

Gesetzentwurf

der Bundesregierung

Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes

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. Die Sicherheit der Informationstechnik (IT) 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 begegnet werden.

B. Lösung

Dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sollen Befugnisse eingeräumt werden, 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 Vollzugaufwand

Keine

2. Vollzugaufwand

Die neu zu schaffenden Befugnisse des BSI sind mit einem entsprechenden Vollzugaufwand 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 Vollzugaufwands zu rechnen.

Für die Wahrnehmung der übertragenen neuen Aufgaben aufgrund des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) benötigt das BSI ca. zehn zusätzliche Planstellen/Stellen sowie Personal- und Sachkosten in Höhe von ca. 1 180 000 Euro jährlich. Die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (BNetzA) benötigt für die Wahrnehmung der in § 109 des Telekommunikationsgesetzes (TKG) definierten neuen Aufgaben zusätzlich drei Planstellen des gehobenen technischen Dienstes sowie Personal- und Sachkosten in Höhe von ca. 300 000 Euro jährlich. Die Kosten werden Gegenstand der Haushaltsaufstellung 2010 sein.

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. Informationspflichten für Bürgerinnen und Bürger entstehen nicht.

BUNDESREPUBLIK DEUTSCHLAND
DIE BUNDESKANZLERIN

Berlin, 16. Februar 2009

An den
Präsidenten des
Deutschen Bundestages
Herrn Dr. Norbert Lammert
Platz der Republik 1
11011 Berlin

Sehr geehrter Herr Präsident,

hiermit übersende ich den von der Bundesregierung beschlossenen

Entwurf eines Gesetzes zur Stärkung der Sicherheit in der
Informationstechnik des Bundes

mit Begründung und Vorblatt.

Ich bitte, die Beschlussfassung des Deutschen Bundestages herbeizuführen.

Federführend ist das Bundesministerium des Innern.

Die Stellungnahme des Nationalen Normenkontrollrates gemäß § 6 Abs. 1 NKRG
ist als Anlage 2 beigefügt.

Der Gesetzentwurf ist dem Bundesrat am 23. Januar 2009 als besonders
eilbedürftig zugeleitet worden.

Die Stellungnahme des Bundesrates zu dem Gesetzentwurf sowie die Auffassung
der Bundesregierung zu der Stellungnahme des Bundesrates werden
unverzüglich nachgereicht.

Mit freundlichen Grüßen



Anlage 1

Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes¹

Vom ...

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1

Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG)

§ 1

Bundesamt für Sicherheit in der Informationstechnik

Der Bund unterhält ein Bundesamt für Sicherheit in der Informationstechnik als Bundesoberbehörde. Es untersteht dem Bundesministerium des Innern.

§ 2

Begriffsbestimmungen

(1) Die Informationstechnik im Sinne dieses Gesetzes umfasst alle technischen Mittel zur Verarbeitung oder Übertragung von Informationen.

(2) Sicherheit in der Informationstechnik im Sinne dieses Gesetzes bedeutet die Einhaltung bestimmter Sicherheitsstandards, die die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von Informationen betreffen, durch Sicherheitsvorkehrungen

1. in informationstechnischen Systemen, Komponenten oder Prozessen oder
2. bei der Anwendung von informationstechnischen Systemen, Komponenten oder Prozessen.

(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 nicht öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen, des Bundestages, des Bundesrates, des Bundespräsidenten und des Bundesrechnungshofes ist nicht Kommunikationstechnik des Bundes, soweit sie ausschließlich in deren eigener Zuständigkeit betrieben wird.

(4) Schnittstellen der Kommunikationstechnik des Bundes im Sinne dieses Gesetzes sind sicherheitsrelevante Netzwerkübergänge innerhalb der Kommunikationstechnik des Bundes sowie zwischen dieser und der Informationstechnik

der einzelnen Bundesbehörden, Gruppen von Bundesbehörden oder Dritter. Dies gilt nicht für die Komponenten an den Netzwerkübergängen, die in eigener Zuständigkeit der in Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane betrieben werden.

(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.

§ 3

Aufgaben des Bundesamtes

(1) Das Bundesamt fördert die Sicherheit in der Informationstechnik. Hierzu nimmt es folgende Aufgaben wahr:

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;

¹ Die Verpflichtungen aus der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22. Juni 1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 204, S. 37), zuletzt geändert durch die Richtlinie 2006/96/EG vom 20. November 2006 (ABl. L 363, S. 81) sind beachtet worden.

