DeutscherAnwaltVerein

Stellungnahme

des Deutschen Anwaltvereins durch den Ausschuss Informationsrecht

zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Stellungnahme Nr.: 67/2014 **Berlin, im Dezember 2014**

Mitglieder des Ausschusses

- Rechtsanwalt Dr. Helmut Redeker
- Rechtsanwältin Isabell Conrad
- Rechtsanwalt Prof. Niko Härting
- Rechtsanwalt Peter Huppertz, LL.M (Berichterstatter)
- Rechtsanwalt Prof. Dr. Jochen Schneider
- Rechtsanwalt Dr. Robert Selk, LL.M. (EU)
- Rechtsanwalt Prof. Dr. Holger Zuck

Zuständig in der DAV-Geschäftsführung

- Rechtsanwalt Thomas Marx

Deutscher Anwaltverein
Littenstraße 11, 10179 Berlin
Tel.: +49 30 726152-0
Fax: +49 30 726152-190
E-Mail: dav@anwaltverein.de

Büro Brüssel
Rue Joseph II 40
1000 Brüssel, Belgien
Tel.: +32 2 28028-12
Fax: +32 2 28028-13
E-Mail: bruessel@eu.anwaltverein.de
Transparenz-Registernummer:
87980341522-66

www.anwaltverein.de

Verteiler

Ausschuss für Recht und Verbraucherschutz
Innenausschuss

Bundesministerium der Justiz und für Verbraucherschutz
Bundesministerium des Inneren

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit
Die Datenschutzbeauftragten der Bundesländer

Arbeitskreise Recht der Bundestagsfraktionen

Justizministerien und Justizsenatoren der Länder
Innenminister der Länder

Bundesrechtsanwaltskammer
Bundesnotarkammer
Bundesverband der Freien Berufe
Deutscher Richterbund
Deutscher Notarverein e.V.
Deutscher Steuerberaterverband
Bundesverband der Deutschen Industrie (BDI)
GRUR
BITKOM
DGRI

DAV-Vorstand und Geschäftsführung
Vorsitzende der DAV-Gesetzgebungsausschüsse
Vorsitzende der DAV-Landesverbände
Vorsitzende des FORUMs Junge Anwaltschaft

Frankfurter Allgemeine Zeitung
Süddeutsche Zeitung GmbH
Berliner Verlag GmbH
Redaktion NJW
Juve-Verlag
Redaktion Anwaltsblatt
Juris
Redaktion MultiMedia und Recht (MMR)
Redaktion Zeitschrift für Datenschutz (ZD)
Redaktion Heise Online

Der Deutsche Anwaltverein (DAV) ist der freiwillige Zusammenschluss der deutschen Rechtsanwältinnen und Rechtsanwälte. Der DAV mit derzeit ca. 67.000 Mitgliedern vertritt die Interessen der deutschen Anwaltschaft auf nationaler, europäischer und internationaler Ebene.

Vorbemerkung

Am 18. August 2014 hat das Bundesministerium des Innern (BMI) einen Referentenentwurf für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vorgelegt. Das BMI hatte bereits zuvor am 5. März 2013 einen Referentenentwurf für ein IT-Sicherheitsgesetz präsentiert, welcher nunmehr durch den neuen Entwurf überarbeitet und in nicht unerheblichem Umfang ergänzt wird. Die Schaffung eines IT-Sicherheitsgesetzes mit verbindlichen Mindestanforderungen an die IT-Sicherheit für kritische Infrastrukturen und der Verpflichtung zur Meldung von IT-Sicherheitsvorfällen wird ausdrücklich im Koalitionsvertrag vom Dezember 2013 erwähnt (wie dort Seite 147). Ferner ist der vorliegende Entwurf für ein IT-Sicherheitsgesetz wesentlicher Teil der von der Bundesregierung am 20. August 2014 veröffentlichten „Digitalen Agenda 2014 – 2017“. Wie bereits der vorherige Referentenentwurf ist auch der nunmehr vorliegende Entwurf als Artikelgesetz ausgestaltet, welches diverse Änderungen im BSIG, TMG, TKG, BKAG und AWG vorsieht. Kernziele des IT-Sicherheitsgesetzes sollen eine Verbesserung der IT-Sicherheit bei Unternehmen, ein verstärkter Schutz der Bürgerinnen und Bürger in einem sicheren Netz, der Ausbau der IT-Sicherheit der Bundesverwaltung und in diesem Zusammenhang auch eine Stärkung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie des Bundeskriminalamtes (BKA) sein. Diese ohne Zweifel wichtigen Ziele sollen im Wesentlichen durch die Schaffung eines gesetzlichen Mindeststandards an IT-Sicherheit sowie die Verpflichtung zur Meldung von IT-Sicherheitsvorfällen an das BSI erreicht werden. Aufgrund der Zuständigkeit des Ausschusses beschränkt sich die nachfolgende Stellungnahme auf die informations- und datenschutzrechtlich relevanten Änderungen des BSIG, des TMG und des TKG:

