Entwurf

Stand: 01. Dezember 2008

Gesetzentwurf

der Bundesregierung

Entwurf eines

Ersten Gesetzes zur Änderung des BSI-Errichtungsgesetzes und anderer Gesetze

A. Problem und Ziel

Die Bedeutung der Informations- und Kommunikationstechnologie (IKT) hat sich in den vergangenen Jahren stark gewandelt: Sie ist mittlerweile Voraussetzung für das Funktionieren des Gemeinwesens. Ohne funktionierende IKT-Strukturen ist die Versorgung mit Energie oder Wasser gefährdet, fallen wichtige Infrastrukturen (z.B. Verkehrsmittel, bargeldlose Zahlungswege von der Ladenkasse bis zur Rentenzahlung) aus. Angriffe auf IKT-Infrastrukturen können auch Unfälle mit unmittelbaren Auswirkungen auf Leben und Gesundheit vieler Menschen auslösen, z.B. durch gezieltes Umgehen von eingebauten Sicherheitsmaßnahmen. Schwachstellen in IKT-Infrastrukturen werden auch zur Wirtschafts-, Industrie- und Forschungsspionage genutzt, mit unmittelbaren Auswirkungen auf den Wohlstand und letztlich die innere Sicherheit Deutschlands. IT-Sicherheit ist damit ein wesentlicher Bestandteil der inneren und äußeren Sicherheit der Bundesrepublik Deutschland.

Auch die Verwaltung ist auf sichere und verfügbare Kommunikationstechnik angewiesen. Die zunehmende Vernetzung gewachsener IT-Strukturen verknüpft dabei sehr inhomogene IT-Systeme miteinander. Dies erschwert es, einheitliche Sicherheitsstandards einzuführen und birgt damit die Gefahr, dass Schwachstellen an einer Stelle ein Eindringen in die IT-Systeme einer Vielzahl von Behörden ermöglichen. Dieser Gefahr kann nur durch die Festlegung einheitlicher und strenger Sicherheitsstandards durch eine zentrale Stelle auf Bundesebene begegnet werden.

B. Lösung

Dem BSI sollen Befugnisse eingeräumt werden, sowohl in abstrakter Form als auch einzelfallbezogen technische Vorgaben für die Sicherung der Informationstechnik in der Bundesverwaltung zu machen und Maßnahmen umzusetzen, um Gefahren für die Sicherheit der Informationstechnik des Bundes abzuwehren. Als zentrale Meldestelle für IT-Sicherheit sammelt das BSI Informationen über Sicherheitslücken und neue Angriffsmuster, wertet diese aus und gibt Informationen und Warnungen an die betroffenen Stellen oder die Öffentlichkeit weiter.

C. Alternativen

Keine.

D. Finanzielle Auswirkungen auf die öffentlichen Haushalte

1. Haushaltsausgaben ohne Vollzugsaufwand

Keine.

2. Vollzugsaufwand

Die neu zu schaffenden Befugnisse des BSI sind mit einem entsprechenden Vollzugsaufwand verbunden. Dessen Umfang und damit die Höhe der Vollzugskosten sind maßgeblich von der zukünftigen Entwicklung der IT-Sicherheitslage abhängig und insoweit nur schwer zu beziffern. Den Großteil der zukünftig anfallenden administrativen Aufgaben erfüllt das BSI bereits heute in Form unverbindlicher Beratungsangebote und im Rahmen von Amtshilfeersuchen. Bei unveränderter Sicherheitslage ist daher nur mit einer geringfügigen Erhöhung des Vollzugsaufwands zu rechnen.

Für die Wahrnehmung der übertragenen neuen Aufgaben aufgrund des BSIG benötigt das BSI ca. 10 zusätzliche Planstellen/Stellen sowie Personal- und Sachkosten in Höhe von ca. 1.180.000 € jährlich. Die Bundesnetzagentur (BNetzA) benötigt für die Wahrnehmung der im § 109 TKG definierten neuen Aufgaben zusätzlich drei Planstellen des gehobenen technischen Dienstes sowie Personal- und Sachkosten in Höhe von ca. 300.000 € jährlich. Die zusätzlichen Planstellen/Stellen und Kosten sind aus dem Gesamthaushalt zu finanzieren. Eine Kompensation aus den Einzelplänen 06 und 09 ist nicht möglich.

E. Sonstige Kosten

Für Leistungen gegenüber der Wirtschaft im Rahmen der Zertifizierungsverfahren fallen wie bisher Kosten nach der BSI-Kostenverordnung an.

F. Bürokratiekosten

Das Gesetz enthält fünf neue Informationspflichten für die Verwaltung. Durch den hier vorgesehenen Informationsaustausch können Synergieeffekte genutzt und der Aufbau paralleler Strukturen beim BSI und anderen Behörden vermieden werden. Von den bestehenden Regelungsalternativen wurde hier insoweit die kostengünstigste gewählt. Neue Informationspflichten für die Wirtschaft sind nicht vorgesehen.

Entwurf eines

Ersten Gesetzes zur Änderung des BSI-Errichtungsgesetzes und anderer Gesetze

Vom [Datum der Ausfertigung]

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Änderung des BSI-Errichtungsgesetzes

Das BSI-Errichtungsgesetz vom 17. Dezember 1990 (BGBl. I S. 2834), zuletzt geändert durch Artikel 25 der Verordnung vom 31. Oktober 2006 (BGBl. I S. 2407), wird wie folgt geändert:

1. § 2 wie folgt geändert:

   a) In Absatz 2 Nummer 1 und 2 werden jeweils die Wörter „Systemen oder Komponenten" durch die Wörter „Systemen, Komponenten oder Prozessen" ersetzt.

   b) Nach Absatz 2 werden die folgenden Absätze 3 bis 9 angefügt:

   „(3) Kommunikationstechnik des Bundes im Sinne dieses Gesetzes ist die Informationstechnik, die von einer oder mehreren Bundesbehörden oder im Auftrag einer oder mehrerer Bundesbehörden betrieben wird und der Kommunikation oder dem Datenaustausch der Bundesbehörden untereinander oder mit Dritten dient. Kommunikationstechnik der Bundesgerichte, soweit sie öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen, des Bundestags, des Bundesrats, des Bundespräsidenten oder des Bundesrechnungshofs ist dann Kommunikationstechnik des Bundes, wenn und soweit diese Stellen die Kommunikationstechnik des Bundes im Einvernehmen mitnutzen.

   (4) Schnittstellen der Kommunikationstechnik des Bundes im Sinne dieses Gesetzes sind sicherheitsrelevante Netzwerk-Übergänge innerhalb der Kommunikationstechnik des Bundes sowie zwischen dieser und der Informationstechnik der einzelnen Bundesbehörden, Gruppen von Bundesbehörden oder Dritter.

   (5) Schadprogramme im Sinne dieses Gesetzes sind Programme und sonstige informationstechnische Routinen und Verfahren, die dem Zweck dienen, unbefugt Daten zu nutzen oder zu löschen oder die dem Zweck dienen, unbefugt auf sonstige informationstechnische Abläufe einzuwirken.

   (6) Sicherheitslücken im Sinne dieses Gesetzes sind Eigenschaften von Programmen oder sonstigen informationstechnischen Systemen, durch deren Ausnutzung es möglich ist, dass sich Dritte gegen den Willen des Berechtigten Zugang zu fremden informationstechnischen Systemen verschaffen oder die Funktion der informationstechnischen Systeme beeinflussen können.

   (7) Zertifizierung im Sinne dieses Gesetzes ist die Feststellung durch eine Zertifizierungsstelle, dass ein Produkt, ein Prozess, ein System, ein Schutzprofil (Sicherheitszertifizierung), eine Person (Personenzertifizierung) oder ein IT-Sicherheitsdienstleister bestimmte Anforderungen erfüllt.

(8) Protokolldaten im Sinne dieses Gesetzes sind Steuerdaten, eines informationstechnischen Protokolls zur Datenübertragung, die unabhängig vom Inhalt eines Kommunikationsvorgangs übertragen oder auf den am Kommunikationsvorgang beteiligten Servern gespeichert werden und zur Gewährleistung der Kommunikation zwischen Empfänger und Sender notwendig sind. Protokolldaten können Verkehrsdaten gemäß § 3 Nummer 30 des Telekommunikationsgesetzes und Nutzungsdaten nach § 15 Absatz 1 des Telemediengesetzes enthalten.

(9) Datenverkehr im Sinne dieses Gesetzes sind die mittels technischer Protokolle übertragenen Daten. Der Datenverkehr kann Telekommunikationsinhalte nach § 88 Absatz 1 des Telekommunikationsgesetzes und Nutzungsdaten nach § 15 Absatz 1 des Telemediengesetzes enthalten."

2. § 3 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) Satz 1 wird durch folgende zwei Sätze ersetzt:

„Das Bundesamt fördert die Sicherheit in der Informationstechnik. Hierzu nimmt es folgende Aufgaben wahr:"

bb) Vor Nummer 1 werden folgende Nummern 1 und 2 eingefügt:

„1. Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes.