3. Untersuchung von Sicherheitsrisiken bei Anwendung der Informationstechnik sowie Entwicklung von Sicherheitsvorkehrungen, insbesondere von informationstechnischen Verfahren und Geräten für die Sicherheit in der Informationstechnik (IT-Sicherheitsprodukte), soweit dies zur Erfüllung von Aufgaben des Bundes erforderlich ist, einschließlich der Forschung im Rahmen seiner gesetzlichen Aufgaben;
4. Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und für die Prüfung und Bewertung der Konformität im Bereich der IT-Sicherheit;
5. Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und Erteilung von Sicherheitszertifikaten;
6. Prüfung und Bestätigung der Konformität im Bereich der IT-Sicherheit von informationstechnischen Systemen und Komponenten mit technischen Richtlinien des Bundesamtes;
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;
8. Herstellung von Schlüsseldaten und Betrieb von Krypto- und Sicherheitsmanagementsystemen für informationssichernde 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 amtlich geheim gehaltener 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;
12. Unterstützung der für Sicherheit in der Informationstechnik zuständigen Stellen des Bundes, insbesondere soweit sie Beratungs- oder Kontrollaufgaben wahrnehmen; dies gilt vorrangig für den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, dessen Unterstützung im Rahmen der Unabhängigkeit erfolgt, die ihm bei der Erfüllung seiner Aufgaben nach dem Bundesdatenschutzgesetz zusteht;
13. Unterstützung
 - a) der Polizeien und Strafverfolgungsbehörden bei der Wahrnehmung ihrer gesetzlichen Aufgaben,
 - b) der Verfassungsschutzbehörden bei der Auswertung und Bewertung von Informationen, die bei der

Beobachtung terroristischer Bestrebungen oder nachrichtendienstlicher Tätigkeiten im Rahmen der gesetzlichen Befugnisse nach den Verfassungsschutzgesetzen des Bundes und der Länder anfallen,

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

Die Unterstützung darf nur gewährt werden, soweit sie erforderlich ist, um Tätigkeiten zu verhindern oder zu erforschen, die gegen die Sicherheit in der Informationstechnik gerichtet sind oder unter Nutzung der Informationstechnik erfolgen. Die Unterstützungsersuchen sind durch das Bundesamt aktenkundig zu machen;

14. Beratung und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;
15. Aufbau geeigneter Kommunikationsstrukturen zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung sowie Koordinierung der Zusammenarbeit zum Schutz der kritischen Informationsinfrastrukturen im Verbund mit der Privatwirtschaft.

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

§ 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 Absatz 2 Nummer 1 bekannt, die für die Erfüllung von Aufgaben oder die Sicherheit der Informationstechnik anderer Behörden von Bedeutung sind, unterrichten diese ab dem 1. Januar 2010 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 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 Absatzes 3.

§ 5

Abwehr von Schadprogrammen und Gefahren für die Kommunikationstechnik des Bundes

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

1. Protokoll- und Daten, 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 Protokoll- und Daten, sofern diese weder personenbezogene noch dem Fernmeldegeheimnis unterliegende Daten beinhalten. Behördeninterne Protokoll- und Daten dürfen nur im Einvernehmen mit der jeweils betroffenen Behörde erhoben werden.

(2) Protokoll- und Daten nach Absatz 1 Satz 1 Nummer 1 dürfen über den für die automatisierte Auswertung nach Absatz 1 Satz 1 Nummer 1 erforderlichen Zeitraum hinaus, längstens jedoch für 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 die Absätze 1 und 2 hinausgehende Verwendung personenbezogener Daten ist nur zulässig, wenn bestimmte Tatsachen den Verdacht begründen, dass

1. diese ein Schadprogramm enthalten,
2. diese 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 personenbezogener 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 oder in seiner Funktionsweise gehindert werden. Die nicht automatisierte Verwendung der Daten nach den Sätzen 1 und 2 darf nur durch einen Bediensteten des Bundesamtes mit der Befähigung zum Richteramt angeordnet 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 der Absätze 4 und 5 erfolgt die Benachrichtigung durch die dort genannten Behörden in entsprechender Anwendung der für diese Behörden geltenden Vorschriften. Enthalten diese keine Bestimmungen zu Benachrichtigungspflichten, sind die Vorschriften der Strafprozessordnung entsprechend anzuwenden.

(4) Das Bundesamt kann die nach Absatz 3 verwendeten personenbezogenen Daten an die Strafverfolgungsbehörden zur Verfolgung einer Straftat von erheblicher Bedeutung oder einer mittels Telekommunikation begangenen Straftat übermitteln. Es kann diese Daten ferner übermitteln

1. zur Abwehr einer Gefahr für die öffentliche Sicherheit, die unmittelbar von einem Schadprogramm ausgeht, an die Polizeien des Bundes und der Länder,
2. zur Unterrichtung über Tatsachen, die sicherheitsgefährdende oder geheimdienstliche Tätigkeiten für eine fremde Macht erkennen lassen, an das Bundesamt für Verfassungsschutz.

