

(A) ~~Anträgen und Gesetzentwürfen in den Bundestag eingebracht.~~

~~Zentraler Aspekt einer neuen Beteiligungskultur ist die Absenkung des aktiven Wahlalters auf 16 Jahre. Wir haben dazu als einzige Fraktion einen Vorschlag zur Abstimmung gestellt. Dies ist der Weg, auf dem alle, die sich für mehr Beteiligung junger Menschen einsetzen, weiter vorangehen sollten! Vor allem die Kolleginnen und Kollegen von der SPD lade ich herzlich ein, den Worten ihres Parteivorsitzenden Müntefering Taten folgen zu lassen und unseren Gesetzentwürfen zur Absenkung des aktiven Wahlalters auf 16 Jahre zuzustimmen! Damit würden wir mehr und früher Demokratie wagen, das brächte mehr Generationengerechtigkeit und Jugendfreundlichkeit.~~

~~Die von einigen der Antragsteller vertretene These, die Einführung des Stellvertreterwahlrechts wäre im Gegensatz zum grünen Wahlalter 16 Vorschlag durch einfache Gesetzesänderung möglich, ist dagegen absurd. Das Stellvertreterwahlrecht könnte zwar kurzfristig in das Wahlgesetz geschrieben werden, bliebe jedoch verfassungswidrig und würde damit spätestens bei einer gerichtlichen Überprüfung nichtig.~~

~~Der Schaufenster Antrag zum Stellvertreterwahlrecht ist ein Fall fürs Parlamentsarchiv – jetzt muss es um ehrgeizige und vor allem umsetzbare Vorschläge zur Stärkung der demokratischen Rechte von Jugendlichen gehen. Und deshalb fordern wir als grüne Bundestagsfraktion geschlossen ein aktives Wahlrecht ab 16 Jahren.~~

(B) ~~Ich fordere alle auf, dabei mitzumachen, anstatt durch illusionäre Vorschläge eine Wahlalterherabsetzung zu verhindern!~~

Anlage 39

Zu Protokoll gegebene Reden**zur Beratung des Entwurfs eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes (Tagesordnungspunkt 41)**

~~**Clemens Binninger (CDU/CSU):** Die Informations- und Kommunikationstechnik entwickelt sich rasant. Das erleben wir jeden Tag. Deutschland hat bereits 1991 mit dem Bundesamt für Sicherheit in der Informationstechnik, BSI, eine Behörde geschaffen, die als zentraler Dienstleister zuständig für die IT-Sicherheit der Bundesverwaltung ist. Seit 1991 wurde die Rechtsgrundlage des BSI kaum verändert. Eine Novellierung ist daher überfällig. Mit dem Gesetz, das wir heute beraten, wird das BSI auch in Zukunft zu einem hohen Sicherheitsstandard für die IT-Struktur des Bundes und darüber hinaus beitragen können. An den relevanten Schnittstellen der IT-Infrastruktur von Bund und Ländern wird dies in Abstimmung geschehen, sofern die Länder betroffen sind.~~

~~IT-Sicherheit ist ein integraler Bestandteil innerer Sicherheit geworden. Die Informations- und Kommunikationstechnologie ist eine zentrale Voraussetzung für das~~

~~Funktionieren unseres Gemeinwesens. Vom Bankautomaten über die Energie- und Wasserversorgungen bis hin zu Flughäfen und Bahnhöfen ist die IT-Infrastruktur von zentraler Bedeutung. Angriffe auf diese Infrastruktur können immense Schäden anrichten. Davon sind auch die öffentliche Verwaltung und die Verwaltung des Bundes betroffen, sei es bei der täglichen Bürokommunikation via E-Mail im gemeinsamen Netz des Bundes, sei es im Sicherheitsbereich, wo es um den Zugriff auf sicherheitsrelevante Informationen geht. Nicht zuletzt ist auch sichere Kommunikation in Krisensituationen zu gewährleisten. Dies alles gilt es unter sich nahezu täglich verändernden Rahmenbedingungen angemessen zu schützen.~~

