Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)284 B

UNIKASSEL VERSITÄT

Fachbereich Wirtschaftswissenschaften

Institut für Wirtschaftsrecht

Prof. Dr. Alexander Roßnagel

Universität Kassel
Nora-Platiel-Str. 5 • D - 34109 Kassel

An den Vorsitzenden des Innenausschusses
Des Deutschen Bundestags
Herrn Wolfgang Bosbach

Universität Kassel
Fachgebiet Öffentliches Recht,
insb. Umwelt- und Technikrecht
Nora-Platiel-Straße 5
34109 Kassel

a.rossnagel@uni-kassel.de
fon +49-561 804 3130
fax +49-561 804 3737

Sekretariat: Edith Weise
fon +49-561 804 2874

14. April 2015

Schriftliche Stellungnahme zur Sachverständigenanhörung am 20. April 2015 zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)

Der Gesetzentwurf ist grundsätzlich zu begrüßen, da er das Ziel verfolgt, die „IT-Sicherheit von Unternehmen“ zu verbessern und den „Schutz der Bürgerinnen und Bürger im Internet“ zu verstärken. Mit ihm soll „eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme in Deutschland“ erreicht werden. Die neuen Regelungen sollen dazu dienen, „den Schutz der Systeme im Hinblick auf die Schutzgüter der IT-Sicherheit (Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität) zu verbessern, um den aktuellen und zukünftigen Gefährdungen der IT-Sicherheit wirksam begegnen zu können“.[1]

Dieser Zielsetzung ist eine eminent hohe Bedeutung beizumessen, da Informationstechnik inzwischen alle Bereiche des gesellschaftlichen Lebens durchdringt. Insbesondere Kritische Infrastrukturen, deren Funktionieren für das gesellschaftliche Zusammenleben entscheidend ist, sind von der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der von ihnen genutzten Informationstechnik existenziell abhängig. Ihr Ausfall, ihre Manipulation oder ihre Beeinträchtigung könnte gravierende Schäden und Folgen in alle gesellschaftlichen Bereiche hervorrufen.[2] Daher ist es notwendig, dass alle Kritischen Infrastrukturen ein hohes und gleichmäßiges Niveau der IT-Sicherheit gewährleisten.

Um dieses Ziel zu erreichen, ist vorgesehenen, dass alle Betreiber Kritischer Infrastrukturen ein Mindestniveau an IT-Sicherheit einhalten und nachweisen sowie IT-Sicherheitsvorfälle an das BSI melden. Dieses wertet die Vorfälle aus und stellt seine Erkenntnisse den Betreibern zur Verfügung, damit diese ihre Infrastrukturen besser schützen können. Zusätzlich werden alle Anbieter von Telemedien und Telekommunikation zu entsprechenden Sicherheitsmaßnahmen verpflichtet. Die Telekommunikationsanbieter sollen zudem IT-Sicherheitsvorfälle, die zu einem unerlaubten Zugriff auf die Systeme der Nutzerinnen und Nutzer führen können, melden und betroffene Nutzerinnen und Nutzer über bekannte Störungen informieren.

---

1 BT-Drs. 18,/4096, 1.

2 S. hierzu bereits die Szenarien in Roßnagel/Wedde/Hammer/Pordesch, Die Verletzlichkeit der Informationsgesellschaft, Wiesbaden 1989.

Zu dem Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme sind die folgenden Bemerkungen angebracht:

1. „Sicherheit der Informationstechnik"