(5) Für sonstige Zwecke kann das Bundesamt die Daten übermitteln

1. 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,
2. an die Verfassungsschutzbehörden des Bundes und der Länder, wenn tatsächliche Anhaltspunkte für Bestrebungen in der Bundesrepublik Deutschland vorliegen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungsmaßnahmen gegen die in § 3 Absatz 1 des Bundesverfassungsschutzgesetzes genannten Schutzgüter gerichtet sind.

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

(6) Eine über die vorstehenden Absätze hinausgehende inhaltliche Auswertung zu anderen Zwecken und die Weiter-

gabe 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 des Bundesdatenschutzgesetzes 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.

(7) 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.

§ 6

Löschung

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 worden sind, oder für eine etwaige gerichtliche Überprüfung nicht mehr benötigt werden. Soweit die Löschung lediglich für eine etwaige gerichtliche Überprüfung von Maßnahmen nach § 5 Absatz 3 zurückgestellt ist, dürfen die Daten ohne Einwilligung des Betroffenen nur zu diesem Zweck verwendet werden; sie sind für andere Zwecke zu sperren. § 5 Absatz 6 bleibt unberührt.

§ 7

Warnungen

(1) Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 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 14 kann das Bundesamt die Öffentlichkeit unter Nennung der Bezeichnung und des Herstellers des betroffenen Produkts vor Sicherheitslücken in informationstechnischen Produkten und Diensten und vor Schad-

programmen 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.

§ 8

Vorgaben des Bundesamtes

(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, werden diese Inhalte im Benehmen mit dem Rat der IT-Beauftragten der Bundesregierung festgelegt. Für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach diesem Absatz empfehlenden Charakter.

(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. Die Sätze 4 und 5 gelten nicht für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane.

§ 9

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 ange-

messener 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.

§ 10

Ermächtigung zum Erlass von Rechtsverordnungen

(1) Das Bundesministerium des Innern bestimmt nach Anhörung der betroffenen Wirtschaftsverbände und im Einvernehmen mit dem Bundesministerium für Wirtschaft und Technologie durch Rechtsverordnung ohne Zustimmung des Bundesrates das Nähere über das Verfahren der Erteilung von Sicherheitszertifikaten und Anerkennungen nach § 9 und deren Inhalt.

(2) Für Amtshandlungen nach diesem Gesetz und nach den zur Durchführung dieses Gesetzes erlassenen Rechtsverordnungen werden Gebühren und Auslagen erhoben. Die Höhe der Gebühren richtet sich nach dem mit den Amtshandlungen verbundenen Verwaltungsaufwand. Das Bundesministerium des Innern bestimmt im Einvernehmen mit dem Bundesministerium der Finanzen durch Rechtsverordnung ohne Zustimmung des Bundesrates die gebührenpflichtigen Tatbestände, die Gebührensätze und die Auslagen.

§ 11

Einschränkung von Grundrechten

Das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) wird durch § 5 eingeschränkt.

§ 12

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.

Artikel 2

Änderung des Telekommunikationsgesetzes

§ 109 des Telekommunikationsgesetzes vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 2 des Gesetzes vom 21. Dezember 2007 (BGBl. I S. 3198) geändert worden ist, wird wie folgt geändert:

1. In Absatz 2 werden nach Satz 2 die folgenden Sätze 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. Absatz 3 wird wie folgt geändert:

- a) Nach Satz 4 wird folgender Satz eingefügt:

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

- b) Der bisherige 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 Dienstes genutzten technischen Einrichtungen erheben und verwenden. Absatz 8 Satz 2 und 3 gilt entsprechend.“

Artikel 4

Inkrafttreten, Außerkrafttreten

Dieses Gesetz tritt am Tag nach der Verkündung in Kraft. Gleichzeitig tritt das BSI-Errichtungsgesetz vom 17. Dezember 1990 (BGBl. I S. 2834), das zuletzt durch Artikel 25 der Verordnung vom 31. Oktober 2006 (BGBl. I S. 2407) geändert worden ist, außer Kraft.

Begründung

A. Allgemeiner Teil

I. Ziel und Inhalt des Entwurfs

Das Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSIG) ist 1991 in Kraft getreten und seitdem im Wesentlichen unverändert geblieben. Die an das Bundesamt für Sicherheit in der Informationstechnik (BSI) gestellten Erwartungen, welche Aufgaben es wahrnehmen soll, werden im Gesetz nicht mehr vollständig wiedergespiegelt.

