Deutscher Bundestag **Drucksache 16/13259**

16. Wahlperiode 29. 05. 2009

Beschlussempfehlung und Bericht

des Innenausschusses (4. Ausschuss)

zu dem Gesetzentwurf der Bundesregierung – Drucksachen 16/11967, 16/12225 –

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

A. Problem

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.

Annahme des Gesetzentwurfs in geänderter Fassung mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN

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 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.

Beschlussempfehlung

Der Bundestag wolle beschließen,

den Gesetzentwurf auf Drucksache 16/11967 mit folgenden Maßgaben, im Übrigen unverändert anzunehmen:

1. Artikel 1 wird wie folgt geändert:
   a) § 5 wird wie folgt geändert:
      aa) Absatz 2 wird wie folgt geändert:
         aaa) Nach Satz 2 wird folgender Satz eingefügt:

         „Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist.“

         bbb) Nach dem neuen Satz 4 werden folgende Sätze angefügt:

         „Soweit hierzu die Wiederherstellung des Personenbezugs pseudonymisierter Daten erforderlich ist, muss diese durch den Präsidenten des Bundesamtes angeordnet werden. Die Entscheidung ist zu protokollieren.“

      bb) Absatz 3 wird wie folgt gefasst:

      „(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.“

      cc) Nach Absatz 3 wird folgender Absatz eingefügt:

      „(4) 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. Das Bundesamt legt Fälle, in denen es von einer Benachrichtigung absieht, dem behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem weiteren Bediensteten des Bundesamtes, der die Befähigung zum Richteramt hat, zur Kontrolle vor. Der behördliche Datenschutzbeauftragte ist bei Ausübung dieser Aufgabe wei-

sungsfrei und darf deswegen nicht benachteiligt werden (§ 4f Absatz 3 des Bundesdatenschutzgesetzes). Wenn der behördliche Datenschutzbeauftragte der Entscheidung des Bundesamtes widerspricht, ist die Benachrichtigung nachzuholen. Die Entscheidung über die Nichtbenachrichtigung ist zu dokumentieren. Die Dokumentation darf ausschließlich für Zwecke der Datenschutzkontrolle verwendet werden. Sie ist nach zwölf Monaten zu löschen. In den Fällen der Absätze 5 und 6 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."

dd) In dem neuen Absatz 5 Satz 1 werden die Wörter „einer Straftat von erheblicher Bedeutung oder einer mittels Telekommunikation begangenen Straftat" durch die Wörter „einer mittels eines Schadprogramms begangenen Straftat nach den §§ 202a, 202b, 303a oder 303b des Strafgesetzbuchs" ersetzt.

ee) Der neue Absatz 6 wird wie folgt gefasst:

„(6) Für sonstige Zwecke kann das Bundesamt die Daten übermitteln

1. an die Strafverfolgungsbehörden zur Verfolgung einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100a Absatz 2 der Strafprozessordnung bezeichneten Straftat,
2. an die Polizeien des Bundes und der Länder zur Abwehr einer Gefahr für den Bestand oder die Sicherheit des Staates oder Leib, Leben oder Freiheit einer Person oder Sachen von bedeutendem Wert, deren Erhalt im öffentlichen Interesse geboten ist,
3. an die Verfassungsschutzbehörden des Bundes und der Länder, wenn tatsächliche Anhaltspunkte für Bestrebungen in der Bundesrepublik Deutschland vorliegen, die durch Anwendung von Gewalt oder darauf gerichtete Vorbereitungshandlungen gegen die in § 3 Absatz 1 des Bundesverfassungsschutzgesetzes genannten Schutzgüter gerichtet sind.

