: Untersagung des Betriebs informationstechnischer Systeme; § 68b BKAG-E

Die neue gesetzliche Regelung sieht vor, den Betrieb von IT-Systemen zu untersagen, wenn von diesen Systemen eine Cybergefahr ausgeht. Dadurch wird sichergestellt, dass störseitiger Infrastruktur sowie infizierter Systeme abgeschaltet werden. Dies kann z.B. die Deaktivierung von infizierten Bots oder von (Command & Control) -Servern bedeuten. Eine solche Deaktivierung kann durch Verpflichtung oder Inanspruchnahme der relevanten Dienstanbieter erfolgen. Es wird angenommen, dass zur jährlichen Aufgabenerfüllung ca. 70.400 Stunden (44 MAK) notwendig sind. Unter Berücksichtigung des durchschnittlichen Lohnsatzes für die Bundesverwaltung in Höhe von 44,40 Euro sowie jährliche Sachkosten in Höhe von 300.000 Euro ergibt sich in Summe ein laufender Erfüllungsaufwand in Höhe von ca. 3.426.000 Euro auf Ebene des Bundes.

Lfd. Nr. 4.3.15: Einschränkung, Unterbindung und Umleitung von Datenverkehr; § 68c BKAG-E

Mit der gesetzlichen Änderung wird das BKA ermächtigt, Datenverkehr, der eine Cybergefahr verursacht zu unterbinden und umzuleiten. Eine Umleitung auf ein polizeilich kontrolliertes System bzw. an ein sog. Sinkhole kann im Zusammenhang mit Maßnahmen zur Bereinigung von Botnetzen (Computersystemen die mit Malware infiziert sind) erfolgen. Es wird angenommen, dass zur jährlichen Aufgabenerfüllung ca. 32.000 Stunden (20 MAK) notwendig sind. Unter Berücksichtigung des durchschnittlichen Lohnsatzes für die Bundesverwaltung in Höhe von 44,40 Euro sowie jährlichen Sachkosten in Höhe von 600.000 Euro ergibt sich in Summe ein laufender Erfüllungsaufwand in Höhe von ca. 2.021.000 Euro auf Bundesebene.

Lfd. Nr. 4.3.16: Auslesen, Löschen und Veränderung von Daten in informationstechnischen Systemen; § 68d BKAG-E

Das BKA darf künftig in informationstechnischen Systemen bestimmte Daten erheben, verändern und löschen, sofern eine Cybergefahr nicht durch andere Mittel abgewehrt werden

kann. Die Regelung legt auch Maßnahmen zur Minderung der Intensität des Eingriffs fest und schreibt vor, dass nur solche Änderungen vorgenommen werden dürfen, die für die Löschung und Änderung der Daten unerlässlich sind. Es wird angenommen, dass zur jährlichen Aufgabenerfüllung ca. 112.000 Stunden (70 MAK) notwendig sind. Unter Berücksichtigung des durchschnittlichen Lohnsatzes für die Bundesverwaltung in Höhe von 44,40 Euro sowie jährliche Sachkosten in Höhe von 2.300.000 Euro ergibt sich in Summe ein laufender Erfüllungsaufwand in Höhe von ca. 7.273.000 Euro auf Bundesebene.

5. Weitere Kosten

Auswirkungen auf Einzelpreise und das allgemeine Preisniveau, insbesondere auf die Verbraucherpreise, sind nicht zu erwarten.

6. Weitere Gesetzesfolgen

Durch den Gesetzesentwurf wird die Versorgungssicherheit für Verbraucherinnen und Verbraucher erhöht. Die bestehenden Regelungen des BSI-Gesetzes zum Verbraucherschutz werden nicht berührt.

Die Regelungen des Gesetzentwurfs sind inhaltlich geschlechtsneutral aufgrund der vorrangig gegebenen unmittelbaren Betroffenheit der Zielgruppe des Regelungsvorhabens und damit ohne Gleichstellungsrelevanz. Die weitere Stärkung und Förderung der Cyber- und Informationssicherheit betrifft jedoch sowohl mittel- als auch unmittelbar Frauen und Männer. § 4 Absatz 3 Satz 1 des Bundesgleichstellungsgesetzes bestimmt, dass Rechts- und Verwaltungsvorschriften des Bundes die Gleichstellung von Frauen und Männern auch sprachlich zum Ausdruck bringen sollen. Dies wurde in der Entwicklung der Gesetzesformulierung unter Einbeziehung bereits gegebener Diktion berücksichtigt.

Die Regelungen entsprechen zudem den Anforderungen des „Gleichwertigkeits-Checks“. Der Gesetzentwurf dient der Gewährleistung der flächendeckenden Grundversorgung mit Telekommunikation und der Erreichbarkeit von Dienst- und Verwaltungsleistungen hierüber. Auch wird dem Schutz einer Daseinsvorsorge mit ihren unterschiedlichen Bereichen, die eine wesentliche Voraussetzung für gleichwertige Lebensverhältnisse der Menschen und den gesellschaftlichen Zusammenhalt Rechnung getragen. Auswirkungen auf die vorhandene Siedlungs- und Raumstruktur oder demographische Belange sind nicht zu erwarten

VII. Exekutiver Fußabdruck

Der Inhalt des Gesetzentwurfs hat sich durch Vorträge von Interessenvertreterinnen und Interessenvertretern sowie von der Bundesregierung beauftragten Dritten nicht wesentlich geändert.

VIII. Befristung; Evaluierung

Eine Befristung der Regelungen ist nicht vorgesehen. Die sicherheitsrechtlichen Anforderungen, denen das Gesetz Rechnung trägt, besteht unabhängig von der einzelnen Lageentwicklung fort. Eine zeitliche Befristung würde daher zu Rechtsunsicherheit führen und die notwendige Kontinuität und Verlässlichkeit der Aufgabenerfüllung der Sicherheitsbehörden beeinträchtigen.

Eine Evaluierung der Regelungen dieses Gesetzes ist ebenfalls nicht vorgesehen. Die neuen Befugnisse knüpfen an bestehenden gesetzlichen Aufgaben und Befugnisse der Behörden an und erweitern diese. Die Auswirkungen des Gesetzes sind im Wesentlichen prognostizierbar und im Rahmen der Gesetzesfolgenabschätzung/ Erfüllungsaufwand be-

rücksichtigt worden. Die Anwendung der Befugnisse sowie deren Auswirkung unterliegt einer kontinuierlichen Kontrolle, insbesondere durch die parlamentarische Kontrolle, die Fach- und Rechtsaufsicht sowie die bestehenden Berichtspflichten und gerichtliche Rechtsschutzmöglichkeiten. Die Wirkung der Regelungen wird im Rahmen der bestehenden Kontroll- und Aufsichtsmechanismen fortlaufend beobachtet. Außerdem ist eine statistische Erfassung vorgesehen, sodass der Nutzen laufend nachvollzogen werden kann. Vor diesem Hintergrund wird von der Aufnahme einer Evaluationsklausel abgesehen.

B. Besonderer Teil

Zu Artikel 1 (Änderung des Bundespolizeigesetzes)

Zu Nummer 1

Es handelt sich um eine redaktionelle Folgeänderung im Inhaltsverzeichnis.

Zu Nummer 2

Mit dem neuen § 41a erhält die Bundespolizei Befugnisse zur Abwehr von Angriffen auf die Sicherheit in der Informationstechnik im Rahmen ihrer bestehenden Aufgaben nach § 1 Absatz 3 bis 5 sowie den §§ 2 bis 8 BPolG. Diese Anpassung trägt der zunehmenden Anzahl von Bedrohungen aus dem Cyberraum Rechnung, auf die die Bundespolizei im Rahmen ihrer bestehenden Zuständigkeiten mit adäquaten Befugnissen reagieren können muss. Die Gefahrenabwehrzuständigkeiten der Länder werden durch die Befugniserweiterung nicht berührt, Feststellungen im Zuständigkeitsbereich der Länder werden an die jeweils zuständige Stelle abgegeben.

Bereits heute ist die Bundespolizei darauf angewiesen, Gefahren aus dem Cyberraum, die ihre Aufgabenwahrnehmung beeinträchtigen könnten, vorzubeugen. Nach den Vorgaben des BSI ist die Bundespolizei etwa gehalten, die Integrität, die Verfügbarkeit und die Vertraulichkeit ihrer Informationen zu schützen, um somit die Funktionsfähigkeit der Bundespolizei und eine effektive Aufgabenerfüllung sicherstellen zu können. Darüber hinaus setzt die Bundespolizei ihre diesbezüglichen Fähigkeiten zur Strafverfolgung, zur Sicherung eigener Einrichtungen und zur Unterstützung anderer Behörden erfolgreich ein.

Infolge der fortschreitenden technologischen Entwicklung bestehen vielfältige Einwirkungsmöglichkeiten aus dem Cyberraum, die sämtliche Aufgabenbereiche der Bundespolizei betreffen. Hieraus ergibt sich die Notwendigkeit weitergehender Befugnisse. Beispielsweise besteht im Rahmen der Aufgabenwahrnehmung nach § 2 BPolG die Notwendigkeit zur Abwehr von Gefahren für biometriegestützte Grenzkontrollsysteme oder sonstige Einrichtungen der Grenzkontrolle. Denkbar sind ferner im Rahmen der Aufgabenwahrnehmung nach § 3 BPolG Angriffe auf informationstechnische Systeme der Bahn, in deren Folge Gefahren für die Benutzer, die Anlagen oder den Betrieb der Bahn entstehen, etwa weil Steuerungssysteme nicht mehr funktionieren. Die Schaffung der hierzu notwendigen Befugnisnormen ist daher unabdingbar.

Sachverhalte, die Maßnahmen nach dieser Vorschrift erfordern, sind in der Regel andauernde, komplexe Angriffe auf die Sicherheit in der Informationstechnik. In vielen Fällen werden die konkreten Störungen noch nicht erkennbar sein. Akteure, die zu solchen Angriffen fähig sind, sind dauerhaft aktiv, entwickeln die Angriffsinfrastrukturen permanent weiter und bedienen sich hierbei verschiedener Verschlüsselungsverfahren. Charakteristisch für diese andauernden, komplexen Bedrohungskampagnen ist aus technischer Sicht, dass Schadsoftware in Opfersysteme eingebracht wird, welche sich über einen oder mehrere Proxyserver (Weiterleitungsserver) verbindet und direkt über das Internet erreichbar ist. Die Datenkommunikation ist in der Regel verschlüsselt. Der Letzte in einer Kette von Proxy-Ser-

vern verbindet sich oftmals über ein weiteres Verschlüsselungsverfahren (VPN-Zugangstechnik) mit einem VPN-Server (Virtual Private Network), welcher das Tor in ein verschlüsseltes Netzwerk öffnet. Diese Netzwerke enthalten regelmäßig den oder verschiedene Steuerungsserver (Command & Control Server), welcher Befehle für weitere Aktionen auf den von den Angriffen bedrohten IT-Systemen entgegennimmt bzw. den Angreifern Informationen aus diesen Systemen bereitstellt. Ein Angreifer meldet sich typischerweise über eine ähnliche Infrastrukturkette in diesem Netzwerk an. Über den dargestellten Aufbau kann der für Maßnahmen zur Abwehr von Gefahren für die Sicherheit in der Informationstechnik relevante Steuerungsserver nicht mehr direkt im Internet angesprochen bzw. aufgeklärt (detektiert) werden. Der Betrieb solcher Server erfolgt weitgehend anonym.

Um die hieraus möglichen Gefahrenlagen wirksam abzuwehren, ist es erforderlich, Schwachstellen in der Informationstechnik der Angreiferinfrastrukturen zu suchen, die Infrastruktur (von der Angreifer-IT bis hin zu bedrohten IT-Systemen) möglichst umfassend aufzuklären bzw. ein Monitoring bedrohter IT-Systeme zu ermöglichen bzw., sofern technisch umsetzbar, auch unmittelbaren Zugriff auf die Inhalte des Servers bzw. das Angreifernetzwerk zu erhalten. Der Angriff, welcher durch mehrere verschiedene IT-Systeme organisiert ist, kann im Idealfall nach entsprechender Aufklärung an verschiedenen Stellen unterbrochen werden. Die Identifizierung entsprechender IT-Systeme ist regelmäßig eindeutig möglich (anhand von IP-Adressen, Adressbereichen, spezifischen Netzwerkmerkmalen und Schadsoftwaresignaturen, wie beispielsweise Hashwerten, Cookies, verwendeten User-Agents, etc.). Dadurch können Metadaten des Telekommunikations- oder Netzwerkverkehrs gefiltert werden, um bedrohte IT-Systeme eindeutig zu identifizieren.

Bis zum Eintritt einer konkreten IT-Störung, die bei ungehindertem Verlauf geeignet wäre, erhebliche Rechtsgutverletzungen hervorzurufen, durchlaufen Angriffe auf die Sicherheit in der Informationstechnik üblicherweise mehrere Phasen. Um die Störung abwehren zu können, sind (ohne dass bereits die konkrete Störung eingetreten ist) IT-forensische Analysen notwendig und bei Vorliegen der rechtlichen Voraussetzungen auch Zugriffe auf verschlüsselte Kommunikation zwingend erforderlich. Sofortige „Abschaltmaßnahmen“ sind technisch oftmals nicht möglich oder aufgrund der noch unzureichenden Aufklärung der Systeme der Angreifer hinsichtlich der technischen Folgen noch nicht abschätzbar. Auf welchem konkreten Weg eine IT-Bedrohung oder IT-Störung abgewendet werden kann, hängt vom Einzelfall ab (Aufklärungsergebnisse, Zugangsmöglichkeiten zu informationstechnischen-Systemen und Netzen). Darüber hinaus ist denkbar, dass Angreifer die Zugriffe durch die Polizei ihrerseits detektieren und auf andere Systeme oder Server-Ketten ausweichen.

Zu Absatz 1

Absatz 1 normiert, dass die Bundespolizei zur Erfüllung ihrer Aufgaben nach § 1 Absatz 3 bis 5 sowie den §§ 2 bis 8 besondere Abwehrmaßnahmen ergreifen kann, um eine Gefahr durch einen Angriff auf die Sicherheit in der Informationstechnik abzuwehren. Unbeschadet der in Absatz 5 normierten qualifizierten Gefahrenschwelle bei Maßnahmen, die in private informationstechnische Systeme eingreifen und eine Erhebung dort gespeicherter Daten ermöglichen, erfordert Absatz 1 lediglich das Vorliegen einer konkreten Gefahr durch einen Angriff auf die Sicherheit in der Informationstechnik. Zur Konkretisierung, wann eine Gefahr durch einen Angriff auf die Sicherheit in der Informationstechnik vorliegt, werden die Straftatbestände aufgezählt, bei deren Verwirklichung des objektiven Tatbestandes ein solcher Angriff vorliegt.

Dabei gilt, dass die besonderen Abwehrmaßnahmen – wie alle Gefahrenabwehrmaßnahmen – nach § 16 Absatz 3 unverzüglich zu beenden sind, sobald die Gefahr abgewehrt ist oder erkennbar ist, dass diese nicht abgewehrt werden kann.

Zu Satz 1 Nummer 1

Satz 1 Nummer 1 ermächtigt die Bundespolizei, zur Abwehr eines Angriffs auf die Sicherheit in der Informationstechnik den Betrieb eines informationstechnischen Systems zu untersagen. Die Befugnisnorm dient u.a. dem Zweck des Abschaltens störerseitiger Infrastruktur sowie infizierter Systeme.

Die Untersagung kann sich an private Personen, juristische Personen und an die Stellen nach Absatz 9 richten. Typischerweise wird sie sich an Anbieter von Telekommunikationsdiensten nach dem Telekommunikationsgesetz sowie Anbieter digitaler Dienste nach dem Digitale-Dienste-Gesetz richten.

Zu Satz 1 Nummer 2

Die Norm gibt der Bundespolizei zum einen die Möglichkeit, Datenverkehr zur Gefahrenabwehr an eine von der Bundespolizei vorgegebene Zieladresse umzuleiten und den umgeleiteten Datenverkehr aufzuzeichnen. Die Zulässigkeit der Verarbeitung der auf diese Weise erhobenen Daten richtet sich nach den allgemeinen Vorschriften. Die Bundespolizei kann die Umleitung selbst vornehmen oder nach Absatz 9 Satz 1 die Verpflichteten nach § 170 Absatz 1 und 2 des Telekommunikationsgesetzes sowie nach § 1 Absatz 4 Nummer 5 des Digitale-Dienste-Gesetzes anweisen, die Umleitung vorzunehmen.

Ziel der Maßnahme ist entweder die Umleitung des Datenverkehrs zwischen informationstechnischen Systemen zum Zwecke des Verwerfens oder die Umleitung des Datenverkehrs auf ein anderes Zielsystem zur Auswertung bzw. Analyse der transportierten Daten.

So kann etwa im Zusammenhang mit Maßnahmen zur Bereinigung von mit Malware infizierten Computersystemen (Botnetz) nach Sicherstellung der im Kontext des Steuerungssystems des Botnetzes (Command&Control-Server) genutzten Domain der maliziöse Datenverkehr auf ein polizeilich kontrolliertes System bzw. an ein sog. Sinkhole umgeleitet werden. Die Umleitung von Datenverkehr an ein Sinkhole kann zu unterschiedlichen Zwecken erfolgen:

Erstens kann sie dazu dienen, die Kommunikation zwischen den Opferrechnern mit den Täterrechnern zu verwerfen. In der Folge wird der Angriff vereitelt, da sich die Gefahr nicht verwirklichen kann.

Zweitens können Informationen über die eingesetzte Schadsoftware sowie über die Wege der Angreifer-Opfer-Kommunikation festgestellt werden, um den Angriff abzuwehren.

Drittens kann weitere Täter-Infrastruktur (Rückkanäle in den Verkehrsdaten) über das Sinkhole erschlossen werden. Ziel ist hier die Aufklärung der Täterinfrastruktur zur Identifikation weiterer Angriffswege und damit zur Abwehr der Gefahr.

Viertens kann der Täter in einem Sinkhole durch eine aktive Opfer-Simulation (Honeypot/-net) herausgefordert werden, weitere hochwertigere Schadsoftware einzusetzen. Dadurch kann die Gefahr unbekannter oder versteckter Schadfunktionen reduziert werden. Hierbei werden keine privaten Daten Dritter gespeichert oder ausgewertet.

Zuletzt kann über ein Sinkhole eine Benachrichtigung von Gefährdeten bzw. Opfern – durch Erfassung der betroffenen IP-Adressen in Log-Dateien im Sinkhole – über den Angriff erfolgen. Der Inhalt der Daten ist in der Regel verschlüsselt. Dennoch können beispielsweise durch die Auswertung von IP-Adressen (Verkehrsdaten) Informationen über weitere Gefährdete zwecks deren Benachrichtigung erhoben werden.

Die Aufzeichnung des umgeleiteten Datenverkehrs ist erforderlich, damit die Bundespolizei den Ursprung des Angriffs feststellen kann. Ferner müssen Kommunikationsverbindungen

aufgezeichnet werden können, um Rückschlüsse auf typische Angriffsmuster ziehen zu können. Die Maßnahme zielt dabei auch auf die Aufzeichnung und Auswertung des Datenverkehrs zwischen Angreifer und bedrohtem IT-System ab. Die Weiterverarbeitung der aufgezeichneten Daten ist nach den allgemeinen Vorschriften der §§ 42 ff. zulässig. Satz 1 Nummer 2 gibt der Bundespolizei ferner die Möglichkeit, Datenverkehr einzuschränken und zu unterbinden. Die Befugnisnorm dient u.a. dem Zweck des Abschaltens krimineller Infrastruktur sowie infizierter Systeme. Dies kann z.B. die Deaktivierung von infizierten Bots oder von Command&Control-Servern bedeuten. Eine solche Deaktivierung kann auch durch Verpflichtung oder Inanspruchnahme der relevanten Diensteanbieter erfolgen.

Eine Einschränkung oder Unterbindung von Datenverkehr wird in der Regel durch Anordnung gegenüber den Stellen nach Absatz 9 Satz 1 realisiert werden. Die Bundespolizei kann diesen gegenüber anordnen, schadhafte Datenverkehre, welche etwa im Ausland ihren Ursprung haben, nach Deutschland zu blocken.

Zu Satz 1 Nummer 3

Nach Satz 1 Nummer 3 wird der Bundespolizei die Befugnis eingeräumt, in einem informationstechnischen System auch durch den Eingriff mit technischen Mitteln in ein informationstechnisches System und ohne Wissen der Betroffenen gefahrgegenständliche Daten auszulesen, zu löschen oder zu verändern. Eingreifen bedeutet das Eindringen oder Aufschalten auf ein informationstechnisches System, in der Regel durch Überwindung einer Zugangsbarriere, wie zum Beispiel einem Passwort. Diese Maßnahme zielt sowohl auf informationstechnische Systeme von Angreifern wie auch diejenigen von Geschädigten („Opfersysteme“).