2. Sammlung und Auswertung von Informationen über Sicherheitsrisiken und Sicherheitsvorkehrungen und Zurverfügungstellung der gewonnenen Erkenntnisse für andere Stellen, soweit dies zur Erfüllung ihrer Aufgaben oder zur Wahrung ihrer Sicherheitsinteressen erforderlich ist,"

cc) Die bisherige Nummer 1 wird zur Nummer 3. Hinter den Wörtern „Geräten für die Sicherheit in der Informationstechnik" wird der Klammerzusatz „(IT-Sicherheitsprodukte)" eingefügt. Am Ende werden die Wörter „einschließlich der Forschung im Rahmen seiner gesetzlichen Aufgaben," eingefügt.

dd) Die bisherige Nummer 2 wird zur Nummer 4. Nach dem Wort „Komponenten" wird das Komma gestrichen und werden die Wörter„und für die Prüfung und Bewertung der Konformität im Bereich der IT-Sicherheit," eingefügt.

ee) Die bisherige Nummer 3 wird Nummer 5. Danach wird folgende Nummer 6 eingefügt:

„6. Prüfung und Bestätigung der Konformität im Bereich der IT-Sicherheit von informationstechnischen Systemen und Komponenten mit technischen Richtlinien des Bundesamtes,"

ff) Die bisherige Nummer 4 wird Nummer 7und wie folgt gefasst:

„7. Prüfung, Bewertung und Zulassung von informationstechnischen Systemen oder Komponenten, die für die Verarbeitung oder Übertragung amtlich geheim gehaltener Informationen nach § 4 des Sicherheitsüberprüfungsgesetzes im Bereich des Bundes oder bei Unternehmen im Rahmen von Aufträgen des Bundes eingesetzt werden sollen,"

gg) Nach Nummer 7 werden folgende Nummern 8 bis 11 eingefügt:

„8. Herstellung von Schlüsseldaten und Betrieb von Krypto- und Sicherheitsmanagementsystemen für informationssichernden Systeme des Bundes, die im Bereich des staatlichen Geheimschutzes oder auf Anforderung der betroffenen Behörde auch in anderen Bereichen eingesetzt werden.

9. Unterstützung und Beratung bei organisatorischen und technischen Sicherheitsmaßnahmen sowie Durchführung von technischen Prüfungen zum Schutz von amtlich geheim gehaltenen Informationen nach § 4 des Sicherheitsüberprüfungsgesetzes gegen die Kenntnisnahme durch Unbefugte,

10. Entwicklung von sicherheitstechnischen Anforderungen an die einzusetzende Informationstechnik des Bundes und an die Eignung von Auftragnehmern im Bereich von Informationstechnik mit besonderem Schutzbedarf,

11. Bereitstellung von IT-Sicherheitsprodukten für Stellen des Bundes,"

hh) Die bisherigen Nummern 5 und 6 werden Nummern 12 und 13. Nach Nummer 13 Buchstabe b) wird folgender Buchstabe c) eingefügt:

„c) des Bundesnachrichtendienstes bei der Wahrnehmung seiner gesetzlichen Aufgaben.

ii) Die bisherige Nummer 7 wird Nummer 14. Nach dem Wort „Beratung" werden die Wörter „und Warnung der Stellen des Bundes, der Länder sowie" eingefügt.

jj) Nach Nummer 14 wird folgende Nummer 15 angefügt:

„15. Aufbau geeigneter Kommunikationsstrukturen zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung sowie Koordinierung der Zusammenarbeit zum Schutz der kritischen Informationsinfrastrukturen im Verbund mit der Privatwirtschaft."

b) Absatz 2 wird wie folgt gefasst:

„(2) Das Bundesamt kann die Länder auf Ersuchen bei der Sicherung ihrer Informationstechnik unterstützen."

3. Nach § 3 werden folgende §§ 4 bis 8 eingefügt:

„§ 4
Zentrale Meldestelle für die Sicherheit in der Informationstechnik

(1) Das Bundesamt ist die zentrale Meldestelle für die Zusammenarbeit der Bundesbehörden in Angelegenheiten der Sicherheit in der Informationstechnik.

(2) Das Bundesamt hat zur Wahrnehmung dieser Aufgabe

1. alle für die Abwehr von Gefahren für die Sicherheit in der Informationstechnik erforderlichen Informationen, insbesondere zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweise zu sammeln und auszuwerten,

2. die Bundesbehörden unverzüglich über die sie betreffenden Informationen nach Nummer 1 und die in Erfahrung gebrachten Zusammenhänge zu unterrichten.

(3) Werden anderen Bundesbehörden Informationen nach Absatzes 2 Nummer 1 bekannt, die für die Erfüllung von Aufgaben oder die Sicherheit der Informationstechnik anderer Behörden von Bedeutung sind, unterrichten diese das Bundesamt hierüber unverzüglich, soweit andere Vorschriften dem nicht entgegenstehen.

(4) Ausgenommen von den Unterrichtungspflichten nach Absatz 2 Nummer 2 und Absatz 3 sind Informationen, die aufgrund von Regelungen zum Geheimschutz oder Vereinbarungen mit Dritten nicht weitergegeben werden dürfen oder deren Weitergabe im Widerspruch zu der der verfassungsrechtlichen Stellung eines Abgeordneten des Bundestages oder eines Verfassungsorgans oder der gesetzlich geregelten Unabhängigkeit einzelner Stellen stünde.

(5) Die Vorschriften zum Schutz personenbezogener Daten bleiben unberührt.

(6) Das Bundesministerium des Innern erlässt nach Zustimmung durch den Rat der IT-Beauftragten der Bundesregierung allgemeine Verwaltungsvorschriften zur Durchführung des Absatz 3.

§ 6
Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes

(1) Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes

1. Protokolldaten, die beim Betrieb von Kommunikationstechnik des Bundes anfallen, erheben und automatisiert auswerten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist,

2. die an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten automatisiert auswerten, soweit dies für die Erkennung und Abwehr von Schadprogrammen erforderlich ist.

Sofern nicht die nachfolgenden Absätze eine weitere Verwendung gestatten, muss die automatisierte Auswertung dieser Daten unverzüglich erfolgen und müssen diese nach erfolgtem Abgleich sofort und spurenlos gelöscht werden. Die Verwendungsbeschränkungen gelten nicht für Protokolldaten, sofern diese weder personenbezogene noch dem Fernmeldegeheimnis unterliegende Daten beinhalten. Behördeninterne Protokolldaten dürfen nur im Einvernehmen mit der jeweils betroffenen Behörde erhoben werden.

(2) Protokolldaten nach Absatz 1 Nummer 1 dürfen über den für die automatisierte Auswertung nach Absatz 1 Nummer 1 erforderlichen Zeitraum hinaus, längstens jedoch für drei Monate, gespeichert werden, soweit tatsächliche Anhaltspunkte bestehen, dass diese für den Fall der Bestätigung eines Verdachts nach Absatz 3 Satz 2 zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich sein können. Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Auswertung der nach diesem Absatz gespeicherten Daten nur automatisiert erfolgt. Eine nicht automatisierte Auswertung oder eine personenbezogene Verwendung ist nur nach Maßgabe der nachfolgenden Absätze zulässig.

(3) Eine über Absatz 1 und 2 hinausgehende Verwendung personenbezogener Daten ist nur zulässig, wenn bestimmte Tatsachen den Verdacht begründen, dass diese

1. ein Schadprogramm enthalten,

2. durch ein Schadprogramm übermittelt wurden oder

3. sich aus ihnen Hinweise auf ein Schadprogramm ergeben können,

und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen. Im Falle der Bestätigung ist die weitere Verarbeitung personenbezogene Daten zulässig, soweit dies

1. zur Abwehr des Schadprogramms,

2. zur Abwehr von Gefahren, die von dem aufgefundenen Schadprogramm ausgehen oder

3. zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist.

Ein Schadprogramm kann beseitigt und in seiner Funktionsweise gehindert werden. Die Beteiligten des Kommunikationsvorgangs sind spätestens nach dem Erkennen und der Abwehr eines Schadprogramms oder von Gefahren, die von einem Schadprogramm ausgehen, zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßige weitere Ermittlungen möglich ist und nicht überwiegende schutzwürdige Belange Dritter entgegenstehen. Die Unterrichtung kann unterbleiben, wenn die Person nur unerheblich betroffen wurde und anzunehmen ist, dass sie an einer Benachrichtigung kein Interesse hat. In den Fällen von Absatz 4 erfolgt die Benachrichtigung durch die dort genannten Behörden nach Maßgabe der für diese Verfahren geltenden Vorschriften.

(4) Das Bundesamt kann die nach Absatz 3 verwendeten personenbezogenen Daten an die Polizeien des Bundes und der Länder, an Strafverfolgungsbehörden und sonstige öffentliche Stellen übermitteln, soweit dies erforderlich ist

1. 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, oder,

2. zur Verfolgung von Straftaten, wenn ein Auskunftsverlangen nach der Strafprozessordnung zulässig wäre.

§ 18 des Bundesverfassungsschutzgesetzes bleibt unberührt.

(5) Eine über die vorstehenden Absätze hinausgehende inhaltliche Auswertung zu anderen Zwecken und Weitergabe von personenbezogenen Daten an Dritte sind unzulässig. Werden aufgrund der Maßnahmen der Absätze 1 bis 3 Erkenntnisse aus dem Kernbereich privater Lebensgestaltung oder Daten im Sinne des § 3 Absatz 9 Bundesdatenschutzgesetz erlangt, dürfen diese nicht verwendet werden. Erkenntnisse aus dem Kernbereich privater Lebensgestaltung sind unverzüglich zu löschen. Bestehen Zweifel, ob Erkenntnisse dem Kernbereich privater Lebensgestaltung zuzurechnen sind, sind diese entweder ebenfalls zu löschen oder unverzüglich dem Bundesministerium des Innern zur Entscheidung über ihre Verwertbarkeit oder Löschung vorzulegen. Die Tatsache ihrer Erlangung und Löschung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist zu löschen, wenn sie für diese Zwecke nicht mehr erforderlich ist, spätestens jedoch am Ende des Kalenderjahres, das dem Jahr der Dokumentation folgt.