1. Erfüllungsaufwand für die Verwaltung

Im Referentenentwurf wird unter E.3. auf Seite 7 der Erfüllungsaufwand für die Verwaltung im Einzelnen dargestellt. Im direkten Vergleich zum vorherigen Referentenentwurf fällt auf, dass die Planstellen / Stellen für das BSI (vorher: 198 / aktuell: 133) und das BKA (vorher: 105 / aktuell: 79) reduziert wurden. Demgegenüber enthielt der vorherige Referentenentwurf keine Planstellen / Stellen für das Bundesamt für Verfassungsschutz (BfV). Im aktuellen Entwurf sind für das BfV insgesamt 55 Planstellen / Stellen ausgewiesen. In der Gesetzesbegründung wird dieser zusätzliche Ressourcenbedarf beim BfV mit einem Hinweis auf § 8b Abs. 2 Nr. 2 BSIG-E begründet. Gemäß § 8 b Abs. 2 Nr. 2 BSIG-E soll das BSI in Zusammenarbeit mit zuständigen Bundesbehörden die potentiellen Auswirkungen auf die Verfügbarkeit der kritischen Infrastrukturen analysieren. Offensichtlich soll daher das BfV einen nicht unerheblichen Anteil dieser Analysetätigkeit übernehmen. Aufgrund der Kürzung der Planstellen / Stellen des BKA kann man vermuten, dass diese Aufgabe zunächst dem BKA zugedacht war. Die eigentlich interessante Frage, in welchem Umfang das BSI gemeldete IT-Sicherheitsvorfälle in Zusammenarbeit mit dem BfV analysieren wird bzw. darf, lässt sich dem Referentenentwurf bislang nicht mit der in diesem sensiblen Bereich wünschenswerten Transparenz entnehmen. Die in § 1 BSIG-E enthaltene Aufwertung des BSI als „Nationale Informationssicherheitsbehörde“ dürfte das Bedürfnis der Öffentlichkeit nach mehr Transparenz in diesem Zusammenhang eher steigern.

2. Zu § 2 Abs. 10 BSIG-E

In § 2 Abs. 10 BSIG-E wird hinsichtlich der Festlegung und Definition der „Kritischen Infrastrukturen“ im Sinne des BSIG auf die nach § 10 Abs. 1 BSIG-E noch zu erlassende Rechtsverordnung verwiesen. Hieraus ergibt sich im Ergebnis eine nicht unerhebliche Unbestimmtheit des gesamten Gesetzesentwurfs, zumal eine Identifizierung der adressierten Betreiber von kritischen Infrastrukturen nur dann möglich ist, wenn klar ist, was unter den „Kritischen Infrastrukturen“ zu verstehen ist. Aufgrund der mangelnden Bestimmtheit des zentralen Begriffs

„Kritische Infrastrukturen“ bleibt daher auch die in § 8a Abs. 1 BSIG-E vorgesehene Verpflichtung zu einem Mindeststandard für die IT-Sicherheit unbestimmt.

Die grundlegende verfassungsrechtliche Dimension der Verwendung unbestimmter Rechtsbegriffe bezogen auf das BSIG-E bedarf einer eingehenderen Betrachtung. Jedenfalls sollten betroffene Unternehmen aus einem Gesetz und nicht nur aus Durchführungsvorschriften erkennen können, ob sie Adressaten der vom Gesetzgeber vorgesehen umfangreichen Verpflichtungen sind.