Die Befugnis ist z.B. in Fällen erforderlich, in denen ein informationstechnisches System mit einem Schadprogramm infiziert ist, dessen Löschung einen Angriff auf die Sicherheit in der Informationstechnik verhindern oder beenden würde. Die Weiterverarbeitung der ausgelesenen Daten ist nach den allgemeinen Vorschriften der §§ 42 ff. zulässig.

Ein Eingreifen zur Speicherung gefahrgegenständlicher Informationen wie IP-Adressen, Benutzernamen, Passwörtern oder Konfigurationsdaten kann erforderlich sein, um beispielsweise die Command&Control-Software in ihrer Funktionsweise zu analysieren und um Schwachstellen in der Infrastruktur des Angreifers zu suchen.

Ermöglicht wird des Weiteren ein Fernzugriff auf Systeme, zum Beispiel ein Zugriff auf IoT-Geräte zur Installation von lückenschließender Software (Patches), um einen DDoS-Angriff zu unterbinden. Auch kann ein Eingriff in einen Steuerungs-Server mittels Installation eigener Software, die auf der Grundlage vorheriger Aufklärungsmaßnahmen entwickelt wurde, erforderlich sein, um ein Botnetz abzuschalten. Die Übernahme bzw. Steuerung des Command&Control-Servers in einer Botnetz-Infrastruktur kann der Vorbereitung zum Senden des in der Schadsoftware bereits enthaltenen Deinstallationsbefehls (sog. Kill-Switch) oder zum Senden eines Updates mit geänderten Kommunikationsparametern an die infizierten Bots dienen. Diese kommunizieren anschließend mit einer von der Bundespolizei vorgegebenen Anschlusskennung (sog. Sinkhole). Daneben können Veränderungen an einem IT-System des Angreifers vorgenommen werden, die dazu dienen, einen Angriff direkt abzuwehren, indem z.B. direkte Veränderungen am System in angreiferseitigen Skripten den Angriff aufhalten oder umlenken. Eine Veränderung oder Löschung von Datensammlungen kommt sowohl für technische Daten (der vom Angriff auf die Sicherheit in der Informationstechnik bedrohten IT-Systeme oder Steuerungscodes) als auch für abgeschöpfte Dokumente in Frage.

Ein Eingreifen in informationstechnische Systeme ist ferner in Fällen relevant, in denen die Anbieter von Servern nicht zur Abschaltung der infizierten Server verpflichtet werden können. Dies kann der Fall sein, wenn der Provider oder OTT-Dienstleister oder auch ein betroffenes Unternehmen gehackt wurde und daher nicht erreichbar ist. In diesen Situationen

kann es zur Abwehr der Gefahr erforderlich sein, unmittelbar selbst durch Eingreifen in Systeme Abwehrmaßnahmen zu ergreifen.

Der Zugriff auf informationstechnische Systeme kann auf verschiedene Weisen erfolgen. Er kann unter Zuhilfenahme von aus einer anderen polizeilichen Maßnahme rechtmäßig erlangten Zugangsdaten geschehen. Möglich ist ferner die Ausnutzung vorhandener Schwachstellen. Die Nutzung von bekannten Zugangsdaten ist weniger aufwendig und hat ggf. weniger Auswirkungen auf das System selbst, da es ein dafür vorgesehener Zugang ist.

Zu Absatz 1 Satz 2

Absatz 1 Satz 2 weist darauf hin, dass besondere Abwehrmaßnahmen nach Satz 1 Nummer 3, die ohne Einwilligung der Betroffenen durch Eingriff in private informationstechnische Systeme eine Datenerhebung ermöglichen, nur unter den Voraussetzungen der Absätze 5 bis 8 durchgeführt werden dürfen.

Zu Absatz 2

In Absatz 2 wird legaldefiniert, welche Daten gefahrengegenständliche Daten sind und dementsprechend nach Absatz 1 Satz 1 Nummer 3 ausgelesen, gelöscht oder verändert werden dürfen. Erfasst sind sowohl die Daten, aus denen das Schadprogramm oder das sonstige informationstechnische Angriffswerkzeug besteht, als auch Spuren und Daten, die Gegenstand des Angriffs waren. Beispielsweise kann es zur Abwehr eines Angriffs auf die Sicherheit in der Informationstechnik erforderlich sein, abgeschöpfte Daten von Geschädigten zu löschen, um sie dem Zugriff der Täter zu entziehen.

Zu Absatz 3

Nach Absatz 3 dürfen die Maßnahmen nach Absatz 1 Satz 1 auch dann durchgeführt werden, wenn Dritte unvermeidbar betroffen werden. Der Begriff des „Dritten“ ist dabei in Abgrenzung zu den „Betroffenen“ im Sinne der Vorschrift zu verstehen. Betroffene im Sinne der Vorschrift sind die Betreiber oder die Nutzer der informationstechnischen Systeme, gegen welche die Maßnahmen dieser Vorschrift angewandt werden können, weil entweder von ihnen Gefahren für die Sicherheit in der Informationstechnik ausgehen oder für die Systeme selbst eine Gefahr für die Sicherheit in der Informationstechnik besteht. Beispielsweise können IT-Systeme unbeteiligter Dritter betroffen sein, wenn der Datenverkehr über diese geroutet wird, ohne dass von diesen oder für diese Gefahren für die Sicherheit in der Informationstechnik ausgehen bzw. bestehen.

Zu Absatz 4

Als Ausprägung des Verhältnismäßigkeitsgrundsatzes legt Absatz 4 in Bezug auf Maßnahmen nach Absatz 1 Satz 1 Nummer 3 Anforderungen hinsichtlich der eingesetzten Mittel fest.

Nach Absatz 4 Nummer 1 sind, soweit dies möglich ist, technische Vorkehrungen zu treffen, dass ein Auslesen von Informationen auf gefahrgegenständliche Daten beschränkt wird.

Absatz 4 Nummer 2 sieht vor, dass die vorgenommenen Veränderungen rückgängig zu machen sind, soweit dies technisch möglich ist und dem Zweck der Maßnahme nicht widerspricht. Umgekehrt sollen jene Veränderungen nicht rückgängig gemacht werden, die den Angreifer dazu in die Lage versetzen würden, einen erneuten Angriff auszuführen.

Nach Absatz 4 Nummer 2 ist insbesondere die auf dem IT-System installierte (BPOL-eigene) Software vollständig zu löschen und sind Veränderungen an den bei der Installation der Software vorgefundenen Systemdateien rückgängig zu machen.

Nach Absatz 4 Nummer 3 ist das eingesetzte Mittel ferner nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Insbesondere hat die Bundespolizei dafür Sorge zu tragen, dass die eingesetzte Software nicht durch Dritte zweckentfremdet werden kann. Speziell ist sicherzustellen, dass die Software nicht ohne erheblichen Aufwand dazu veranlasst werden kann, an einen anderen Server als den von der Bundespolizei verwendeten zurückzumelden, und dass die Software weder von Unbefugten erkannt noch angesprochen werden kann. Dies soll gewährleisten, dass die Eingriffe in die Integrität des IT-Systems und die Vertraulichkeit der in ihm gespeicherten Daten nicht über das hinausgehen, was nötig ist, um der Bundespolizei die Maßnahme zu ermöglichen.

Zu Absatz 5

Entscheidend für die Systematik des § 41a ist, dass die besonderen Maßnahmen zur Abwehr von Angriffen auf die Sicherheit in der Informationstechnik keine Überwachungsmaßnahmen sind. Ziel ist nicht die Erhebung personenbezogener (Inhalts-) Daten, sondern allein die Abwehr von Angriffen auf die Sicherheit in der Informationstechnik. Die Erhebung oder Löschung personenbezogener Daten wird nur insofern relevant, als sie zur Abwehr eines Angriffs erforderlich sind, etwa weil ein privates System als Opfersystem infiltriert wurde oder personenbezogene Daten von Tätern entwendet worden sind. Häufig werden Angriffe auf die Sicherheit in der Informationstechnik überdies über informationstechnische Systeme ausgeführt, die allein zur Durchführung derartiger Angriffe betrieben werden. Derartige Systeme sind keine privat genutzten Systeme, über die im Falle eines Zugriffs Persönlichkeitsprofile natürlicher Personen erstellt werden können und ein Einblick in deren private Lebensgestaltung gewonnen werden kann. Aufgrund dessen und der grundsätzlich anderen Zielrichtung der besonderen Abwehrmaßnahmen nach Absatz 1 Satz 1 im Gegensatz zu staatlichen Überwachungsmaßnahmen sind auch die Voraussetzungen zur Durchführung der besonderen Abwehrmaßnahmen andere als bei staatlichen Überwachungsmaßnahmen. Grundsätzlich sind für die besonderen Abwehrmaßnahmen daher weder qualifizierte Schutzgüter noch ein Richtervorbehalt erforderlich. Nur wenn in private informationstechnische Systeme eingegriffen und Daten erhoben werden, legen die Absätze 5 bis 8 qualifizierte Anforderungen für die Maßnahmen nach Absatz 1 Satz 1 Nummer 3 fest, um dem IT-Grundrecht der Betroffenen Rechnung zu tragen.

Die Absätze 5 bis 8 finden ferner nur Anwendung, wenn die besondere Abwehrmaßnahme nach Absatz 1 Satz 1 Nummer 3 nicht mit Einwilligung des Betroffenen geschieht. Es liegt nahe, dass eine Einwilligung in der Regel erteilt wird, wenn Systeme kompromittiert wurden und der Nutzer oder Inhaber des Systems insofern selbst Opfer eines Angriffs auf die Sicherheit in der Informationstechnik geworden sind. Hier liegt es im Interesse des Opfers, dass der Zugriff auf sein System abgewehrt und ein Datenabfluss oder eine Datenmanipulation verhindert wird.

Absatz 5 Satz 1 normiert eine qualifizierte Gefahrenschwelle durch das Erfordernis einer dringenden Gefahr für bedeutende Schutzgüter (zeitliche und qualitative Qualifizierung).

Absatz 5 Satz 1 legt insofern fest, dass durch besondere Abwehrmaßnahmen nach Absatz 1 Satz 1 Nummer 3 in private informationstechnische Systeme nur zur Abwehr einer dringenden Gefahr für den Bestand oder die Sicherheit des Bundes oder eines Landes (Nummer 1), für Behörden oder Einrichtungen, deren Funktionieren für das Gemeinwesen oder die Verteidigung von wesentlicher Bedeutung ist (Nummer 2), für die Verfügbarkeit, Vertraulichkeit oder Integrität informationstechnischer Systeme einer großen Anzahl von Personen (Nummer 3) und für Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt für das Gemeinwesen oder die Verteidigung von wesentlicher Bedeutung ist (Nummer 4), eingegriffen werden darf. Die Nennung der Verteidigung, die bereits Teil des Gemeinwesens ist, erfolgt dabei nur zu Klarstellung. Die qualifizierten Schutzgüter stehen in Einklang mit der Rechtsprechung des Bundesverfassungsgerichts zu den Voraussetzungen für Eingriffe in privat genutzte IT-Systeme (IT-Systeme-Grundrecht), die aufgrund ihrer technischen Funktionalität allein oder durch ihre technische Ver-

netzung Daten einer betroffenen Person in einem Umfang und einer Vielfalt vorhalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten (BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 2466/19 (Trojaner I), Leitsatz 2a), Rn. 97; BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 180/23 (Trojaner II), Rn. 173). Das Schutzgut einer Sache von bedeutendem Wert, deren Erhalt für das Funktionieren von wesentlicher Bedeutung ist (Nummer 4), ist gegenüber dem Schutzgut einer Behörde oder Einrichtung, deren Funktionieren für das Gemeinwesen von wesentlicher Bedeutung ist (Nummer 2) ein Auffangtatbestand. Er kommt insbesondere in Betracht, wenn keine Sachgesamtheit, sondern eine einzelne Sache zu schützen ist.

Absatz 5 Satz 2 enthält eine Legaldefinition zum Begriff des privaten informationstechnischen Systems. Ein privates informationstechnisches System liegt insbesondere dann nicht vor, wenn das System nur zur Durchführung von Angriffen auf die Sicherheit in der Informationstechnik betrieben wird. Werden Systeme sowohl für Angriffe auf die Sicherheit in der Informationstechnik als auch privat genutzt, kommt es auf eine Bewertung des Einzelfalls an. Unbedeutende private Mitnutzungen von Systemen, die vorrangig zur Durchführung von Angriffen auf die Sicherheit in der Informationstechnik genutzt werden, führen nicht zur Einordnung eines Systems als privates. Unbedeutende private Mitnutzungen sind Nutzungen, die aufgrund des geringen Umfangs oder der geringen Vielfalt der Daten keinen Einblick in wesentliche Teile der Lebensgestaltung der Person und kein aussagekräftiges Bild der Persönlichkeit ermöglichen. Relevant bei der Bewertung, ob ein privates informationstechnisches System vorliegt, ist ferner, dass die private Nutzung nicht lediglich zu dem Zweck durchgeführt werden darf, dass erhöhte Anforderungen an die Ergreifung besonderer Abwehrmaßnahmen gestellt werden.

Absatz 5 Satz 3 erklärt die Regelung des § 40 Absatz 10 und 11 zum Schutz des Kernbereichs privater Lebensgestaltung für entsprechend anwendbar.

Zu Absatz 6

Absatz 6 verlangt bei Maßnahmen nach Absatz 1 Satz 1 Nummer 3 in Verbindung mit Absatz 5 eine gerichtliche Anordnung der Maßnahme auf Antrag eines begrenzten Personenkreises, namentlich der Präsidentin oder des Präsidenten des Bundespolizeipräsidiums oder einer Bundespolizeidirektion, ihrer oder seiner Vertretung oder der Leiterin oder des Leiters einer Abteilung des Bundespolizeipräsidiums.

Zu Absatz 7

Absatz 7 bestimmt, welchen Inhalt der Antrag nach Absatz 8 haben muss.

Zu Absatz 8

Absatz 8 bestimmt, welchen Inhalt die gerichtliche Anordnung einer Maßnahme hat.

Zu Absatz 9

Absatz 9 Satz 1 und 2 regelt, dass die Verpflichteten nach § 170 Absatz 1 und 2 des Telekommunikationsgesetzes sowie Anbieter digitaler Dienste nach § 1 Absatz 4 Nummer 5 des Digitale-Dienste-Gesetzes auf Anordnung der Bundespolizei die Umleitung oder Unterbindung von Datenverkehr umzusetzen haben und an Maßnahmen der Bundespolizei unverzüglich mitzuwirken und die erforderlichen Auskünfte zu erteilen haben.

Bisher bestand lediglich die Möglichkeit auf Grundlage sog. Abuse-Meldungen unter Verweis auf die Verwendungsweise der durch die Angreifer genutzten Server die Provider zu bitten, diese auf freiwilliger Basis abzuschalten. Da Provider regelmäßig ohne ausdrückliche rechtliche Verpflichtung keinerlei Maßnahmen treffen, die in Rechte ihrer Kunden ein-

greifen, besteht ohne Einfügung der Verpflichtung der Provider das Risiko, dass Server, die einem Botnetz zugehörig sind sowie durch die Betreiber des Botnetzes angemietete Server online bleiben. Die von den Betreibern geforderten Mitwirkungshandlungen können je nach Sachverhalt sehr unterschiedlich ausfallen. Die folgenden Beispiele sollen dies verdeutlichen, sind jedoch nicht abschließend zu verstehen.

Zunächst ist zu klären, wer der richtige Adressat bei der Anordnung zur Mitwirkung ist. Die wirtschaftlichen Beziehungen zwischen verschiedenen Anbietern und Angreifern sind häufig sehr komplex, sodass sie sich nicht ohne weitere Aufklärung erschließen. Ziel ist es, den Dienstleister zu identifizieren, welcher die vom Angreifer genutzten Systeme selbst betreibt. Zur Zielerreichung kann es erforderlich sein, eine schriftliche Auskunft aus den Vertragsunterlagen zu erhalten, um die Kontaktmöglichkeiten des Vertragsnehmers zu erlangen. Sobald der letzte Dienstleister der Kette identifiziert wurde, der gegenüber dem Angreifer Dienstleistung erbringt oder dessen Systeme genutzt werden, sind weitere Schritte des Mitwirkens seitens des Providers oder Digitale-Dienste-Anbieters (z.B. Hoster für Webseiten, virtuelle Server oder physische Server) erforderlich. Diese müssen auf Anforderung gezielt innerhalb ihres Betriebs Anpassungen vornehmen, sodass ein Zugriff auf das spezifische Kundenverhältnis möglich wird, ohne dass der Angreifer Verdacht schöpft. Hierfür kommen unterschiedliche technische Maßnahmen in Frage, die im Folgenden beispielhaft aufgezählt werden.

- Betriebsparameter z.B. von genutzten virtuellen Instanzen

- Veränderung der gespeicherten Daten auf einem Datenträger oder Veränderung volatiler Daten im laufenden System

- Hinzufügen/Verändern/Löschen auf einem Angreifersystem

- Verändern von Einstellungen zu Schutzmaßnahmen der bereitgestellten Systemressourcen, sodass eine gefahrenabwehrende Maßnahme ermöglicht wird, bei der der Dienstleister nicht mehr mitwirken muss

- Veränderung der Erreichbarkeit der Dienstleistung für den Angreifer selbst oder dessen Opfer

- Umleitung der IP ins Leere (Änderung von Routingtabellen auf der eigenen Infrastruktur)

- Umleitung von DNS-Einträgen ins Leere (Änderung von DNS-Zuordnungstabellen auf der eigenen Infrastruktur)

- transparentes Durchleiten des Datenverkehrs über eine eigens kontrollierte Umgebung

- Veränderung des Datenverkehrs zur Verringerung der laufenden/bevorstehenden Gefahr oder zur Selbstoffenbarung des Angreifers

- Erstellen/Veränderung von Filterregeln (Änderungen an Tabellen)

- Erstellen/Umkonfigurieren von Firewall-Regeln

- Duplizieren des Datenverkehres zwischen Angreifer und potentiellen Opfern oder anderen kriminellen Elementen

- Dokumentation der Vorgehensweise des Angreifers

- Aufhellung des Täterkomplexes - Aufklären von bisher unbekannten Opfern.

Gemäß Absatz 9 Satz 3 können diejenigen, die nicht in Satz 1 genannt werden, unter den Voraussetzungen des § 21 BPolG ebenfalls zur Mitwirkung an den Maßnahmen nach Absatz 1 Satz 1 Nummer 2 und 3 oder zur Auskunftserteilung in Anspruch genommen werden. Insbesondere kommen hier Personen, Einrichtungen oder Unternehmen in Betracht, die tatsächliche Verfügungsgewalt über Leitungen, Einrichtungen oder Server haben.

Zu Absatz 10

Absatz 10 enthält eine Benehmensregelung für die Umleitung von Datenverkehr, damit beim BSI ein Gesamtüberblick über Umleitungsmaßnahmen bewahrt werden kann.

Zu Absatz 11

Absatz 11 regelt die Befugnis der Bundespolizei, gegenüber dem Betreiber des informationstechnischen Systems oder dem zur Umleitung, Einschränkung oder Unterbindung von Datenverkehr Verpflichteten anzuordnen, gegenüber den von der Maßnahme Betroffenen die Maßnahme nicht offenbaren zu dürfen, solange die Offenbarung Zwecken der Gefahrenabwehr oder Strafverfolgung entgegensteht. Die Befugnis bezieht sich auf alle besonderen Abwehrmaßnahmen.

Erfolgt die Aufhebung eines Offenbarungsverbots nicht binnen 12 Monaten nach Beendigung der Maßnahme, bedarf die weitere Aufrechterhaltung der gerichtlichen Zustimmung. Auf die Geltung von Absatz 6 Satz 2 bis 5 sowie § 78 Absatz 3 Satz 2 und 3 wird verwiesen.

Zu Absatz 12

Absatz 12 stellt deklaratorisch klar, dass für die Löschung der durch die Maßnahmen nach Absatz 1 Satz 1 Nummer 2 oder 3 erlangten personenbezogenen Daten § 81 Absatz 1 gilt.

Zu Absatz 13

Absatz 13 beinhaltet eine Übermittlungspflicht zugunsten der Bundeswehr, soweit der Bundespolizei im Rahmen ihrer Aufgabenerfüllung nach Absatz 1 Informationen bekannt geworden sind, die für Aufgaben der Verteidigung von Bedeutung sein können.

Zu Nummer 3

Die Maßnahmen nach § 41a Absatz 1 Satz 1 Nummer 2 und 3 werden den in § 77 Absatz 1 geregelten Befugnissen der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unterworfen.

Zu Nummer 4

Soweit ein Eingriff in ein privates informationstechnisches System erfolgt und daraus bei der Maßnahme Daten erhoben werden, stellt sich die Maßnahme als eingriffsintensiv dar. Daher werden Maßnahmen nach § 41a Absatz 1 Satz 1 Nummer 3 der Benachrichtigungspflicht nach § 78 BPolG unterworfen. Zu benachrichtigen ist der Inhaber des informationstechnischen Systems, in das eingegriffen wurde.