(6) Vor Aufnahme der Datenerhebung und -verwendung hat das Bundesamt ein Datenerhebungs- und -verwendungskonzept zu erstellen und für Kontrollen durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit bereitzuhalten. .Das Konzept hat dem besonderen Schutzbedürfnis der Regierungskommunikation Rechnung zu tragen. Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit teilt das Ergebnis seiner Kontrollen nach § 24 des Bundesdatenschutzgesetzes auch dem Rat der IT-Beauftragten der Bundesregierung mit.

§ 6c
Löschung

(1) Soweit das Bundesamt im Rahmen seiner Befugnisse personenbezogene Daten erhebt, sind diese unverzüglich zu löschen, sobald sie für die Erfüllung der Aufgaben, für die sie erhoben wurden, oder für eine etwaige gerichtliche Überprüfung nicht mehr benötigt werden. Soweit die Löschung lediglich für eine etwaige gerichtliche Überprüfung von Maßnahmen nach § 6 Absatz 3 zurückgestellt ist, dürfen die Daten ohne Einwilligung des Betroffenen nur zu diesem Zweck verwendet werden; sie sind für andere Zwecke zu sperren. § 6 Absatz 5 bleibt unberührt.

§ 6d
Warnungen

(1) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 12 kann das Bundesamt Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten und vor Schadprogrammen an die betroffenen Kreise oder die Öffentlichkeit weitergeben oder Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen. Soweit entdeckte Sicherheitslücken oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterverbreitung oder rechtswidrige Ausnutzung zu verhindern oder weil das Bundesamt gegenüber Dritten zur Vertraulichkeit verpflichtet ist, kann es den Kreis der zu warnenden Personen anhand sachlicher Kriterien einschränken; sachliche Kriterien können insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere Zuverlässigkeit des Empfängers sein.

(2) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 12 kann das Bundesamt die Öffentlichkeit unter Nennung der Bezeichnung und des Herstellers des betroffenen Produkts vor Sicherheitslücken in informationstechnischen Produkten und Diensten und vor Schadprogrammen warnen oder Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte empfehlen, wenn hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik hiervon ausgehen. Stellen sich die an die Öffentlichkeit gegebenen Informationen im Nachhinein als falsch oder die zugrunde liegenden Umstände als unzutreffend wiedergegeben heraus, ist dies unverzüglich öffentlich bekannt zu machen.

§ 7
Vorgaben des Bundesamts

(1) Das Bundesamt kann Mindeststandards für die Sicherung der Informationstechnik des Bundes festlegen. Das Bundesministerium des Innern kann nach Zustimmung des Rats der IT-Beauftragten der Bundesregierung die nach Satz 1 festgelegten Anforderungen ganz oder teilweise als allgemeine Verwaltungsvorschriften für alle Stellen des Bundes erlassen. Soweit in einer allgemeinen Verwaltungsvorschrift Sicherheitsvorgaben des Bundesamtes für ressortübergreifende Netze sowie die

für den Schutzbedarf des jeweiligen Netzes notwendigen und von den Nutzern des Netzes umzusetzenden Sicherheitsanforderungen enthalten sind, bedarf es hinsichtlich dieser Inhalte nicht einer Zustimmung des Rats der IT-Beauftragten der Bundesregierung.

(2) Das Bundesamt stellt im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 10 technische Richtlinien bereit, die von den Stellen des Bundes als Rahmen für die Entwicklung sachgerechter Anforderungen an Auftragnehmer (Eignung) und IT-Produkte (Spezifikation) für die Durchführung von Vergabeverfahren berücksichtigt werden. Die Vorschriften des Vergaberechts und des Geheimschutzes bleiben unberührt.

(3) Die Bereitstellung von IT-Sicherheitsprodukten durch das Bundesamt nach § 3 Absatz 1 Satz 2 Nummer 11 erfolgt durch Eigenentwicklung oder nach Durchführung von Vergabeverfahren aufgrund einer entsprechenden Bedarfsfeststellung. Die Vorschriften des Vergaberechts bleiben unberührt. Wenn das Bundesamt IT-Sicherheitsprodukte bereitstellt, können die Bundesbehörden diese Produkte beim Bundesamt abrufen. Durch Beschluss des Rats der IT-Beauftragten der Bundesregierung kann festgelegt werden, dass die Bundesbehörden verpflichtet sind, diese Produkte beim Bundesamt abzurufen. Eigenbeschaffungen anderer Bundesbehörden sind in diesem Fall nur zulässig, wenn das spezifische Anforderungsprofil den Einsatz abweichender Produkte erfordert.

§ 8
Zertifizierung

(1) Das Bundesamt ist nationale Zertifizierungsstelle der Bundesverwaltung für IT-Sicherheit.

(2) Für bestimmte Produkte oder Leistungen kann beim Bundesamt eine Sicherheits- oder Personenzertifizierung oder eine Zertifizierung als IT-Sicherheitsdienstleister beantragt werden. Die Anträge werden in der zeitlichen Reihenfolge ihres Eingangs bearbeitet; hiervon kann abgewichen werden, wenn das Bundesamt wegen der Zahl und des Umfangs anhängiger Prüfungsverfahren eine Prüfung in angemessener Zeit nicht durchführen kann und an der Erteilung eines Zertifikats ein öffentliches Interesse besteht. Der Antragsteller hat dem Bundesamt die Unterlagen vorzulegen und die Auskünfte zu erteilen, deren Kenntnis für die Prüfung und Bewertung des Systems oder der Komponente oder der Eignung der Person sowie für die Erteilung des Zertifikats erforderlich ist.

(3) Die Prüfung und Bewertung kann durch vom Bundesamt anerkannte sachverständige Stellen erfolgen.

(4) Das Sicherheitszertifikat wird erteilt, wenn

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

2. das Bundesministerium des Innern festgestellt hat, dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung nicht entgegenstehen.

(5) Für die Zertifizierung von Personen und IT-Sicherheitsdienstleistern gilt Absatz 4 entsprechend.

(6) Eine Anerkennung nach Absatz 3 wird erteilt, wenn

1. die sachliche und personelle Ausstattung sowie die fachliche Qualifikation und Zuverlässigkeit der Konformitätsbewertungsstelle den vom Bundesamt festgelegten Kriterien entspricht und

2. das Bundesministerium des Innern festgestellt hat, dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung nicht entgegenstehen.

Das Bundesamt stellt durch die notwendigen Maßnahmen sicher, dass das Fortbestehen der Voraussetzungen nach Satz 1 regelmäßig überprüft wird.

(7) Sicherheitszertifikate anderer anerkannter Zertifizierungsstellen aus dem Bereich der Europäischen Union werden vom Bundesamt anerkannt, soweit sie eine den Sicherheitszertifikaten des Bundesamtes gleichwertige Sicherheit ausweisen und die Gleichwertigkeit vom Bundesamt festgestellt worden ist."

4. Die bisherigen §§ 4 und 6 bis 9 werden aufgehoben:

5. Der bisherige § 5 wird § 9 und wie folgt geändert

a) Die Überschrift wird wie folgt gefasst:

„§ 9
Ermächtigung zum Erlass von Rechtsverordnungen".

b) In Absatz 1 wird die Angabe „§ 4" durch die Angabe „§ 8" ersetzt.

c) In Absatz 2 Satz 3 werden die Wörter „und die Gebührensätze" durch ein Komma und die Wörter „die Gebührensätze und die Auslagen." ersetzt.

6. § 10 wird wie folgt gefasst:

„§ 10
Einschränkung von Grundrechten

Das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) wird durch § 6 eingeschränkt."

7. Nach § 10 wird folgender § 11 angefügt:

§ 11
Rat der IT-Beauftragten der Bundesregierung

Wird der Rat der IT-Beauftragten der Bundesregierung aufgelöst, tritt an dessen Stelle die von der Bundesregierung bestimmte Nachfolgeorganisation. Die Zustimmung des Rats der IT-Beauftragten kann durch Einvernehmen aller Bundesministerien ersetzt werden. Wird der Rat der IT-Beauftragten ersatzlos aufgelöst, tritt an Stelle seiner Zustimmung das Einvernehmen aller Bundesministerien.

8. Die bisherigen §§ 6 bis 10 werden gestrichen.

Artikel 2

Änderung des Telekommunikationsgesetzes

Das Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), zuletzt geändert durch Artikel 2 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198), wird wie folgt geändert:

1. § 109 wird wie folgt geändert:

   1. Im Absatz 2 werden nach dem Satz 2 folgende Sätze 3 bis 5 eingefügt:

      „Die Bundesnetzagentur erstellt im Benehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit einen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen. Sie gibt den Herstellern und Betreibern von Telekommunikationsanlagen Gelegenheit zur Stellungnahme. Der Katalog wird von der Bundesnetzagentur veröffentlicht."

   2. im Absatz 3 wird nach Satz 4 folgender Satz 5 eingefügt:

      „Die Bundesnetzagentur prüft in regelmäßigen Abständen unter Berücksichtigung der Bedeutung der Telekommunikationsanlage die Umsetzung des Sicherheitskonzeptes bei dem nach Satz 1 Verpflichteten."

   3. Absatz 3 Satz 6 wird aufgehoben.

Artikel 3

Änderung des Telemediengesetzes

Dem § 15 des Telemediengesetzes vom 26. Februar 2007 (BGBl. I S. 179) wird folgender Absatz 9 angefügt:

„(9) Soweit erforderlich, darf der Diensteanbieter Nutzungsdaten zum Erkennen, Eingrenzen oder Beseitigen von Störungen seiner für Zwecke seines Telemedienangebotes genutzten technischen Einrichtungen erheben und verwenden. Absatz 8 Satz 2 gilt entsprechend."