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. Das 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-Sicherheitsaufgaben 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 Artikel 86 Satz 2 des Grundgesetzes (GG). Dies gilt auch, soweit in § 3 Absatz 1 Nummer 14, Absatz 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 Absatz 1 Nummer 11 GG). Dasselbe gilt für die Änderung des Telemediengesetzes. Die Berechtigung

des Bundes zur Inanspruchnahme dieser Gesetzgebungskompetenz ergibt sich aus 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, z. B. unterschiedliche Voraussetzungen für die Vergabe von Sicherheitszertifikaten, erhebliche Wettbewerbsverzerrungen und störende Schranken für die länderübergreifende Wirtschaftstätigkeit zur Folge hätten. Internationale Abkommen zur gegenseitigen Anerkennung von IT-Sicherheitszertifikaten setzen voraus, dass in jedem Staat nur eine einzige hoheitliche Zertifizierungsstelle existiert. 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 Artikel 73 Absatz 1 Nummer 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 Neufassung des BSIG in größerem Umfang wahrzunehmenden Aufgaben erfordern beim BSI zusätzliche zehn Planstellen/Stellen sowie Personal- und Sachkosten in Höhe von ca. 1 180 000 Euro jährlich. Der Personalbedarf resultiert aus den neu geschaffenen Aufgaben nach § 3 Absatz 1 Nummer 11 (zentrale Bereitstellung von IT-Sicherheitsprodukten), § 4 (zentrale Meldestelle), § 5 Absatz 1 bis 4 (Abwehr von Gefahren für die Kommunikationstechnik des Bundes) sowie aus der neu hinzukommenden Zertifizierung von Dienstleistern (§ 9) und der Mitwirkung bei der Erstellung eines Katalogs von Sicherheitsanforderungen für Telekommunikations- und

Datenverarbeitungssysteme (§ 109 Absatz 2 Satz 3 TKG). Der Mehrbedarf bei den Sachkosten verteilt sich auf den Betrieb eines Meldeportals für die Meldestellenfunktion (500 000 Euro p. a.) und die Bereitstellung von IT-Sicherheitsprodukten (100 000 Euro p. a.). Für die Wahrnehmung der neuen Aufgaben aus § 109 Absatz 2 Satz 3 und 4 TKG, Erstellen, Koordinieren und Pflegen eines Katalogs von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungsanlagen, und § 109 Absatz 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 Euro 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 der BSI-Kostenverordnung (BSI-KostV) 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 Absatz 2 Nummer 2 und Absatz 3 BSIG wird der Informationsaustausch zu Sicherheitslücken, 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 Absatz 2 Nummer 2 konkretisiert. Gegenüber den bisher bestehenden Strukturen, bei denen das BSI auf freiwillige bzw. zufällige Informationen angewiesen ist, schafft die Meldepflicht in § 4 Absatz 3 eine bessere Datenbasis und ermöglicht die zentrale Auswertung und Aufbereitung und Verteilung der IT-Sicherheitsinformationen an die übrigen Bundesbehörden. Würde das BSI nicht wie vorgesehen als zentrale Stelle tätig, müssten im Zweifel alle Bundesbehörden parallel derartige Strukturen und die erforderlichen technischen Fähigkeiten und Fertigkeiten 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 § 5 Abs. 3 Satz 5 (Benachrichtigungspflicht an Betroffene), Absatz 6 Satz 4 (Benachrichtigung des BMI bei Zweifeln über Kernbereichsrelevanz) und § 7 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 Ver-

braucherpreisniveau, 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 (BSI-Gesetz)

Zu § 1

Die Vorschrift legt fest, dass der Bund das BSI im Geschäftsbereich des Bundesministeriums des Innern (BMI) unterhält.

Zu § 2

Zu Absatz 1

Die Regelung bleibt unverändert.

Zu Absatz 2

Redaktionelle Anpassung der Legaldefinition.

Zu Absatz 3

Die neuen Befugnisse sollen sich auf den Schutz der Kommunikationstechnik des Bundes beziehen. Diese wird in § 2 Absatz 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). Die verfassungsrechtliche Stellung des Deutschen Bundestages, des Bundesrates und des Bundespräsidenten sowie der Bundesgerichte ist im Gesetz zu berücksichtigen. Deshalb ist deren Kommunikationstechnik, soweit sie in eigener Zuständigkeit betrieben wird, nicht Gegenstand dieses Gesetzes. In der Praxis besteht hier die Möglichkeit, z. B. für die Kommunikation der Richter einen „Bypass-Anschluss“ einzurichten, der unter Umgehung der innerhalb des Verwaltungsnetzes notwendigen Sicherheitsvorkehrungen einen unmittelbaren Anschluss an das Internet oder andere öffentliche Telekommunikationsnetze ermöglicht.

Zu 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 Behörden-

netzen oder den Netzen einer Gruppe von Behörden sowie zu Ländernetzen, dem Internet und anderen nicht der Bundesverwaltung zuzurechnenden Netzen. Ausgenommen hiervon ist ein direkter bzw. automatisierter Zugriff auf die Protokolldaten und Kommunikationsinhalte, die an den Komponenten der Netzwerkübergänge der in Absatz 3 Satz 2 genannten Verfassungsorgane und Gerichte erzeugt bzw. gespeichert werden, soweit diese in eigener Zuständigkeit betrieben werden.

