TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Informatik Institut für Systemarchitektur

Professur für Datenschutz und Datensicherheit

Technische Universität Dresden, 01062 Dresden

An den
Innenausschuss des Deutschen Bundestages
Platz der Republik 1
11011 Berlin

Prof. Dr.
Andreas Pfitzmann

Telefon: 0351 463-38277
Telefax: 0351 463-38255
Mobiltel.: 0173 148 5074
E-Mail: pfitza@inf.tu-dresden.de

Sekr.: 0351 463-38247
E-Mail: gersonde@inf.tu-dresden.de

AZ:

Dresden, 7. Mai 2009

Stellungnahme zum „Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes“ auf der Basis der Drucksachen 16/11967 und 16/12225

Sehr geehrte Damen und Herren,

wie erbeten, erhalten Sie nachfolgend meine persönliche Stellungnahme zum „Entwurf eines Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes“. Dieser Text bezieht Aspekte und Argumente ein, die in einer Stellungnahme zu einem früheren Zustand des Gesetzentwurfes durch die Gesellschaft für Informatik (GI; die größte Vereinigung von Informatikern im deutschsprachigen Raum), an der ich mitgearbeitet habe, frühzeitig dem BMI zugeleitet und auch publiziert wurden (u.a. Informatik-Spektrum 32/2 (2009) Seiten 188-190).

Meine Stellungnahme ist nach den problematischen Paragrafen des Art. 1 (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik – BSIG-E) gegliedert, d.h. nach §§ 5, 7 und 9 BSIG-E, aus denen ich fünf Haupt-Forderungen ableite. Daran schließen sich wenige kleine Anmerkungen insbesondere zu angeratenen Klarstellungen im Gesetzestext sowie eine Zusammenfassung an.

§ 5 BSIG-E ist leider auch in der aktuell vorgeschlagenen Fassung immer noch erheblich zu weit gefasst und geeignet, das Vertrauen in die Bundesverwaltung im Allgemeinen wie auch in das BSI im Speziellen nachhaltig zu erschüttern. Es besteht, um dies deutlich zu sagen, keinerlei sachlich gerechtfertigter Grund, eine derartig umfassende Befugniserweiterung zur Speicherung auch von personenbezogenen Daten (zur Erklärung: viele Protokolldaten (z.B. IP-Adressen) sind personenbeziehbare Daten und damit personenbezogene Daten nach

Postadresse (Briefe)
TU Dresden, Fakultät Informatik
Institut für Systemarchitektur
01062 Dresden

Postadresse (Pakete u.ä.)
TU Dresden, Fakultät Informatik
Institut für Systemarchitektur
Helmholtzstraße 10
01069 Dresden

Besucheradresse
Sekretariat:
01187 Dresden
Nöthnitzer Str. 46
Zi. 3070

Internet
http://dud.inf.tu-dresden.de

Bundesdatenschutzgesetz (BDSG)) vorzunehmen.

Die diesbezüglich vom Bundesrat geäußerten „erheblichen Zweifel“, „ob die in § 5 BSIG-E formulierten Eingriffsschwellen einen verhältnismäßigen Ausgleich zwischen dem hier gravierenden Grundrechtseingriff und der Schutzgutgefährdung herbeiführen“, kann ich nur nachhaltig unterstützen. Da anscheinend die Bundesregierung diese Zweifel bisher nicht versteht oder verstehen will, möchte ich sie nachfolgend am Beispiel der Auswirkungen eines Verbreitungsrahmens für Schadprogramme detailliert erläutern und begründen:

§ 5 Abs. 3 BSIG-E erlaubt eine „über die Absätze 1 und 2 hinausgehende Verwendung“ von „Protokolldaten“, und – noch weitaus tiefer in Persönlichkeitsrechte eingreifend – aller „an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten“, „wenn bestimmte Tatsachen den Verdacht begründen, dass“ ... „3. sich aus ihnen Hinweise auf ein Schadprogramm ergeben können, und soweit die Datenverarbeitung erforderlich ist, um den Verdacht zu bestätigen oder zu widerlegen.“