~~Um zu erkennen, dass diese Bedrohung für die IT-Infrastruktur und gerade die Kommunikationsnetze der staatlichen Verwaltung nicht nur theoretisch ist, sondern real existiert, braucht man nicht nach Estland zu schauen, wo eine Botnetzattacke tagelang große Teile des Behördennetzes lahmgelegt hat. Es gibt auch in Deutschland immer wieder Angriffe auf einzelne Behörden mit dem Ziel, Kommunikation zu sabotieren. Sogenannte Denial-of-Service-Attacken oder verteilte Denial-of-Service-Attacken führen dazu, dass Server mit Massen von Anfragen überflutet werden, die nicht verarbeitet werden können, sodass die Server ihren Dienst versagen und zusammenbrechen.~~

~~Auch die Zahl und Qualität von Computerviren, trojanischen Pferden, Würmern und weiteren Computerschädlingen hat zugenommen. Ein Beispiel der letzten Monate ist Conficker. Der sogenannte Confickerwurm hat sich seit 2008 weltweit stark ausgebreitet. Wie Anfang des Jahres bekannt wurde, sind auch Rechner der Bundeswehr von dem Schadprogramm angegriffen worden.~~

~~Cyberangriffe haben nicht nur Manipulation und Sabotage zum Ziel. Angriffe zielen zunehmend auch auf Spionage. So wurde im März 2009 bekannt, dass kanadische Forscher ein sogenanntes Ghostnet, ein riesiges Spionagenetz, entdeckt haben, das mindestens 1.295 Rechner in 103 Staaten infiltriert hat. Besonders von den Angriffen betroffen: Rechner mit hohem Informationswert in Außenministerien, Sicherheitsbehörden, Botschaften oder internationalen Organisationen.~~

~~Eine weitere Entwicklung, ein weiteres Risiko, das auch der Lagebericht des BSI zur IT-Sicherheit für das Jahr 2009 anspricht, ist, dass solche Angriffe zunehmend auf Prozesssteuerung ausgerichtet sind. Ziel ist es nicht mehr, nur unmittelbaren Schaden anzurichten, sondern Infrastrukturen, die von der IT-Technik abhängig sind, zu beeinflussen und zu manipulieren. Das ist eine reale und zunehmende Gefahr vor allem für die Wirtschaft, aber auch für staatliche Infrastrukturen.~~

~~Diesen Herausforderungen begegnen wir mit dem neuen BSI-Gesetz, welches folgende Kernpunkte enthält: Erstens. Das BSI wird nach § 4 als zentrale Meldestelle des Bundes für die Zusammenarbeit der Bundesbehörden zuständig sein und in Sachen IT-Sicherheit Informationen zu Sicherheitslücken, Schadprogrammen oder Angriffen sammeln und auswerten. So können Angriffe und Angriffsmuster besser erkannt und Gegen-~~

(A) ~~maßnahmen eingeleitet werden. In diesem Zusammenhang mit diesen Vorgaben wird das BSI innerhalb der Bundesverwaltung Maßnahmen umsetzen können, um Gefahren, die von Schadprogrammen ausgehen, abzuwehren. Bisher war das BSI lediglich beratend tätig ohne eigene Befugnisse.~~

~~Zweitens. Mit § 5 regeln wir die Abwehr von Schadprogrammen. Er sieht die vorübergehende Speicherung von Protokolldaten zum Erkennen und zur Abwehr von Angriffen vor. Dabei haben wir in allen Fällen, in denen es um den Austausch von Daten geht, auf verstärkte Datenschutzstandards Wert gelegt. Bei der Suche nach Schadprogrammen wird in einem abgestuften Verfahren vorgegangen. Die Behauptung – die vor allem vonseiten der FDP immer wieder in Umlauf gebracht wird –, dass hier die gesamte Kommunikation zwischen Bürgern und Behörden überwacht wird, ist blanker Unfug und soll nur die Öffentlichkeit verunsichern.~~

~~Im Kern geht es darum, dass das BSI mit seinen Möglichkeiten eine Art Schadprogrammscanner über den Datenverkehr der Bundesbehörden legt. Nur so können Schadprogramme erkannt und abgewehrt werden, bevor sie Schaden anrichten.~~