3. Zu § 2 Abs. 11 BSIG-E

Begrüßenswert ist sicherlich, dass in § 2 Abs. 11 BSIG-E Kleinstunternehmen im Sinne der Empfehlung 2003/361/EG der Kommission vom 6. Mai 2013 betreffend die Definition der Kleinstunternehmen sowie der kleineren mittleren Unternehmen (ABl. L 124 vom 20. Mai 2003, Seite 36) vom Anwendungsbereich des Gesetzes ausgenommen werden. Kleinstunternehmen sind hiernach Unternehmen, die weniger als 10 Personen beschäftigen und deren Jahresumsätze bzw. Jahresbilanzen 2 Mio. Euro nicht überschreiten. Im Umkehrschluss bedeutet diese Ausnahme allerdings, dass alle anderen, größeren Unternehmen zum Adressatenkreis des IT-Sicherheitsgesetzes zählen. Je nach Festlegung der Kriterien für das Vorliegen der kritischen Infrastrukturen könnte eine sehr große Anzahl von Unternehmen zum Adressatenkreis des IT-Sicherheitsgesetzes zählen. Je größer dieser Kreis letztendlich wird, umso eher könnte es Sinn machen, die Ausnahmeregelung durch höhere Umsatzgrenzen und eine erhöhte Beschäftigtenanzahl zu erweitern.

4. Zu § 8a Abs. 1 BSIG-E

Aus der Regelung in § 8a Abs. 1 BSIG-E wird weder deutlich, wer als Betreiber kritischer Infrastrukturen gesetzlich verpflichtet wird, noch welche organisatorischen und technischen Vorkehrungen und sonstigen Maßnahmen zur

IT-Sicherheit dieser Betreiber umsetzen muss. Auch insoweit fehlt es an der notwendigen Bestimmtheit, vgl. oben unter 2.1..

5. Zu § 8a Abs. 4 BSIG-E

In § 8a Abs. 4 BSIG-E wird zunächst bestimmt, dass die Verpflichtungen von § 8a Abs. 1 – Abs. 3 BSIG-E nicht auf die Betreiber öffentlicher Telekommunikationsnetze sowie öffentlich zugänglicher Telekommunikationsdienste Anwendung finden. Dies ist folgerichtig, da letztere bereits durch das TKG – insbesondere von §§ 100 Abs. 1, 109 Abs. 5 TKG – entsprechend gegenüber der Bundesnetzagentur verpflichtet sind. Allerdings sollen die Absätze 1 – 3 auch für solche Betreiber kritischer Infrastrukturen nicht gelten, für die aus oder aufgrund von sonstigen Rechtsvorschriften des Bundes vergleichbare oder weitergehende Anforderungen im Sinne von § 8a Abs. 1 – Abs. 3 BSIG-E bestehen. Grundsätzlich ist es sicherlich richtig, dass eine unnötige Doppelregulierung zu vermeiden ist. Welche Betreiber unter diese Ausnahme fallen, bleibt allerdings im Ergebnis unklar, da eine genaue Zuordnung zu dieser Ausnahmeregelung einen konkreten Vergleich der anwendbaren sonstigen Rechtsvorschriften mit den Vorgaben von § 8a Abs. 1 – Abs. 3 BSIG-E erfordert. Dies ist jedoch in Folge der Unbestimmtheit des BSIG-E nicht mit der nötigen Trennschärfe möglich. Besser wäre es daher, wenn der Gesetzgeber die betroffenen Ausnahmen ausdrücklich festlegt (z.B. § 25a KWG, § 11 Abs. 1 EnWG).

5. Zu § 8b Abs. 1 BSIG-E

In § 8b Abs. 1 i.V.m. Abs. 4 und Abs. 5 BSIG-E wird festgelegt, dass IT-Sicherheitsvorfälle an das BSI zu melden sind. In der Gesetzesbegründung zu § 8b BSIG-E wird ausgeführt, dass die Meldungen üblicherweise rein technischer Natur sind und daher in der Regel keinen Personenbezug haben dürften. Soweit im Einzelfall Personenbezug gegeben sein sollte, soll sich die Übermittlungsbefugnis nach den allgemeinen datenschutzrechtlichen Regelungen richten. Problematisch hieran ist, dass gemäß § 4 Abs. 1 BDSG eine Übermittlung entweder einen gesetzlichen Erlaubnistatbestand erfordert oder aber der Betroffene in die Übermittlung eingewilligt hat. Da eine vorherige Einwilligung des

Betroffenen nicht in Betracht kommen dürfte, sollte zur Klarstellung aufgenommen werden, dass im Rahmen der gesetzlichen Vorgaben rechtmäßig erhobene Daten auch im Rahmen der Meldepflicht an das BSI übermittelt werden können.