Artikel 4

Inkrafttreten

Art. 1 Nummer 3 § 4 Absatz 3 tritt am 1.Januar 2010 in Kraft. Im Übrigen tritt dieses Gesetz am Tag nach seiner Verkündung in Kraft.

Begründung

A. Allgemeiner Teil

I. Ziel und Inhalt des Entwurfs

Das BSI-Errichtungsgesetz (BSIG) ist 1991 in Kraft getreten und seitdem im Wesentlichen unverändert geblieben. Die an das BSI gestellten Erwartungen, welche Aufgaben es wahrnehmen soll, werden im Gesetz nicht mehr vollständig widergespiegelt.

De lege lata sind die wesentlichen Aufgaben des BSI die Unterstützung anderer Behörden in IT-Sicherheitsfragen und die Vergabe von Sicherheitszertifikaten. Allein mit der Vergabe von Sicherheitszertifikaten kann das BSI allerdings keinen entscheidenden Einfluss auf die Gestaltung der IT-Infrastrukturen nehmen. Auch ist eine Beratung der Öffentlichkeit im BSIG nicht ausdrücklich angelegt. Die Unterstützungsfunktion für andere Behörden ist zwar als Aufgabe im BSIG enthalten, aber nicht weiter ausgestaltet. BSI hat insbesondere keine eigenen Befugnisse, sondern wird nur auf und im Rahmen einer Anforderung tätig.

Durch die Änderungen im BSIG sollen dem BSI eigene Befugnisse eingeräumt werden, auch ohne Amtshilfeersuchen anderer Behörden zur Erhöhung der IT-Sicherheit in der Bundesverwaltung und zur Abwehr von Gefahren für die Informationstechnik des Bundes tätig zu werden. Dies beinhaltet die Vorgabe von allgemeinen technischen Richtlinien für die Sicherheit, von konkreten Vorgaben für die Konfiguration der Informationstechnik im Einzelfall und Maßnahmen zur Abwehr konkreter Gefahren. Als Zentralstelle für IT-Sicherheit sammelt das BSI Informationen zu Schwachstellen und Schadprogrammen, wertet diese aus und informiert die betroffenen Stellen oder warnt die Öffentlichkeit.

Soweit hierdurch Synergieeffekte genutzt und Bürokratiekosten eingespart werden können, werden bestimmte IT-Sicherheits-Aufgaben im Telekommunikationsgesetz (TKG) auf das BSI übertragen.

II. Gesetzgebungskompetenz

Für die Regelungen, die unmittelbar die Sicherung der Informationstechnik in der Bundesverwaltung betreffen, hat der Bund eine ungeschriebene Gesetzgebungskompetenz kraft Natur der Sache sowie aus Art. 86 Satz 2 GG. Dies gilt auch, soweit in den §§ 3 Abs. 1 Nr. 14, 3 Abs. 2 und 5 BSIG die Unterstützung insbesondere von Landesbehörden auf deren Ersuchen als Aufgabe einer Bundesbehörde geregelt wird. Soweit das Bundesamt durch Empfehlungen von Sicherheitsstandards, die Ausgabe des Sicherheitszertifikats, Warnungen und Empfehlungen sowie durch die Koordinierung der notwendigen Maßnahmen zum Schutz der Informationstechnik kritischer Infrastrukturen in der Wirtschaft wettbewerbsrelevante außenwirksame Tätigkeiten entfaltet, folgt die Gesetzgebungskompetenz für diese Teilbereiche aus der konkurrierenden Gesetzgebungskompetenz für das Recht der Wirtschaft (Artikel 74 Abs. 1 Nr. 11 GG). Dasselbe gilt für die Änderung des Telemediengesetzes. Die Berechtigung des Bundes zur Inanspruchnahme dieser Gesetzgebungskompetenz ergibt sich aus Artikel 72 Abs. 2 Grundgesetz. 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, z.B. unterschiedliche Voraussetzungen für die Vergabe von Sicherheitszertifikaten, erhebliche Wettbewerbsverzerrungen und störende Schranken für die länderübergreifende Wirtschaftstätigkeit zur Folge hätten. Internationale Abkommen

zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten setzten voraus, dass in jedem Staat nur eine einzige hoheitliche Zertifizierungsstelle existiert. Gerade Telemedienangebote sind typischerweise bundesweit zugänglich. Unterschiedliche technische 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. Regelungen auf dem Gebiet der Telekommunikation können auf die ausschließliche Gesetzgebungskompetenz des Bundes nach Art. 73 Abs. 1 Nr. 7 GG gestützt werden.

III. Vereinbarkeit mit dem Recht der Europäischen Union

Der Gesetzentwurf ist mit dem Recht der Europäischen Union vereinbar.

IV. Kosten

Das Gesetz bewirkt keine Haushaltsausgaben ohne Vollzugsaufwand.

Die neu zu schaffenden Befugnisse des BSI sind mit einem entsprechenden Vollzugsaufwand verbunden. Dessen Umfang und damit die Höhe der Vollzugskosten sind maßgeblich von der zukünftigen Entwicklung der IT-Sicherheitslage abhängig und daher nicht zu beziffern. Den Großteil der zukünftig anfallenden administrativen Aufgaben erfüllt das BSI bereits heute in Form unverbindlicher Beratungsangebote und im Rahmen von Amtshilfeersuchen. Bei unveränderter Sicherheitslage ist daher nur mit einer geringfügigen Erhöhung des Vollzugsaufwands zu rechnen.

Die neuen oder zukünftig aufgrund der Änderung des BSIG in größerem Umfang wahrzunehmenden Aufgaben erfordern beim BSI zusätzliche 10 Planstellen/Stellen sowie Personal- und Sachkosten in Höhe von ca. 1.180.000 € jährlich. Der Personalbedarf resultiert aus den neu geschaffenen Aufgaben nach §§ 3 Abs. 1 Nr. 11 (zentrale Bereitstellung von IT-Sicherheitsprodukten), 4 (zentrale Meldestelle), 6 Abs. 1 bis 4 (Abwehr von Gefahren für die Kommunikationstechnik des Bundes), sowie aus der neu hinzukommenden Zertifizierung von Dienstleistern (§ 8) und der Mitwirkung bei der Erstellung eines Katalogs von Sicherheitsanforderungen für Telekommunikations- und Datenverarbeitungssysteme (§ 109 Abs. 2 Satz 3 TKG). Der Mehrbedarf bei den Sachkosten verteilt sich auf den Betrieb eines Meldeportals für die Meldestellenfunktion (500.000 € p.a.) und die Bereitstellung von IT-Sicherheitsprodukten (100.000 € p.a.). Für die Wahrnehmung der neuen Aufgaben aus § 109 Abs. 2 Satz 3 bis 4 TKG, Erstellen, Koordinieren und Pflegen eines Katalogs von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungsanlagen, und § 109 Abs. 3 Satz 5 TKG, regelmäßige Prüfung der Umsetzung der Sicherheitskonzepte, benötigt die BNetzA zusätzlich drei Planstellen im gehobenen technischen Dienst sowie Personal- und Sachkosten in Höhe von ca. 300.000 € jährlich.

Soweit Kosten für die Entwicklung oder zentrale Beschaffung von IT-Sicherheitsprodukten entstehen, können diese durch Einsparungen bei anderen Stellen kompensiert werden, die entsprechende Produkte nicht mehr einzeln beschaffen müssen. Zusätzliches Einsparungspotenzial ergibt sich aus der Nutzung von Synergien und Mengenrabatten.

Kosten für die Wirtschaft können wie bislang bei Beantragung eines Sicherheitszertifikats nach Maßgabe BSI-Kostenverordnung entstehen. Da das BSI-Sicherheitszertifikat freiwillig ist, können es die Unternehmen von einer Wirtschaftlichkeitsbetrachtung abhängig machen, ob sie ihr Produkt einem Zertifizierungsverfahren mit der damit ggf. einhergehenden Kostenfolge unterziehen.

Das Gesetz enthält fünf neue Informationspflichten für die Verwaltung. Durch die Informationspflichten in § 4 Abs. 2 Nr. 2. und Abs. 3 BSIG wird der Informationsaustausch zu Si-

cherheitslücken, Sicherheitsvorkehrungen über das BSI kanalisiert. Das BSI informiert, insbesondere über das CERT-Bund (CERT = Computer Emergency Response Team) schon heute die Bundesbehörden zeitnah zu aktuellen IT-Sicherheitsfragen. Dies wird durch die Informationspflicht in § 4 Abs. 2 Nr. 2 konkretisiert. Gegenüber den bisher bestehenden Strukturen, bei denen das BSI auf freiwillige bzw. zufällige Informationen angewiesen ist, schafft die Meldepflicht in § 4 Abs. 3 eine bessere Datenbasis und ermöglicht die zentrale Auswertung und Aufbereitung und Verteilung der IT-Sicherheits-Informationen an die übrigen Bundesbehörden. Würde das BSI nicht wie vorgesehen als zentrale Stelle tätig, müssten im Zweifel alle Bundesbehörden parallel derartige Strukturen und das erforderliche Know-How aufbauen, um auf dem für den Betrieb und Schutz ihrer internen Informationstechnik erforderlichen Wissensstand zu bleiben. Insofern wurde die kostengünstigste Regelungsalternative gewählt, die im höchstmöglichen Maß Synergieeffekte nutzt.