~~Dabei folgt das Verfahren einem sehr strengen Datenschutzkonzept. Die Daten werden automatisiert – also ohne dass jemand in irgendeiner Weise Einblick hat – auf Schadsoftware gescannt. Wenn nichts gefunden wird, werden die Daten sofort und spurlos gelöscht. Nur in den wenigen Fällen, in denen Hinweise auf Angriffe bestehen, wird manuell nachgeprüft. Diese manuelle Nachschau findet ebenfalls unter engen Voraussetzungen statt. Die Daten müssen nämlich automatisch pseudonymisiert werden. Alle personenbezogenen Daten werden also durch Pseudonyme ersetzt. Zusätzlich müssen die betroffenen Kommunikationsteilnehmer im Nachhinein informiert werden.~~

(B) ~~Eine Entpseudonymisierung oder Weitergabe von Daten an Sicherheitsbehörden ist nur in sehr eng definierten Grenzen möglich. Das betrifft zum einen die Strafverfolgung bei Straftaten, die mittels Schadprogrammen begangen wurden, konkret: das Ausspähen und Abfangen oder das Verändern von Daten oder Computersabotage. Darüber hinaus ist auch die Weitergabe bei der Verfolgung erheblicher Straftaten insbesondere im Sinne des § 100 a Abs. 2 der Strafprozessordnung, also zum Beispiel Mord oder Totschlag, möglich. Relevante Informationen dürfen dabei nur mit richterlicher Zustimmung weitergegeben werden. Kernbereichsrelevante Inhalte sollen – in den seltenen Fällen, in denen theoretisch überhaupt solche Inhalte betroffen sind – nicht erfasst oder sofort wieder gelöscht werden. Auch ist die Verwendung von Daten, die sich auf das Zeugnisverweigerungsrecht nach § 53 Abs. 1 Satz 1 beziehen, nicht zulässig.~~

~~In diesem Zusammenhang ist es wichtig, darauf hinzuweisen, dass es sich bei den Angriffen, die es abzuwehren gilt, nicht etwa um leicht erkennbare Viren handelt, die mit handelsüblichen Virenschutzprogrammen erkennbar wären. Es handelt sich hier vielmehr um Cyberattaeken via Datenaustausch, bei denen auch mit~~

sogenannten Totalfälschungen gearbeitet wird. Bei diesen ist nicht erkennbar, ob zum Beispiel eine entsprechende E-Mail von einer Behörde stammt oder einem Kriminellen. Um solche komplexen Angriffe geht es, für die es in den meisten Fällen bislang eben keine ausreichende zertifizierte Sicherheitssoftware gibt. (C)

~~Der dritte zentrale Punkt des Gesetzentwurfs: Das BSI wird in § 8 befugt, technische Vorgaben und verbindliche Mindeststandards für die Sicherung der Informationstechnik innerhalb der Bundesverwaltung zu machen. Das betrifft auch Richtlinien für die Beschaffung von IT-Produkten. Darüber hinaus werden die Regelungen zur Zertifizierung durch das BSI modernisiert. Das BSI ist darüber hinaus nur in begründeten Ausnahmefällen befugt, selbst Software für Bundesbehörden herzustellen.~~

~~Nicht mehr im Gesetz enthalten ist Art. 3 des ursprünglichen Gesetzentwurfs, die Änderung des Telemediengesetzes, die vorsah, dass Diensteanbieter personenbezogene Daten speichern dürfen, um Angriffe auf ihr Angebot abzuwehren. Wir haben uns entschlossen, diese Änderung im Rahmen des BSI-Gesetzes nicht weiter zu verfolgen. Dennoch – da sind sich die Innenpolitiker der Großen Koalition einig – besteht hier weiterhin Handlungsbedarf.~~

~~Lassen Sie mich abschließend vor allem eines deutlich machen: Dieses Gesetz leistet einen außerordentlich wichtigen Beitrag zur Sicherheit unserer gesamten IT-Infrastruktur. Es ist wichtig, es heute zu beschließen. Es duldet keinen Aufschub. Es ist ein Gesetz, in das viele Änderungswünsche und Anregungen von Sachverständigen und auch des Bundesdatenschutzbeauftragten aufgenommen wurden, was dazu geführt hat, dass sowohl der Datenschutzbeauftragte als auch der Berichterstatter der Grünen in der abschließenden Beratung im Innenausschuss anerkennende Worte für das Gesetz gefunden haben. (D)~~

~~Wir legen ein Gesetz vor, mit dem wir sicherstellen, dass das BSI auch in Zukunft seine Aufgabe erfolgreich erfüllen kann, und das unsere Zustimmung verdient.~~

Frank Hofmann (Volkach) (SPD): Ich möchte an meinen Redebeitrag zur ersten Lesung zum BSI-Gesetzentwurf erinnern, wo ich viele kritische Fragen hatte und enttäuscht und wütend war, dass dem Parlament so ein schlechter und schlampiger Gesetzentwurf vorgelegt wurde.