Die Aufgaben des BSI, deren Erfüllung durch diesen Entwurf unterstützt werden soll, beruhen auf der Schutzpflicht des Staates für die Verwirklichung der Grundrechte der Bürger und der staatlichen Verantwortung für das Funktionieren der Infrastrukturen, die für das gesellschaftliche Zusammenleben entscheidend sind. [3] Dies gilt nicht nur für den Schutz und die Förderung der Grundrechte auf freie Entfaltung der Persönlichkeit, Leben und körperliche Unversehrtheit und Freiheit der Fortbewegung, freie Berufsausübung und Schutz des Eigentums, sondern insbesondere auch auf Fernmeldegeheimnis, informationeller Selbstbestimmung sowie Vertraulichkeit und Integrität informationstechnischer Systeme.[4] Zwar hat der Staat einen großen Entscheidungsspielraum, wie er seine Schutzpflicht erfüllt. Dieser ist erst dann überschritten, wenn der Schutz ein Untermaß unterschreitet. Doch kann es bei der Verbesserung des BSIG nicht darum gehen, nur das absolute Mindestmaß an Bürgersicherheit zu erreichen. Vielmehr muss das Ziel sein, eine angemessene Bürgersicherheit zu gewährleisten, die der Bürger von einem um seine Sicherheit bemühten Staat erwarten kann. Bürger und Unternehmen sind von der (Un-)Sicherheit der IT und der Telekommunikation stark betroffen. Sie benötigen vor allem Informationen über IT-Risiken und Unterstützung bei Schutzmaßnahmen. Beides zu bieten, ist die vornehmste Aufgabe des BSI.

In diesem Sinn würde man in einem Gesetz, das den Titel trägt „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)" unter anderem Regelungen zu folgenden Themen der IT-Sicherheit erwarten:

- Sicherheitsanforderungen an Hersteller von Hardware und Software (Produktsicherheit),
- Nachbesserungspflichten von Herstellern von Hard- und Software,
- Sicherheitsanforderungen an IT-Dienstleister und IT-Dienstleistungen,
- Verringerung von Abhängigkeiten hinsichtlich einzelner IT-Systeme,
- Reduzierung von Schadenspotentialen,
- Haftung für Sicherheitsverletzungen von Herstellern (Produkthaftung, Produzentenhaftung, Schutzgesetze), Verkäufer von Hardware und Software (Gewährleistung, Fehlerbegriff, zugesicherte Eigenschaft, berechtigte Erwartung des Käufers) sowie Dienstleistern (Sicherheitspflichten und berechtigte Sicherheitserwartung der Nutzer),
- Instrumente, die Anreize für die Nutzer bieten, Maßnahmen zur IT-Sicherheit in ihren Geräten und Programmen zu nutzen
- Infrastrukturen für Dienstleister und Nutzer, die sie in die Lage versetzen, selbstbestimmt IT-Sicherheit für ihre Interessen herzustellen.
- Beratung und Unterstützung durch staatliche Institutionen, insbesondere durch das BSI, im Sinn von Bürger-Helpdesk für IT-Sicherheit

Der zu kommentierende Gesetzentwurf strebt jedoch nicht an, diese Themen zu bearbeiten, sondern beschränkt sich darauf, die IT-Sicherheit in Kritischen Infrastrukturen zu erhöhen. Dies ist schwer genug. Es

---

[3] S. hierzu bereits die Anmerkungen zum ersten BSIG in Roßnagel/Bizer/Hammer/Pordesch, Ein Bundesamt für die Sicherheit in der Informationstechnik - Kritische Bemerkungen zum Gesetzentwurf der Bundesregierung, DuD 1990, 178 ff. und Roßnagel/Bizer, Sicherheit in der Informationstechnik - Aufgabe für ein neues Bundesamt, Kritische Justiz, 1990, 436 ff.

[4] S. z.B. BVerfGE 38, 1; 49, 89; 57, 295; 73, 118; 90, 60; 114, 371; 119, 181.

wäre schon ein großer Fortschritt, wenn es gelingen würde, wenigsten die Kritischen Infrastrukturen sicherer zu machen und damit indirekt zugleich auch die Sicherheit aller Unternehmen und Bürger zu stärken. Allerdings sollte der Titel des Gesetzes dem Schwerpunkt der Regelungen angepasst werden und keinen Anspruch geltend machen, der nicht eingelöst werden kann.