Die Informationspflichten aus § 6 Abs. 2 Satz 4 (Benachrichtigungspflicht an Betroffene), § 6 Abs. 4 Satz 4 (Benachrichtigung des BMI bei Zweifeln über Kernbereichsrelevanz) und § 6d Abs. 2 Satz 2 (Richtigstellungspflicht) dienen der Wahrung der Rechte der Betroffenen und sind verfassungsrechtlich vorgegeben.

Informationspflichten oder Kosten für Bürgerinnen und Bürger entstehen nicht. Den Wirtschaftsunternehmen entstehen durch dieses Gesetz Kosten, soweit sie ihr Produkt freiwillig einem Zertifizierungsverfahren mit der damit ggf. einhergehenden Kostenfolge unterziehen. Auswirkungen auf die Einzelpreise und das Preisniveau, insbesondere auf das Verbraucherpreisniveau, sind von diesem Gesetz nicht zu erwarten.

V. Auswirkungen von gleichstellungspolitischer Bedeutung

Auswirkungen von gleichstellungspolitischer Bedeutung sind nicht zu erwarten.

B. Besonderer Teil

Zu Artikel 1 (Änderung des BSI-Errichtungsgesetzes)

Zu Nr. 1 (§ 2)

Zu Buchstabe a)

Redaktionelle Anpassung der Legaldefinition.

Zu Buchstabe b)

Absatz 3

Die neuen Befugnisse sollen sich auf den Schutz der Kommunikationstechnik des Bundes beziehen. Diese wird in § 2 Abs. 3 legaldefiniert. Der Begriff „Kommunikationstechnik des Bundes" umfasst grundsätzlich alle informationstechnischen Systeme und deren Bestandteile, soweit sie durch den Bund oder im Auftrag des Bundes für diesen betrieben werden und der Kommunikation oder dem Datenaustausch dienen. Damit sind nicht an Behördennetze angeschlossene Geräte, bei denen Sicherheitslücken i.d.R. keine Auswirkungen auf die Sicherheit der übrigen Informationstechnik haben, ausgenommen. Nicht erfasst ist Kommunikationstechnik, die von Dritten für die Allgemeinheit angeboten wird und *auch* von Behörden genutzt wird (z.B. öffentliche Telekommunikationsnetze). Erfasst sind die Behörden der Bundesverwaltung. Kommunikationstechnik der Bundesgerichte und der anderen Verfassungsorgane (Bundestag, Bundesrat, Bundespräsident) ist dann Kommunikationstechnik des Bundes, wenn und soweit diese sich entschließen, die Kommunikati-

onstechnik des Bundes mitzubenutzen. In der Praxis besteht hier die Möglichkeit, z.B. für die Kommunikation der Richter oder Abgeordneten einen „Bypass-Anschluss" einzurichten, der unter Umgehung der innerhalb des Verwaltungsnetzes notwendigen Sicherheitsvorkehrungen einen unmittelbaren Anschluss an das Internet oder andere öffentliche Telekommunikationsnetze ermöglicht.

Absatz 4

Mit den Schnittstellen der Kommunikationstechnik des Bundes sind die Übergänge beschrieben, an denen aus Gründen der IT-Sicherheit eine Auswertung von Daten notwendig ist bzw. sein kann. Davon erfasst sind Übergänge zwischen den übergreifenden Kommunikationsnetzen der Bundesverwaltung inklusive der Übergänge zwischen virtuellen Netzen oder zwischen unterschiedlichen Schutzzonen innerhalb eines Netzes sowie zwischen einzelnen internen Behördennetzen oder den Netzen einer Gruppe von Behörden, Ländernetzen, dem Internet und anderen nicht der Bundesverwaltung zuzurechnenden Netzen.

Absatz 5 und 6:

Gefahren für die Sicherheit in der Informationstechnik gehen insbesondere von Schadprogrammen sowie von Sicherheitslücken in informationstechnischen Systemen aus, die in den Absätzen 5 und 6 legaldefiniert werden.

Die Definition von Schadprogrammen in Absatz 5 entspricht im Wesentlichen der auch in der Informationstechnik üblichen Terminologie. Maßgeblich ist, dass die Programme dem Zweck dienen, unbefugt unerwünschte Funktionen auszuführen. Nicht erfasst sind damit unbeabsichtigte Sicherheitslücken in normalen Programmen. Diese Funktionen können typischerweise Schäden verursachen, dies ist aber keine zwingende Voraussetzung. Moderne Schadprogramme zeichnen sich gerade dadurch aus, dass sie möglichst unauffällig und klein sind. Schadfunktionen sind zunächst nicht enthalten, können aber ggf. nachgeladen werden. Auch der Versand von Spam, also die massenhafte Versendung unerwünschte Emails, oder sogenannte DoS-Angriffe (Denial of Service, Massenanfragen, um Server durch Überlastung lahmzulegen) sind informationstechnische Routinen, die geeignet sind, unbefugt informationstechnische Prozesse zu beeinflussen.

Sicherheitslücken sind hingegen unerwünschte Eigenschaften von informationstechnischen Systemen, insbesondere Computerprogrammen, die es Dritten erlauben, gegen den Willen des Berechtigten dessen Informationstechnik zu beeinflussen. Eine Beeinflussung muss nicht zwingend darin bestehen, dass sich der Angreifer Zugang zum System verschafft und dies dann manipulieren kann. Es genügt auch, dass die Funktionsweise in sonstiger Weise beeinträchtigt werden kann, z.B. durch ein ungewolltes Abschalten. Der Begriff ist notwendigerweise weit gefasst, da Sicherheitslücken in den unterschiedlichsten Zusammenhängen, oftmals abhängig von der Konfiguration oder Einsatzumgebung, entstehen können.

Absatz 7:

Das Zertifizierungsverfahren des BSI entspricht den Vorgaben der einschlägigen technischen Normen. Um dies auch gesetzlich abzubilden, wird der Begriffe der Zertifizierung in Anlehnung an die insbesondere in der Norm EN ISO/IEC 17000 verwendeten Begriffe definiert.

Die Prüfung und Bestätigung der Konformität im Bereich der IT-Sicherheit beinhaltet zentral die IT-Sicherheitsfunktionalität ergänzt um Interoperabilität und operationelle Funktio-

nalitätsaspekte, insbesondere bei Auflagen, die die Produkte und die Komponenten in bestimmten Systemen bzw. Netzverbünden erfüllen müssen.

Absatz 8 und 9

Störungen, Fehlfunktionen von und Angriffe auf IT-Systeme können technisch oft durch eine Analyse der Protokolldaten erkannt werden. Protokolldaten sind in erster Linie die Steuerdaten, die bei jedem Datenpaket mit übertragen werden, um die Kommunikation zwischen Sender und Empfänger technisch zu gewährleisten. Hinzu treten die Daten, die zwar nicht mit übertragen, aber im Rahmen der Protokollierung von den Servern im Übertragungsprotokoll miterfasst werden, insbesondere Datum und Uhrzeit des Protokolleintrags und ggf. Absender und Weiterleitungskennungen. Von besonderer Relevanz für die Erkennung und Abwehr von IT-Angriffen sind die Kopfdaten (sog. Header) der gängigen Kommunikationsprotokolle (IP, ICMP, TCP, UDP, DSN http und SMTP). Sofern die Datenübertragung zugleich einen Telekommunikationsvorgang darstellt (z.B. das Senden einer Email), sind die Protokolldaten zugleich Verkehrsdaten im Sinne des TKG. Entsprechendes gilt hinsichtlich Protokolldaten, die bei der Nutzung von Telemedien anfallen. Die eigentlichen Kommunikationsinhalte sind nicht Bestandteil der Protokolldaten.

Datenverkehr umfasst dabei die Datenübertragung im Netz mittels technischer Protokolle. Die herkömmliche Telekommunikation (Sprache, Fax) ist hiervon nicht erfasst. Der Datenverkehr kann auch Telekommunikationsinhalte umfassen, sofern die Datenübertragung zugleich einen Telekommunikationsvorgang darstellt.

Zu Nr. 2 (§ 3)

§ 3 zählt die gesetzlichen Aufgaben des BSI auf. Die Aufgabennormen des § 3 selbst enthalten keine Eingriffsbefugnisse des BSI. Sie hindern auch andere Behörden nicht daran, im Rahmen ihrer Zuständigkeiten vergleichbare Aufgaben wahrzunehmen. Dem Bundesministerium der Verteidigung bleibt es unbenommen, eigene militärspezifische informationstechnische Sicherheitsvorkehrungen zu entwickeln, zu prüfen, zu bewerten und zuzulassen.

Zu Buchstabe a)

Zu Buchstabe aa)

Redaktionelle Anpassung.

Zu Buchstabe bb)

Diese Vorschriften erweitern die Aufgaben des BSI, um die Grundlage für die in §§ 4 bis 7 neu zu schaffenden Befugnisse zu bilden. Der konkrete Umfang der Aufgabenwahrnehmung richtet sich nach diesen Befugnisnormen. Diese neuen Aufgaben des BSI nimmt dieses im Rahmen seiner Befugnisse nach den §§ 4 ff. wahr.

Zu Buchstabe cc)

Redaktionelle Anpassungen der Legaldefinition. Klargestellt wird außerdem, dass die Aufgaben nach Nr. 3 die wissenschaftliche Forschung im Rahmen der gesetzlichen Aufgaben des BSI mit umfassen.

Zu Buchstabe dd)

Klarstellung ergänzend zu § 2 Abs. 7.

Zu Buchstabe ee)

Klarstellung ergänzend zu § 2 Abs. 7.