Nach den vielen E-Mails, die wir Abgeordnete bekamen wegen des neuen § 15 des Telemediengesetzes, haben wir in den Koalitionsverhandlungen diesen politisch und juristisch unzulänglichen § 15 abgeräumt. Die Petenten befürchteten, dass jedem Anbieter von Internetdiensten wie Google, Amazon oder StudiVz das Recht gegeben werden sollte, das Lese-, Schreib- und Suchverhalten seiner Besucher ohne Anlass aufzeichnen zu können, vorgeblich zum „Erkennen“ von „Störungen“. Nachdem wir öffentlich gemacht hatten, dass wir den § 15 Telemediengesetz nicht weiter verfolgen, kam keine einzige Reaktion mehr.

(A) Die schriftlich fixierte Kritik des Bundesdatenschutzbeauftragten Schaar, der die fehlende Pseudonymisierung der persönlichen Daten beanstandete, haben wir ebenfalls umgesetzt. Nunmehr erfolgt bei der automatischen Auswertung bei allen Protokolldaten, die nicht sofort gelöscht werden, eine Pseudonymisierung. Die Entschlüsselung dieser pseudonymisierten Daten darf nur vom Präsidenten des Bundesamtes selbst angeordnet werden. Und diese Entscheidung ist zu protokollieren. Damit ist sichergestellt: Der Verantwortliche steht fest. Nicht wie bei Bahn und Telekom, wo man erst suchen muss, wer der Verantwortliche ist. Wir haben die Verantwortlichkeit festgelegt.

Die Sachverständigenanhörung, die wir durchgeführt haben, hat die SPD-Fraktion bestärkt, weitere Verbesserungsvorschläge einzufordern. Wir haben insbesondere über Evaluierung und über die Rechtswegegarantie Art. 19. Abs. 4, und damit über die Benachrichtigung, diskutiert.

Sie werden jetzt sagen: Ja, wo ist sie denn, die Evaluierung? Mich haben hier die Argumente des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des Bundesministeriums des Innern überzeugt. Eine offene, transparente Evaluierung würde in erster Linie den Angreifern Informationen darüber geben, welche Schadprogramme entdeckt wurden und welche nicht. Das ist aber nicht das Ziel der Evaluierung. Wir haben deshalb stattdessen die Kontrolle des Bundesdatenschutzbeauftragten gestärkt und eine Informationspflicht an den Innenausschuss des Deutschen Bundestages eingebaut, der auch VS eingestuft nachfragen und sich grundlegend informieren kann. Das ist aus meiner Sicht eine hervorragende Alternative.

(B)

Nun zur Benachrichtigung. Hier bin ich persönlich nur zu 90 Prozent zufrieden. Falls im Einzelfall eine Benachrichtigung unterbleiben soll, hätte ich diese Entscheidung gerne dem Richter überantwortet. Nun wissen wir alle, dass diese Einschaltung des Richters auch kritisch betrachtet werden kann wegen sachlicher, fachlicher und quantitativer Überforderung. Legt man Wert auf eine sachlich und fachlich gute Entscheidung, dann ist der im Gesetzentwurf gemachte Vorschlag eine gute Grundlage. Es entscheidet der Datenschutzbeauftragte der Behörde, er muss dokumentieren, der Bundesdatenschutzbeauftragte übt die Kontrolle aus und der Innenausschuss des Deutschen Bundestages ist zu unterrichten.