Zu Nummer 5

Um den Schutz personenbezogener Daten, die im Zuge einer besonderen Abwehrmaßnahme nach § 41a Absatz 1 Satz 1 Nummer 2 und 3 erlangt worden sind, Rechnung zu tragen, werden die Maßnahmen der Pflicht zur Löschung von durch Besondere Mittel der Datenerhebung oder vergleichbare Maßnahmen erlangten personenbezogenen Daten

nach § 81 BPolG unterworfen. Bei Maßnahmen nach Absatz 1 Satz 1 Nummer 1 werden keine personenbezogenen Daten erhoben, die gelöscht werden könnten.

Zu Nummer 6

Da der neu geschaffene § 41a Absatz 1 Satz 1 Nummer 3 eingriffsintensive Maßnahmen ermöglicht, werden die Maßnahmen der Vorschrift zur Protokollierung bei eingriffsintensiven Maßnahmen nach § 85 BPolG unterworfen. Zu protokollieren sind bei Maßnahmen nach § 41a Absatz 1 Nummer 3 Angaben zur Identifizierung des informationstechnischen Systems.

Zu Nummer 7

Nach Nummer 7 wird die Zuwiderhandlung gegen die dort genannten vollziehbaren Anordnungen der Bundespolizei bußgeldbewehrt. Im Einzelnen betrifft dies die folgenden Fälle:

Wird nach § 41a Absatz 1 Satz 1 Nummer 1 dem Betreiber eines IT-Systems, von dem eine Gefahr ausgeht, z.B. weil ein Kunde des Betreibers dieses zur Durchführung von Cyberangriffen verwendet, der Betrieb des Systems untersagt, hat der Betreiber dem Folge zu leisten. Ein Verstoß, d.h. der unveränderte Weiterbetrieb, obwohl das Abschalten faktisch und rechtlich möglich wäre, stellt eine Gefahr für die durch den Angriff bedrohten Rechtsgüter da und ist daher als Ordnungswidrigkeit zu ahnden. Die maximale Bußgeldhöhe orientiert sich daran, dass auch die in diesem Bereich vertretenen sehr großen und wirtschaftsstarken Unternehmen durch das Bußgeld von einer Nichtbeachtung von Anordnungen abgehalten werden sollen.

Auch der Verstoß gegen eine Anordnung nach § 41a Absatz 9 Satz 1, die einen Anbieter von TK-Diensten oder digitalen Diensten zum Umleiten von Datenverkehr verpflichtet, bedeutet, dass die Gefahr für die bedrohten Rechtsgüter nicht abgestellt wird, obwohl dies dem Adressaten der Anordnung möglich wäre. Adressaten dieser Anordnung können Anbieter von TK-Diensten sowie Anbieter digitaler Dienste sein. Bei diesen handelt es sich im ersten Fall nie um natürliche Personen, im zweiten Fall in der Regel nicht um natürliche Personen. Die maximale Bußgeldhöhe orientiert sich daher daran, dass auch die in diesem Bereich vertretenen sehr großen und wirtschaftsstarken Unternehmen durch das Bußgeld von einer Nichtbeachtung der Anordnungen abgehalten werden.

Im Fall des Offenbarungsverbots wird bußgeldbewehrt, wenn ein Adressat des Offenbarungsverbot entgegen dem Verbot den oder die von der Maßnahmen Betroffenen über die Maßnahme unterrichtet. Ein Verstoß liegt beispielsweise vor, wenn die Bundespolizei einem Hosting-Diensteanbieter untersagt, einen bestimmten Server weiterzubetreiben, den ein Dritter für Cyberangriffe verwendet, die Bundespolizei dafür ein Offenbarungsverbot ausspricht und der Anbieter den Kunden, d.h. den Angreifer darüber informiert. Die Information kann dann dazu führen, dass der Angreifer Zeit gewinnt, um seine Taktik zu ändern und auf anderen Server auszuweichen, was sonst nicht oder erst später möglich gewesen wäre. Da in Bezug auf das Offenbarungsverbot auch Fälle denkbar sind, in denen natürliche Personen den bußgeldbewehrten Verstoß verantworten, orientiert sich die Bußgeldhöhe an natürlichen Personen.

Zu Nummer 8

Die Maßnahmen nach § 41a Absatz 1 Satz 1 Nummer 2 und 3 werden der Berichtspflicht gegenüber dem Deutschen Bundestag nach § 106 BPolG unterworfen.

Zu Artikel 2 (Änderung des BSI-Gesetzes)

Zu Nummer 1

Es handelt sich um eine Folgeänderung aufgrund der Einfügung des neuen § 16a.

Zu Nummer 2

Die Ergänzung in § 4 Absatz 2 Nummer 2 ist erforderlich, da die Streitkräfte nicht bereits Teil der Bundesverwaltung sind. Die Einbeziehung der Streitkräfte in die normierten Unterrichtungspflichten in § 4 Absatz 2 ist notwendig, um die effektive Erfüllung des Verteidigungsauftrags durch die Streitkräfte, einschließlich der Aufrechterhaltung der Verteidigungsfähigkeit und der Eigensicherung, sicherzustellen.

Zu Nummer 3

Zu Buchstabe a

Durch die Änderung in Absatz 2 Satz 1 wird das BSI befugt, neben Protokolldaten nach Absatz 1 Nummer 1 auch Daten, die auf externe Ressourcen im Internet verweisen, wie insbesondere Uniform Ressource Locators (URLs), und die bei der automatisierten Auswertung der Schnittstellendaten nach Absatz 1 Nummer 2 anfallen, unter engen Voraussetzungen zu speichern. Diese Änderung ist erforderlich, da sich die Methoden der Angreifer in den letzten Jahren stark verändert haben. Nutzten früher Angreifer zur Infektion von Endsystemen überwiegend Schadprogramme in Dateianlagen von E-Mails, werden gegenwärtig stattdessen zunehmend lediglich URLs verschickt, die auf Webseiten verweisen, auf denen die Schadprogramme platziert werden. Diese wird dann über die URL nur ausgeliefert, wenn diese auf dem Rechner des Empfängers angefordert wird (z.B.: Sandboxerkennung, Prüfung des Useragents, Prüfung der IP-Adresse, etc.). Mit der Speicherung von URLs aus E-Mails in Ergänzung zu den Protokolldaten wird sichergestellt, dass solche Angriffe auch im Nachhinein erkannt werden, wenn das BSI Kenntnis von neuen maliziösen URLs erhält, und die betroffenen Behörden gewarnt werden können. Dies ist etwa bei Ransomware wichtig, die PCs bei Behörden verschlüsseln kann, da es durchaus möglich ist, dass Anwender die URL auf Schadsoftware noch nicht geöffnet haben oder zumindest die weitere Verbreitung der Schadsoftware in der Behörde verhindert werden kann. Die Regelung setzt voraus, dass durch technische Mittel sichergestellt wird, dass lediglich die in Absatz 2 Satz 1 genannten Daten bei der Detektion erfasst und bei der Auswertung automatisiert genutzt werden.

Absatz 2 Satz 5 beinhaltet eine Folgeänderung dazu. Die weitere Änderung in Absatz 2 Satz 5 sieht die Möglichkeit vor, die Anordnungsbefugnis an einen Bediensteten mit Befähigung zum Richteramt zu übertragen. Dies ermöglicht dem BSI eine zügige De-Pseudonymisierung bestimmter Protokolldaten in Fällen, in denen es aufgrund ihrer Natur einer besonders schnellen Reaktion des BSI (wie etwa der Alarmierung und ggf. weiterer Aufklärung und Unterstützung betroffener Behörden) bedarf.

Durch die Änderung in Absatz 3 Satz 1 wird die bestehende Befugnis zur manuellen Auswertung von Protokolldaten auf Schnittstellendaten nach Absatz 1 Satz 1 Nummer 2 ausgeweitet. Die Regelung in Absatz 3 Satz 1 lässt zu den in Absatz 1 geregelten Fällen ausnahmsweise eine ausschließlich auf Zwecke der Fehlerkorrektur begrenzte manuelle Auswertung zu. Die Regelung stellt lediglich eine Ausnahme für Zwecke der Fehlerkorrektur dar. Im Anschluss sind die Daten nach Maßgabe des Absatz 1 Satz 2 BSIG unverzüglich zu löschen. Dabei sind die anfallenden Daten vor Weiterverwendung zu pseudonymisieren, so dass insbesondere ein Bezug auf behördeninterne Empfänger ausgeschlossen ist.

Zu Buchstabe b

Zu Doppelbuchstabe aa

Die Änderung dient der Angleichung der Bezugsvorschriften zum StGB zur Begrenzung auf Computerdelikte zwischen BSIG, BPolG und BKAG.

Zu Doppelbuchstabe bb

Die Änderung in Absatz 6 dient dem Einbezug der Bundeswehr durch eine neue Nummer 4.

Zu Buchstabe c

Die Änderung in Absatz 7 dient ausschließlich der redaktionellen Korrektur falscher Verweise.

Zu Nummer 4

Mit den Änderungen wird klargestellt, dass das BSI in herausgehobenen Fällen einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit von informationstechnischen Systemen der in Absatz 1 genannten Einrichtungen oder bei Anhaltspunkten hierfür nicht nur reaktiv, d.h. wenn sich ein Schaden bereits verwirklicht hat, tätig werden kann, sondern schon bei tatsächlichen Anhaltspunkten für Vorbereitungsmaßnahmen des Angreifers auf diesem informationstechnischen System (sogenanntes Prepositioning). Diese Vorbereitungshandlungen stellen bereits eine Beeinträchtigung der Sicherheit des betroffenen informationstechnischen Systems dar, auch wenn sich eine konkrete Funktionsbeeinträchtigung noch nicht manifestiert hat.

Anhaltspunkte dafür, dass ein Angreifer mit Vorbereitungshandlungen auf einem informationstechnischen System begonnen hat, bestehen etwa, wenn konkrete Informationen zu der von einem Angreifer avisierten Zielgruppe vorliegen bzw. konkrete Ereignisse Hinweise auf Angriffe ergeben. Erforderliche Maßnahmen zur Abwehr und Eindämmung des Angriffs umfassen in diesem Fall auch die systematische Suche nach Angreiferspuren (sogenanntes Threat Hunting).

Zu Buchstabe a

Die Änderungen in Absatz 1 nehmen die Suche und Identifikation von Beeinträchtigungen für die Sicherheit und Funktionsfähigkeit von informationstechnischen Systemen der Einrichtungen der Bundesverwaltung, besonders wichtigen Einrichtungen oder wichtigen Einrichtungen ausdrücklich auf. Die Befugnis bleibt auf herausgehobene Fälle nach Absatz 2 beschränkt.

Zu Buchstabe b

Die Ergänzungen in Absatz 3 stellen klar, dass die speziellen datenschutzrechtlichen Vorgaben für die Identifikation und notwendige Suche nach Bedrohungen dieselben datenschutzrechtlichen Rahmenbedingungen gelten, wie für den Fall der Wiederherstellung der Funktionsfähigkeit von informationstechnischen Systemen.

Zu Nummer 5

Die Bundesverwaltung sowie besonders wichtige und wichtige Einrichtungen sowie die Verlässlichkeit und Funktionsfähigkeit der Kommunikationsinfrastruktur selbst sind täglich bedroht durch eine Vielzahl von Angriffen auf die Verfügbarkeit, Vertraulichkeit und Integrität informationstechnischer Systeme. Im Zusammenhang mit der Bereitstellung von Telekom-

munikations- und digitalen Diensten fallen eine Vielzahl von Daten an, deren Auswertung für die Erkennung und Abwehr von Cyberangriffen sehr wertvoll sind. Diese Daten werden im Rahmen des Betriebs von Angriffserkennungssystemen regelmäßig auch durch die Betreiber selbst verarbeitet, um Angriffe frühzeitig und in großem Umfang zu erkennen.

Mit dem neuen Absatz 6 wird eine spezielle Auskunftspflicht für diese Diensteanbieter geschaffen, die auf die vorgenannten sicherheitsrelevanten Informationen, die durch die Diensteanbieter zunächst zu eigenen Zwecken erhoben werden, beschränkt ist. Hierzu zählen Verkehrs- und Steuerungsdaten sowie technische Informationen, die von den Anbietern zur Verkehrsanalyse zur eigenen Qualitätssicherung und im Rahmen von technischen Vorkehrungen nach § 12 Absatz 1 und § 19 Absatz 4 TDDDG sowie § 165 Absatz 2 TKG auswerten. Solche sicherheitsrelevanten Informationen sind unter anderem Metainformationen über Datenflüsse zur Identifizierung verdächtiger Ursprünge und Ziele, Paket- und Byte-Zahlen (zur Überwachung von Volumenanomalien), Zeitstempel (zur zeitlichen Analyse des Verkehrs und zur Korrelation von Ereignissen), DNS-Anfragedaten (zur Erkennung von DNS-Amplification-Angriffen und der Kommunikation mit Botnet-Kontrollservern), sogenannte Indicators of Compromise („IOCs“) zu relevanten beobachteten Angriffen und Beispieldateien (Samples) von selbst beobachteten Schadprogrammen (etwa über sogenannte „Honeypots“ oder „Sinkholes“) sowie ihnen bekannte Informationen zu Domains, von denen Sicherheitsrisiken für die Informationstechnik ausgehen (sogenannte maliziöse Domains).

Durch eine betreiberübergreifende Auswertung durch das BSI wird die Sicht auf die aktuelle Bedrohungslage und der Schutz der Bundesverwaltung sowie von besonders wichtigen und wichtigen Einrichtungen erheblich verbessert.

Absatz 6 Satz 1 enthält eine Befugnis des BSI, gegenüber Anbietern Auskunft zu verlangen, und in Satz 2 die Pflicht, Daten bereitzustellen. Es wird ein Satz 3 ergänzt, der zugunsten der Anbieter regelt, dass sie zum Zweck der Erfüllung dieser Pflichten personenbezogene und Verkehrsdaten verarbeiten dürfen. Dies erfüllt die Anforderungen der „Doppeltür“-Rechtsprechung des Bundesverfassungsgerichts (Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238).

Zu Nummer 6

Zu Buchstabe a

Die in einer Anordnung nach Absatz 1 Satz 1 als Störquelle bezeichneten Angreifer ändern für Cyberangriffe genutzte Domain-Namen oder IP-Adressen teilweise regelmäßigen, auch kurzfristigen Abständen (bis zu mehrmals täglich), um die Wirkung von Umleitungsmaßnahmen gezielt auszuhebeln. Mit den neuen Sätzen 4 und 5 wird klargestellt, dass im Rahmen einer Anordnung nach Satz 1 Nummer 1 ergänzend auf durch das BSI für den Anordnungsempfänger bereitgestellte Listen mit Domain-Namen oder IP-Adressen verwiesen werden kann, die der in der Anordnung bezeichneten Störquellen zuzuordnen sind und die bei Bedarf geändert werden kann, ohne dass sich das BSI erneut mit der Bundesnetzagentur ins Benehmen setzen muss. Durch die Regelung wird den Anordnungsadressaten eine schnelle und unbürokratische Umsetzung der Anordnungen erleichtert und dem BSI sowie der beteiligten Bundesnetzagentur ermöglicht, rechtzeitig auf taktische Änderungen einer bekannten Störquelle zu reagieren.

Zu Buchstabe b

Die Ergänzung ist erforderlich, weil die Kommunikationstechnik der Bundeswehr nicht Teil der Kommunikationstechnik des Bundes im Sinne des § 2 Nummer 21 ist.

Zu Buchstabe c

Mit der Umleitung von Daten auf eigene Sinkhole-Server nach Absatz 1 Satz 1 Nummer 1 und Absatz 4 wird das BSI in die Lage versetzt, die technischen Voraussetzungen und Abläufe eines Angriffs zu analysieren und auszuwerten. Diese Analyse ist neben der wirksamen Unterbindung eines laufenden Angriffs (etwa zur Erkennung möglicher und wichtiger Schutzmaßnahmen etwa zur Bereinigung betroffener Systeme) insbesondere auch auf einem verbesserten Schutz vor zukünftigen Angriffen gerichtet (s.a. BT-Drs. 19/26106, S. 75f.). Mit der Änderung in Absatz 5 Satz 2 wird die zulässige Höchstspeicherdauer für Daten, die von einem Diensteanbieter nach Absatz 1 Satz 1 Nummer 1 i.V.m. Absatz 4 umgeleitet wurden, auf 24 Monate erweitert. Die in der Praxis gewonnenen Erkenntnisse haben gezeigt, dass aufgrund der Komplexität der möglichen Angriffe und des hieraus bei der Analyse resultierenden Aufwands die bisherige Höchstspeicherfrist deutlich zu kurz ist:

Bei der Umleitung nach Absatz 1 und 4 wird der Datenverkehr, der an eine bestimmte IP-Adresse gerichtet ist, an einen Server des BSI umgeleitet (sog. Sinkholing). Im Regelfall handelt es sich dabei um Datenverkehr, der von kompromittierten Systemen aus ohne Wissen der Betroffenen an einen bestimmten Kontroll-Server des Angreifers adressiert ist, an dessen IP-Adresse die Umleitung in diesem Fall anknüpft. Im Sinkhole aufgezeichnet wird nur die bösartige Kommunikation zwischen dem Schadprogramm auf dem infizierten Rechner und Kontrollserver; typischerweise begrenzt auf den ersten Verbindungsversuch des Schadprogramms mit dem Angreiferserver. Durch die Umleitung können kompromittierte Systeme vor weiteren Zugriffen der Angreifer, aber auch Dritte vor einem Mißbrauch der kompromittierten Systeme (etwa als Bots im Rahmen zielgerichteter, komplexer Angriffe) geschützt werden. Aus der automatisierten Auswertung der Sinkholedaten kann das BSI die IP-Adressen der kompromittierten IT-Systeme, von denen die Malwarekommunikation mit dem Angreiferserver ausgeht, identifizieren und die Betroffenen über die Telekommunikationsprovider, denen diese IP-Adressen zugeordnet werden können, warnen (vgl. § 169 TKG).

Neben den IP-Adressen, die zur Opferbenachrichtigung verwendet werden müssen, beinhalten die anfallenden Sinkhole-Daten wertvolle technische Informationen, die Rückschlüsse über die Art und Funktionsweise eines Angriffs zulassen, etwa zum verwendeten Schadprogramm und zu betroffenen Systemen (adressierte Ports, Betriebssystem- und Softwarekennungen, die Rückschlüsse auf typischerweise ausgenutzte Hersteller, Hardwareplattformen Betriebssysteme oder Softwarestand zulassen, sowie im Zusammenhang mit dem Angriff generierte Merkmale wie Hashwerte) und möglichen Einfallsvektoren Einfallsvektor (z.B. eine Schwachstelle). Diese Erkenntnisse sind für das BSI von großer Bedeutung, um gegebenenfalls Produktwarnungen auszusprechen (etwa zu ab Werk infizierten IT-Produkten), über Schwachstellen zu informieren und dabei zu unterstützen, Systeme abzusichern.

Dass bereits bei dem Kommunikationsversuch des Schadprogramms mit dem Angreiferserver neben diesen technischen Informationen auch bereits Daten des Betroffenen übermittelt werden (beispielsweise Zugangsdaten) ist unwahrscheinlich, aber rein theoretisch nicht auszuschließen, da die Programmierung der Malware durch den Angreifer erfolgt. In diesen Fällen wären diese Daten für das BSI aber regelmäßig nicht lesbar, weil auch Schadprogramme ihre Kommunikation verschlüsseln, bzw. nicht verständlich, weil die Kommunikation des jeweiligen Schadprogramms so spezifisch ist, dass sie ohne genaue Kenntnisse des Schadprogramms nicht ohne weiteres nachvollzogen werden kann, so dass ein Personenbezug für das BSI entfällt. Tatsächlich verwendet das BSI bereits bei der Erhebung der Daten einen Filter, um gezielt nur die benötigten technischen angriffsbezogenen Informationen zu erheben. Zudem wären solche Daten nicht zur Analyse des Schadprogramms bzw. des Cyberangriffs oder zur Benachrichtigung von Opfern erforderlich und sind daher unabhängig von einer Höchstspeicherfrist bereits unmittelbar nach Absatz 5 Satz 2 zu löschen.