Zu Buchstabe ff) und gg)

Nr. 7 und Nr. 8:

Die Aufgaben der bisherige Nr. 4 wird zur besseren Verständlichkeit auf zwei Nummern aufgeteilt und die Aufgabenbeschreibung an die technische Entwicklung angepasst: Der Betrieb von Krypto- und Sicherheitsmanagementsystemen, z.B. Public Key Infrastructures (PKI) zur Verteilung von Schlüsseldaten, ist eine notwendige Ergänzung der Schlüsselherstellung in modernen Kommunikationssystemen. Außerdem wird die Legaldefinition von Verschlusssachen durch Bezugnahme auf die des SÜG vereinheitlicht.

Nr. 9:

Die Aufgaben des technischen Geheimschutzes sollen wegen des engen Sachzusammenhangs und des erforderlichen informationstechnischen Know-Hows durch das BSI wahrgenommen werden. Die Vorschrift entspricht der Formulierung § 3 Abs. 2 Nr. 3 BVerfSchG. Das Bundesamt ist insbesondere für die Durchführung von Abstrahlsicherheits- und Lauschabwehrprüfungen, Penetrationstests sowie die Abnahme von technischen Sicherheitseinrichtungen nach der VSA zuständig.

Nr. 10:

Die Aufgabennorm bildet die Grundlage für die Befugnisse nach § 7 Abs. 1 und 2.

Nr. 11:

Die Aufgabennorm bildet die Grundlage für die Befugnisse nach § 7 Abs. 3.

Zu Buchstabe hh)

Redaktionelle Anpassung. Neben den im Gesetz bislang allein aufgeführten Verfassungsschutzbehörden sind hier auch die Nachrichtendienste (BND, MAD) zu nennen.

Zu Buchstabe ii)

Klarstellung, dass die Beratungsaufgaben auch Warnmeldungen umfassen.

Zu Buchstabe jj)

Seit einigen Jahren haben Staat und Wirtschaft erkannt, dass Unternehmen, insbesondere solche, die als kritische Infrastrukturen angesehen werden, durch Angriffe gegen die Kommunikations- und Informationstechnik empfindlich betroffen sein können. Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen einträten. Deshalb wird es von staatlicher Seite und der Wirtschaft für erforderlich gehalten, auf freiwilliger Basis Kommunikationsstrukturen zur Krisenprävention und Krisenbewältigung vorzuhalten und sich gegenseitig zu informieren. Erste Arbeiten zur Früherkennung und Bewältigung von IT-Krisen sind abgeschlossen. Dem Bundesamt kommen in diesem Zusammenhang Aufbau- und Koordinierungsaufgaben zu, die gesetzlich abgesichert werden sollten.

Zu Buchstabe b)

Absatz 2 stellt klar, dass das BSI auch die Länder auf Ersuchen unterstützen kann. Ob das BSI diesem Ersuchen nachkommt, steht in seinem Ermessen.

Zu Nr. 3

§ 4

Die Vorschrift regelt die Funktion des BSI als zentrale Meldestelle für Informationssicherheit: Das BSI soll Informationen zu Sicherheitslücken, Schadprogrammen und IT-Sicherheitsvorfällen zentral sammeln und auswerten. Sind Informationen für andere Behörden von Interesse, weil diese z.B. bestimmte Software einsetzen, die von neu entdeckten Sicherheitslücken betroffen ist oder weil der Verdacht auf Straftaten besteht, informiert das BSI diese unverzüglich. Dies kann auch Erkenntnisse, die im Rahmen der Zusammenarbeit nach § 5 gewonnen werden, umfassen. Umgekehrt informieren Bundesbehörden das BSI, wenn dort Erkenntnisse z.B. zu neuen Schadprogrammen, neuen Angriffsmustern oder IT-Sicherheitsvorfällen gewonnen werden.

Die im Rahmen von § 4 übermittelten Informationen sind üblicherweise rein technischer Natur und haben keinen Personenbezug. Sollte im Einzelfall ein Personenbezug gegeben sein, richtet sich die Übermittlungsbefugnis nach den allgemeinen datenschutzrechtlichen Regelungen oder ggf. spezialgesetzlichen Regelungen.

Die Übermittlung und Weitergabe von eingestuften Informationen an das BSI durch die Nachrichtendienste des Bundes richtet sich nach dem BVerfSchG, dem MADG und dem BNDG. Dort bestehende Übermittlungsvorschriften können einer Übermittlung von Informationen i.S.d. § 4 Abs. 2 Satz 2 Nr. 1 an das BSI entgegenstehen.. Stellen, denen Kraft Verfassung oder Gesetz eine besondere Unabhängigkeit zukommt, wie dem Bundesbeauftragten für Datenschutz und Informationsfreiheit oder den Verfassungsorganen Bundestag, Bundesrat und dem Bundespräsidenten, sind von der Unterrichtungspflicht ausgenommen, wenn eine Übermittlung im Widerspruch zu dieser Unabhängigkeit stehen würde.

Die Einzelheiten des Meldeverfahrens, insbesondere hinsichtlich der Frage, welche Informationen für die Arbeit des BSI bzw. den Schutz der Informationstechnik des Bundes relevant sind, werden in Verwaltungsvorschriften des BMI mit Zustimmung des Rats der IT-Beauftragten der Bundesregierung festgelegt. Damit die Verwaltungsvorschriften rechtzeitig fertig gestellt werden können, tritt die Meldepflicht nach § 4 Absatz 3 erst zu einem späteren Zeitpunkt in Kraft (Art. 4). Das Instrument der allgemeinen Verwaltungsvorschriften wurde hier gewählt, um deutlich zu machen, dass die Bundesregierung nur im Rahmen ihrer Weisungsbefugnisse verbindliche Regelungen treffen kann. Andere Verfassungsorgane sind an diese nicht gebunden.

§ 6:

Absatz 1 gibt dem BSI die Befugnis, zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes die in Absatz 1 aufgezählten Daten zu speichern und automatisiert auszuwerten.

Gemäß Nr. 1 kann das BSI Protokolldaten, also Logfiles von Servern, Firewalls etc. erheben und automatisiert auswerten. Dies erfolgt zum einen, um Anzeichen für bevorstehende IT-Angriffe zu finden. Hierzu können die Logfiles automatisiert ausgewertet werden, z.B. hinsichtlich des Datenvolumens oder durch das automatisierte „Absurfen" von aus dem Bundesnetz heraus aufgerufenen URLs, um Phishing-Seiten zu identifizieren. Sofern Logfiles nach Absatz 1 Nr. 1 ausgewertet werten, darf diese nur anonymisiert erfolgen, d.h. ohne einen Bezug zu den Beteiligten des Kommunikationsvorgangs.

Von besonderer Relevanz für die Erkennung und Abwehr von IT-Angriffen sind die Kopfdaten (sog. Header) der gängigen Kommunikationsprotokolle (IP, ICMP, TCP, UDP, DSN http und SMTP). Die Begrenzung auf beim Betrieb der Kommunikationstechnik des Bundes anfallende Protokolldaten stellt klar, dass keine Datenerhebung bei Dritten von der Regelung erfasst wird.

Gemäß Nr. 2 kann das BSI auch automatisiert auf („technische") Telekommunikationsinhalte zugreifen, um diese auf Schadprogramme zu untersuchen oder auf Links zu Internetseiten, die ihrerseits Schadsoftware enthalten, die sich beim Aufruf versucht automatisch auf dem Rechner des Benutzers zu installieren. Dies betrifft den Einsatz von Virenscannern und ähnlichen Detektionstools, der bislang nur mit Einwilligung der Betroffenen möglich ist. Die automatisierte Auswertung gestattet nicht die Speicherung der Inhalte über den für die technische Abwicklung des Kommunikations- und Erkennungsvorgangs ohnehin notwendigen Umfang hinaus.

Soweit nicht eine Weiterverarbeitung nach Absatz 2 oder 3 ausnahmsweise zulässig ist, insbesondere weil sich ein konkreter Verdacht ergibt, sind die nach Absatz 1 erhobenen Daten sofort nach der Auswertung spurenlos zu löschen, so dass ein weitergehender Zugriff auf die Daten nicht mehr möglich ist (BVerfG v. 11.03.2008, 1BvR 2074/05, 1 BvR 1254/07). Protokolldaten nach Absatz 1 Nr. 1, die weder personenbezogene noch dem Fernmeldegeheimnis unterfallende Daten enthalten (z.B. Angaben zur Serverlast), unterfallen nicht der Löschungspflicht.

Eine personenbezogene Verwendung der Protokolldaten nach Absatz 1 Nr. 1 zu anderen Zwecken, insbesondere zur Erstellung von Kommunikationsprofilen oder der Verhaltens- und Leistungskontrolle von Mitarbeitern, ist ausgeschlossen.

Die Datenerhebung nach Nr. 2 erfolgt nur an den Schnittstellen der Kommunikationstechnik des Bundes. Die behördeninterne Kommunikation ist nicht erfasst. Die Datenverarbeitungsbefugnis nach Nr. 1 unterliegt diesen Beschränkungen zwar nicht, da im Einzelfall eine Untersuchung auch der innerhalb einer Behörde anfallenden Protokolldaten erforderlich sein kann. Insoweit ist allerdings die jeweils betroffene Behörde Herrin der Daten und kann die Datenverarbeitung nur im Einvernehmen mit dieser erfolgen.