6. Zu § 8b Abs. 3 BSIG-E

In § 8b Abs. 3 BSIG-E wird bestimmt, dass dem BSI 15 Warn- und Alarmierungskontakte zu benennen sind. Diese Regelung dürfte für kleinere Unternehmen nicht unbedingt Sinn machen. Insoweit müsste nämlich z.B. auch ein Unternehmen mit 10 Mitarbeitern, welches gemäß § 2 Abs. 11 BSIG-E in den Anwendungsbereich fallen kann, die genannten 15 Warn- und Alarmierungskontakte benennen.

7. Zu § 8b Abs. 4 BSIG-E

Gemäß § 8b Abs. 4 BSIG-E sind die Betreiber der kritischen Infrastrukturen verpflichtet, Beeinträchtigungen dem BSI zu melden, die entweder zu einem Ausfall oder einer Beeinträchtigung der von ihnen betriebenen kritischen Infrastruktur führen können. Im vorherigen Referentenentwurf war noch das weitere Qualitätskriterium „schwerwiegende Beeinträchtigung“ enthalten. Gerade im Hinblick auf die Meldepflicht bei einer reinen möglichen Beeinträchtigung der Infrastruktur stellt sich die Frage, welche Qualität die Beeinträchtigung haben muss, um eine Meldepflicht auszulösen. In der Gesetzesbegründung wird hierzu auf Seite 42 des Referentenentwurfs ausgeführt, dass das BSI unter Einbeziehung der Betreiber und Aufsichtsbehörden einen Kriterienkatalog für meldungsrelevante Sicherheitsvorfälle erstellen wird. Auch dies trägt jedoch zunächst nicht zu der wünschenswerten Bestimmtheit der zentralen Meldepflicht für die Betreiber bei. Die gleichen Erwägungen gelten im Übrigen auch für § 8b Abs. 5 BSIG-E, der immer dann greift, wenn es bereits zu einem Ausfall oder zu einer Beeinträchtigung der kritischen Infrastruktur gekommen ist. Im letzteren Fall ist dann auch eine ausdrückliche Nennung des Betreibers erforderlich, welche nach § 8 Abs. 4 BSIG-E gerade nicht erforderlich ist (anonyme Meldung).

8. Zu § 8b Abs. 7 BSIG-E

In § 8b Abs. 7 BSIG-E findet sich erneut eine Regelung zur Vermeidung der Doppelregulierung. Auch hier werden zunächst die TK-Anbieter von der Meldepflicht gemäß § 8b Abs. 3 – Abs. 6 BSIG-E ausgenommen. Ebenso werden erneut auch solche Betreiber von der Meldepflicht ausgenommen, für die aus oder aufgrund von sonstigen Rechtsvorschriften des Bundes vergleichbare oder weitergehende Meldepflichten bestehen. Auf die kritischen Ausführungen zu § 8a Abs. 4 BSIG-E kann daher verwiesen werden. Ergänzend ist anzumerken, dass Betreiber, die dieser Ausnahme unterfallen, offenbar nicht auf die Möglichkeit einer anonymen Meldung gemäß § 8b Abs. 4 BSIG-E zurückgreifen können, es sei denn, eine anonyme Meldeverpflichtung ist auch in der sonstigen Rechtsvorschrift gegeben. Letzteres ist jedenfalls im Bereich des TKG nicht der Fall.

9. Zu § 10 BSIG-E

Am Ende von § 10 BSIG-E wird bestimmt, dass Zugang zu den Akten, die die noch zu erlassende Rechtverordnung betreffen, nicht gewährt wird. Hierdurch werden im Ergebnis alle Unterlagen zum Inhalt der Rechtsverordnung als geheim deklariert. Das Auskunftsrecht ist daher sehr eingeschränkt und die Transparenz gegenüber der Öffentlichkeit nicht hinreicht gewahrt. Es sollte alternativ möglich sein, die berechtigten Geheimhaltungsinteressen der betroffenen Betreiber auch auf andere Art und Weise angemessen zu schützen, ohne die entsprechenden Akten insgesamt und ohne weitere Differenzierung als geheim zu deklarieren.