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

ff) Der neue Absatz 7 wird wie folgt geändert:

aaa) Nach Satz 1 wird folgender Satz eingefügt:

„Soweit möglich, ist technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden."

bbb) Der neue Satz 5 wird wie folgt gefasst:

„Dies gilt auch in Zweifelsfällen."

ccc) Folgender Satz wird angefügt:

„Werden im Rahmen der Absätze 4 oder 5 Inhalte oder Umstände der Kommunikation von in § 53 Absatz 1 Satz 1 der Strafprozessordnung genannten Personen übermittelt, auf die sich das Zeugnisverweigerungsrecht der genannten Personen erstreckt,

ist die Verwertung dieser Daten zu Beweiszwecken in einem Strafverfahren nur insoweit zulässig, als Gegenstand dieses Strafverfahrens eine Straftat ist, die im Höchstmaß mit mindestens fünf Jahren Freiheitsstrafe bedroht ist.“

gg) In dem neuen Absatz 8 wird nach Satz 2 folgender Satz eingefügt:

„Die für die automatisierte Auswertung verwendeten Kriterien sind zu dokumentieren.“

hh) Folgende Absätze 9 und 10 werden angefügt:

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

1. die Anzahl der Vorgänge, in denen Daten nach Absatz 5 Satz 1, Absatz 5 Satz 2 Nummer 1 oder Absatz 6 Nummer 1 übermittelt wurden, aufgegliedert nach den einzelnen Übermittlungsbefugnissen,
2. die Anzahl der personenbezogenen Auswertungen nach Absatz 3 Satz 1, in denen der Verdacht widerlegt wurde,
3. die Anzahl der Fälle, in denen das Bundesamt nach Absatz 4 Satz 2 oder 3 von einer Benachrichtigung der Betroffenen abgesehen hat.

(10) Das Bundesamt unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Innenausschuss des Deutschen Bundestages über die Anwendung dieser Vorschrift.“

b) In § 6 Satz 3 wird die Angabe „6“ durch die Angabe „7“ ersetzt.

c) In § 7 Absatz 1 wird nach Satz 1 folgender Satz eingefügt:

„Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung von diese Produkte betreffenden Warnungen zu informieren, sofern hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks nicht gefährdet wird.“

d) § 8 Absatz 3 wird wie folgt geändert:

aa) Nach Satz 1 wird folgender Satz eingefügt:

„IT-Sicherheitsprodukte können nur in begründeten Ausnahmefällen durch eine Eigenentwicklung des Bundesamtes zur Verfügung gestellt werden.“

bb) In dem neuen Satz 7 wird die Angabe „4 und 5“ durch die Angabe „5 und 6“ ersetzt.

2. Artikel 3 wird aufgehoben.

3. Der bisherige Artikel 4 wird Artikel 3.

Berlin, den 27. Mai 2009

Der Innenausschuss

Sebastian Edathy Vorsitzender	**Clemens Binninger** Berichterstatter	**Frank Hofmann (Volkach)** Berichterstatter
	Gisela Piltz Berichterstatterin	**Ulla Jelpke** Berichterstatterin
	Wolfgang Wieland Berichterstatter	

Bericht der Abgeordneten Clemens Binninger, Frank Hofmann (Volkach), Gisela Piltz, Ulla Jelpke und Wolfgang Wieland

I. Zum Verfahren

1. Überweisung

Der Gesetzentwurf auf **Drucksache 16/11967** und die Gegenäußerung der Bundesregierung zu der Stellungnahme des Bundesrates auf **Drucksache 16/12225** wurden in der 211. Sitzung des Deutschen Bundestages am 19. März 2009 an den Innenausschuss federführend sowie an den Rechtsausschuss, den Ausschuss für Wirtschaft und Technologie, den Verteidigungsausschuss und den Ausschuss für Kultur und Medien zur Mitberatung überwiesen.

2. Voten der mitberatenden Ausschüsse

Der **Rechtsausschuss** hat in seiner 144. Sitzung am 27. Mai 2009 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN die Annahme des Gesetzentwurfs in der Fassung des Änderungsantrags der Koalitionsfraktionen der CDU/CSU und SPD auf Ausschussdrucksache 16(4)620 empfohlen.