Zu den Absätzen 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 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. Schadprogramme 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 unerwünschter E-Mails, oder sogenannte DoS-Angriffe (Denial of Service, Massenabfragen, 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 dieses 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.

Zu Absatz 7

Das Zertifizierungsverfahren des BSI entspricht den Vorgaben der einschlägigen technischen Normen. Um dies auch gesetzlich abzubilden, wird der Begriff der Zertifizierung in Anlehnung an die insbesondere in der Norm DIN EN ISO/IEC 17 000 verwendeten Begriffe definiert.

Die Prüfung und Bestätigung der Konformität im Bereich der IT-Sicherheit beinhaltet zentral die IT-Sicherheitsfunktionalität ergänzt um Interoperabilität und operationelle Funktionalitätsaspekte, insbesondere bei Auflagen, die die Produkte und die Komponenten in bestimmten Systemen bzw. Netzverbänden erfüllen müssen.

Zu Absatz 8

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, DNS, HTTP und SMTP). Sofern die Datenübertragung zugleich einen Telekommunikationsvorgang darstellt (z. B. das Senden einer E-Mail), sind die Protokolldaten zugleich Verkehrsdaten im Sinne des TKG. Entsprechendes gilt hinsichtlich der Protokolldaten, die bei der Nutzung von Telemedien anfallen. Die eigentlichen Kommunikationsinhalte sind nicht Bestandteil der Protokolldaten.

Zu Absatz 9

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

Zu § 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. Das Bundesministerium der Verteidigung kann für seinen Geschäftsbereich für die Verarbeitung oder Übertragung von Informationen eigene informationstechnische Sicherheitsvorkehrungen ergreifen, Systeme, Komponenten oder Prozesse entwickeln, prüfen, bewerten und zulassen, Schlüsseldaten herstellen und Krypto- und Sicherheitsmanagementsysteme betreiben sowie eigene Maßnahmen zur Abwehr von Gefahren für seine Informations- und Kommunikationstechnik ergreifen.

Zu Absatz 1

Zu den Nummern 1 und 2

Diese Vorschriften erweitern die Aufgaben des BSI, um die Grundlage für die in den §§ 4 bis 8 neu zu schaffenden Befugnisse zu bilden. Der konkrete Umfang der Aufgabewahrnehmung richtet sich nach diesen Befugnisnormen. Diese neuen Aufgaben nimmt das BSI im Rahmen seiner Befugnisse nach § 4 ff. wahr.

Zu Nummer 3

Die Vorschrift entspricht im Wesentlichen dem bisherigen § 3 Absatz 1 Nummer 1 BStG. Klargestellt wird, dass die Aufgaben nach Nummer 3 die wissenschaftliche Forschung im Rahmen der gesetzlichen Aufgaben des BSI mit umfassen.

Zu den Nummern 4 bis 6

Die Vorschriften entsprechen im Wesentlichen dem bisherigen § 3 Absatz 1 Nummer 2 und 3 BStG. Neben der Sicher-

heitszertifizierung wird auch die Konformitätsbewertung als eigenständige Aufgabe ergänzt. Sie enthalten eine Klarstellung ergänzend zu § 2 Absatz 8.

Zu den Nummern 7 und 8

Die Aufgaben der bisherigen Nummer 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 im Sicherheitsüberprüfungsgesetz enthaltene Begriffsbestimmung vereinheitlicht. Die Änderung der Nummerierung wird in der BSI-KostV nachvollzogen werden. Die Geheimschutzbetreuung von Unternehmen soll weiterhin kostenfrei bleiben.

Zu Nummer 9

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

Zu Nummer 10

Die Aufgabennorm bildet die Grundlage für die Befugnisse nach § 8 Absatz 1 und 2.

Zu Nummer 11

Die Aufgabennorm bildet die Grundlage für die Befugnisse nach § 8 Absatz 3.

Zu den Nummern 12 und 13

Die Regelungen entsprechen dem bisherigen § 3 Absatz 1 Nummer 5 und 6 BSIG. Neben den im Gesetz bislang allein aufgeführten Verfassungsschutzbehörden ist hier auch der Bundesnachrichtendienst (BND) zu nennen.

Zu Nummer 14

Die Vorschrift entspricht im Wesentlichen dem bisherigen § 3 Absatz 1 Nummer 7 BSIG. Es wird klargestellt, dass die Beratungsaufgaben auch Warnmeldungen umfassen.