Schadprogramme können regelmäßig erst mit einem zeitlichen Verzug von mehreren Tagen oder Wochen (abhängig von deren Verbreitung) detektiert werden. Wenn ein neues Schadprogramm gefunden wurde, besteht daher die Notwendigkeit, auch rückwirkend zu untersuchen, ob dieses bereits zuvor innerhalb der Bundesverwaltung verbreitet wurde, im hierdurch verursachte Schäden zu vermeiden oder zu begrenzen. Einzig zu diesem Zweck dürfen nach Absatz 2a die insoweit relevanten Protokolldaten im Sinne des Absatz 1 Nr. 1 auch länger gespeichert und im Falle eines bei Abgleich der Daten nach Absatz 1 Nr. 2 bestätigten Fundes automatisiert auf weitere Verdachtsfälle ausgewertet werden. Im Trefferfall erfolgt die Weiterverarbeitung der trefferrelevanten Daten nach Absatz 2. Die Vorgaben des Absatz 2a sind auch durch organisatorische und technische Maßnahmen sicherzustellen. Die Dauer der Speicherung ist abhängig von der technischen Entwicklung und richtet sich danach, innerhalb welcher Zeit nach dem ersten Auftreten ein Schadprogramm in der Regel durch die Detektionsmechanismen des BSI erkannt wird. Derzeit liegen zwischen dem Auftreten eines neuen Schadprogramms und deren Erkennbarkeit im Rahmen der Maßnahmen nach Absatz 1 in der Regel etwa 3 Monate. Nach Ablauf dieser Zeitspanne sind die Protokolldaten spurenlos zu löschen.

Wenn, insbesondere aufgrund der Maßnahmen nach Absatz 1, ein konkreter Verdacht auf das Vorliegen eines Schadprogramms besteht, sind nach Absatz 3 weitergehende Maßnahmen möglich. In einem ersten Schritt sind diejenigen Untersuchungen zulässig, um den konkreten Verdacht zu bestätigen oder zu widerlegen. Im Falle eines Fehlalarms ist die betroffene Behörde bzw. der betroffene Mitarbeiter, soweit feststellbar, hiervon zu unterrichten und sind die Daten, ggf. nach Weiterleitung an den ursprünglichen Adressaten,

wieder zu löschen. Im Falle der Bestätigung können die Daten zum Zweck der Abwehr des Schadprogramms oder ähnlicher Schadprogramme, z.B. durch Untersuchung der Funktionsweise des Schadprogramms, durch Aufnahme der Virensignatur o.ä. verwendet werden. Außerdem kann ein durch das Schadprogramm ausgelöster ungewollter Datenstrom detektiert und ggf. unterbunden werden. Dabei sind sie gemäß § 3a BDSG soweit möglich zu anonymisieren oder zu pseudonymisieren. Auch hiervon sind die betroffene Person oder Behörde zu unterrichten. Die Unterrichtung des Absenders des Schadprogramms dürfte im Regelfall nicht möglich sein, weil der Absender bereits technisch, etwa aufgrund von gefälschten Adressen, nicht ermittelbar ist. Die Unterrichtung unterbleibt ferner, wenn dieser schutzwürdige Belange Dritter entgegenstehen. Werden die Daten aufgrund der Befugnis nach Absatz 3 für ein Strafverfahren oder für Zwecke der Verfassungsschutzbehörden weiterverwendet, erfolgt die Benachrichtigung durch die insoweit zuständigen Behörden nach Maßgabe der für diese geltenden Vorschriften der Strafprozessordnung, der Polizeigesetze oder der Verfassungsschutzgesetze.

Angriffe auf die IT des Bundes stellen regelmäßig auch Straftaten oder eine Gefahr für die öffentliche Sicherheit und Ordnung dar. Absatz 4 gestattet dem BSI daher über den eigentlichen Zweck der Gefahrenabwehr hinaus, die Daten auch an die insoweit zuständigen Behörden zu übermitteln, sofern die Daten auch nach den für diese Behörden geltenden Vorschriften erhoben werden dürften. Dasselbe gilt für die Verfassungsschutzbehörden von Bund und Ländern, insbesondere im Falle des Verdachts einer sicherheitsgefährdenden oder geheimdienstlichen Tätigkeit für eine fremde Macht im Sinne des § 18 Bundesverfassungsschutzgesetz.

Eine darüber hinaus gehende Nutzung oder Verarbeitung von Telekommunikationsinhalten, insbesondere des semantischen Inhalts, ist untersagt (Absatz 5). Wird im Rahmen der Überprüfung nach Absatz 2 festgestellt, dass Daten dem Kernbereich privater Lebensgestaltung zuzurechnen sind, sind diese unverzüglich zu löschen und ist die Tatsache ihrer Erlangung und Löschung aktenkundig zu machen. Auf eine Pflicht zur begleitenden Kernbereichskontrolle wurde verzichtet, da diese gegenüber der eigentlichen Maßnahme einen größeren Grundrechtseingriff darstellte: Die Inhaltsauswertung durch das BSI beschränkt sich auf die Durchsicht der technischen Steuerbefehle. Semantische Inhalte können hierbei allenfalls als Zufallsfunde in Ausnahmefällen erkannt werden. Eine ständige Kontrolle auf Kernbereichsrelevanz würde hingegen die inhaltliche Auswertung auch der „menschlichen" Kommunikationsanteile erforderlich machen.

Da Ziel der Maßnahmen die Suche nach Schadprogrammen, also technischen Inhalten, aber nicht die Auswertung der eigentlichen Kommunikationsinhalte ist, ist ein Richtervorbehalt wie bei den vergleichbaren Regelungen in § 64 Abs. 1 TKG oder § 14 Abs. 7 EMVG nicht erforderlich.

Die Befugnisse des BSI im § 6 erlauben eine Erhebung und Verarbeitung von personenbezogenen Daten. Diese unterliegt gemäß § 24 BDSG der Kontrolle durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI). Vor Aufnahme der Datenverarbeitung hat das BSI ein Datenschutzkonzept zu erstellen und für Prüfungen durch den BfDI bereit zu halten. Aufgrund der hohen Verantwortung der Ressorts gegenüber der Vertraulichkeit der Kommunikation der Mitarbeiter und Mitarbeiterinnen, soll der BfDI neben der Berichtspflicht aus § 24 Absatz 5 Satz 1 BDSG auch den Rat der IT-Beauftragten der Bundesregierung über das Ergebnis seiner Kontrollen informieren.

§ 6c

Die Vorschrift konkretisiert die Löschungspflichten nach dem Bundesdatenschutzgesetz sowie nach § 6, wenn erhobene personenbezogene oder personenbeziehbare Daten (z.B. Email-Adressen in Logfiles) nicht mehr benötigt werden. Im Übrigen gelten die Vorschrif-

ten des Bundesdatenschutzgesetzes (BDSG) für die Verarbeitung personenbezogener Daten durch das BSI. So sind personenbezogene Daten insbesondere nach Maßgabe des § 3a BDSG zu anonymisieren oder zu pseudonymisieren und gilt das Gebot der Datensparsamkeit.

§ 6d

Die Vorschrift regelt die genauen Umstände, unter denen das BSI aufgrund von gewonnen Erkenntnissen über Sicherheitslücken oder Schadprogramme die Öffentlichkeit oder betroffene Stellen informieren darf und Produktwarnungen oder –empfehlungen aussprechen kann. Warnungen gegenüber Bundesbehörden regelt § 4 Abs. 2.

§ 7

Absatz 1

Absatz 1 regelt die Befugnis des BSI, allgemeine technische Mindeststandards für die IT-Sicherheit zu machen, wie dies bereits heute z.B: in Form des Grundschutzhandbuchs oder in Prüfvorschriften erfolgt. Soweit erforderlich kann das Bundesministerium des Innern mit Zustimmung des Rats der IT-Beauftragten der Bundesregierung bestimmte Vorgaben als allgemeine Verwaltungsvorschriften erlassen und dadurch für die Bundesverwaltung für verbindlich erklären. Dies kann eingeschränkt werden, z.B. auf bestimmte Einsatzszenarien. . Das Instrument der allgemeinen Verwaltungsvorschriften wurde hier gewählt, um deutlich zu machen, dass die Bundesregierung nur im Rahmen ihrer Weisungsbefugnisse verbindliche Regelungen treffen kann. Andere Verfassungsorgane sind an diese nicht gebunden. Die Ausnahme hinsichtlich der Zustimmungsbedürftigkeit des Erlasses einer allgemeinen Verwaltungsvorschrift beruht auf der besonderen Bedeutung der ressortübergreifenden Netze der Bundesregierung und ihres Schutzes und entspricht dem im Umsetzungsplan Bund vom Bundeskabinett verabschiedeten IT-Sicherheitskonzept für die Bundesverwaltung. Die Sicherheit der ressortübergreifenden Netze hängt sowohl von den innerhalb des Netzes umgesetzten Sicherheitsvorkehrungen als auch von den Sicherheitsmaßnahmen der diese Netze nutzenden Behörden ab. Sicherheitslücken auf Behördenseite können dabei die Gesamtsicherheit des Regierungsnetzes und damit aller anderen Behörden gefährden

Absatz 2

Absatz 2 ermächtigt das BSI, für die Beschaffung von Informationstechnik verbindliche Richtlinien zu verfassen. Diese sind bei der Bedarfsfestlegung durch die beschaffende Stelle zu berücksichtigen. Dies beinhaltet z.B. Vorschriften zur Risikoanalyse, zur Auswahl und zu den IT-Sicherheits-Anforderungen, die z.B. im Rahmen eines Vergabeverfahrens an die Eignung der Anbieter und die ausgeschriebenen Leistungen zu berücksichtigen sind. Ein einmal erworbenes unsicheres Produkt kann auch durch entsprechende Konfiguration in der Regel nicht mehr hinreichend abgesichert werden. Die so geschaffenen Sicherheitslücken können ggf. auch die Informationstechnik anderer vernetzter Behörden gefährden. Die steigende Abhängigkeit der Verwaltung von Informationstechnik einerseits, die zunehmende Komplexität und damit Angreifbarkeit dieser Technik andererseits machen es erforderlich, dass abstrakte Qualitätskriterien bereits für die Auswahl von Informationstechnik durch eine zentrale Stelle wie das BSI festgelegt werden.