Die angriffsbezogenen Daten benötigt das BSI jedoch regelmäßig über einen deutlich längeren Zeitraum als mit der bisherigen drei monatigen Höchstspeicherfrist. Die praktische Anwendung der Vorschrift hat gezeigt, dass die Analyse der Schadprogramme und Einfallsvektoren zunehmend komplex und regelmäßig nicht in drei Monaten abzuschließen ist. Behörden, Unternehmen und andere wichtige Einrichtungen in Deutschland, wie etwa Krankenhäuser, werden regelmäßig Opfer von Cyberangriffen. Das BSI unterstützt eine Vielzahl betroffener Institutionen bei der Reaktion auf diese Vorfälle (sogenanntes Incident Response). Mit der Anpassung in § 11 soll für einen verbesserten Schutz vor komplexen Angriffen das BSI Einrichtungen der Bundesverwaltung sowie besonders wichtige und wichtige Einrichtungen nach § 28 zudem auch in Fällen des sogenannten Prepositioning unterstützen können. Dabei ist häufig eine Schadprogramm-Infektion der Einfallsvektor für die Kompromittierung ganzer IT-Systeme und nachfolgend auch von kompletten Netzwerken. Teilweise finden die initialen Schadprogramm-Infektionen bereits viele Monate statt, bevor der Angriff von den Betroffenen überhaupt entdeckt wird. Zudem wird häufig von den Betroffenen zwar die initiale Schadprogramm-Infektion nach einiger Zeit grundlegend bereinigt, ein darüber von den Tätern zwischenzeitlich bereits geschaffener persistenter Zugriff auf die Systeme jedoch übersehen, sodass die Täter auch noch lange Zeit nach der (vermeintlich) bereinigten Schadprogramm-Infektion aktiv bleiben können. Um bei der Reaktion auf spätere Cyberangriffe konkrete Schadprogramm-Infektionen als Einfallsvektor für solche persistenten Zugriffe jeweils identifizieren zu können, müssen die entsprechenden Sinkhole-Daten zur Erkennung dieses Angriffsvektors noch vorliegen. Darüber hinaus wurde das BSI in der Mehrheit der bisher aufgetretenen Fälle erst über 12 Monate nach einem Vorfall von Partnerbehörden wie BKA, BfV kontaktiert, die beim BSI anfragen, ob ein bestimmter Vorfall dem BSI aus Sinkholing-Maßnahmen bekannt ist und ob Daten zu Infektionswegen und Betroffenen vorliegen, die für die weitere Aufklärung und Verfolgung von Cyberangriffen benötigt werden. Während private Stellen und andere öffentliche Stellen nicht über eine vergleichbar Höchstspeicherfrist verfügen, kann das BSI entsprechende Anfragen derzeit dann nicht mehr beantworten, weil es seine Daten bereits löschen musste.

Vor diesem Hintergrund ist die Anpassung der Höchstspeicherfrist aufgrund der Beschränkung auf technische Informationen zum Angriff der in Sinkholes aufgezeichneten Kommunikation zwischen Schadsoftware und Angreiferserver einerseits und der hohen Bedeutung der Erkenntnisse zur Analyse, Detektion und Verfolgung von Cyberangriffen sowie zur Opferbenachrichtigung mit potentiell hohem Schadenspotential gerechtfertigt.

Unabhängig von der Höchstspeicherfirst sind die in einem Sinkhole anfallenden Daten umgehend zu löschen, soweit sie nicht zur Aufklärung des Cyberangriffs einschließlich der mit diesem konkret verbundenen IT-Sicherheitsrisiken erforderlich sind. Nach Erreichen der Höchstspeicherfrist von 24 Monaten sind alle Daten in jedem Fall zu löschen.

Zu Buchstabe d

Mit den neuen Absätzen 6 und 7 soll der Schutz vor maliziösen Domains verbessert werden.

Nach Absatz 6 Satz 1 führt das BSI eine öffentlich einsehbare Liste von Domains, von denen Sicherheitsrisiken für die Informationstechnik ausgehen (sogenannte maliziöse Domains). Hierunter fallen öffentlich erreichbare Webseiten, die den Anschein der Erbringung bestimmter Leistungen (z.B. Online-Shops) mit dem Ziel erwecken, Schadsoftware auszuführen bzw. den Nutzer dazu zu bringen, vertrauliche Zugangsdaten (z.B. Passwörter, sog. „Phishing“) preiszugeben. Die Verbreitung von Schadsoftware über entsprechend präparierte Webseiten stellt zunehmend eine der Hauptbedrohungen einer sicheren Nutzung der Telekommunikationsinfrastruktur dar. Auf diesem Weg auf IT-Systemen der Nutzer installierte Schadsoftware kann – je nach Design der Schadsoftware – von dort aus auch andere Systeme infizieren oder dazu genutzt werden, die Funktionsweise der IT-Systeme, etwa Router, zu verändern und diese ferngesteuerten Systeme ihrerseits für Angriffe auf Dritte zu nutzen. Infizierte Systeme können auch im Verbund durch von Angreifern kontrollierte

Server gesteuert und als sogenanntes „Bot-Netz“ erhebliche Risiken für die Funktionsfähigkeit der Telekommunikationsinfrastruktur darstellen. Auch Phishing-Angriffe über entsprechend präparierte Webseiten stellen eine erhebliche Bedrohung für die Sicherheit des Internets dar. Angreifer versuchen, persönliche Informationen wie Zugangsdaten und Passwörter, oder andere sensible Daten von gutgläubigen Nutzern zu stehlen.

Mit Veröffentlichung von maliziösen Domains durch das BSI nach Absatz 6 Satz 1 soll die Transparenz zu entsprechenden Verbreitungswegen erhöht und die Voraussetzungen für eine technische Unterstützung zum Nutzerschutz durch bestimmte kommerzielle Diensteanbieter nach Absatz 7 verbessert werden. Bei der Erhebung und Auswertung von Informationen hat das BSI nach Absatz 6 Satz 2 auch Beschwerden von Domain-Inhabern und Bürgern entgegenzunehmen und zu überprüfen. Die öffentliche Bereitstellung einer Liste maliziöser Domains schließt eine regelmäßige Überprüfung auf deren Aktualität hin mit ein.

DNS-Diensteanbieter nach § 2 Nummer 8 Buchstabe a sind nach Absatz 7 verpflichtet, ihren Nutzern auf deren Wunsch hin einen DNS-basierten Schutz vor solchen maliziösen Domains bereitzustellen. Dabei ist der Kreis der Verpflichteten auf Anbieter, die mindestens 50 Mitarbeiter beschäftigen oder einen Jahresumsatz und eine Jahresbilanzsumme von mehr als 10 Millionen Euro aufweisen, begrenzt.

Zu Nummer 7

Botnetze nutzen häufig Domainnamen, um eine Verbindung zur Infrastruktur des Angreifers zu etablieren. Nach der bestehenden Befugnis in § 16 Absatz 1 Nummer 1 kann das BSI bereits bisher eine Umleitung von Domainnamen durch Telekommunikationsdiensteanbieter veranlassen und setzt diese Maßnahmen unter anderem zur Abwehr von Angriffen über Botnetze erfolgreich ein. Die Umleitung durch Telekommunikationsdiensteanbieter nach § 16 Absatz 1 Nummer 1 kann Aktivitäten einer maliziösen Infrastruktur allerdings nicht flächendeckend unterbinden, da zahlreiche Endnutzer Domainnamen zunehmend nicht primär durch ihren Internetanbieter, sondern durch andere Anbieter auflösen oder eigene Systeme zur Namensauflösung betreiben. Der neue § 16a und der neue § 17 Absatz 2 schließen diese Lücke, indem eine entsprechende Anordnungsbefugnis gegenüber Top Level Domain Name Registries (§ 3 Absatz 1 Satz 2 Nummer 42) und Registrare (Domain-Name-Registry-Dienstleister nach § 3 Absatz 1 Satz 2 Nummer 9) sowie gegenüber Anbieter bestimmter digitaler Dienste geschaffen wird.

§ 16a Absatz 1 Satz 1 erlaubt dem BSI, zur Abwehr von erheblichen Gefahren ausschließlich für die in § 16 Absatz 3 benannten Schutzgüter gegenüber gegenüber Top Level Domain Name Registries (§ 3 Absatz 1 Satz 2 Nummer 42) und Registrare (Domain-Name-Registry-Dienstleister nach § 3 Absatz 1 Satz 2 Nummer 9) die Änderung oder Ergänzung der dort vorgehaltenen Nameserver-Einträge anzuordnen. Dies schließt auch die Dekonnektierung einer Domain auf dieser Ebene ein, das heißt die Löschung des Nameserver-Eintrags, so dass eine bestehende Domain nicht mehr erreichbar ist. Zudem kann es notwendig sein, Änderungen an den Nameserver-Einträgen vorzunehmen, um ein gültiges Zertifikat für den betroffenen Domainnamen erstellen zu können. Mit der Regelung soll telekommunikationsspezifischen Gefahren begegnet werden, die sich insbesondere im Hinblick auf die vorgenannten maliziösen Angreiferinfrastrukturen (Botnetze) für die grundlegende Kommunikationsinfrastruktur ergeben. Neben der Gewährleistung einer verlässlichen und sicheren Nutzung der Telekommunikationsinfrastruktur dient die Regelung speziell auch dem Schutz der Kommunikationstechnik des Bundes und besonders wichtiger oder wichtiger Einrichtungen (§ 2 Nummer 21 und § 28). Die gefahrenabwehrrechtliche Annexkompetenz besteht für die Anordnungsbefugnisse des BSI gegenüber Anbietern von Telekommunikations- und Digitalen Diensten (einschließlich den Anbietern von Domainname-Diensten) mit Blick auf die Notwendigkeit eines bundeseinheitlichen Niveaus von Cybersicherheit der Diensteanbieter bezüglich im Telekommunikationsgesetz verankerter gewerblicher Pflichten dieser Anbieter sowie mit Blick auf die Notwendigkeit der näheren Überwachung der im Digitale-Dienste-Gesetz verankerten gewerberechtlichen Pflichten der Digi-

tale Diensteanbieter. Hier ist zur Aufrechterhaltung sicherer IT-Strukturen und -anwendungen eine bundesweit einheitliche Gefahrenabwehr erforderlich.

Absatz 1 Satz 2 sieht die sofortige Vollziehbarkeit der Anordnungen des BSI nach Absatz 1 Satz 1 vor. Die sofortige Vollziehbarkeit beruht hier auf einem überwiegenden öffentlichen Interesse an einer raschen Unterbindung der erheblichen Gefahr, die z.B. für die Regierungsnetze, besonders wichtige und wichtige Einrichtungen besteht, gegenüber dem Interesse des Domaininhabers an der uneingeschränkten Erreichbarkeit seiner Domain.

Die Befugnis in Absatz 2 Satz 1 zur Anordnung gegenüber TLD-Name-Registries, Domain-Name-Registries und -Dienstleistern den an bestimmte Second-Level- oder eine auf einer Ebene darunter liegende Domain gerichtete Nameserveranfragen an einen vom BSI benannten Nameserver umzuleiten, entspricht der Regelung in § 16 Absatz 4. Wie dort wird durch die Regelung dem BSI die Möglichkeit eröffnet, den Datenverkehr bei Bedarf zu analysieren, soweit dies erforderlich ist, um Erkenntnisse über Schadprogramme oder andere Sicherheitsrisiken zu erlangen. Mit Absatz 2 Satz 2 wird sichergestellt, dass für die Verarbeitung dieser Daten dieselben datenschutzrechtlichen Grundsätze, einschließlich des Schutzes des Kernbereichs privater Lebensgestaltung, gelten. Wie bei Umleitungen nach § 16 sind die anfallenden Daten danach umgehend zu löschen, soweit sie nicht zur Aufklärung des Cyberangriffs einschließlich der mit diesem konkret verbundenen IT-Sicherheitsrisiken erforderlich sind. Nach Erreichen der Höchstspeicherfrist von 24 Monaten sind alle Daten in jedem Fall zu löschen.

In Absatz 3 wird festgelegt, wann die Änderung von Einträgen bei einer TLD-Registry oder einem Registrar wieder zu beenden ist.

§ 17 Absatz 1 ist unverändert. Mit dem neuen § 17 Absatz 2 wird die bisherige Regelung zur Umleitung von Datenverkehren in § 16 ergänzt und eine Lücke in der Bekämpfung von Schadsoftware und Botnetzen geschlossen. Eine DNS-basierte Umleitung von Datenverkehren kann bisher nur durch eine Anordnung nach § 16 Absatz 1 über die von den dort benannten Telekommunikationsdiensten betriebenen DNS-Resolvern bewirkt werden. Da Botnetze zunehmend neue Techniken wie „DNS over HTTPS“ verwenden, bei denen zur Namensauflösung nicht die Systeme der Anbieter von öffentlich zugänglichen Telekommunikationsdiensten verwendet werden, erfassen Umleitungen nach § 16 Absatz 1 einen sehr großen Anteil des Botnetzverkehrs nicht. Daher werden zusätzlich zu Telekommunikationsanbietern auch bestimmte Webhoster und Contentanbieter in den Kreis der möglichen Adressaten aufgenommen. Die Umleitung der Botnetzverkehrs ist hierdurch auch in Fällen möglich, in denen die Betreiber der Netzwerke bewusst die TK-Anbieter umgehen. Adressiert werden mit Anbietern von Cloud-Computing-Diensten und Content Delivery Networks, Managed Security Service Providern und Managed Service Providern sowie Anbietern von Rechenzentrumsdiensten nach § 2 Nummer 4, 5, 25, 26 und 35 lediglich die Anbieter, die zentrale DNS-Dienste im Internet erbringen. Mit Satz 2 wird sichergestellt, dass für die Verarbeitung dieser Daten dieselben datenschutzrechtlichen Grundsätze, einschließlich des Schutzes des Kernbereichs privater Lebensgestaltung, gelten. Wie bei Umleitungen nach § 16 sind die anfallenden Daten danach umgehend zu löschen, soweit sie nicht zur Aufklärung des Cyberangriffs einschließlich der mit diesem konkret verbundenen IT-Sicherheitsrisiken erforderlich sind. Nach Erreichen der Höchstspeicherfrist von 24 Monaten sind alle Daten in jedem Fall zu löschen.

Zu Nummer 8

Die Anpassung entwickelt die Funktionalität der bereits in den kritischen Anlagen vorliegenden Systeme zur Angriffserkennung weiter, indem sie eine Anbindung an das BSI vorsieht. Dadurch kann der Nutzwert der Systeme für die Wahrnehmung der Aufgabe des BSI erheblich gesteigert werden, ohne dass es einer wesentlichen Umstrukturierung bedarf: mittels einer direkten Schnittstelle, deren Anforderungen das BSI festlegt und veröffentlicht, werden Informationen zu der Verfügbarkeit der kritischen Anlage und ihrer aktuellen Bedro-

hungslage unmittelbar und regelmäßig aus den bestehenden Systemen an das BSI versandt. Das BSI nutzt diese Informationen zur Aggregation eines Echtzeitlagebildes und zur Analyse von Angriffsmustern und Sicherheitsrisiken und ist durch die Anpassung imstande, Verfügbarkeitsunterbrechungen und Anomalien, die auf eine Bedrohung oder Beeinträchtigung der Sicherheit in der Informationstechnik hindeuten können, ohne Zeitverzug zu erkennen. Das BSI nutzt diese Informationen, um andere Betreiber kritischer Anlagen entsprechend zu warnen und somit seinen Aufgaben aus § 3 Absatz 1 Nummer 2 BSIG nachzukommen. Diese sollen anlassbezogen überstellt werden. Mittels Informationen über angegriffene Schwachstellen lässt sich durch das BSI eine deutlich detailliertere Einschätzung über die Natur und mögliche Folgen des Angriffs erstellen und Rückschlüsse über mögliche Auswirkungen/Risiken auf potenzielle andere Opfer ziehen. Die genutzten Verfügbarkeitsindikatoren der IT-Systeme der kritischen Anlage sollen als fortlaufende, kontinuierliche Zustandsanzeige (z. B. minütlich) an das BSI ausgeleitet werden. Zusätzlich sind Betreiber von kritischen Anlagen verpflichtet, Indikatoren zu potenziellen und tatsächlichen Angriffen sowie Informationen zu angegriffenen Schwachstellen an das BSI zu übermitteln. Bei Indikatoren zu potenziellen und tatsächlichen Angriffen handelt es sich um verschiedene Parameter und Merkmale marktgängiger Systeme zur Angriffserkennung. Dazu gehören insbesondere Netzwerkverkehr mit bekannten, bösartigen IPs oder Domains, zu ungewöhnlichen Ports, bösartige Hashes, unerwartete Skripte, fehlerhafte Anmeldungen sowie anomale Netzwerk- oder Benutzeraktivität. Solche Indikatoren fallen bei jedem Betreiber kritischer Anlagen an, der seiner gesetzlichen Verpflichtung, Systeme zur Angriffserkennung einzusetzen, nachkommt. Insbesondere wird hierdurch keine Pflicht begründet, ein bestimmtes System zur Angriffserkennung zu nutzen. Es müssen nur Indikatoren übermittelt werden, sofern die Systeme zur Angriffserkennung erhebliche, d.h. über das alltägliche Gros der Systemmeldungen hinausgehende Bedrohungen, Störungen oder Beeinträchtigungen erkennen. Details kann das BSI im Rahmen seiner Festlegungen nach Absatz 6 regeln. Zur Gewährleistung einer unveränderten Absicherung der kritischen Anlagen und uneingeschränkten Hoheit der Unternehmen über ihre Systeme soll die Ausleitung der Daten automatisiert mittels einer gesicherten, unidirektionalen Verbindung rückwirkungsfrei hin zum BSI erfolgen. Die Ergänzung in Absatz 2 stellt sicher, dass die Systeme zur Angriffserkennung auch vom BSI separat bereitgestellte Informationen verarbeiten können. Die Einzelheiten der Anbindung und Ausleitung legt das BSI auf Grundlage von Absatz 6 in Form einer technischen Richtlinie fest und veröffentlicht sie auf seiner Internetseite, um den Betreibern eine ordnungsgemäße Anbindung und Ausleitung zu ermöglichen. Darin enthaltene Festlegungen zu den zu übermittelnden Indikatoren und deren Übermittlungsstandard sind notwendig, um die Anzahl der Meldungen auf die relevanten Alarme zu begrenzen und die übermittelten Informationen automatisiert verarbeiten zu können. Die Frist von zwölf Monaten soll den Betreibern ermöglichen, die Anforderungen technisch umzusetzen. Dem BSI steht darüber hinaus die Möglichkeit offen, im Einzelfall auf eine Anbindung und Übermittlung der Informationen zu verzichten. Dies kann etwa vorübergehend dann der Fall sein, wenn sich herausstellt, dass die Anbindung für einige Anbieter insbesondere wirtschaftlich nicht zumutbar ist.

§ 31 Absatz 4 BSIG-E stellt die Rechtsgrundlage für die Ausleitung dar und erfüllt damit die Anforderungen des Bundesverfassungsgerichts im Sinne der „Doppeltür-Rechtsprechung“ (Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, 1 BvR 2618/13 –, BVerfGE 155, 119–238). Es wird eine Rechtsgrundlage zur Datenverarbeitung zugunsten der Betreiber ergänzt. Zudem darf das BSI personenbezogene Daten verarbeiten, um seinen Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 2, 22, 24 und 25 nachzukommen.

Zu Nummer 9

Durch die Anpassungen zur ordnungsgemäßen Anbindung der Systeme zur Angriffserkennung erhält das BSI kontinuierlich unmittelbare Informationen über die Verfügbarkeit und die Bedrohungslage bei den kritischen Anlagen. Dadurch entfällt die Notwendigkeit für einen eigenständigen Nachweis zu diesen Systemen zur Angriffserkennung.

Zu Nummer 10

Mit den Änderungen in Absatz 1 wird klargestellt, dass die in § 2 Nummer 2 genannten Stellen unter Angabe der Bestimmung, die ihnen eine Erhebung der in Absatz 1 genannten Bestandsdaten erlaubt, zur Erfüllung ihrer eigenen Aufgaben zum Abruf berechtigt sind. Die Verantwortung für die Zulässigkeit der Übermittlung tragen die ersuchenden Stellen. Ein berechtigtes Interesse wird nachgewiesen, indem auf die entsprechende Befugnisnorm verwiesen wird.

Zu Nummer 11

Mit der Vorschrift wird dem Zitiergebot des Artikels 19 Absatz 1 Satz 2 des Grundgesetzes nachgekommen.

Zu Nummer 12

Zu Buchstabe a

Zu Doppelbuchstabe aa

Für Verstöße gegen die neu eingefügten §§ 16a und 17 Absatz 1, die die in § 16 für Telekommunikationsanbieter bestehenden Pflichten auf weitere Diensteanbieter (Top-Level Domain Name Registries und Domain-Name-Registry-Dienstleister sowie ein enger Kreis von Anbietern digitaler Dienste) ausweiten, wird der Bußgeldrahmen mit einer Bußgeldhöhe von bis zu 500.000 Euro an den entsprechenden Regelungen für das BPolG und das BKAG (Art. 1 Nummer 7 und Art. 3 Nummer 14) ausgerichtet. Der Bußgeldrahmen für § 16 wird entsprechend von bis zu 2 Millionen auf 500.000 Euro abgesenkt.