Zu Nummer 15

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, erheb-

liche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten. 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 Absatz 2

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 § 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, informiert das BSI diese unverzüglich. 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 Bundesverfassungsschutzgesetz, dem MAD-Gesetz und dem BND-Gesetz. Dort bestehende Übermittlungsvorschriften können einer Übermittlung von Informationen im Sinne von § 4 Absatz 2 Satz 2 Nummer 1 an das BSI entgegenstehen. Stellen, denen kraft Verfassung oder Gesetzes eine besondere Unabhängigkeit zukommt, wie dem Bundesbeauftragten für den Datenschutz und die 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 fertiggestellt werden können, findet die Meldepflicht nach § 4 Absatz 3 erst ab 1. Januar 2010 Anwendung. 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 nicht an sie gebunden.

Zu § 5**Zu Absatz 1**

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

Gemäß Nummer 1 kann das BSI Protokolldaten, also sog. Logfiles von Servern, Firewalls usw. 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 sog. Phishingseiten zu identifizieren.

Von besonderer Relevanz für die Erkennung und Abwehr von IT-Angriffen sind die Kopfdaten (sog. Header) der gängigen Kommunikationsprotokolle (IP, ICMP, TCP, UDP, DNS, HTTP und SMTP).

Gemäß Nummer 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 beim Aufruf versucht, sich automatisch auf dem Rechner des Benutzers zu installieren. Dies betrifft den Einsatz von Virencannern 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 spurlos zu löschen, so dass ein weitergehender Zugriff auf die Daten nicht mehr möglich ist (BVerfG v. 11. März 2008, 1 BvR 2074/05, 1 BvR 1254/07). Protokolldaten nach Absatz 1 Nummer 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 Nummer 1 zu anderen Zwecken, insbesondere zur Erstellung von Kommunikationsprofilen oder der Verhaltens- und Leistungskontrolle von Mitarbeitern, ist ausgeschlossen.

Die Datenerhebung nach Nummer 2 erfolgt nur an den Schnittstellen der Kommunikationstechnik des Bundes. Die Begrenzung auf beim Betrieb der Kommunikationstechnik des Bundes anfallende Protokolldaten stellt klar, dass keine Datenerhebung bei Dritten von der Regelung erfasst wird. Die behördeninterne Kommunikation ist ebenfalls nicht erfasst.

Die Datenverarbeitungsbefugnis nach Nummer 1 unterliegt der letzteren Beschränkung 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; die Datenverarbeitung kann nur im Einvernehmen mit ihr vorgenommen werden.

Zu Absatz 2

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, um hierdurch verursachte Schäden zu vermeiden oder zu begrenzen. Einzig zu diesem Zweck dürfen nach Absatz 2 die insoweit relevanten Protokolldaten im Sinne des Absatzes 1 Nummer 1 auch länger gespeichert und im Falle eines bei Abgleich der Daten nach Absatz 3 Satz 2 bestätigten Fundes oder anderer Hinweise auf neue Schadprogramme automatisiert auf weitere Verdachtsfälle ausgewertet werden.

Die Dauer der Speicherung ist abhängig von der technischen Entwicklung und richtet sich danach, innerhalb welchen Zeitraums eine Rückschau auf bereits stattgefundene Angriffe verhältnismäßig ist. Sobald das BSI einen neuartigen Angriff unter Verwendung von Schadprogrammen entdeckt, werden die Protokolldaten nach Bezügen zu diesem neuen Angriff untersucht. Dies führt regelmäßig zur Entdeckung von ähnlichen Angriffen, die bereits stattgefunden haben. Aufgrund dieser Erkenntnisse werden die betroffenen Behörden informiert, um die notwendigen Maßnahmen zur Verhinderung von Schäden und zur Abwehr weiterer Angriffe treffen zu können. Die Speicherdauer von maximal drei Monaten ist auch angemessen: Nach den bisherigen Erfahrungen wird der größte Teil (ca. 80 Prozent) der Angriffe innerhalb der ersten drei Monate entdeckt, womit lediglich etwa 20 Prozent der Angriffe noch entdeckt würden, wenn die Daten länger als drei Monate gespeichert werden könnten. Unter Berücksichtigung des Schutzbedarfs der Behörden wird deshalb die maximale Speicherdauer der zur Erkennung von Schadprogrammen relevanten Protokolldaten auf drei Monate festgelegt. Nach Ablauf dieser Zeitspanne sind die Protokolldaten spurlos zu löschen.

Im Trefferfall erfolgt die Weiterverarbeitung der trefferrelevanten Daten nach Absatz 3. Die Vorgaben des Absatzes 2 sind auch durch organisatorische und technische Maßnahmen sicherzustellen.