Der **Ausschuss für Wirtschaft und Technologie** hat in seiner 95. Sitzung am 27. Mai 2009 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen FDP und DIE LINKE. bei Stimmenthaltung der Fraktion BÜNDNIS 90/DIE GRÜNEN empfohlen, den Gesetzentwurf in der Fassung des Änderungsantrags der Koalitionsfraktionen anzunehmen.

Der **Verteidigungsausschuss** hat in seiner 107. Sitzung am 27. Mai 2009 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN die Annahme des Gesetzentwurfs in der Fassung des Änderungsantrags der Koalitionsfraktionen empfohlen.

Der **Ausschuss für Kultur und Medien** hat in seiner 80. Sitzung am 27. Mai 2009 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN empfohlen, den Gesetzentwurf in der Fassung des Änderungsantrags der Koalitionsfraktionen anzunehmen.

3. Beratungen im federführenden Ausschuss

Der Innenausschuss hat in seiner 89. Sitzung am 25. März 2009 beschlossen, eine öffentliche Anhörung zum Gesetzentwurf auf Drucksache 16/11967 durchzuführen.

Die öffentliche Anhörung, an der sich sieben Sachverständige beteiligt haben, hat der Innenausschuss in seiner 94. Sitzung am 11. Mai 2009 durchgeführt. Hinsichtlich des Ergebnisses wird auf das Protokoll Nr. 16/94 hingewiesen.

Der **Innenausschuss** hat den Gesetzentwurf auf Drucksache 16/11967 in seiner 98. Sitzung am 27. Mai 2009 abschließend beraten. Als Ergebnis der Beratungen wurde mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktionen FDP, DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN empfohlen, den Gesetzentwurf der Bundesregierung auf Drucksache 16/11967 in der Fassung des Änderungsantrags der Koalitionsfraktionen auf Ausschussdrucksache 16(4)620 anzunehmen. Zuvor wurde der Änderungsantrag der Koalitionsfraktionen auf Ausschussdrucksache 16(4)620 mit den Stimmen der Fraktionen der CDU/CSU und SPD gegen die Stimmen der Fraktion der FDP bei Stimmenthaltung der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN angenommen.

II. Zur Begründung

1. Zur Begründung wird allgemein auf Drucksache 16/11967 hingewiesen. Die vom Innenausschuss auf Grundlage des Änderungsantrags der Koalitionsfraktionen auf Ausschussdrucksache 16(4)620 empfohlenen Änderungen begründen sich wie folgt:

   Zu Nummer 1

   Zu Buchstabe a

   aa) Die nach Absatz 2 gespeicherten Protokolldaten sind durch technische und organisatorische Maßnahmen vor Missbrauch zu schützen. Hierzu gehört insbesondere, soweit mit vertretbarem Aufwand möglich, die Ersetzung von personenbezogenen Daten durch Pseudonyme. Dies ist insbesondere hinsichtlich der in den Protokolldaten enthaltenen E-Mail-Adressen erforderlich, um die Erstellung von Kommunikationsprofilen zu verhindern. Um den Grundrechtseingriff nicht zu vertiefen, soll die Pseudonymisierung automatisiert erfolgen. Eine Entpseudonymisierung darf nur erfolgen, wenn dies für die Weiterverarbeitung nach Maßgabe der nachfolgenden Absätze erforderlich ist. Dies ist der Fall bei bestätigten Verdachtsfällen hinsichtlich eines Schadprogramms, um die Betroffenen warnen und erforderliche weitere Schutzmaßnahmen ergreifen zu können, sowie zur Erfüllung der Benachrichtigungspflichten nach Absatz 3. Die Entpseudonymisierung ist durch den Präsidenten anzuordnen und zu protokollieren. Technisch kann dies durch Verschlüsselung der entsprechenden Datenfelder erfolgen.

   bb) Zur besseren Lesbarkeit wird der Absatz 3 in zwei Absätze aufgeteilt.