Zu Doppelbuchstabe bb

Die Ergänzung in Doppelbuchstabe bb) betrifft das Unterlassen des Einsatzes von Systemen zur Angriffserkennung und ihrer Anbindung beim BSI sowie das damit verbundene automatische Ausleiten von Verfügbarkeitsindikatoren, Indikatoren zu potenziellen und tatsächlichen Angriffen und Informationen zu Schwachstellen an das BSI gemäß § 31 Absatz 3 BSIG-E. Dies war nicht eigens sanktionierbar. Mit der Anpassung wird der gesteigerten Bedeutung ihrer Nutzung und Anbindung Rechnung getragen.

Zu Buchstabe b

Die Änderung legt die Bußgeldhöhe für die neu eingefügten Bußgeldtatbestände in Absatz 2 Nummern 3a bis 3b auf bis zu einer Millionen Euro fest. Infolge der neuen Verpflichtungen in § 31 Absatz 2 und 3 BSIG-E werden bestimmte Nachweispflichten für Betreiber kritischer Anlagen in § 39 Absatz 1 BSIG-E gestrichen. Die neu eingeführten Pflichten in § 31 Absatz 2 und 3 zur Anbindung an das BSI treten damit an die Stelle der bisherigen Pflicht zur Erbringung entsprechender Nachweise über die Systeme zur Angriffserkennung. Daher ist es angemessen, auch die Höhe der Bußgeldbewehrung für einen Verstoß gegen diese neuen Pflichten an der Höhe für einen Verstoß gegen die bisherigen Nachweispflichten auszurichten. Gleichzeitig entspricht der Bußgeldrahmen damit der spezialgesetzlichen Regelung in Artikel 5 Nummer 2.

Zu Artikel 3 (Änderung des Bundeskriminalamtgesetzes)

Ziel der Ergänzung des Bundeskriminalamtgesetzes ist die Verbesserung der Möglichkeiten bei der Abwehr schwerwiegender Cyberbedrohungen durch das Bundeskriminalamt (BKA).

Das BKA nimmt bereits heute im Bereich international koordinierter Cybercrime-Bekämpfung eine tragende Rolle ein. Das BKA ist unter anderem Zentralstelle für die deutsche Kriminalpolizei, Kontaktpunkt für Interpol, Europol und die etablierten Cybercrime-Netzwerke der G7 bzw. des Europarates (Budapest Convention on Cybercrime). Das BKA ist auch im Bereich der Strafverfolgung im Phänomenbereich Cybercrime im engeren Sinne bereits heute bei Taten gegen die innere und äußere Sicherheit der Bundesrepublik Deutschland sowie gegen Behörden oder Einrichtungen des Bundes bzw. Stellen von lebenswichtigen Einrichtungen originär zuständig. Darüber hinaus nimmt das BKA jederzeit auf Ersuchen einer Landesbehörde oder auch des Generalbundesanwaltes die polizeilichen Aufgaben auf dem Gebiet der Strafverfolgung wahr. In diesem Rahmen werden umfangreiche, national und international zu koordinierende Ermittlungsverfahren durch das BKA geführt. Insgesamt sind insbesondere (aber nicht abschließend) Ermittlungsverfahren im Zusammenhang mit Botnetzen, Schadsoftwarevarianten, DDoS-Angriffen und Netzwerkeinbrüchen umfasst.

Cyberkriminalität ist eines der sich am dynamischsten verändernden Kriminalitätsphänomene. Die Täter passen sich nicht nur den gesellschaftlichen Entwicklungen an, sondern agieren auch äußerst flexibel in Hinblick auf technische bzw. technologische Trends. Um Gefahren durch die verschiedenen Ausprägungen von Cybercrime sinnvoll abwehren zu können, bedarf es deshalb flankierend zu den klassischen polizeilichen Befugnissen spezieller, an das Phänomen Cyberkriminalität und dessen Modi Operandi angepasster Maßnahmen.

Das BKA erhält deshalb zum Schutz hochrangiger Rechtsgüter entsprechende Befugnisse zur Abwehr von Cyberbedrohungslagen. Die in Artikel 3 neu eingeführten Befugnisse ermöglichen es dem BKA zum einen künftig, im Rahmen der bestehenden Aufgaben (Abwehr von Gefahren des internationalen Terrorismus, Schutz von Mitgliedern der Verfassungsorgane und der Leitung des Bundeskriminalamtes, Zeugenschutz sowie Sicherung des Bundeskriminalamtes, behördlicher Eigenschutz) Gefahrenabwehrmaßnahmen gegen Cyberangriffe umzusetzen. Darüber hinaus erhält das BKA in eng eingegrenzten Fallkonstellationen neue Aufgaben zur Gefahrenabwehr.

Zu Nummer 1

Nummer 1 setzt Folgeänderungen in der Inhaltsübersicht um.

Zu Nummer 2

Im Rahmen seiner Aufgaben als polizeiliche Zentralstelle nimmt das BKA nach § 2 Absatz 5 BKAG Unterstützungsmaßnahmen auf Ersuchen der Polizeien des Bundes und der Länder wahr. In Ergänzung der bisherigen Unterstützung bei kriminaltechnischen Untersuchungen (Nummer 3) und der Datenverarbeitung (Nummer 4) kann das BKA nach der neu eingefügten Nummer 5 Polizeien des Bundes und der Länder im Einzelfall und auf deren Ersuchen bei der Durchführung von Maßnahmen im Bereich der Cyberabwehr unterstützen. Hierbei kann es sich beispielsweise um eine DDoS-Attacke mittels DNS-Servern handeln. Das BKA unterstützt das Land, in welchem sich der verursachende Server befindet, auf Ersuchen bei der Umsetzung technischer Maßnahmen, wie z.B. dem Umleiten von Datenverkehr, zur Abwehr der Gefahr. Es handelt sich bei solchen Unterstützungshandlungen in der Regel um Amtshilfe, die grundsätzliche Verantwortlichkeit für die Maßnahmen verbleibt bei der ersuchenden Stelle.

Voraussetzung für eine Unterstützung des BKA in Amtshilfe ist, dass sowohl das ersuchende Land als auch das BKA über entsprechende Befugnisse zur Abwehr von Cybergefahren verfügen.

Zu Nummer 3

Der neu eingefügte § 3a BKAG regelt die Aufgabe des BKA zur Cyberabwehr im Rahmen der internationalen Verbrechensbekämpfung, bei Angriffen gegen Einrichtungen und Behörden des Bundes sowie bei Cybergefahren, welche die auswärtigen Angelegenheiten oder die Verteidigung der Bundesrepublik Deutschland betreffen. Dabei handelt es sich nicht um eine allgemeine Zuständigkeit für die polizeiliche Gefahrenabwehr gegen Cyberangriffe, die in der Regel internationale Bezüge aufweisen. Vielmehr geht es um eine Zuständigkeit allein für die Abwehr solcher Cybergefahren, die schwerwiegend sind und nur in Kooperation mit Behörden anderer Staaten abgewehrt werden können, die den Bund selbst betreffen oder die aus anderen Gründen eine besondere Relevanz für die auswärtigen Angelegenheiten oder die Verteidigung haben. Es handelt sich damit um eine punktuelle Aufgabenerweiterung. Die generelle Zuständigkeit für die Gefahrenabwehr im Cyberraum liegt weiterhin bei den Ländern; dazu gehört insbesondere die Cyberabwehr im Zusammenhang mit sicherheitsempfindlichen Stellen von lebenswichtigen Einrichtungen, soweit im Einzelfall keine spezielle Zuständigkeit auf Bundesebene gegeben ist.

Im Einzelnen:

Nach Absatz 1 Nummer 1 nimmt das BKA die Abwehr schwerwiegender Cyberangriffe in Fällen wahr, in denen Gefahrenabwehrmaßnahmen nur gemeinsam mit den zuständigen Stellen anderer Staaten umgesetzt werden können. Hierbei geht es um international durchgeführte polizeiliche Operationen, bei denen die Behörden und Stellen verschiedener Staaten in koordinierter Weise vorgehen, um einen Cyberangriff abzustellen, der z.B. von verschiedenen über Staatengrenzen hinweg verteilten IT-Systemen ausgeführt wird. Ein Beispiel dafür sind sogenannte Bot-Netzwerke, d.h. Netzwerke aus vielen kompromittierten, mit dem Internet verbundenen Geräten, die von Angreifern ferngesteuert werden, um schädliche Aktionen wie Spam-Versand, DDoS-Angriffe oder Datendiebstahl durchzuführen. Das geschieht oft, ohne dass die Gerätebesitzer etwas davon merken, da sie über das Internet mit Schadsoftware infiziert wurden. Aufgrund der dezentralen Struktur lassen sich solche Netzwerke häufig nur durch gleichzeitige Maßnahmen in verschiedenen Staaten unschädlich machen, da ein isoliertes Unterbinden der Angriffe in nur einem Staat durch die IT-Systeme in anderen Staaten kompensiert werden würde.

Absatz 1 Nummer 1 knüpft an die internationale Kooperation bei der Gefahrenabwehr an. International koordinierte Gefahrenabwehrmaßnahmen dürften schon aufgrund des Aufwands der Koordination in der Regel nur schwerwiegende Fälle betreffen, gleichwohl wird diese Voraussetzung auch explizit als Voraussetzung in die Aufgabenzuordnung zur Bundesebene aufgenommen. Die Teilnahme an derartigen internationalen Operationen kann praktisch nur durch eine Bundesbehörde erfolgen. Sie setzt eine etablierte internationale Vernetzung und Erfahrung voraus, dementsprechend ist der Kreis der an solchen komplexen Operationen mitwirkenden Behörden begrenzt und beteiligte Staaten sind in der Regel durch eine nationale Behörde vertreten, die diese Voraussetzungen erfüllt. Dies ist in Deutschland das BKA. Ohne Aufgabenwahrnehmung durch das BKA bestünde in diesen schwerwiegenden Fällen eine Schutzlücke, weil eine Gefahrenabwehr von deutscher Seite nicht erfolgen könnte. Absatz 1 Nummer 1 stellt damit sicher, dass die Bundesrepublik Deutschland in den beschriebenen Konstellationen an der internationalen Abwehr von komplexen Cyberangriffen teilnehmen und sich und die mitwirkenden Partnerstaaten in diesem Rahmen auch schützen kann.

Demgegenüber bleibt die Zuständigkeit für Fälle, die keine schwerwiegende Gefahr mit dem Erfordernis internationaler Kooperation darstellen – vorbehaltlich anderer Zuständigkeitszuweisungen an den Bund – bei den Ländern.

Die Übertragung der Aufgabe zur Gefahrenabwehr nach dieser Vorschrift auf das BKA ähnelt im Übrigen der bisherigen Praxis im Rahmen der bereits bestehenden Aufgabe der Strafverfolgung.

Nach Absatz 1 Nummer 2 ist das BKA künftig für die Abwehr von Cyberangriffen zuständig, die eine Gefahr für die Funktionsfähigkeit der Einrichtungen und Behörden des Bundes darstellen. Die Einschränkung auf die Funktionsfähigkeit folgt der Gesetzgebungskompetenz des Bundes kraft Natur der Sache in eigenen Angelegenheiten und bedeutet, dass nicht jede Cybergefahr für Bundesbehörden oder -einrichtungen die Aufgabe des BKA eröffnet, sondern nur solche, die die jeweilige Behörde oder Einrichtung derart betreffen könnten, dass die Arbeitsfähigkeit bedroht ist. Die Abgrenzung zur allgemeinen Zuständigkeit für die Gefahrenabwehr erfolgt dabei analog zur Abgrenzung der Zuständigkeitsabgrenzungen bei der sonstigen Gefahrenabwehr auf den Grundstücken der Behörden und Einrichtungen des Bundes. Die Regelung bezieht sich nur auf die polizeiliche Gefahrenabwehr. Sonstige Aufgaben im Bereich der IT-Sicherheit der Einrichtungen und Behörden wie der Schutz ihrer eigenen informationstechnischen Systeme sowie die Aufgaben des BSI bleiben von der Regelung unberührt.

Nach Absatz 1 Nummer 3 kann das BKA Gefahrenabwehrmaßnahmen gegen Cyberangriffe auch dann umsetzen, wenn sich die Angriffe ihrer Art nach oder wegen der zur Abwehr erforderlichen Maßnahmen auf die Stellung der Bundesrepublik Deutschland in der Staatengemeinschaft oder die Verteidigung auswirken können. Dabei ist vor allem an Maßnahmen zu denken, die zwar aus Deutschland heraus ausgeführt werden, die aber IT-Systeme im Ausland betreffen, wie z.B. das Verändern und Löschen von Daten auf IT-Systemen der Angreifer. Die dabei zu berücksichtigenden außen- und sicherheitspolitischen Abwägungen können nur durch den Bund erbracht werden, weil nur der Bund über die in der Regel kurzfristig erforderlichen außen- und sicherheitspolitischen Lageeinschätzungen verfügt. Zudem kann auch nur der Bund aus seiner Zuständigkeit für die auswärtigen Angelegenheiten heraus mögliche auswärtige Auswirkungen solcher polizeilicher Gefahrenabwehrmaßnahmen abwägen und darüber entscheiden. Zudem geht es zum Beispiel um polizeiliche Gefahrenabwehrmaßnahmen in Fällen, bei denen ein anderer Staat die Bundesrepublik Deutschland um Unterstützung bittet oder bei denen ein Angriff gegen Ziele in Deutschland von einer fremden Macht ausgeht oder von dieser unterstützt wird. Eine Auswirkung auf die Verteidigung kann zum Beispiel bei einem gewichtigen Angriff auf einen Hersteller von Rüstungsgütern gegeben sein. Für Maßnahmen der polizeilichen Cyberabwehr in diesen Konstellationen wird eine Zuständigkeit des BKA vorgesehen. Die Zuständigkeit für die Verteidigung bleibt davon unberührt bei den Streitkräften.

Absatz 2 bestimmt, dass unter Gefahren durch Angriffe auf die Sicherheit in der Informationstechnik nur Cybergefahren im engeren Sinne, d.h. Angriffe auf IT-Systeme zu verstehen sind. Cybergefahren im weiteren Sinne, d.h. sonstige Gefahren im Cyberraum wie die Verwirklichung von Sexualdelikten, Rauschgifthandel usw., sind keine Gefahren im Sinne dieser Regelung.

Absatz 3 definiert, welche Gefahren schwerwiegende Cybergefahren im Sinne des Absatz 1 Nummer 1 darstellen. Die Regelung bezieht sich nur auf Fälle der internationalen Zusammenarbeit nach Absatz 1 Nummer 1. Dazu gehören solche Cyberbedrohungen, die sich gegen die innere oder äußere Sicherheit der Bundesrepublik Deutschland oder der genannten Behörden oder Einrichtungen richten. Dies können etwa Angriffe auf Einrichtungen der Energie- und Wasserversorgung, des Gesundheitswesens oder der Lebensmittelversorgung sein. Erfasst sind darüber hinaus auch Angriffe, die die Vertraulichkeit und Integrität informationstechnischer Systeme einer großen Anzahl von Personen verletzten. Diese Fallgruppe bezieht sich insbesondere auf Sachverhalte, in denen zahlreiche (oft mehrere Tausend) IT-Systeme mit Schadsoftware infiziert und durch den Schädiger per Fernsteuerung zu einem „Botnetz“ zusammengeschlossen wurden, um für bestimmten Aktionen, wie etwa die weitere Verbreitung von Schadsoftware, missbraucht werden. Zur Eingrenzung der Formulierung „informationstechnischer Systeme einer großen Anzahl von Personen“ dient die Voraussetzung einer gemeinen Gefahr. Dieser bereits im Grundgesetz, im Strafgesetzbuch und in vielen Landespolizeigesetzen verwendete Begriff beschreibt einen Zustand, in dem eine unbestimmte Anzahl von Personen gefährdet ist, ohne dass vorhersehbar ist, wen genau die Gefahr betreffen könnte. Die in Absatz 3 genannten Kriterien orientieren sich an

§ 4 Absatz 1 Nummer 5 und beschreiben die Fälle, in denen die internationale Zusammenarbeit im Gleichlauf mit Aufgaben im Rahmen der Strafverfolgung sachgerecht durch den Bund erfolgen müssen.

Durch die Einschränkungen des Aufgabenbereichs in den Absätzen 1, 2 und 3 wird sichergestellt, dass sich die Aufgaben des BKA nach § 3a einerseits nur auf Cyberangriffe und nicht auf sonstige Straftaten im Cyberraum bezieht und andererseits nur auf Fälle mit besonderem Bundesbezug (einschließlich der Verteidigung) sowie auf besonders herausgehobene Fälle der internationalen Zusammenarbeit beschränkt. Die Zuständigkeit für alle anderen Fälle verbleibt bei den Ländern, die allgemein für die Gefahrenabwehr und damit auch allgemein für die Abwehr von Cyberangriffen und sonstigen Gefahren im Cyberraum zuständig sind.

Absatz 4 Satz 1 stellt klar, dass die Aufgaben und Befugnisse anderer Bundesbehörden, einschließlich der Bundespolizei, sowie der Länder von der neuen Aufgabe des Bundeskriminalamts unberührt bleiben.

Absatz 4 Satz 2 regelt eine Benachrichtigungspflicht des BKA gegenüber den Ländern. Die Benachrichtigung dient der Information der Länder über Cyberabwehrmaßnahmen, die IT-Systeme in ihrem Landesgebiet betreffen, zur Berücksichtigung im Rahmen ihrer eigenen Aufgabenerfüllung.

Zu Nummer 4

Dem Bundeskriminalamt obliegt nach § 4 Absatz 1 Satz 1 Nummer 5 die Aufgabe der Strafverfolgung bei Cyberstraftaten nach den §§ 202a, 202b, 202c, 263a, 303a und 303b StGB in den in § 4 Absatz 1 Satz 1 Nummer 5 Buchstabe a und b genannten Fallkonstellationen.

Bei den relevanten Straftatbeständen wurde auf die Cyberstraftaten des StGB im engeren Sinne abgestellt. In diesem Kontext ist auch § 202d StGB (Datenhehlerei) zu sehen. § 202d StGB wurde in die Aufgabennorm der mit Änderungsgesetz vom 17. Juli 2015 zuletzt geänderten Regelung des § 4 Absatz 1 Satz 1 Nummer 5 nur deshalb nicht aufgenommen, da diese Strafvorschrift zu diesem Zeitpunkt noch nicht existierte. Der Straftatbestand der Datenhehlerei wurde vielmehr erst im Dezember 2015 gesetzlich normiert. Um dem BKA in den gesetzlich genannten Fallkonstellationen eine umfassende Verfolgung aller Straftaten der Cyberkriminalität im engeren Sinne zu ermöglichen, wird nunmehr die erforderliche Ergänzung in § 4 Absatz 1 Satz 1 Nummer 5 vorgenommen.

Zu Nummer 5

Die begriffliche Änderung erfolgt zur sprachlichen Anpassung des BKAG an die Terminologie des § 94 StPO. Hierdurch wird eine einheitliche Begriffsverwendung bei präventiven und repressiven Maßnahmen im Hinblick auf elektronische Daten gewährleistet und Auslegungsschwierigkeiten vermieden.

Der bisherige § 59 ermächtigt bislang lediglich zur Durchsuchung von Sachen. Sachen werden nach zivilrechtlicher Definition im Sinne des § 90 BGB als körperliche Gegenstände definiert. Hierunter lassen sich zwar physische Datenträger subsumieren, auf denen elektronische Daten gespeichert werden, nicht jedoch elektronische Daten als solche. Die begriffliche Änderung stellt klar, dass von der Befugnisnorm neben körperlichen Gegenständen auch nichtkörperliche Gegenstände, insbesondere elektronische Daten, erfasst werden.

Zu Nummer 6

Auch die Änderung des Begriffs „Sache“ in „Gegenstand“ in § 60 BKAG dient der zu Nummer 5 ausgeführten Angleichung des BKAG an die StPO und der Einbeziehung von unverkörperten Daten.

Die Zulässigkeit der Sicherstellung eines Gegenstandes im Rahmen der Aufgabenwahrnehmung des BKA zur Abwehr von Gefahren des internationalen Terrorismus (§ 5 BKAG) sowie im Rahmen der Abwehr von Angriffen auf die Sicherheit in der Informationstechnik nach § 68a BKAG für die Aufgaben nach § 3a, 6, 7 und 8 BKAG richtet sich nach der Befugnisnorm des § 60. Zur Abwehr von Gefahren kann es auch erforderlich sein, einen Gegenstand (einschließlich elektronischer Daten), der sich im Gewahrsam einer dritten Person befindet, in polizeiliche Obhut zu nehmen, um etwa notwendige Erkenntnisse für die Durchführung einer gefahrenabwehrenden Folgemaßnahme zu gewinnen.

Neben elektronischen Daten – etwa aus einem Cloud- oder Mail-Account – können auch weiterhin „analoge“ Gegenstände wie schriftliche Unterlagen, Gepäckstücke, Grundstoffe (die z.B. geeignet sind zur Herstellung einer unkonventionellen Spreng- und Brandvorrichtung), die etwa ein Störer einer dritten Person zur Aufbewahrung übergeben hatte, in Betracht kommen.