Zu Absatz 3

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 die notwendigen Untersuchungen zulässig, die nötig sind, 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. Die Daten sind dann, 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. Dabei sind personenbezogene Daten gemäß § 3a BDSG soweit möglich zu anonymisieren oder zu pseudonymisieren. Außerdem kann ein durch das Schadprogramm ausgelöster ungewollter Datenstrom detektiert und ggf. unterbunden werden. Auch hiervon ist 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 Befugnisse nach Absatz 4 oder 5 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. So gilt z. B. für Mitteilungen durch das Bundesamt für Verfassungsschutz die Regelung des § 9 Abs. 3 BVerfSchG, nach dem bei den dort genannten besonders grundrechtsrelevanten Eingriffen eine Mitteilung an den Betroffenen erforderlich ist, sobald eine Gefährdung des Zweckes des Eingriffs ausgeschlossen werden kann. Soweit keine Regelung zur Benachrichtigung existiert, gelten die Vorschriften der Strafprozessordnung.

Zu Absatz 4

Angriffe auf die Informationstechnik des Bundes mittels Schadprogrammen stellen zugleich auch Straftaten oder eine Gefahr für die öffentliche Sicherheit dar. Absatz 4 Satz 1 gestattet dem BSI daher, die Daten auch an die insoweit zuständigen Behörden zu übermitteln, sofern dies zur Verfolgung einer Straftat von erheblicher Bedeutung oder einer mittels Telekommunikation begangenen Straftat erforderlich ist. Außerdem darf das BSI Daten im Rahmen des ursprünglichen Verwendungszwecks übermitteln, also wenn eine Gefahr für die öffentliche Sicherheit unmittelbar von dem gefundenen Schadprogramm ausgeht oder wenn ein nachrichtendienstlicher Hintergrund vorliegt.

Zu Absatz 5

Eine zweckändernde Übermittlung möglicher Zufallsfunde an die Polizeien oder Verfassungsschutzbehörden ist hingegen nur unter den engen Voraussetzungen des Absatzes 5 zulässig. Diese bedarf der gerichtlichen Zustimmung bzw., im Falle der Übermittlung an die Verfassungsschutzbehörden, der Beachtung des Verfahrens nach dem Artikel 10-Gesetz.

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 des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmitteln (EMVG) nur bei dieser zweckändernden Übermittlung erforderlich.

Zu Absatz 6

Eine darüber hinausgehende Nutzung oder Verarbeitung von Telekommunikationsinhalten, insbesondere des semantischen Inhalts, ist untersagt. Wird im Rahmen der Überprüfung nach Absatz 2 festgestellt, dass Daten dem Kernbereich privater Lebensgestaltung zuzurechnen sind, sind diese unverzüglich zu löschen; die Tatsache ihrer Erlangung und Löschung ist aktenkundig zu machen. Auf eine Pflicht zur begleitenden Kernbereichskontrolle wurde verzichtet, da diese gegenüber der eigentlichen Maßnahme einen stärkeren 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.

Zu Absatz 7

Die Befugnisse des BSI nach § 5 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 bereitzuhalten. 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.

Zu § 6

Die Vorschrift konkretisiert die Löschungspflichten nach dem Bundesdatenschutzgesetz sowie nach § 5, wenn erhobene personenbezogene oder personenbeziehbare Daten (z. B. E-Mail-Adressen in Logfiles) nicht mehr benötigt werden. Im Übrigen gelten für die Verarbeitung personenbezogener Daten durch das BSI die Vorschriften des Bundesdatenschutzgesetzes. So sind personenbezogene Daten insbesondere nach Maßgabe des § 3a Satz 2 BDSG zu anonymisieren oder zu pseudonymisieren; zudem gilt das Gebot der Datensparsamkeit nach § 3a Satz 1 BDSG.

Zu § 7

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 Absatz 2.

Zu § 8

Zu Absatz 1

Absatz 1 regelt die Befugnis des BSI, allgemeine technische Mindeststandards für die IT-Sicherheit zu entwickeln, 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. Für andere Verfassungsorgane sowie Bundesgerichte haben die Vorgaben lediglich empfehlenden Charakter.

Zu 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-Sicherheitsanforderungen, die z. B. im Rahmen eines Vergabeverfahrens an die Eignung der Anbieter und an die ausgeschriebenen Leistungen gestellt werden müssen. 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 Gesetzes gegen Wettbewerbsbeschränkungen (GWB) bleiben unberührt. Die festzulegenden Anforderungen sollen den beschaffenden Behörden im Vorfeld von Vergabeverfahren Leitlinien an die Hand geben, wie Eignungs- und Leistungsanforderungen abhängig vom Einsatzzweck der Informationstechnik zu entwickeln und zu formulieren sind, um ein der Risikoeinschätzung entsprechendes Sicherheitsniveau zu erhalten. Soweit Vorschriften des Geheimschutzes, wie beispielsweise die Verschlusssachenanweisung, besondere Vorgaben für öffentliche Beschaffungsvorgänge machen, gehen diese vor.