   cc) Da es sich bei den Maßnahmen nach § 5 nicht um eine personen- oder inhaltsbezogene heimliche Überwachungsmaßnahme handelt, sondern lediglich um eine weitgehend automatisierte Suche nach technischen Schadfunktionen, bedarf die Durchführung der Aufgabe selbst nicht der richterlichen Anordnung. Um stattdessen eine nachträgliche Kontrolle hinsichtlich der auch nichtautomatisert verwendeten Daten zu ermöglichen, kommt der Benachrichtigung der Betroffenen eine besondere Bedeutung zu. Von der Benachrichtigung darf, wie auch nach § 101 Absatz 4 der Strafprozessordnung (StPO), nur in besonderen Ausnahmefällen abgewichen werden. Diese

Fälle sind dem behördlichen Datenschutzbeauftragten sowie einem weiteren Mitarbeiter, der die Befähigung zum Richteramt hat, zur Kontrolle vorzulegen. Hält einer der beiden eine Benachrichtigung für erforderlich, kann er die zuständigen Mitarbeiter oder die Behördenleitung hiervon in Kenntnis setzen. Der behördliche Datenschutzbeauftragte ist nach § 4f Absatz 3 des Bundesdatenschutzgesetzes (BDSG) in der Ausübung seines Amtes unabhängig. Die Letztentscheidung liegt beim behördlichen Datenschutzbeauftragten. Die Zahl der Fälle, in denen von einer Benachrichtigung abgesehen wird, unterliegt der Unterrichtungspflicht nach den Absätzen 9 und 10. Die Nichtbenachrichtigung ist für die Zwecke der Datenschutzkontrolle durch den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit oder durch die Gerichte zu dokumentieren und zwölf Monate aufzubewahren. Diese Dokumentation darf nicht für andere Zwecke verwendet werden.

dd) Für die zweckbewahrende Übermittlung von Verdachtsfällen nach Absatz 5 sind, anders als im Fall des § 100g Absatz 1 StPO, nicht alle mittels Telekommunikation begangenen Straftaten, sondern nur die Straftatbestände der §§ 202a, 202b, 303a oder 303b StGB einschlägig, sofern sie mittels eines Schadprogramms begangen worden sind.

ee) Die Übermittlung von Zufallsfunden soll höheren Schranken unterworfen sein als die zweckbewahrende Übermittlung bei Schadprogrammfunden. Absatz 6 sieht daher zusätzliche Schranken, insbesondere einen Richtervorbehalt vor.

Dieser Systematik soll auch die Übermittlung zu Strafverfolgungszwecken unterworfen werden. Daher wird die Übermittlungsbefugnis zur Verfolgung von Straftaten von erheblicher Bedeutung von Absatz 5 in Absatz 6 verschoben. Der Wortlaut entspricht § 100g Absatz 1 Nummer 1 StPO.

Die Änderung in Satz 2 dient der Klarstellung. Der Rechtsbegriff der Zustimmung umfasst im bürgerlichen Recht sowohl die Einwilligung (vorherige Zustimmung) als auch die Genehmigung (nachträgliche Zustimmung), vgl. Legaldefinitionen in § 183 Satz 1 und § 184 Absatz 1 des Bürgerlichen Gesetzbuchs (BGB). Die Übermittlungsfälle des § 5 Absatz 6 bedürfen allerdings der vorherigen Zustimmung.

Da mit dem Auftreten erster Übermittlungsfälle aufgrund des voraussichtlichen Zeitpunktes des Inkrafttretens nicht vor Anfang September 2009 zu rechnen ist, kann sogleich und ausschließlich auf das Gesetz über das Verfahren in Familiensachen und in den Angelegenheiten der freiwilligen Gerichtsbarkeit (FamFG) verwiesen werden. Das FamFG tritt am 1. September 2009 in Kraft und löst das Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit (FGG) ab.

ff) Dass dem Bundesamt bei der Suche nach Schadprogrammen kernbereichsrelevante Inhalte zur Kenntnis gelangen, ist unwahrscheinlich. Soweit möglich, sollte schon technisch sichergestellt werden, dass diese nicht erhoben werden (so auch § 20k Absatz 7 Satz 2 BKAG). Um etwaige Eingriffe gleichwohl möglichst gering zu halten, sollen diese Inhalte unverzüglich gelöscht werden. Dies soll auch dann geschehen, wenn Zweifel bestehen, ob die Inhalte kernbereichsrelevant sind oder nicht.