10. Zu § 13 Abs. 7 TMG-E

Im Hinblick auf die Regelung in § 13 Abs. 7 TMG-E ist ausdrücklich zu begrüßen, dass Anbieter von personalisierten Telemediendiensten den Nutzern die Anwendung eines sicheren und dem Schutzbedarf angemessenen Authentifizierungsverfahrens anzubieten haben. Um von vorneherein einen Missbrauch zu vermeiden, sollte noch ergänzt werden, dass diese

Authentifizierungsverfahren den Nutzern zu angemessenen Bedingungen anzubieten sind.

11. Zu § 15 Abs. 9 TMG-E

In § 15 Abs. 9 TMG-E wird nunmehr eine mit § 100 Abs. 1 TKG vergleichbare Regelung in das Telemediengesetz aufgenommen. Dieser Ansatz ist grundsätzlich unbedenklich. Fraglich ist allerdings, ob der Verweis auf § 15 Abs. 8 Satz 2 TMG zur Bestimmung der Speicherfrist für die erhobene Nutzungsdaten gelungen ist. Hiernach muss der Diensteanbieter die Daten unverzüglich löschen, wenn die Datenspeicherung für die Zwecke der Rechtsverfolgung nicht mehr benötigt werden. Dieser Zeitraum kann jedoch, z.B. im Hinblick auf zivilrechtliche Verjährungstatbestände, erheblich viel länger sein, als die vom Bundesgerichtshof im Zusammenhang mit § 100 Abs. 1 TKG statuierte siebentägige Speicherfrist für IP-Adressen (vgl. BGH Urteil vom 13. Januar 2011 – III ZR 146/10; bestätigt durch: BGH, Urteil vom 3. Juli 2014 – III ZR 391/13). Vor diesem Hintergrund erscheint es vorteilhafter, entweder den Verweis auf § 15 Abs. 8 Satz 2 TMG ganz weg zu lassen oder alternativ eine ausdrückliche Festlegung der Speicherfrist zu regeln. In diesem Zusammenhang ist ferner zu erwähnen, dass im Gesetzesentwurf der Bundesregierung für das Gesetzes zur Stärkung der Sicherheit in der Informationstechnik des Bundes (Drucksache 16/11967 vom 16. Februar 2009) bereits schon einmal eine entsprechende Ergänzung des Telemediengesetzes vorgeschlagen wurde. Dort wurde hinsichtlich der Speicherfrist ebenfalls auf § 15 Abs. 8 Satz 2 TMG verwiesen. Zusätzlich wurde jedoch auch die entsprechende Geltung von § 15 Abs. 8 Satz 3 TMG bestimmt. Nach dieser Regelung ist der betroffene Nutzer zu unterrichten, sobald dies ohne Gefährdung des mit der Maßnahme verfolgten Zweckes möglich ist. Da sich eine entsprechende Regelung ohnehin in § 100 Abs. 4 Satz 4 TKG findet, sollte der Verweis auf die entsprechende Geltung von § 15 Abs. 8 Satz 3 TMG wiederaufgenommen werden. Es lässt sich schlichtweg kein Argument dafür finden, weshalb der Betroffene unter diesen Voraussetzungen nicht über die Speicherung seiner Nutzungsdaten informiert werden sollte.

12. Zu § 100 Abs. 1 TKG-E

Die Möglichkeit zur Speicherung von Nutzungsdaten bei jeder noch so geringen Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten erscheint zu weitgehend und sollte angemessen korrigiert werden. Zum Beispiel könnte an dieser Stelle anstatt des Begriffs der „Verfügbarkeit“ der ohnehin im IT-Sicherheitsgesetz verwendete Begriff der „Ausfalls“ verwendet werden.

13. Zu § 109 Abs. 5 TKG-E

In § 109 Abs. 5 TKG-E wird die Meldepflicht der Betreiber unter anderem an eine „beträchtlichen Sicherheitsverletzung“ angeknüpft. Hier ist zu überlegen, ob dies eine qualitativ schwerwiegendere Beeinträchtigung meint, als die in § 8b Abs. 4 und Abs. 5 BSIG-E bestimmte Beeinträchtigung von kritischen Infrastrukturen. Insoweit sollte darauf geachtet werden, dass die Qualitätskriterien für die Entstehung der Meldepflicht für alle Betreiber von kritischen Anlagen inhaltsgleich gestaltet werden.