Auch im Kontext der Cyberabwehr sind neben elektronischen Daten auch physische Gegenstände im Rahmen der Sicherstellung bei Dritten von Bedeutung, etwa Datenträger oder sonstige Hardware, die vom Eigentümer oder rechtmäßigen Inhaber der tatsächlichen Gewalt (etwa der Störer) bei Dritten vergessen, verliehen, in Schließfächern gelagert oder auf der Arbeitsstelle zurückgelassen oder zur Reparatur gegeben wurden. Die Sicherstellung erfolgt dann durch einen physischen Zugriff.

Absatz 3 stellt klar, dass die Einbeziehung von Daten in die Sicherstellungsbefugnis nicht dazu dienen darf, dass die höheren Anforderungen bestimmter Überwachungsbefugnisse – wie der sog. Online-Durchsuchung nach § 49 BKAG – durch eine Sicherstellung der Daten umgangen werden können. Kommt eine Sicherstellung in ihrer Wirkung der Eingriffstiefe einer Maßnahme nach den §§ 49 bis 51 BKAG gleich, sind daher die dort jeweils geregelten Vorgaben zu beachten. Dazu gehört z.B. ein Richtervorbehalt. Unabhängig davon gilt für jede Sicherstellung der Grundsatz der Verhältnismäßigkeit nach § 16 BPolG, der über die entsprechenden Verweise im BKAG auch für das Bundeskriminalamt gilt.

Zu Nummer 7

Bei Sicherstellung eines Gegenstandes (einschließlich elektronischer Daten) nach § 60 sind über die Verweisung in das BPolG die Formvorschriften nach den §§ 72 bis 74 BPolG zu berücksichtigen, wozu auch die Pflicht gehört, „…den Eigentümer oder den rechtmäßigen Inhaber der tatsächlichen Gewalt“ unverzüglich zu unterrichten (§ 72 Absatz 2 Satz 3 BPolG). Im Einzelfall kann die Gefahr bestehen, dass eine solche unverzügliche Unterrichtung den Zweck der Maßnahme vereitelt, wenn der Betroffene (etwa der Störer) frühzeitig Kenntnis von der Maßnahme erlangt. Aus diesem Grund kann es erforderlich werden, die Unterrichtung des Betroffenen über die erfolgte Sicherstellung zurückzustellen. Im Einzelfall kann es zusätzlich erforderlich sein, ein Offenbarungsverbot auszusprechen, um sicherzustellen, dass der Eigentümer oder rechtmäßige Inhaber nicht von einem Dritten von der Sicherstellung erfährt. Der neue § 60a orientiert sich insoweit an der Regelung in § 95a StPO.

Der Begriff der Zurückstellung der „Benachrichtigung“ ist ebenfalls § 95a StPO entnommen, darf aber nicht verwechselt werden mit der Benachrichtigung nach § 74 BKAG für eingriffsintensive und verdeckte Maßnahmen. § 74 BKAG ist aber insofern relevant, da die Zurückstellung der nach § 74 Absatz 1 Satz 1 BKAG erforderlichen Benachrichtigung grundsätzlich nicht erfolgen muss, wenn die Voraussetzungen des § 74 Absatz 1 Satz 2 bis 4 BKAG erfüllt

sind. Das gilt zum Beispiel für Fälle, in denen der Benachrichtigung überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen oder Nachforschungen zur zu benachrichtigenden Person unverhältnismäßig wären.

Da eine zurückgestellte Benachrichtigung sowie das Offenbarungsverbot einen tiefergehenden Eingriff in die Rechte des Betroffenen darstellen können, erfolgt die Anordnung durch ein Gericht, wenn die Benachrichtigung nicht schon nach den vorgenannten Voraussetzungen des § 74 Absatz 1 Satz 2 bis 4 ausbleiben kann.

Zu Nummer 8

Es handelt sich um Folgeänderungen der sprachlichen Neufassung von Sachen zu Gegenständen entsprechend den Änderungen unter Nummer 6 und 7.

Zu Nummer 9 (Abschnitt 8a - Befugnisse zur Abwehr von Angriffen auf die Sicherheit in der Informationstechnik)

Der neue Abschnitt 8a regelt abweichend von der bisherigen Systematik des BKA-Gesetzes die cyberabwehrspezifischen Befugnisse für alle gefahrenabwehrrechtlichen Aufgaben des BKA, das heißt sowohl für die neu geschaffene Aufgabe nach § 3a als auch für die bestehenden Aufgaben nach den §§ 5 bis 8.

In Wahrnehmung all dieser Aufgaben kann das BKA durch die Neuregelung zur Abwehr von Cyberangriffen zunächst auf die bereits bestehenden polizeilichen Befugnisse im BKAG, wie etwa Observation, Sicherstellung, Durchsuchung oder Telekommunikationsüberwachung zurückgreifen. Um Cybergefahren effektiv und zielgerichtet abwehren zu können, bedarf es als Ergänzung zu diesen Befugnissen der Schaffung cyberspezifischer Eingriffsbefugnisse im BKAG.

Zu § 68a (Befugnisse)

§ 68a enthält in Absatz 1 Nummer 1 zunächst eine polizeiliche Generalklausel für die Cyberabwehr. Auf Grundlage dieser Generalklausel kann das BKA polizeiliche Gefahrenabwehrmaßnahmen gegen Cyberangriffe umsetzen, soweit die jeweilige Maßnahme nicht besonders, d.h. unter weiteren Voraussetzungen, geregelt ist. Zu diesen besonderen Befugnissen gehören durch Verweis in Absatz 1 Nummer 2 auf die §§ 39 Absatz 1 und 3, 40 bis 46, 49 bis 53, 54 und 58 bis 62 zunächst solche besonderen Befugnisse, die bereits im BKAG enthalten sind (im Abschnitt 5 „Befugnisse zur Abwehr von Gefahren des internationalen Terrorismus“) und die auch im Bereich der Cyberabwehrmaßnahmen erforderlich sind. Insbesondere der Sicherstellung von IT-Systemen und Domains der Angreifer dürfte im Rahmen der polizeilichen Cyberabwehr eine wichtige Rolle zukommen. Soweit das BKA über § 68a Absatz 1 Nummer 2 zur Abwehr von Cybergefahren auf die „klassichen“ Eingriffsbefugnisse des 5. Abschnitts zurückgreift, gelten die dort genannten Voraussetzungen entsprechend, das heißt, soweit sie sich nicht sinngemäß nur auf die Abwehr von Gefahren des internationalen Terrorismus beziehen. Das gilt insbesondere für die Regelungen des § 62 BKAG, der auch dann gilt, wenn eine Maßnahme nach dem 5. Abschnitt über den Verweis in § 68a Absatz 1 Nummer 2, ergriffen wird. Danach ist zum Beispiel eine Online-Durchsuchung bei einer zeugnisverweigerungsberechtigten Person unzulässig, wenn diese voraussichtlich Erkenntnisse erbringen würden, über die die Person das Zeugnis verweigern dürfte.

Soweit das BKA nicht im Rahmen der cyberspezifischen Aufgabennorm des § 3a BKAG, sondern im Rahmen bereits bestehender Aufgabennomen, z.B. nach § 5 BKAG (Abwehr von Gefahren des internationalen Terrorismus) tätig wird, ist Voraussetzung für alle Befugnisse, dass eine zweifache Gefahr vorliegt. Es muss dann sowohl eine aufgabenspezifische Gefahr (z.B. eine Gefahr nach § 5 Absatz 1 Satz 2 BKAG) sowie gleichzeitig ein Angriff auf die Sicherheit in der Informationstechnik vorliegen.

Der Schutzauftrag des BKA nach § 6 BKAG erstreckt sich nicht nur auf den physischen Personenschutz von Mitgliedern der Verfassungsorgane, bestimmten ausländischen Gästen der Verfassungsorgane und der Leitung des Bundeskriminalamtes. Cyberangriffe auf Smart-Home-Systeme, wie z.B. Überwachungskameras oder „smarte“ Schließsysteme oder auch private digitale Endgeräte können zu einer unmittelbaren Gefährdung der Schutzpersonen führen. Durch die umfassende Nutzung digitaler Endgeräte sind auf diesen weitreichenden Informationen zu den zu schützenden Personen vorhanden. Eine Veröffentlichung oder Kenntnisnahme durch unbefugte Dritte kann zu einer Beeinflussung der freien Willensbildung und Mandatsführung einer nach § 6 BKAG zu schützenden Person führen.

Das BKA muss daher auch seinem Personenschutzauftrag nach § 6 BKAG im digitalen Raum nachkommen können und auch bei schwerwiegenden Cyberangriffen in der Lage sein, diese abzuwehren.

Das BKA betreibt im Rahmen seiner Aufgabe nach § 2 Absatz 3 BKAG den polizeilichen Informationsverbund zwischen Bund und Ländern. Darüber hinaus werden auch weitere relevante Informations- und Auskunftssysteme im Rahmen der Zentralstellenaufgabe des BKA betrieben. Die Verfügbarkeit des polizeilichen Informationsverbunds und der weiteren Informations- und Auskunftssysteme sind elementar für die tägliche Aufgabenerledigungen bei den Polizeien des Bundes und der Länder. Eine Unterbrechung dieses Betriebes durch Cyberangriffe würde zu massiven Auswirkungen auf die Auskunftsfähigkeit des BKA gegenüber den Polizeien des Bundes und der Länder führen. Darüber hinaus muss auch das BKA selbst weiterhin handlungsfähig bleiben und auch Cyberangriffe auf die eigenen Liegenschaften (z.B. Zutritt- und Kontrollsysteme, Energieinfrastruktur) abwehren können.

Das BKA benötigt daher die Befugnisse für seine Aufgabe nach § 8 BKAG, um schwerwiegende Cyberangriffe abwehren zu können, um einerseits als Behörde selbst handlungsfähig zu bleiben und darüber hinaus auch als Zentralstelle für die deutsche Polizei.

Absatz 2 legt fest, dass eine Gefahr im Sinne dieses Abschnitts eine im Einzelfall bestehende Gefahr im Sinne des § 3a Absatz 2 BKAG ist. Der Gefahrbegriff gilt damit für alle cyberspezifischen Befugnisse nach Abschnitt 8a, unabhängig davon, ob die Aufgabenwahrnehmung nach § 3a BKAG oder einer anderen gefahrenabwehrrechtlichen Aufgabe erfolgt.

Absatz 3 verweist auf die §§ 16 bis 21 des Bundespolizeigesetzes und regelt damit die Geltung des Grundsatzes der Verhältnismäßigkeit sowie weiterer gefahrenabwehrrechtlicher Grundsätze.

Absatz 4 enthält eine Übermittlungspflicht des BKA in Richtung der Bundeswehr für den Fall tatsächlicher Anhaltspunkte, dass die Aufgaben der Verteidigung betroffen sind.

Zu 68b (Untersagung des Betriebs informationstechnischer Systeme)

Nach § 68b darf das BKA zur Abwehr von Angriffen auf die IT-Sicherheit den Betrieb von IT-Systemen untersagen.

In bestimmten Konstellationen kann bereits durch die Untersagung des Betriebes eines informationstechnischen Systems die Cybergefahr abgewehrt werden. Dementsprechend sieht § 68b eine Befugnis zur Untersagung des Betriebs eines informationstechnischen Systems vor, wozu als Unterfall der Untersagung auch die teilweise Untersagung oder Einschränkung des Betriebs gehört.

Die Befugnisnorm dient u.a. dem Zweck des Abschaltens störerseitiger Infrastruktur sowie infizierter Systeme. Dies kann z.B. die Deaktivierung von infizierten Bots oder von (Command & Control-) Servern bedeuten. Eine solche Deaktivierung kann durch Verpflichtung oder Inanspruchnahme der relevanten Diensteanbieter erfolgen. Typische Adressaten sind Anbieter von Telekommunikationsdiensten nach dem Telekommunikationsgesetz sowie

Anbieter digitaler Dienste nach dem Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz.

Würde eine Mitteilung an den Kunden den Erfolg der Gefahrenabwehr gefährden, kann das BKA dem Anbieter nach § 68f untersagen, den Kunden vor Ablauf einer bestimmten Frist über die Maßnahme zu unterrichten.

Zu 68c (Einschränkung, Unterbindung und Umleitung von Datenverkehr)

Zu Absatz 1

Die Regelung gibt dem BKA die Möglichkeit, zur Abwehr von Angriffen auf die IT-Sicherheit Datenverkehr einzuschränken, zu unterbinden und umzuleiten.

Eine Umleitung kann etwa im Zusammenhang mit Maßnahmen zur Bereinigung von mit Malware infizierten Computersystemen (Botnetz) nach Sicherstellung der im Kontext des Steuerungssystems des Botnetzes (Command & Control-Server, C&C-Server) genutzten Domain durch Umleitung des maliziösen Datenverkehrs auf ein polizeilich kontrolliertes System bzw. an ein sog. Sinkhole erfolgen. Dies gilt ebenso für eine Umleitung auf IP-Adressebene. Im Falle einer Umleitung von Datenverkehr auf eine Zieladresse des BKA, darf dieses den umgeleiteten Datenverkehr auch aufzeichnen. Die Weiterverwendung der aufgezeichneten Daten erfolgt nach den allgemeinen Datenverarbeitungsregelungen im BKAG.

Zu Absatz 2

Die Inanspruchnahme von Telekommunikationsdiensteanbietern und Anbietern digitaler Dienste, die den Regelfall der Unterbindung und Umleitung von Datenverkehr darstellen dürfte, ist in Absatz 2 geregelt. Erfolgt ein Cyberangriff unter Nutzung bestimmter Muster (z.B. Paketinhalte, bestimmte Absende/Ziel- Adressen oder IP-Adressbereiche), so kann der dem Angriff zugeordnete Datenverkehr bei den Telekommunikationsdiensteanbietern (z.B. Access-Providern) durch Umleitung eingeschränkt werden, um diesen zu einem späteren Zeitpunkt verwerfen zu können oder zu Analysezwecken an eine abweichende, durch das BKA vorgegebene IP-Adresse, zu transportieren.

Auch im Rahmen von DDoS-Attacken besteht die Möglichkeit des Verhinderns und Verwerfens von Datenverkehr. So kann beispielsweise die Generierung von Angriffsdatenverkehr auf dem jeweiligen Angriffs-Computersystem verhindert werden oder etwa bei der Durchführung einer sog. Reflection-Attacke (Amplification-Attacke) der Datenverkehr an einen bestimmten Server verworfen werden, der die Angriffspakete „ungewollt“ weiterleitet.

Wird Datenverkehr auf eine vom BKA vorgegebene Zieladresse umgeleitet, kann die Datenverarbeitung auch mit dem Ziel erfolgen, den von der Maßnahme nach Absatz 1 Betroffenen zu benachrichtigen sowie die Geschädigten darüber zu informieren, dass sie Opfer einer Straftat wurden. Die Informationsweitergabe dient ferner dem Ziel, die zumeist neben der Schadsoftware zur Übernahme des Opfersystems nachgeladene Schadsoftware zu entfernen.

Bei den zu analysierenden Daten handelt es sich in der Regel um Steuerungsinformationen der Schadprogramme, mit denen die betroffenen informationstechnischen Systeme infiziert sind. Umfasst sind regelmäßig auch IP-Adressen oder andere Internetkennungen der informationstechnischen Systeme, die zu einem Botnetz zusammengeschlossen sind. Je nach Schadprogramm ist es nicht ausgeschlossen, dass auch andere auf den betroffenen Systemen gespeicherte Informationen in den umgeleiteten Daten enthalten sind. Es ist beispielsweise vorstellbar, dass Schadsoftware Zugangsdaten von den infizierten Systemen (Bots) an die C&C-Server leitet.

Nach Satz 3 dürfen nicht nach dem TKG und TDDDG Verpflichtete nur nach den zusätzlichen Voraussetzungen der in § 21 Absatz 1 BPolG geregelten Inanspruchnahme nicht verantwortlicher Personen in Anspruch genommen werden, d.h. wenn eine dringende Gefahr abzuwehren ist, Maßnahmen gegen den Verpflichteten nach TKG oder TDDDG nicht oder nicht rechtzeitig möglich sind oder keinen Erfolg versprechen, das BKA die Gefahr nicht oder nicht rechtzeitig selbst oder durch einen Beauftragten abwehren kann und die Betroffenen ohne erhebliche eigene Gefährdung und ohne Verletzung höherwertiger Pflichten in Anspruch genommen werden können.

In bestimmten Fällen kann eine Selbstvornahme durch das BKA erforderlich sein. Hierunter fallen z.B. Konstellationen, in denen Telekommunikationsdiensteanbieter nach § 170 Absatz 1 und 2 TKG nicht verpflichtet werden können oder eine Umsetzung der Maßnahmen bei einem Telemediendienst erfolgt oder die Selbstvornahme durch das BKA ein milderes Mittel darstellt.

Zu Absatz 3

Im Falle einer Anordnung zur Umleitung von Datenverkehr setzt sich das BKA mit dem BSI ins Benehmen, damit beim BSI ein Gesamtüberblick über Umleitungsmaßnahmen bewahrt werden kann.

Zu Absatz 4

Die Löschung von durch Umleitung erlangter Daten erfolgt – wie in Absatz 4 klargestellt – nach den allgemeinen Regelungen des § 79.

Zu 68d (Auslesen, Löschen und Verändern von Daten in informationstechnischen Systemen)

Die Vorschrift räumt dem BKA die Befugnis ein, in informationstechnischen Systemen näher definierte gefahrgegenständliche Daten auszulesen, zu verändern oder zu löschen, sofern eine Cybergefahr nicht durch mildere Mittel abgewehrt werden kann.

Ermöglicht wird damit z.B. der Eingriff in Störersysteme, von denen im Rahmen eines Cyberangriffs eine Gefahr ausgeht, um dieses unter Ausschluss des Berechtigten (des Störers) zu steuern oder abzuschalten. Der Eingriff erfolgt durch technische Mittel oder der Verwendung rechtmäßig erlangter Passwörter oder Zugangsdaten, und muss zur Abwehr der Gefahr erforderlich sein. Der Eingriff kann ohne Wissen des Betroffenen erfolgen, um ein Umziehen der Infrastruktur sowie frühzeitiges Entgegenwirken des Störers durch andere Maßnahmen zu verhindern. Anders als im Falle klassischer Überwachungsbefugnisse ist es für den Erfolg der Maßnahme aber nicht Voraussetzung, dass diese ohne Wissen des Betroffenen erfolgt. Das Auslesen, Löschen und Verändern kann auch mit Wissen des Betroffenen umgesetzt werden und es ist auch davon auszugehen, dass der Betroffene die Maßnahme zu einem gewissen Zeitpunkt feststellen wird, z.B. weil der geplante Cyberangriff scheitert. Es handelt sich damit nicht um eine klassische verdeckte Maßnahme, wie z.B. eine Telekommunikationsüberwachung, die ihrem Wesen nach nur ohne Wissen der Betroffenen sinnvoll umgesetzt werden kann. Um dies klarzustellen, wird der Begriff „auch“ verwendet.

Die Übernahme bzw. Steuerung des C&C-Servers einer Botnetz-Infrastruktur kann beispielsweise der Vorbereitung zum Senden des in der Schadsoftware bereits enthaltenen Deinstallationsbefehls (sog. Kill-Switch) oder zum Senden eines Updates mit geänderten Kommunikationsparametern an die infizierten Bots dienen. Diese kommunizieren anschließend mit einer vom BKA vorgegebenen Anschlusskennung (sog. Sinkhole). Daneben können Veränderungen an einem Störersystem vorgenommen werden, die dazu dienen, einen Angriff direkt abzuwehren, indem z.B. direkte Veränderungen am System in störerseitigen Skripten den Angriff aufhalten oder umlenken.

Erfolgt ein DDoS-Angriff über Server in Deutschland, bei dem der zuständige Anbieter nicht zur Abschaltung des entsprechenden Servers verpflichtet werden kann, ist das BKA befugt, unter Zuhilfenahme von aus einer anderen polizeilichen Maßnahme rechtmäßig erlangten Zugangsdaten auf den Server zugreifen. Dabei können Datenveränderungen des informationstechnischen Systems erforderlich sein, um den Angriff abzuwehren.

Die neue Befugnis gestattet im Einzelfall auch begrenzte Eingriffe in informationstechnische Systeme von Geschädigten („Opfersysteme“), von denen im Rahmen eines Cyberangriffs eine Gefahr ausgeht. Zum Zweck der Bereinigung dürfen Konfigurationsdaten der Schadsoftware verändert und gelöscht werden.

Soweit die Schadsoftware (Bsp. Emotet) über einen bereits integrierten Deinstallationsbefehl verfügt, kann dieser an die Opfersysteme gesendet werden, um die Schadsoftware von den kontaktierenden infizierten Endgeräten (Bots) zu entfernen bzw. zu deaktivieren.