Für die Kommunikation von zeugnisverweigerungsberechtigten Berufsgruppen mit der Bundesverwaltung wird ein Beweisverwertungsverbot nach dem Vorbild des § 108 Absatz 3 StPO eingefügt. Anders als dort ist das Zeugnisverweigerungsrecht nicht auf Journalisten beschränkt.

gg) Neben dem (abstrakten) Datenschutzkonzept sind auch die im Rahmen der automatisierten Auswertung konkret verwendeten Kriterien (Überprüfungsroutinen, Virensignaturen) zu dokumentieren.

hh) Absatz 9 sieht zusätzliche Kontrollmöglichkeiten vor, indem eine Unterrichtungspflicht über die Zahl der zweckändernden Übermittlungen, der Fehltreffer („false positives“) und der Fälle, in denen aufgrund der Ausnahmetatbestände des Absatzes 4 Satz 2 und 3 von einer Benachrichtigung der Betroffenen abgesehen wurde, gegenüber dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit geschaffen wird.

Außerdem soll das Bundesamt nach Absatz 10 jährlich den Innenausschuss umfänglich über die Umsetzung dieser Vorschrift, insbesondere die Bedrohungslage und die technische Entwicklung, unterrichten. Die Unterrichtung nach Absatz 10 beinhaltet auch die Zahlen nach Absatz 9.

Zu Buchstabe b

Folgeänderung wegen der Absatzaufspaltung in § 5.

Zu Buchstabe c

Nach dem in der IT-Wirtschaft geübten Prinzip der verantwortungsvollen Weitergabe („responsible disclosure“) werden in der Regel zunächst die Hersteller betroffener Produkte über entdeckte Sicherheitslücken informiert, um diesen Gelegenheit zu geben, Sicherheits-Updates zu entwickeln und ihren Kunden zur Verfügung zu stellen. Dieses Prinzip soll auch im Rahmen des § 7 Absatz 1 Beachtung finden. Eine Vorabinformation Dritter, insbesondere der Öffentlichkeit, ist allerdings dann geboten, wenn der Zweck der Maßnahme sonst nicht erreicht würde (vgl. § 40 Absatz 3 des Lebensmittel- und Futtermittelgesetzbuchs).

Zu Buchstabe d

Aus Gründen der Wirtschaftlichkeit ist bei der Bereitstellung von IT-Sicherheitsprodukten grundsätzlich auf Produkte abzustellen, die am Markt erworben werden können. Spezifische Anforderungen der Verwaltung an Funktion und Sicherheit bestimmter Produkte haben allerdings teilweise zur Folge, dass keine geeigneten Produkte durch zuverlässige Hersteller am Markt angeboten werden. In solchen begründeten Ausnahmefällen kann das Bundesamt auch entsprechende Produkte selber entwickeln.

Zu den Nummern 2 und 3

Aufgrund der besonderen Eilbedürftigkeit der übrigen Regelungen des Gesetzentwurfs wird die Änderung des Telemedienrechts im Rahmen dieses Gesetzgebungsvorhabens nicht weiterverfolgt.