Um zu verdeutlichen, wie leicht eine Situation entstehen kann, in der das BSI alle an den Schnittstellen der Kommunikationstechnik des Bundes anfallenden Daten gemäß Gesetzentwurf zeitlich unbegrenzt speichern darf, skizziere ich nachfolgend ein generisches Schadprogramm und zeige dessen Konsequenzen auf:

Nehmen wir an, es gibt einen Verbreitungsrahmen für Schadprogramme, der Wirkfunktionen nachlädt, indem er folgendermaßen probiert: Nimm jede Nachricht, addiere zu ihr diejenige Nachricht, die möglichst genau 5 Jahre später eintrifft, interpretiere die Summe der Nachrichten als Binärcode und wenn dies ausführbarer Binärcode ist, dann führe ihn aus. Etwas kürzer und übersichtlicher geschrieben:

(beliebige) Nachricht $\oplus$ Nachricht 5 Jahre später = Schadprogramm ?

Jede der beiden Nachrichten allein ist absolut harmlos, jedoch ihre Kombination durch den skizzierten Verbreitungsrahmen für Schadprogramme macht sie gefährlich.

Die Erfindung solch eines Rahmens für Schadprogramme liegt auf der Hand, die Frist von 5 Jahren ist natürlich ein frei wählbarer Zeitraum. Hieraus ergibt sich, dass Maximalfristen für eine Speicherung von „Bösewichten“ immer verlängerbar sind, so dass letztlich nach Gesetzesentwurf alle Nachrichten unbefristet gespeichert werden dürfen.

Das Vorliegen solch eines Verbreitungsrahmens für Schadprogramme ist die Tatsache, die einen Verdacht begründet. Aus der Aufzeichnung aller Nachrichten inkl. Absender und Adressat für – im Beispiel – mindestens 5 Jahre können sich Hinweise auf ein Schadprogramm ergeben. Die Speicherung ist erforderlich, um den Verdacht zu bestätigen oder zu widerlegen. Kurzum: § 5 BSIG-E ist eine Generalermächtigung, die keiner Kontrolle (außer durch das BMI) unterliegt.

Hieraus folgen meine ersten drei Haupt-Forderungen:

➔ Für ein Bundesamt mit weitreichenden Eingriffsbefugnissen, erheblichen Speicher-

und Auswertebefugnissen auch für personenbezogene Daten ist eine **parlamentarische Kontrollkommission nötig**, da die Macht solch eines Bundesamtes in einer Informationsgesellschaft über die Macht klassischer Geheimdienste deutlich hinausgehen kann.

- ➔ Möglichst vor der Einleitung von Eingriffen in die informationelle Selbstbestimmung von Bürgern, spätestens aber 3 Tage nach Beginn des Eingriffs ist für den Eingriff eine **richterliche Anordnung** einzuholen.
- ➔ **§ 5 BSIG-E ist deutlich restriktiver und klarer zu fassen**.

Wie erwähnt, ist Vertrauen von Bürgern und Wirtschaft in das BSI und die Kommunikation mit der Bundesverwaltung extrem wichtig. Dies hat Implikationen über § 5 BSIG-E hinaus:

In **§ 7 BSIG-E** wird es in das nicht näher spezifizierte Ermessen des BSI gestellt („kann"), Erkenntnisse über Sicherheitslücken und Schadprogramme an die Betroffenen weiterzugeben und die Öffentlichkeit zu warnen. Hier ist zu beachten, dass durch die im BKA-Gesetz vorgesehene Online-Durchsuchung eine Interessenkollision im Dienstbereich des BMI, dem BSI und BKA unterstehen, induziert wird. Da durch neue Schadprogramme und unveröffentlichte Sicherheitslücken – nachweislich und der Bundesregierung bekannt – sehr große Schäden entstehen (können), muss vor dem Hintergrund dieser Interessenkollision eine Pflicht zur Benachrichtigung und Warnung formuliert werden. Anderenfalls ist die Sicherheit der Bundesrepublik Deutschland gefährdet, so die GI in ihrer bereits erwähnten Stellungnahme. Die minimal notwendige Änderung am Gesetzestext besteht in der Ersetzung von „kann" in § 7 Abs. 1 und 2 BSIG-E durch „soll" sowie in der Aufnahme einer Regelung zur Überprüfung aller Entscheidungen, Erkenntnisse über Sicherheitslücken und Schadprogramme nicht umgehend zu veröffentlichen, durch die einzurichtende parlamentarische Kontrollkommission (s.o.).