Verfügt die Schadsoftware nicht über einen integrierten Deinstallationsbefehl, kann den Geschädigtensystemen beispielsweise über den polizeilich übernommenen Command&Control-Server ein „Update“ mit veränderten Kommunikationsparametern geschickt werden, sodass Systeme nicht mehr zur Infrastruktur des Störers, sondern zu der vom BKA vorgegebenen Zieladresse kommunizieren. Zu der vom BKA vorgegebenen Zieladresse sollen durch eine solche Maßnahme lediglich solche Daten der betroffenen infizierten Systeme ausgeleitet werden, die für deren Identifizierung und Bereinigung zwingend erforderlich sind.

Das Senden von Deinstallations- oder Updatebefehlen kann Datenveränderungen auf Geschädigtensystemen verursachen, welche jedoch, soweit möglich auf die Konfigurationsdaten der Schadsoftware beschränkt werden sollen und die ausschließlich dem Zweck der Bereinigung dienen.

Die in den Beispielen erhobenen Daten, wie öffentliche IP-Adressen bzw. Computernamen sollen anderen Behörden (konkret dem BSI) zur Verfügung gestellt werden. Das BSI soll die Informationen auf geeignete Weise den zuständigen (Access-/Hosting-)Providern zur Verfügung stellen, um eine Benachrichtigung der Betroffenen zu ermöglichen.

Als weitere Ausprägung des Verhältnismäßigkeitsgrundsatzes schreibt die Regelung Maßnahmen zur Mitigation der Eingriffsintensität vor. So sind nur solche Veränderungen vorzunehmen, die unerlässlich zur Löschung und Veränderung der Daten sind; zudem sind diese rückgängig zu machen, soweit dies technisch möglich ist und das Rückgängigmachen dem Zweck der Maßnahme nicht widerspräche.

So wäre das Rückgängigmachen einer Maßnahme zur Unbrauchbarmachung störerseitig betriebener Infrastruktur eben nicht zweckmäßig, da die Gefahr damit wieder „hergestellt“ würde, indem Störer ihre Infrastruktur wieder übernehmen und die Angriffe fortsetzen. Gleiches gilt bei der Bereinigung von infizierten Computersystemen.

Insbesondere ist eine auf dem IT-System installierte Software vollständig zu löschen und sind Veränderungen an den bei der Installation der Software vorgefundenen Systemdateien rückgängig zu machen. Die Rückgängigmachung der vorgenommenen Veränderungen hat im Interesse einer möglichst zuverlässigen und einfachen Abwicklung grundsätzlich automatisiert zu geschehen. Soweit eine automatisierte Rückgängigmachung technisch unmöglich ist, sind die vorgenommenen Veränderungen manuell rückgängig zu machen.

Zudem ist das eingesetzte Mittel nach dem Stand der Technik gegen unbefugte Nutzung zu schützen. Erhobene Daten sind nach dem Stand der Technik gegen Veränderung, unbefugte Löschung und unbefugte Kenntnisnahme zu schützen. Insbesondere hat das BKA dafür Sorge zu tragen, dass die eingesetzte Software nicht durch Dritte zweckentfremdet werden kann. Speziell ist sicherzustellen, dass die Software nicht ohne erheblichen Auf-

wand dazu veranlasst werden kann, an einen anderen Server als den vom BKA verwendeten zurückzumelden, und dass die Software weder von Unbefugten erkannt noch angesprochen werden kann. Dies soll gewährleisten, dass die Eingriffe in die Integrität des IT-Systems und die Vertraulichkeit der in ihm gespeicherten Daten nicht über das hinausgehen, was nötig ist, um dem BKA die Maßnahme zu ermöglichen. Die Verpflichtung, das eingesetzte Mittel „nach dem Stand von Wissenschaft und Technik“ gegen unbefugte Nutzung zu schützen, bedeutet, dass sich das BKA der fortschrittlichsten technischen Verfahren bedienen muss, die nach Auffassung führender Fachleute aus Wissenschaft und Technik auf der Grundlage neuester wissenschaftlicher Erkenntnisse erforderlich sind. Hierfür muss es die einschlägigen Aktivitäten auf den Gebieten der Wissenschaft und Technik umfassend und sorgfältig beobachten und auswerten.

Zu 68e (Besondere Bestimmungen für Eingriffe in private informationstechnische Systeme)

Für die Befugnis zum Auslesen von Daten nach § 68d gilt wie für alle neuen cyberspezifischen Maßnahmen zur Abwehr von Angriffen auf die Sicherheit in der Informationstechnik, dass diese keine Überwachungsmaßnahmen sind. Ziel ist nicht die Erhebung personenbezogener (Inhalts-) Daten, sondern allein die Abwehr von Angriffen auf die Sicherheit in der Informationstechnik. Das Auslesen oder Löschen von Daten wird nur insofern relevant, als sie zur Abwehr eines Angriffs erforderlich sind, etwa weil ein privates System als Opfersystem infiltriert wurde oder personenbezogene Daten von Tätern entwendet worden sind. Aufgrund dessen und der grundsätzlich anderen Zielrichtung der Cyber-Abwehrmaßnahmen im Gegensatz zu staatlichen Überwachungsmaßnahmen sind auch die Voraussetzungen zur Durchführung der Abwehrmaßnahmen andere als bei staatlichen Überwachungsmaßnahmen. Grundsätzlich sind für die besonderen Abwehrmaßnahmen daher weder qualifizierte Schutzgüter noch ein Richtervorbehalt erforderlich. Nur wenn in private informationstechnische Systeme eingegriffen wird und der Eingriff eine Kenntnisnahme dort gespeicherter Daten ermöglicht, legt § 68e qualifizierte Anforderungen für Maßnahmen fest, um dem IT-Grundrecht der Betroffenen Rechnung zu tragen.

Diese finden ferner nur Anwendung, wenn die besondere Abwehrmaßnahme nicht mit Einwilligung des Betroffenen geschieht. Eine Einwilligung wird in der Regel erteilt, wenn Systeme kompromittiert wurden und der Nutzer oder Inhaber des Systems insofern selbst Opfer eines Angriffs auf die Sicherheit in der Informationstechnik geworden sind. Hier liegt es im Interesse des Opfers, dass der Zugriff auf sein System abgewehrt und ein Datenabfluss oder eine Datenmanipulation verhindert wird. Hier zeigt sich auch der systematische Unterschied zu Überwachungsmaßnahmen wie einer Telekommunikationsüberwachung. Für diese ist eine Einwilligung nicht geregelt, da eine Einwilligung dem Zweck der Maßnahme zuwiderlaufen würde.

Die Vorschrift legt zudem fest, dass durch besondere Abwehrmaßnahmen Eingriffe in private informationstechnische Systeme nur zum Schutz des Bestandes oder der Sicherheit des Bundes oder eines Landes (Nummer 1), zum Schutz von Behörden oder Einrichtungen, deren Funktionieren für das Gemeinwesen von wesentlicher Bedeutung ist (Nummer 2), zum Schutz der Vertraulichkeit und Integrität informationstechnischer Systeme einer großen Anzahl von Personen (Nummer 3) und zum Schutz von Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse liegt (Nummer 4), eingegriffen werden darf. Die qualifizierten Schutzgüter stehen in Einklang mit der Rechtsprechung des Bundesverfassungsgerichts zu den Voraussetzungen für Eingriffe in privat genutzte IT-Systeme (IT-Systeme-Grundrecht), die aufgrund ihrer technischen Funktionalität allein oder durch ihre technische Vernetzung Daten einer betroffenen Person in einem Umfang und einer Vielfalt vorhalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten (BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 2466/19 (Trojaner I), Leitsatz 2a), Rn. 97; BVerfG, Beschluss vom 24. Juni 2025 – 1 BvR 180/23 (Trojaner II), Rn. 173). Das Schutzgut einer

Sache von bedeutendem Wert, deren Erhalt für das Funktionieren von wesentlicher Bedeutung ist (Nummer 4) ist gegenüber dem Schutzgut einer Behörde oder Einrichtung, deren Funktionieren für das Gemeinwesen von wesentlicher Bedeutung ist (Nummer 2) ein Auffangtatbestand. Er kommt insbesondere in Betracht, wenn keine Sachgesamtheit, sondern eine einzelne Sache zu schützen ist.

Absatz 2 enthält eine Legaldefinition zum Begriff des privaten informationstechnischen Systems. Ein privates informationstechnisches System liegt insbesondere dann nicht vor, wenn das System nur zur Durchführung von Angriffen auf die Sicherheit in der Informationstechnik betrieben wird. Werden Systeme sowohl für Angriffe auf die Sicherheit in der Informationstechnik als auch privat genutzt, kommt es auf eine Bewertung des Einzelfalls an. Unbedeutende private Mitnutzungen von Systemen, die vorrangig zur Durchführung von Angriffen auf die Sicherheit in der Informationstechnik genutzt werden, führen nicht zur Einordnung eines Systems als privates. Unbedeutende private Mitnutzungen sind Nutzungen, die aufgrund des geringen Umfangs oder der geringen Vielfalt der Daten keinen Einblick in wesentliche Teile der Lebensgestaltung der Person und kein aussagekräftiges Bild der Persönlichkeit ermöglichen. Häufig werden Angriffe auf die Sicherheit in der Informationstechnik über informationstechnische Systeme ausgeführt, die allein zur Durchführung derartiger Angriffe betrieben werden. Derartige Systeme sind keine privat genutzten Systeme, über die im Falle eines Zugriffs Persönlichkeitsprofile natürlicher Personen erstellt werden können und ein Einblick in deren private Lebensgestaltung gewonnen werden kann. Relevant bei der Bewertung, ob ein privates informationstechnisches System vorliegt, ist ferner, dass die private Nutzung nicht lediglich zum Zweck durchgeführt werden darf, dass erhöhte Anforderungen an die Ergreifung besonderer Abwehrmaßnahmen gestellt werden.

Zudem ergehen gerichtliche Anordnungen über Maßnahmen auf Antrag der zuständigen Abteilungsleitung des BKA oder ihrer oder seiner Vertretung. Bei Gefahr im Verzug kann die Anordnung durch ebendiese selbst getroffen werden, wobei eine gerichtliche Entscheidung binnen drei Tagen nachzuholen ist.

Absatz 5 legt die Inhalte des Antrags fest. Demnach muss dieser die Kennung des Anschlusses oder des Endgerätes des informationstechnischen Systems, in das eingegriffen werden soll, sowie Art, Umfang und Dauer der Maßnahme, den Sachverhalt und eine entsprechende Begründung beinhalten.

Absatz 6 bestimmt, welchen Inhalt die gerichtliche Anordnung einer Maßnahme hat.

Absatz 7 regelt den Schutz des Kernbereichs privater Lebensgestaltung durch Verweis auf § 51 Absatz 7 und 8.

Zu § 68fg: Offenbarungsverbot

Für Maßnahmen nach den §§ 68b bis 62d BKAG kann das Bundeskriminalamt nach § 68f Betreiber informationstechnischer Systeme oder zur Unterbindung oder Umleitung von Datenverkehr Verpflichtete mit einem Offenbarungsverbot belegen. Die entsprechende Anordnung soll unter Würdigung aller Umstände und Abwägungen der Interessen jeweils einer Einzelfallprüfung unterzogen werden. Adressat in den Fällen der Untersagung des Betriebs von IT-Systemen sowie beim Auslesen, Löschen und Verändern von Daten ist jeweils der Betreiber des von der Maßnahme betroffenen IT-Systems.

Zu den zu würdigenden Umständen gehört insbesondere die Gefahr, dass eine Offenbarung dem Untersuchungszweck – der Abwehr von Cybergefahren nach § 68a Absatz 2 BKAG – zuwiderläuft, weil die Störer ihre Angriffstaktik auf die Umleitung anpassen und auf andere Wege für die Fortsetzung der Angriffe ausweichen. Es wird daher die Möglichkeit geschaffen, die Bekanntgabe an den Betroffenen (etwa den Störer) zurückzustellen, wenn diese Zwecke der Gefahrenabwehr oder Strafverfolgung vereiteln würde. Hierbei steht das öffentliche Interesse an der erfolgreichen Abwehr der Gefahr und damit Vermeidung eines

Schadenseintritts für bedeutende Rechtsgüter oder zumindest dessen Beendigung sowie einer wirksamen Strafverfolgung durch Zurückstellen der Offenbarung dem individuellen Informations- und Rechtsschutzinteresse des von der Maßnahme Betroffenen gegenüber und ist stets im Einzelfall abzuwägen.

Die Zurückstellung kommt ausschließlich dann in Betracht, wenn die sofortige Bekanntgabe der Gefahrenabwehrmaßnahme nach §§ 68b bis 68d BKAG gegenüber dem Störer den Zweck der Maßnahme gefährden würde. Damit wird zum einem dem Verhältnismäßigkeitsgrundsatz Rechnung getragen; denn nur dann ist das Offenbarungsverbot und die damit einhergehende Einschränkung der Rechtsschutzmöglichkeiten erforderlich und angemessen.

Zur Beurteilung der Zweckgefährdung, kann auf die geltenden Grundsätze zu § 74 BKAG, der die Zurückstellung der Benachrichtigung bei den verdeckt ausgestalteten Gefahrenabwehrmaßnahmen regelt, zurückgegriffen werden. Danach ist eine Gefährdung des Zwecks der Maßnahme so lange gegeben, wie die begründete Erwartung besteht, dass durch die verdeckte Gefahrenabwehrmaßnahmen weitere gefahrenabwehrrelevante Erkenntnisse gewonnen werden können, deren Erlangung in Frage steht, wenn der Störer Kenntnis von den gegen ihn gerichteten Gefahrenabwehrmaßnahmen erlangt, wenn also die Abwehr der Gefahr mittels aller zulässigen Gefahrenabwehrhandlungen durch die sofortige Offenlegung gefährdet ist. Es ist darauf abzustellen, ob die Abwehr der Gefahr, durch die sofortige Offenlegung gefährdet ist.

Die Offenbarung gegenüber dem Störer kann die Gefahr der Aufdeckung oder der Vereitelung des Gefahrenabwehrerfolgs und damit der Rechtsgüterschutz bewirken, wenn etwa zeitgleich durchgeführte verdeckte Gefahrenabwehrmaßnahmen ihren Sinn verlieren, wenn der Störer von der gegen ihn gerichteten Gefahrenabwehrmaßnahme in Kenntnis gesetzt wird und daher mit weiteren gegen ihn gerichteten Gefahrenabwehrmaßnahmen rechnet und seine gefahrenverursachenden Aktivitäten so ändert, dass die Gefahr nicht abgewehrt werden kann. Relevant wird dies, wenn die Gefahrenabwehrmaßnahme zwar bei einer unverdächtigen dritten Person erfolgt, hierdurch aber auch die Rechte des Störers betroffen sind, weil es sich um ihn betreffende Informationen oder Daten handelt.

Zu Nummer 10 (§ 69 BKAG)

Die Ergänzung bezieht die neuen Cyberabwehrbefugnisse in den Aufgabenbereich der oder des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit nach § 69 BKAG ein.

Zu Nummer 11 (§ 74 BKAG)

Soweit ein Eingriff in ein privates informationstechnisches System erfolgt und daraus bei der Maßnahme Daten erhoben werden, stellt sich die Maßnahme als eingriffsintensiv dar. Aus diesem Grund werden die entsprechenden Maßnahmen in dieser Konstellation der Benachrichtigungspflicht nach § 74 BKAG unterworfen. Zu benachrichtigen sind der Inhaber des von der jeweiligen Maßnahme betroffenen privaten informationstechnischen Systems.

Zu Nummer 12 (§ 79 BKAG)

Die Änderung ergänzt die neuen Befugnisse des Abschnitts 8a in der bereits bestehenden Regelung zu Löschpflichten in § 79 BKAG.

Zu Nummer 13 (§ 82 BKAG)

Das oben zu Nummer 11 Gesagte gilt auch für die Protokollierung. Zu protokollieren sind bei Maßnahmen nach § 68d die Angaben zur Identifizierung des privaten informationstechnischen Systems, beispielsweise eine eindeutige Kennung, zu protokollieren.

Zu Nummer 14

Mit den Änderungen wird die bestehenden Bußgeldregelung zu den neuen § 60a Absatz 2, § 68b, § 68c Absatz 2 Satz 1 und § 68f Absatz 1 ergänzt. Zur Abwehr von Gefahren für die Sicherheit in der Informationstechnik kann das Bundeskriminalamt Dritte zur Mitwirkung verpflichten (in den Fällen des § 68c Absatz 2 Satz 1 sowie des § 68b). Um die vorgesehenen Gefahrenabwehrbefugnisse auch durchsetzen zu können, ist eine Bußgeldbewehrung erforderlich, damit die rechtswidrige Nichtmitwirkung sanktioniert werden kann. Ferner wird der Verstoß gegen ein § 60a Absatz 2 oder § 68f Absatz 1 angeordnetes Offenbarungsverbot bußgeldbewehrt, um dessen Befolgung zu sichern.

Im Einzelnen wird bußgeldbewehrt:

Wird dem Betreiber eines IT-Systems, von dem eine Gefahr ausgeht, z.B. weil ein Kunde des Betreibers diesen zur Durchführung von Cyberangriffen verwendet, der Betrieb des Systems untersagt (§ 68b), hat der Betreiber dem Folge zu leisten. Ein Verstoß, d.h. der unveränderte Weiterbetrieb, obwohl das Abschalten faktisch und rechtlich möglich wäre, stellt eine Gefahr für die durch den Angriff bedrohten Rechtsgüter da und ist daher als Ordnungswidrigkeit zu ahnden.

Auch der Verstoß gegen eine Anordnung zum Umleiten von Datenverkehr (§ 68c Absatz 2 Satz 1) bedeutet, dass die Gefahr für die bedrohten Rechtsgüter nicht abgestellt wird, obwohl dies dem Adressaten der Anordnung möglich wäre. Adressaten dieser Anordnung können Anbieter von TK-Diensten sowie Anbieter digitaler Dienste sein. Bei diesen handelt es sich im ersten Fall nie um natürliche Personen, im zweiten Fall in der Regel nicht um natürliche Personen. Die maximale Bußgeldhöhe orientiert sich daher daran, dass diese auch für die in diesem Bereich vertretenen sehr großen wirtschaftsstarken Unternehmen durch das Bußgeld von einer Nichtbeachtung von Anordnungen abgehalten werden.

Im Fall des Offenbarungsverbots (§§ 60a Absatz 2, 68f Absatz 1) wird bußgeldbewehrt, wenn ein Adressat des Offenbarungsverbot entgegen dem Verbot den oder die von der Maßnahmen Betroffenen über die Maßnahme unterrichtet. Ein Verstoß liegt beispielsweise vor, wenn das Bundeskriminalamt einem Hostingdiensteanbieter untersagt, einen bestimmten Server weiterzubetreiben, den ein Dritter für Cyberangriffe verwendet, das Bundeskriminalamt dafür ein Offenbarungsverbot ausspricht und der Anbieter den Kunden, d.h. den Angreifer darüber informiert. Die Information kann dann dazu führen, dass der Angreifer Zeit gewinnt, seine Taktik zu ändern und auf anderen Server auszuweichen, was sonst nicht oder erst später möglich gewesen wäre. Da in Bezug auf das Offenbarungsverbot auch Fälle denkbar sind, in denen natürliche Personen den bußgeldbewehrten Verstoß verantworten, orientiert sich die Bußgeldhöhe an natürlichen Personen.

Zu Artikel 4 (Änderungen des Telekommunikation-Digitale-Dienste-Datenschutz-Gesetzes)

Mit den neu eingeführten Absätzen 5 und 6 werden Anbieter digitaler Dienste dazu verpflichtet, ihre Nutzer über Störungen (Absatz 5) bzw. konkrete Gefahren (Absatz 6) zu informieren, die von einem ihrer Dienste ausgehen, und Informationen des BSI über konkrete Gefahren, die Kunden der Anbieter betreffen, an ihre Nutzer weiterzugeben, soweit diese bekannt sind und eine Benachrichtigung möglich ist. Die Verpflichtung dient dem Zweck, Schäden durch verwundbare oder bereits kompromittierte Dienste zu vermeiden. Solche Schäden können sowohl beim Nutzer selbst als auch bei anderen Internet-Teilnehmern

entstehen, wenn sie über die betroffenen Dienste angegriffen werden (z. B. Schadprogramme, Phishing oder DDoS-Angriffe).