2. Die **Koalitionsfraktionen der CDU/CSU und SPD** betonen, der Bereich der Sicherheit in der Informationstechnik habe in den letzten Jahren mit der technischen Entwicklung nicht Schritt gehalten. Deutschland sei nicht hinreichend gegen Hackerangriffe geschützt, die die Infrastruktur bedrohten. Die überfällige gesetzliche Regelung, die jetzt vorgelegt werde, sei im parlamentarischen Verfahren noch einmal verbessert worden und trage den wichtigsten Kritikpunkten Rechnung. So habe man sich darauf verständigt, die Änderung des Telemediengesetzes in dieser Legislaturperiode nicht mehr weiter zu verfolgen. Hier seien noch einmal vertiefte Erörterungen mit allen Beteiligten erforderlich. Des Weiteren werde durch den Gesetzentwurf auch keineswegs ermöglicht, den gesamten Kommunikationsverkehr mit Bundesbehörden zu durchleuchten und jede E-Mail mitzulesen. Die Kontrolle erfolge vielmehr in einem automatisierten Verfahren, gleichsam in einer „Black-Box“. Nur wenn es Hinweise auf Schadprogramme gebe, erfolge eine Öffnung. Dateien, die solche Hinweise enthielten, würden zudem pseudonymisiert. Man habe auch die Übermittlung an andere Behörden durch den Verweis auf die Straftatbestände in § 100a Absatz 2 StPO enger gefasst und den Schutz zeugnisverweigerungsberechtigter Personen sowie die Benachrichtigungspflichten besser geregelt.

   Die **Fraktion der FDP** bezweifelt, dass der vorliegende Gesetzentwurf ein geeignetes Mittel sei, das durchaus begrüßenswerte Ziel zu erreichen, kritische Infrastrukturen besser zu schützen. In der Anhörung hätten die Sachverständigen den Gesetzentwurf insofern einhellig als untauglich angesehen. Auch wenn einige Erkenntnisse offenbar in den Änderungsantrag eingeflossen seien, bleibe bedauerlich, dass es keine hinreichende Pflicht zur Information der Öffentlichkeit gebe, dass man – wie in anderen Sicherheitsgesetzen – unklare und zu weit reichende Formulierungen verwendet habe und dass Berufsgeheimnisträger durch § 5 Absatz 7 nur unzureichend geschützt würden.

   Die **Fraktion DIE LINKE.** schließt sich der Kritik der Fraktion der FDP an und erklärt, die Anhörung habe ein erschütterndes Bild geboten. Die Sachverständigen hätten einhellig erklärt, dass das Gesetz das angestrebte Ziel nicht erreichen könne. Trotz der von der Koalition vorgenommenen Änderungen sei es immer noch so, dass mit diesem Gesetzentwurf unter dem Dach des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eine gigantische Kontrollbehörde für den gesamten IT-Bereich geschaffen werden solle. Des Weiteren sehe der Gesetzentwurf weiterhin vor, das Surfverhalten durch die Behörden des Bundes umfassend zu protokollieren.

   Die **Fraktion BÜNDNIS 90/DIE GRÜNEN** räumt ein, dass der Gesetzentwurf durch den Änderungsantrag verbessert werde. Nach wie vor sei aber nicht einzusehen, warum der Umgang mit Zufallsfunden breit im Gesetzentwurf geregelt werden müsse, wenn es wirklich nur um die Sicherheit in der Informationstechnik gehe. Es würde insofern reichen, bestimmte Ausnahmen für „ticking-bomb-Szenarios“ vorzusehen. Bei der Übermittlung habe man zwar die Hürden höher gelegt, es könne aber weiterhin zu viel vom BSI an andere Behörden weitergegeben werden. Die vorgesehene Pseudonymisierung könne auch wieder aufgehoben werden. Der Schutz von Berufsgeheimnisträgern schließlich sei zu schwach und willkürlich ausgestaltet.

Berlin, den 27. Mai 2009

Clemens Binninger Berichterstatter	**Frank Hofmann (Volkach)** Berichterstatter	**Gisela Piltz** Berichterstatterin
Ulla Jelpke Berichterstatterin	**Wolfgang Wieland** Berichterstatter	

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Amsterdamer Str. 192, 50735 Köln, Telefon (02 21) 97 66 83 40, Telefax (02 21) 97 66 83 44
ISSN 0722-8333