Zu Absatz 3

Die Vorschrift regelt die Befugnis des BSI, bestimmte IT-Sicherheitsprodukte (z. B. Virens Scanner, Firewalls, Verschlüsselungstechnik usw.) 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 (etwa durch Mengenrabatte) Kosten gespart werden können. Hierzu ist insbesondere im Vorfeld eine Bedarfsermittlung durchzuführen. Wenn das BSI von seiner Befugnis Gebrauch macht, kann die Abnahme für

die Behörden durch Beschluss des Rats der IT-Beauftragten der Bundesregierung verpflichtend gemacht werden.

Zu § 9

Zu den Absätzen 1 und 2

§ 9 entspricht im Wesentlichen dem bisherigen § 4 BSIG. 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. 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.

Zu Absatz 3

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

Zu Absatz 4

Entspricht dem bisherigen § 4 Absatz 3.

Zu Absatz 5

Folgerregelung zu Absatz 2.

Zu Absatz 6

Absatz 6 regelt die Voraussetzungen für eine Anerkennung gemäß § 9 Absatz 3.

Zu Absatz 7

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

Zu § 10

Redaktionelle Anpassung des bisherigen § 5 (Nennung auch der Auslagen in der Verordnungsermächtigung).

Zu § 11

Durch die Befugnisse nach § 5 Absatz 2 bis 5 wird in das Fernmeldegeheimnis aus Artikel 10 GG eingegriffen. Durch § 10 wird dem Zitiergebot aus Artikel 19 Absatz 1 GG Genüge getan.

Zu § 12

Einzelne Bestimmungen verweisen auf eine Zustimmung des Rats der IT-Beauftragten der Bundesregierung (IT-Rat), so § 4 Absatz 6 und § 8 Absatz 1 Satz 2 und Absatz 3 Satz 4. Dieser ist im Rahmen des IT-Steuerungskonzepts der Bun-

desregierung mit Beschluss des Bundeskabinetts vom Dezember 2007 eingerichtet worden und entscheidet einstimmig. 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, etwa 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 Artikel 2 (Änderung des Telekommunikationsgesetzes)

§ 109 Absatz 2 TKG wird dahingehend ergänzt, dass die Bundesnetzagentur 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 Absatz 3 von den Unternehmen zu erstellenden Sicherheitskonzepte dienen soll, um insgesamt eine höhere Sicherheit sowohl in den Telekommunikations- und Datenverarbeitungssystemen als auch in den Telekommunikationsnetzen zu gewährleisten.

Der neue Satz 5 in Absatz 3 ermächtigt die Bundesnetzagentur, 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 zu erheben und zu verwenden, falls dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen

seiner technischen Einrichtungen 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 Erkennung und Abwehr bestimmter Angriffe gegen Webseiten und andere Telemedien ist die Erhebung und kurzfristige Speicherung und Auswertung der Nutzungsdaten erforderlich. Diese soll durch den neuen § 15 Absatz 9 TMG, der sich an § 100 Absatz 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 des Diensteanbieters, die dieser benötigt, um sein Telemediensangebot zur Verfügung zu stellen. Insbesondere ist das der Datenspeicher (Server), auf dem das Telemediensangebot zum Abruf bereitgehalten wird. Der Begriff der Störung ist umfassend zu verstehen als jede vom Diensteanbieter nicht gewollte Veränderung der von ihm für sein Telemediensangebot genutzten technischen Einrichtungen, also beispielsweise auch eine Veränderung, welche die technische Einrichtung selbst nur als Zwischenstation nutzt, um die Nutzer des Telemediensangebots anzugreifen.

Zu Artikel 4 (Inkrafttreten, Außerkrafttreten)

Die Vorschrift regelt das Inkrafttreten. Zeitgleich tritt das bisherige BSI-Errichtungsgesetz außer Kraft.

Anlage 2**Stellungnahme des Nationalen Normenkontrollrates**

Der Nationale Normenkontrollrat hat das Regelungsvorhaben auf Bürokratiekosten, die durch Informationspflichten begründet werden, geprüft.

Mit dem Regelungsvorhaben werden fünf Informationspflichten für die Verwaltung neu eingeführt. Das Ressort hat die Informationspflichten und daraus resultierende bürokratische Auswirkungen nachvollziehbar dargestellt.

Danach dienen drei Informationspflichten der Wahrung der Rechte von Betroffenen und sind verfassungsrechtlich vorgegeben. Zwei Informationspflichten dienen dem verbesserten Informationsaustausch zu Sicherheitslücken und Sicherheitsvorkehrungen in der Informationstechnik. Dabei hat das Ressort deutlich gemacht, dass durch die zentrale Sammlung, Aufbereitung und Verteilung von IT-Sicherheitsinformationen durch das Bundesamt für Sicherheit in der Informationstechnik eine Regelungsalternative gewählt wurde, die im höchstmöglichen Maß Synergieeffekte nutzt.

Der Nationale Normenkontrollrat hat daher im Rahmen seines gesetzlichen Prüfauftrags keine Bedenken gegen das Regelungsvorhaben.