Gegenüber dem Gesetzentwurf der Bundesregierung haben wir die Übermittlung von personenbezogenen Daten an die Strafverfolgungsbehörden bei Zufallsfunden präzisiert, stark eingengt und unter den Vorbehalt vorheriger gerichtlicher Zustimmung gestellt. Soweit die Weitergabe Personen betrifft, die aus beruflichen Gründen ein Zeugnisverweigerungsrecht besitzen, soll auch für das BSI der besondere Schutz gelten, wie wir ihn in der Strafprozessordnung § 108 Abs. 3 kennen (Verwertungsverbot, soweit keine Straftat betroffen ist, die im Höchstmaß mit mindestens fünf Jahren Freiheitsstrafe bedroht ist). Soweit kritisiert wird, dass dies nicht weitgehend genug ist, halte ich entgegen, dass es im Rahmen

der Rechtsordnung sinnvoll ist, keinen Wertungswiderspruch zu erhalten. (C)

Den Kernbereichsschutz privater Lebensgestaltung haben wir, wie vom Verfassungsgericht gefordert, zweistufig ausgebaut: Soweit möglich, ist bereits technisch sicherzustellen, dass Daten, die den Kernbereich privater Lebensgestaltung betreffen, nicht erhoben werden. Bestehen aber auch nur Zweifel, dass Daten dem Kernbereich zuzurechnen sein könnten, sind diese Daten unverzüglich zu löschen.

In der Sitzung des Innenausschusses am 27. Mai 2009 hat der Bundesdatenschutzbeauftragte Schaar die Weiterentwicklung des Gesetzentwurfes durch die Koalitionsfraktionen begrüßt. Er sieht im Großen und Ganzen seine Forderungen als erfüllt an. Wolfgang Wieland von Bündnis 90/Die Grünen hatte kritisiert, dass es überhaupt Zufallsfunde gibt. Ich möchte ihm hier im Plenum erwidern, dass wir nicht vorgehen können wie bei der Maut. Wenn aufgrund einer Entpseudonymisierung bekannt wird, dass eine erhebliche Straftat zu erwarten ist, die mit mehr als fünf Jahren Freiheitsstrafe bedroht ist, dann wird aus der Abwägung, ob man die Strafverfolgung einschalten kann oder nicht, der Ermessensspielraum gegen null reduziert. Ich bin der Überzeugung, da kann der Staat nicht die Augen verschließen, sondern muss die Strafverfolgungsbehörden einschalten.

Bei der Maut gibt es keine echten Zufallsfunde. Hier muss der Staat aktiv werden und nach bestimmten Informationen (zum Beispiel Kfz-Kennzeichen) fragen. Im Gegensatz dazu sind im Falle des BSI diese Informationen unbeabsichtigte Nebenfolgen. Das aber ist etwas ganz anderes. (D)

Sie sehen, im Laufe der parlamentarischen Beratungen ist aus dem Kabinettsentwurf ein völlig neues Gesetz entstanden, das effizient und rechtsstaatlich ist und den Spagat von Sicherheit versus Freiheit schafft.

~~Gisela Piltz (FDP): Wenn man die Bedeutung von Gesetzen an ihrem Platz in der Tagesordnung messen würde, müsste man zu der Erkenntnis kommen, dass dieses Gesetz weitgehend bedeutungslos ist. Liest man aber mal den Gesetzestext, reibt man sich verwundert die Augen: Hier geht es um gravierende Eingriffe in Grundrechte! Diese werden heute Nacht quasi unter Ausschluss der Öffentlichkeit beraten. Dabei hat die auf unsere Initiative im Innenausschuss durchgeführte öffentliche Anhörung ergeben, dass dieses Gesetz ungeeignet und verfassungsrechtlich bedenklich ist. Ich kann nur noch einmal wiederholen, dass die Sicherheit in der IT-Technik von größter Bedeutung ist. Natürlich müssen in unserer digitalen Welt die IT-Systeme geschützt werden. Es ist selbstverständlich, dass darauf ein besonderes Augenmerk gelegt werden muss. Aber wie immer im Leben gilt auch hier: Sicherheit darf nicht auf Kosten einer unverhältnismäßigen Einschränkung der Freiheit erkaufte werden.~~

~~Genau das aber geschieht hier. Das BSI soll künftig jede elektronische Kommunikation mit Bundesbehörden aufzeichnen und auswerten. Das bedeutet, dass jede~~