2. Grundrechtseingriffe

Die vorgesehenen Regelungen sind Eingriffe in das Grundrecht der Betreiber Kritischer Infrastrukturen sowie der Anbieter von Telemediendiensten, der Betreiber von Telekommunikationsnetzen und der Anbieter von Telekommunikationsdiensten auf Ausübung ihrer Berufsfreiheit nach Art. 12 Abs. 1 GG. Ein Eingriff in die Berufsausübung ist auf gesetzlicher Grundlage zulässig, wenn „Gesichtspunkte der Zweckmäßigkeit" ihn verlangen, um Gefahren für andere Grundrechtsträger oder die Allgemeinheit auszuschließen.[5]

Der Schutz Kritischer Infrastrukturen ist von höchstem Allgemeininteresse. Sicherheitsvorkehrungen, um das gebotene Sicherheitsniveau zu gewährleisten, und ihr Nachweis sind ebenso dringende Maßnahmen zur Wahrung dieses Allgemeininteresses wie der Aufbau eines kooperativen Informationssystems für die informationstechnische Sicherheit in Kritischen Infrastrukturen. Der Betrieb Kritischer Infrastrukturen ohne ausreichende Sicherungsmaßnahmen und ohne eine ausreichende Kenntnis über die Sicherheits- und Bedrohungslage, wäre unsachgemäß und würde für alle gesellschaftlichen Bereiche große Gefahren hervorrufen. Daher sind die mit ihnen verbundenen Eingriffe in die Freiheit der Berufsausübung zum Schutz der Rechte Dritter und vor allem zur Sicherheit der Allgemeinheit geboten.

Die genannten Maßnahmen sind auch verhältnismäßig. Sie sind geeignet, um dem Ziel einer ausreichenden Sicherheit für Kritische Infrastrukturen deutlich näher zu kommen. Auf die im Entwurf vorgesehenen Maßnahmen kann nicht grundsätzlich zugunsten anderer, weniger eingreifender Maßnahmen verzichtet werden. Soweit branchenspezifische Standards besser passen, um die erforderliche Sicherheit zu gewährleisten, können diese nach § 8a Abs. 2 BSIG-E für verbindlich erklärt werden. Da der Entwurf auch viele Maßnahmen vorsieht, um die Belastung durch den Grundrechtseingriff gering zu halten, sind die neuen Pflichten auch angemessen. Hierfür ist zu berücksichtigen, dass

- Kleinstunternehmer nach § 8c Abs. 1 BSIG-E vom Anwendungsbereich der Sicherungs- und Meldepflichten ausgenommen sind,
- die Sicherheitsmaßnahmen nach § 8a Abs. 1 Satz 3 BSIG-E ausdrücklich „angemessen" sein müssen,
- für die Sicherheitsanforderungen nach § 8a Abs. 1 Satz 2 BSIG-E, § 13 Abs. 7 TMG und § 109 Abs. 2 TKG nur der Stand der Technik berücksichtigt werden muss und dieser in seiner Definition bereits das Verhältnismäßigkeitsprinzip integriert hat,
- Meldungen, die nicht tatsächliche Ausfälle oder Beeinträchtigungen betreffen, nach § 8b Abs. 4 Satz 3 BSIG-E gegenüber dem BSI anonym mitgeteilt werden können,
- ein hoher Schutz für die gemeldeten Informationen gewährt wird (z.B. nach § 8d BSIG-E).

Die mit dem Gesetzentwurf verbundenen Grundrechtseinschränkungen der freien Berufsausübung sind daher als gesetzliche Eingriffe, die dem Verhältnismäßigkeitsprinzip entsprechen mit Art. 12 Abs. 1 GG vereinbar. [6]

---

[5] S. z.B. BVerfGE 7, 377 (406).

[6] S. zu spezifischen Grundrechtsaspekten noch in den folgenden Ausführungen.