Das Erfordernis der Abgabe der Verdingungsunterlagen an einen anhand unzulänglich aufgestellter Eignungskriterien ausgewählten Auftragnehmer kann bereits wegen der enthaltenen Leistungsanforderungen und sonstigen Informationen ein hohes Sicherheitsrisiko darstellen und die Sicherheitsinteressen der Bundesrepublik Deutschland gefährden.

Die vergaberechtlichen Vorschriften insbesondere des GWB bleiben unberührt. Die festzulegenden Anforderungen sollen den beschaffenden Behörden im Vorfeld von Vergabe-

verfahren Leitlinien an die Hand geben, wie Eignungsanforderungen und Leistungsanforderungen abhängig vom Einsatzzweck der Informationstechnik zu entwickeln und zu formulieren sind, um ein der Risikoeinschätzung entsprechendes Sicherheitsniveau zu erhalten. Soweit insbesondere auf die Ausnahme des § 100 Abs. 2 Buchstabe d) gestützte Vorschriften wie beispielsweise die Verschlusssachenanweisung besondere Vorgaben für öffentliche Beschaffungsvorgänge machen, gehen diese vor.

Absatz 3

Die Vorschrift regelt die Befugnis des BSI, bestimmte IT-Sicherheitsprodukte (z.B. Virenscanner, Firewalls, Verschlüsselungstechnik etc.) für die gesamte Bundesverwaltung selbst zu entwickeln oder öffentliche Aufträge zu vergeben. Ob das BSI von der Befugnis Gebrauch macht, steht in dessen Ermessen und ist insbesondere davon abhängig, ob eine Prognose ergibt, dass durch die zentrale Bereitstellung die IT-Sicherheit erhöht oder (zB durch Mengenrabatte) Kosten gespart werden können. Hierzu ist insbesondere im Vorfeld eine Bedarfsermittlung durchzuführen. Wenn das BSI von seiner Befugnis Gebrauch macht, sollen Bundesbehörden grundsätzlich nur diese BSI-Produkte einsetzen. Durch Beschluss des Rats der IT-Beauftragten der Bundesregierung kann die Abnahme für die Behörden verpflichtend gemacht werden.

Zu Nr. 4 (§ 8)

Absatz 1 und 2

§ 8 entspricht im Wesentlichen dem bisherigen § 4. Das Zertifizierungsverfahren soll durch die redaktionelle Überarbeitung besser als bisher im Gesetz abgebildet werden.

Absatz 1 stellt klar, dass das BSI die nationale Zertifizierungsstelle der Bundesverwaltung für IT-Sicherheit ist. Als solche erteilt das BSI das deutsche IT-Sicherheitszertifikat. Das Recht anderer, insbesondere privatwirtschaftlicher Stellen, eigene andere Zertifikate zu erteilen, bleibt hiervon unberührt. In Absatz 2 wird durch Umstellung der bisherigen Formulierung klargestellt, dass neben Produkten, Komponenten und Systemen auch Personen und IT-Sicherheitsdienstleister zertifiziert werden können. Damit ist das Bundesamt unter anderem für die Zertifizierung von Auditoren, Evaluatoren, Prüfern, Lauschabwehr- und Abstrahlprüfstellen zuständig. Spezialgesetzlich geregelte Befugnisse anderer Behörden, insbesondere der Bundesnetzagentur nach dem Signaturgesetz, sowie Zertifizierungsdienstleistungen der Wirtschaft bleiben unberührt.

Absatz 3

Im Rahmen von Zertifizierungsverfahren kann sich das BSI sachverständiger Stellen bedienen.

Absatz 4

Entspricht dem bisherigen § 4 Absatz 3.

Absatz 5

Folgeregelung zu Absatz 2.

Absatz 6

Absatz 6 regelt die Voraussetzungen für eine Anerkennung gemäß § 8 Abs. 3.

Absatz 7

Entspricht dem bisherigen § 4 Abs. 4. Es wird klargestellt, dass die Gleichwertigkeit eines Zertifikats durch das Bundesamt festgestellt werden muss.

Zu Nr. 5 (§ 9)

Redaktionelle Anpassungen.

Zu Nr. 6 (§ 10)

Durch die Befugnisse nach § 6 Abs. 2 und 3 wird in das Fernmeldegeheimnis aus Art. 10 GG eingegriffen. Durch § 10 wird dem Zitiergebot aus Art. 19 Abs. 1 GG genüge getan.

Zu Nr. 7 (§ 11)

Einzelne Bestimmungen verweisen auf eine Zustimmung des Rats der IT-Beauftragten der Bundesregierung (IT-Rat). Dieser ist im Rahmen des IT-Steuerungskonzepts der Bundesregierung mit Beschluss des Bundeskabinetts vom Dezember 2007 eingerichtet worden. Sollte dieses Gremium wieder aufgelöst werden, gehen die Befugnisse auf die entsprechende Nachfolgeorganisation über, sollte er ersatzlos wegfallen oder nicht mehr zusammentreten, kann an die Stelle der Zustimmung des IT-Rats das Einvernehmen der Bundesministerien treten.

Kommt ein Beschluss des IT-Rats nicht zustande, z.B. weil keine Sitzung stattfindet oder auf dieser Ebene keine Einigung erzielt wird, kann dieser durch das Einvernehmen aller Ressorts ersetzt werden. Eine Ersetzung des IT-Rats-Beschlusses durch einen Beschluss der IT-Steuerungsgruppe ist nicht möglich.

Zu Nr. 8

Die bisherigen Paragraphen 6 bis 10 sind mittlerweile gegenstandslos und können daher gestrichen werden.

Zu Artikel 2 (Änderung des Telekommunikationsgesetzes)

§ 109 Abs. 2 TKG wird dahingehend ergänzt, dass die BNetzA ermächtigt wird, im Benehmen mit dem BSI einen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen zu erstellen und nach Anhörung der Hersteller und Betreiber von Telekommunikationsanlagen zu veröffentlichen, der als Grundlage für die nach Abs. 3 von den Unternehmen zu erstellenden Sicherheitskonzepten dienen soll, um insgesamt eine höhere Sicherheit sowohl in den Telekommunikations- und Datenverarbeitungssystemen als auch in den Telekommunikationsnetzen zu gewährleisten.

Der neue Satz 5 im Absatz 3 ermächtigt die BNetzA die Einhaltung der Sicherheitskonzepte bei den Verpflichteten in regelmäßigen Abständen überprüfen zu können.

Zu Artikel 3 (Änderung des Telemediengesetzes)

Das Telemediengesetz enthält keine dem § 100 Abs. 1 TKG entsprechende Bestimmung, die es Diensteanbietern ermöglicht, Nutzungsdaten (personenbezogene Daten eines Nutzers) für Zwecke der Sicherheit seiner technischen Einrichtungen zu erheben und zu verwenden, falls dies erforderlich ist. Hier besteht eine Lücke im Bereich der Erlaubnistatbestände des Telemediengesetzes, denn auch die Telemedienanbieter brauchen eine entsprechende Ermächtigung, beispielsweise um Angriffe (Denial of Service, Schadprogramme, Veränderung ihrer Webangebote von außerhalb) abwehren zu können. Zur Er-

kennung und Abwehr bestimmter Angriffe gegen Webseiten und andere Telemedien ist die Erhebung und jedenfalls kurzfristige Speicherung und Auswertung der Nutzungsdaten erforderlich. Diese soll durch den neuen § 15 Abs. 9 TMG, der sich an § 100 Abs. 1 TKG anlehnt, geschaffen werden. Dabei ist auch eine Weiterentwicklung der Angriffsmethoden zu berücksichtigen. Zur Durchführung von Angriffen werden neuerdings verstärkt auch manipulierte Webseiten genutzt. Für die Anbieter von (Telemedien)-Diensten im Internet bedeutet dies, dass sich die zu verfolgenden IT-Sicherheitsziele im Internet verändert haben. Sie müssen ihre Systeme nicht nur zum Selbstschutz gegen Manipulationen, Hacking oder Verfügbarkeitsangriffe schützen, sondern sie müssen heute ihre Systeme auch gegen Angriffe härten, die diese Systeme nur als Zwischenstation für Angriffe auf die Nutzer der Dienste missbrauchen. Technische Einrichtungen im Sinne dieser Vorschrift sind alle Einrichtungen, die der Diensteanbieter benötigt, um sein Telemedienangebot zur Verfügung zu stellen. Insbesondere ist das der Datenspeicher (Server), auf dem das Telemedienangebot zum Abruf bereitgehalten wird. Der Begriff der Störung ist umfassend zu verstehen als jede vom Diensteanbieter nicht gewollte Veränderung des Telemedienangebotes, also beispielsweise auch eine Veränderung, welche die technische Einrichtung selbst nur als Zwischenstation nutzt, um die Nutzer des Telemedienangebots anzugreifen.

Zu Artikel 4 (Inkrafttreten)

Die Vorschrift regelt das Inkrafttreten. Die Meldepflichten aus § 4 Absatz 3 treten abweichend erst am 01.01.2010 in Kraft, um die Erarbeitung der ausführenden Verwaltungsvorschriften zu ermöglichen.