Die Regelungen entsprechen den bisher nur für Anbieter von Telekommunikationsdiensten nach § 169 Absatz 5 und 6 TKG geltenden Vorgaben. Mit der entsprechenden Verpflichtung von Anbietern digitaler Dienste sollen Lücken bei der Begegnung entsprechender Gefahren geschlossen werden, die dadurch entstehen, dass regelmäßig auch Systeme betroffen sind, deren Betreiber als Anbieter digitaler Dienste nicht unter das TKG fallen, zu denen das BSI aber täglich bereits viele Erkenntnisse zu verwundbaren oder verwundeten Systemen verarbeitet (wie insbesondere Hosting-Provider, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Content Delivery Networks, Managed Service Provider, Managed Security Service Provider). Diese Erkenntnisse werden aktuell zwar an Anbieter digitaler Dienste weitergeleitet, von diesen mangels gesetzlicher Verpflichtung aber häufig nicht an die betroffenen Nutzer weitergegeben. Damit kann der bestehenden Gefahr regelmäßig nicht effektiv begegnet werden.

Erfasst von den Absätzen 5 und 6 sind nur solche Störungen oder Gefahren, die im Rahmen der Inanspruchnahme eines Dienstes durch einen Nutzer ausgehen. Gemeint sind Fälle, in denen ein Nutzer z.B. einen Hosting-Dienst für den Betrieb einer Website oder zum Betrieb eines E-Mail-Services in Anspruch nimmt und die von ihm verantwortete Website oder der E-Mail-Service kompromittiert und zur Verbreitung von Schadprogrammen oder Phishing-Mails missbraucht werden. Mögliche Beispiele für relevante Störungen sind ein kompromittiertes E-Mail-Konto, über das Spam-Mails versendet werden; ein kompromittierter Server, der für DDoS-Angriffe missbraucht wird oder eine kompromittierte Website, über die Schadprogramme verbreitet werden.

Zu Artikel 5 (Änderung des Energiewirtschaftsgesetzes)

Zu Nummer 1

Die Anpassung im Energiewirtschaftsgesetz soll die in Artikel 2 Nummer 8 vorgesehene automatisierte Ausleitung von Daten an das BSI auf Betreiber kritischer Infrastrukturen im Energie gemäß § 5c Absatz 1 EnWG ausweiten. Für die Ziele der Datenausleitung und die Erläuterung der Indikatoren und Informationen wird grundsätzlich auf die Ausführungen in der Begründung zu Artikel 2 Nummer 8 verwiesen. Da sich eine für die Energieversorgung relevante Einschränkung von Verfügbarkeiten regelmäßig vor allem in Bezug auf übergreifende Funktionalitäten zeigt, zielt die für § 5c Absatz 7 Satz 1 Nummer 1 EnWG vorgeschlagene Regelung zu den Verfügbarkeitsindikatoren vor allem auf kritische Funktionen ab, die unter den Anwendungsbereich des Information Security Management System (ISMS) bzw. Business Continuity Management (BCM) fallen und als Business Prozess z.B. im zentralen Leitsystem abbildbar sind.

Zur Gewährleistung einer unveränderten Absicherung der kritischen Anlagen und uneingeschränkten Hoheit der Unternehmen über ihre Systeme soll die Übermittlung der Daten automatisiert mittels einer gesicherten, unidirektionalen Verbindung rückwirkungsfrei hin zum BSI erfolgen.

Insgesamt sollen sowohl der Umfang der zu übermittelnden Daten als auch der Aufwand für ihre Übermittlung in einem angemessenen Verhältnis zum Nutzen für die tatsächliche Erhöhung der Sicherheit für den Betrieb kritischer Anlagen im Sektor Energie durch die Verwertung dieser Informationen stehen.

Entsprechend der Vorgaben für die Erstellung der IT-Sicherheitskataloge für den Energiesektor, soll eine Konkretisierung der Anforderungen im Rahmen einer Festlegung durch die Bundesnetzagentur im Einvernehmen mit dem BSI erfolgen. Über eine Beteiligung der Branche soll die Praxistauglichkeit der Festlegung sichergestellt werden.

Sofern sich im Rahmen des Festlegungsprozesses, insbesondere aufgrund der Konsultation der Branche zeigt, dass eine Implementierung bei den Betreibern einen längeren zeitlichen Vorlauf benötigt, kann im Rahmen der Festlegung auch eine längere Frist für die Umsetzung vorgesehen werden.

Mit dem neuen Absatz 11 wird dem Zitiergebot des Artikels 19 Absatz 1 Satz 2 des Grundgesetzes nachgekommen.

Zu Nummer 2

Bei der Änderung handelt es sich um eine redaktionelle Korrektur.

Zu Nummer 3

Der Verstoß gegen die Übermittlungspflicht nach Nummer 1 ist bußgeldbewehrt. Da die Übermittlung von Daten vor allem dazu dient, ein aktuelleres Lagebild als Grundlage für eine gesamtsystemisch verbesserte Abwehr von Cyberangriffen zu schaffen, ist der Bußgeldrahmen hier niedriger anzusetzen, als bei den sonstigen Pflichten für Kritis-Betreiber nach dem EnWG, die im Einzelfall der Erhöhung der Sicherheitsniveaus dienen.

Zu Artikel 6 (Einschränkung eines Grundrechts)

Mit der Vorschrift wird dem Zitiergebot des Artikels 19 Absatz 1 Satz 2 des Grundgesetzes nachgekommen.

Zu Artikel 7 (Inkrafttreten)

Artikel 7 regelt das Inkrafttreten des Gesetzes.

Aktualisierte Stellungnahme des Nationalen Normenkontrollrates (NKR) gem. § 6 Abs. 1 NKRG

Entwurf eines Gesetzes zur Stärkung der Cybersicherheit (NKR-Nr. 8007, BMI)

Der Nationale Normenkontrollrat hat den Regelungsentwurf vom 20. Mai 2026 mit folgendem Ergebnis geprüft:

I Zusammenfassung

Bürgerinnen und Bürger	keine Auswirkungen
Wirtschaft	
Jährlicher Erfüllungsaufwand:	rund 10 Mio. Euro
davon aus Bürokratiekosten:	*rund 282 000Euro*
Einmaliger Erfüllungsaufwand:	rund 4,4 Mio. Euro
Verwaltung	
Bund	
Jährlicher Erfüllungsaufwand:	rund 35 Mio. Euro
Einmaliger Erfüllungsaufwand:	rund 19,6 Mio. Euro
Länder	keine Auswirkungen

„One in, one out"-Regel	Im Sinne der erweiterten „One in, one out"-Regel der Bundesregierung stellt der **jährliche** Erfüllungsaufwand in diesem Regelungsvorhaben ein **„In"** von **45 Mio. Euro** dar. Der **einmalige** Erfüllungsaufwand stellt ein weiteres **„In"** von rund **2,4 Mio.** Euro dar (Berücksichtigung von 10 % des gesamten einmaligen Erfüllungsaufwands). Der Erfüllungsaufwand in diesem Regelungsvorhaben stellt im Sinne der „One in, one out"-Regel der Bundesregierung **kein „In"** dar, da er allein aus der Abwehr erheblicher Gefahren resultiert.
Weitere Kosten	keine Auswirkungen
Evaluierung	Das Vorhaben ist evaluierungspflichtig. Das Ressort hat in Abwägung folgender Gründe auf eine Evaluierung verzichtet: • Die neuen Regelungen knüpfen an den bestehenden Rechtsstrukturen an. • Die Auswirkungen des Gesetzes sind im Wesentlichen prognostizierbar und im Rahmen der Gesetzesfolgenabschätzung/Erfüllungsaufwand berücksichtigt worden. • Im Übrigen unterliegen die Anwendung der Befugnisse sowie deren Auswirkung bereits einer kontinuierlichen Kontrolle, insbesondere durch die parlamentarische Kontrolle, die Fach- und Rechtsaufsicht sowie die bestehenden Berichtspflichten und gerichtlichen Rechtsschutzmöglichkeiten. ...
Nutzen des Vorhabens	Verbesserung der Verlässlichkeit und Resilienz digitaler Prozesse innerhalb der Sicherheitsbehörden.
Digitaltauglichkeit (Digitalcheck)	Das Ressort hat Möglichkeiten zum digitalen Vollzug der Neuregelung (Digitaltauglichkeit) geprüft und hierzu einen Digitalcheck mit nachvollziehbarem Ergebnis durchgeführt.

Regelungsfolgen

Die Darstellung der Regelungsfolgen ist nachvollziehbar und methodengerecht. Der Nationale Normenkontrollrat erhebt hiergegen im Rahmen seines gesetzlichen Auftrags keine Einwände.

Darüber hinaus bemerkt der NKR, dass das Vorhaben evaluierungspflichtig ist. Die seitens des Ressorts genannten Gründe für einen Verzicht greifen hier ebenso wenig wie bei den Regelungsvorhaben zur Stärkung digitaler Ermittlungsbefugnisse (NKR-Nrn. 7733 und 7734). Berichtspflichten, die der parlamentarischen, fachlichen und rechtlichen Kontrolle dienen, ersetzen nicht die Pflicht zur Evaluierung gemäß Beschlusslage der Bundesregierung.

II Regelungsvorhaben

Das Regelungsvorhaben dient dem Ausbau der Erkennung und Abwehr von Cyberangriffen und schafft die hierfür erforderlichen Rechtsgrundlagen im Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen (BSIG). Gleichzeitig erhalten die Polizeien des Bundes im Bundeskriminalamtsgesetz (BKAG) und im Gesetz über die Bundespolizei (BPolG) die notwendigen Befugnisse, um eine zukunftsfähige Cyberabwehr aufzubauen.

III Bewertung

Das Regelungsvorhaben verursacht jährlichen Erfüllungsaufwand und Bürokratiekosten für die Wirtschaft. Die Verwaltung wird durch einmaligen und jährlichen Erfüllungsaufwand belastet.

III.1 Erfüllungsaufwand

Bürgerinnen und Bürger

Für die Bürgerinnen und Bürger entsteht kein Erfüllungsaufwand.

Wirtschaft

Der jährliche Erfüllungsaufwand für die Wirtschaft entsteht in Höhe von rund 10 Mio. Euro. Davon sind 282 000 Euro Informationspflichten. Einmaliger Erfüllungsaufwand für die Wirtschaft entsteht in Höhe von rund 4,4 Mio. Euro.

- Anbindung von Systemen zur Angriffserkennung bei Betreibern kritischer Anlagen an das BSI

Die größte Belastung verursacht die Pflicht von Betreibern kritischer Anlagen, Systeme zur Angriffserkennung einzusetzen und an das BSI anzubinden. Das Ressort schätzt, dass pro Jahr ca. 2 100 Fälle von Anbindungen notwendig sind. Unter Berücksichtigung des durchschnittlichen Lohnsatzes für den Wirtschaftszweig von 52,80 Euro und einem Zeitaufwand von 40 Stunden pro Fall ergibt sich ein **laufender Erfüllungsaufwand** in Höhe von rund **4,4 Mio**. Euro. Gleichzeitig verursacht die Vorgabe nach Angaben des Ressorts **einmaligen Erfüllungsaufwand** unter der Annahme derselben Parameter und in gleicher Höhe von **rund 4,4 Mio.** Euro.

- Mitwirkung an Abwehrmaßnahmen gegen Angriffe auf die IT-Sicherheit

Das BKA wird ermächtigt, zur Abwehr von Angriffen auf die IT-Sicherheit den Datenverkehr an eine vorgegebene Zieladresse umzuleiten. Die betroffenen Unternehmen unterliegen dabei einer Mitwirkungspflicht. Unter der Annahme, dass ca. 600 Unternehmen pro Jahr betroffen sind und unter Berücksichtigung des durchschnittlichen Lohnsatzes für den Wirtschaftszweig von

52,80 Euro und einem Zeitaufwand von 100 Stunden pro Fall ergibt sich der zweitgrößte Kostentreiber mit laufendem Erfüllungsaufwand in Höhe von rund **3,2 Mio**. Euro.

Die übrigen Vorgaben für die Wirtschaft verursachen geringfügigeren Erfüllungsaufwand und werden der besseren Übersicht halber tabellarisch dargestellt:

Vorgabe	**Art der Vorgabe**	**Jährlicher Erfüllungsaufwand (in Tsd. Euro)**	**Einmaliger Erfüllungsaufwand (in Tsd. Euro)**
Mitwirkung an Abwehrmaßnahmen gegen Angriffe auf die IT-Sicherheit	weitere Vorgabe	158	0
Mitwirkung an Abwehrmaßnahmen gegen Angriffe auf die IT-Sicherheit	weitere Vorgabe	53	0
Bereitstellung von Informationen durch Anbieter von Telekommunikationsdiensten und digitalen Anbietern	Informationspflicht	106	0
Auf Grundlage der vom BSI veröffentlichten Informationen Kunden einen DNS-basierten Schutz vor Angriffen im Zusammenhang mit sicherheitsriskanten Domains anbieten	weitere Vorgabe	264	0
Umsetzung der Anordnungsbefugnis gegenüber Top Level Registries und Registraren	weitere Vorgabe	11	0
Bei Anordnung des BSI Datenverkehr an eine benannte Domain oder Anschlusskennung umzuleiten oder zu unterbinden	weitere Vorgabe	106	0
Zugang zu Domain-Namen-Registrierungsdaten gewähren	weitere Vorgabe	21	0
Benachrichtigungen durch Dienstanbieter	Informationspflicht	177	0
Untersagung des Betriebs eines informationstechnischen Systems	weitere Vorgabe	1.584	0
Summe		**2.479**	**0**
davon aus Bürokratiekosten		**282**	

Verwaltung

Das Regelungsvorhaben verursacht jährlichen Erfüllungsaufwand von rund 35 Mio. Euro und einmaligen Erfüllungsaufwand von rund 19,6 Mio. Euro, der ausschließlich bei der Verwaltung des Bundes anfällt.

Jährlich

- Abwehr von Gefahren durch Angriffe auf die Sicherheit in der Informationstechnik

Die größte Belastung entsteht durch die Abwehr von Gefahren durch Angriffe auf die Sicherheit in der Informationstechnik beim BKA.

Die neue gesetzliche Regelung sieht zusätzliche Aufgaben und Befugnisse des BKA bei Angriffen auf die Sicherheit in der Informationstechnik vor, wenn u. a. eine internationale Tragweite bzw. außenpolitische Belange des Bundes betroffen sind. Zudem erweitern sich die datenschutzrechtlichen Aufsichtsmaßnahmen des BfDI. Das Ressort schätzt, dass zur jährlichen Aufgabenerfüllung (einschließlich der erweiterten datenschutzrechtlichen Aufsichtsmaßnahmen) ca. 172 000 Stunden (107,5 MAK) notwendig sind. Unter Berücksichtigung des durchschnittlichen Lohnsatzes für die Bundesverwaltung in Höhe von 44,40 Euro sowie jährlichen Sachkosten in Höhe von 1,8 Mio. Euro ergibt sich in Summe ein laufender Erfüllungsaufwand in Höhe von rund **9,4 Mio**. Euro.

- Erheben, Löschen und Veränderung von Daten in informationstechnischen Systemen

Die zweitgrößte Belastung resultiert aus dem Erheben, dem Löschen und der Veränderung von Daten in informationstechnischen Systemen.

Das BKA darf künftig in informationstechnischen Systemen technische Daten erheben, verändern und löschen, sofern eine Cybergefahr nicht durch andere Mittel abgewehrt werden kann. Das Ressort nimmt an, dass zur jährlichen Aufgabenerfüllung ca. 112 000 Stunden (70 MAK) notwendig sind. Unter Berücksichtigung des durchschnittlichen Lohnsatzes für die Bundesverwaltung in Höhe von 44,40 Euro sowie jährliche Sachkosten in Höhe von 2,3 Mio. Euro ergibt sich in Summe ein laufender Erfüllungsaufwand in Höhe von rund **7,3 Mio.** Euro.

Die übrigen Vorgaben für die Bundesverwaltung verursachen geringfügigeren Erfüllungsaufwand und werden der besseren Übersicht halber tabellarisch dargestellt:

Vorgabe	Verwaltungsebene	Jährlicher Aufwand		Jährlicher Erfüllungsaufwand (in Tsd. Euro)
		Jährlicher Personalaufwand (in Tsd. Euro)	Jährliche Sachkosten (in Tsd. Euro)	
Aufsichtsmaßnahmen BfDI	Bund	64	0	64
Umleitung von Datenverkehr auf eine vorgegebene Zieladresse	Bund			2.967
Eingriff in ein informationstechnisches System	Bund	0	0	1.902
Untersagung des Betriebs eines informationstechnischen Systems	Bund	0	0	3.820
Maßnahmen zur Abwehr und Eindämmung von Angriffen, einschließlich der systematischen Suche nach Angriffspuren (Threat Hunting)	Bund	0	0	595
Datenverarbeitung und Information zur Bekämpfung von Domainphishing	Bund	0	0	213
Anordnung gegenüber Top Level Domains	Bund	0	0	36
Verarbeitung und Auswertung umgeleiteter Daten	Bund	0	0	213
Anbindung von Systemen zur Angriffserkennung bei Betreibern kritischer Anlagen an das BSI	Bund	0	0	1.119
Bußgeldverfahren und Sanktionierung bei Fehlen eines geeigneten Systems zur Angriffserkennung	Bund	0	0	107
Unterstützung bei der Durchführung technischer Maßnahmen der Abwehr von Angriffen auf die Sicherheit in der Informationstechnik	Bund	0	0	710
Eigenschutz der Liegenschaften, sonstiger Einrichtungen und Veranstaltungen des BKA	Bund	0	0	995

Untersagung des Betriebs informationstechnischer Systeme	Bund	0	0	3.426
Einschränkung, Unterbindung und Umleitung von Datenverkehr	Bund	0	0	2.021
	Summe	**64**	**0**	**18.188**

Einmalig

Bei dem einmaligen Erfüllungsaufwand in Höhe von 19,6 Mio. Euro handelt es sich fast ausschließlich um Sachkosten durch die folgende Vorgabe:

- Besondere Abwehrmaßnahmen gegen Angriffe auf die Sicherheit in der Informationstechnik

Nach Angaben des Ressorts ist die Bundespolizei darauf angewiesen, vorbeugende Maßnahmen zu ergreifen, um Bedrohungen aus dem Cyberraum entgegenzuwirken, die ihre Einsatzfähigkeit beeinträchtigen könnten. Darüber hinaus setzt die Bundespolizei Cyberfähigkeiten zur Strafverfolgung, zur Sicherung ihrer eigenen Einrichtungen und zur Unterstützung anderer Behörden ein. Künftig kann die Bundespolizei zur Erfüllung ihrer Aufgaben besondere Abwehrmaßnahmen ergreifen, um Angriffe auf die Sicherheit in der Informationstechnik abzuwehren. Zur Sicherstellung der besonderen Abwehrmaßnahmen werden nach Angaben des Ressorts einmalige Sachkosten in Höhe von ca. 19,4 Mio. Euro notwendig.

III.2 Evaluierung

Entgegen der Pflicht zur Evaluierung gemäß § 44 Absatz 7 GGO, wonach in der Begründung zum Gesetzentwurf durch das federführende Ressort festzulegen ist, ob und nach welchem Zeitraum zu prüfen ist, ob die beabsichtigten Wirkungen erreicht worden sind, ob die entstandenen Kosten in einem angemessenen Verhältnis zu den Ergebnissen stehen und welche Nebenwirkungen eingetreten sind, sieht das Ressort mit folgender Begründung keine Evaluierung vor:

„*Eine gesonderte Evaluierung der Regelungen dieses Gesetzes ist nicht vorgesehen. Die neuen Regelungen knüpfen an den bestehenden Rechtsstrukturen an. Die Auswirkungen des Gesetzes sind im Wesentlichen prognostizierbar und im Rahmen der Gesetzesfolgenabschätzung/Erfüllungsaufwand berücksichtigt worden. Im Übrigen unterliegen die Anwendung der Befugnisse sowie deren Auswirkung bereits einer kontinuierlichen Kontrolle, insbesondere durch die parlamentarische Kontrolle, die Fach- und Rechtsaufsicht sowie die bestehenden Berichtspflichten und gerichtliche Rechtsschutzmöglichkeiten. Vor diesem Hintergrund wird von der Aufnahme einer Evaluationsklausel abgesehen.*“

Berichtspflichten, die der parlamentarischen, fachlichen und rechtlichen Kontrolle dienen, beantworten nicht die Frage, die im Rahmen der Evaluierung beantwortet wird, ob nämlich eine Regelung die intendierten Auswirkungen hat (hier: Schutz der IT der Bundesverwaltung im Cyberraum und Eindämmung der Ausbreitung maliziöser Infrastruktur).

Der NKR empfiehlt die Einhaltung der GGO und der Beschlusslage der Bundesregierung durch die Aufnahme einer Evaluierungsklausel. Diese sollte die Ziele enthalten, die bei der Evaluierung zugrunde gelegt werden und welche Kriterien für die Zielerreichung dabei voraussichtlich herangezogen werden. Dies ermöglicht es, Vorsorge dafür zu treffen, dass zum Zeitpunkt der Evaluierung die voraussichtlich erforderlichen Daten zur Verfügung stehen.

21. Mai 2026

Lutz Goebel
Vorsitzender

Prof. Dr. Sabine Kuhlmann
Berichterstatterin für das Bundesministerium des Innern