Dies ergibt meine vierte Haupt-Forderung:

- ➔ Im Gesetz ist explizit und grundsätzlich festzulegen, dass **das BSI alle seine Erkenntnisse über Sicherheitslücken und Schadprogramme umgehend an Betroffene weiterzugeben und zeitnah zu veröffentlichen hat**. Über Ausnahmen hiervon ist die parlamentarische Kontrollkommission umgehend zu informieren. Bei Meinungsverschiedenheiten mit ihr hat die parlamentarische Kontrollkommission das Recht, die Öffentlichkeit zu informieren.

Nach **§ 9 Abs. 4 Nr. 2 BSIG-E** kann das BMI festlegen, ein Sicherheitszertifikat nicht zu erteilen und damit massiven Einfluss auf die Privatwirtschaft nehmen, wenn das BMI „festgestellt hat, dass überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung" „entgegenstehen." Diese Machtposition des BMI könnte zur Durchsetzung von Sicherheitslücken in zertifizierten Sicherheitsprodukten genutzt werden, etwa um Online-Durchsuchungen zu unterstützen. Solch eine Machtposition zu schaffen, wäre sicherheitspolitisch sehr unklug und dem Vertrauen von Bürgern und Wirtschaft in Sicherheitszertifikate alles andere als zuträglich. Ich rate, diese nahezu willkürlich nutzbare Einflussmöglichkeit des BMI zu streichen oder aber zumindest ihre Nutzung ebenfalls einer parlamentarischen Kontrolle zu unterwerfen (s.o.). Entsprechendes gilt für § 9 Abs. 6 Nr. 2 BSIG-E.

Dies ergibt meine fünfte Haupt-Forderung:

- ➔ Zur Stärkung des Vertrauens in das BSI im Allgemeinen sowie in die von ihm verliehenen Sicherheitszertifikate im Besonderen sind **willkürlich nutzbare Einflussmöglichkeiten des BMI auf die fachliche Arbeit des BSI zu minimieren**. Insbesondere sind § 9 Abs. 4 Nr. 2 sowie § 9 Abs. 6 Nr. 2 BSIG-E ersatzlos zu streichen.

Es sei erwähnt, dass auch § 11 BSIG-E, wo lapidar von einer Einschränkung von Artikel 10 GG gesprochen wird, nach einer institutionalisierten parlamentarischen Kontrolle und einem Richtervorbehalt ruft.

Die folgenden kleinen Änderungen am Text sind zur Klarstellung dringend angeraten:

§ 2 Abs. 5 BSIG-E würde in seiner jetzigen Fassung Schadprogramme, die Daten nur unbefugt ändern, nicht aber nutzen oder löschen, nicht umfassen. Deshalb sollte „ , zu ändern“ nach „zu nutzen“ eingefügt werden.

In § 3 Abs. 1 Nr. 2 BSIG-E ist die Formulierung „für andere Stellen“ zu präzisieren, da sonst die Normenklarheit verletzt und das Vertrauen der Bürger in das BSI geschwächt wird.

Zusammengefasst erteilt der momentane Gesetzentwurf dem BSI insbesondere im Bereich der Speicherung personenbezogener Daten Befugnisse in einem Umfang, der aus meiner Sicht für eine vertrauensvolle Zusammenarbeit von Bürgern und öffentlicher Verwaltung kontraproduktiv ist, verfassungsrechtlich mehr als bedenklich und so generalermächtigend, dass die Überschrift zu Artikel 1 treffender „Gesetz über das Bundesamt für *Speicherung* in der Informationstechnik (BSI-Gesetz – BSIG)“ lauten müsste. Für das Vertrauen der Bürger in ihren Staat im Allgemeinen sowie die Bundesverwaltung wie auch das BSI im Speziellen wäre sehr vorteilhaft, bereits der Gesetzgeber würde die sachlich gebotenen Änderungen vornehmen und nicht ein weiteres sogenanntes Sicherheitsgesetz beschließen, das nach einer Korrektur durch das Bundesverfassungsgericht geradezu ruft.