3. Definition Kritischer Infrastrukturen

Nach § 2 Abs. 10 BSIG-E werden Kritische Infrastrukturen sehr abstrakt umschrieben als „Einrichtungen, Anlagen oder Teile“ in Infrastrukturen, die 1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und 2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“. In § 10 Abs. 1 Satz 1 BSIG-E wird das Bundesministerium ermächtigt, die Kritischen Infrastrukturen im Sinne dieses Gesetzes näher zu bestimmen. In der Begründung zu § 10 Abs. 1 Satz 1 BSIG-E wird näher ausgeführt, nach welcher Methode die Bestimmung erfolgen soll.

Der Gesetzestext ist jedoch erheblich weniger präzise als die Begründung. Es stellt sich deshalb die Frage, ob diese Verordnungsermächtigung entsprechend Art. 10 GG „Inhalt, Zweck und Ausmaß“ ausreichend bestimmt benennt. Dagegen spricht, dass die Adressaten des Gesetzes in diesem selbst nicht eindeutig benannt werden, obwohl das Gesetz für sie schwerwiegende Rechtsfolgen festlegt.[7]

Bei der Anwendung der rechtsstaatlichen und demokratieschützenden Vorgaben des Art. 80 Abs. 1 Satz 2 GG ist zu beachten, dass diese Vorschrift bezweckt, die Entscheidungshoheit des Bundestages zu wahren und die Vorhersehbarkeit der Verordnungsregelungen für die Betroffenen zu gewährleisten.[8] Zugleich ist aber auch die Eigenlogik, Komplexität und Dynamik des zu regelnden Bereiches zu beachten.[9] Hinsichtlich der rechtsstaatlichen Zielsetzung wird eine sehr genaue Bestimmung der betroffenen Adressaten nach eindeutigen Merkmalen notwendig. Es wird eine Beschreibung der Typen von Einrichtungen, Anlagen oder Teile in Infrastrukturen erforderlich sein, die qualitative und quantitative Merkmale enthält, die ausreichend unterscheidungsstark sind. Im Detaillierungsgrad, in der Darstellungsform und im Umfang[10] könnte die Aufstellung dem Katalog von immissionsschutzrechtlich genehmigungsbedürftigen Anlagen im Anhang zur Vierten Bundes-Immissionsschutzverordnung entsprechen. Ein solcher Detaillierungsgrad ist in einer gesetzlichen Definition jedoch nicht möglich.

Für den Katalog im Anhang zur Vierten Bundes-Immissionsschutzverordnung gilt die Ermächtigungsgrundlage in § 4 Abs. 1 Satz 1 BImSchG seit 1974 als ausreichend bestimmt. Nach dieser dürfen Anlagen als genehmigungsbedürftig in einer Rechtsverordnung festgelegt werden, die „auf Grund ihrer Beschaffenheit oder ihres Betriebs in besonderem Maße geeignet sind, schädliche Umwelteinwirkungen hervorzurufen oder in anderer Weise die Allgemeinheit oder die Nachbarschaft zu gefährden, erheblich zu benachteiligen oder erheblich zu belästigen“. Diesem Grad an Bestimmtheit genügen auch §§ 10 Abs. 1 Satz 1 i.V.m. § 2 Abs. 10 BSIG-E. Eine konkretere Bestimmung der Adressaten im Gesetz ist nicht notwendig. In Verbindung mit einer Rechtsverordnung, die das Präzisionsniveau der Vierten Bundes-Immissionsschutzverordnung erfüllt, ist dem rechtsstaatlichen Bestimmtheitsgebot Genüge getan.

---

7 S. hierzu z.B. Roos, Der neue Entwurf eines IT-Sicherheitsgesetzes, MMR 2014, 724f.; Roth, Neuer Referentenentwurf zum IT-Sicherheitsgesetz, ZD 2015, 19; kritisch ebenfalls Leisterer/Schneider, Der überarbeitete Entwurf für ein IT-Sicherheitsgesetz. Überblick und Problemfelder, CR 2014, 577; eine Konkretisierung des Betreiberbegriffs fordert Eckardt, Der Referenten-Entwurf zum IT-Sicherheitsgesetz – Schutz der digitalen Zukunft?, ZD 2014, 600.

8 S. z.B. BVerfGE 78, 249 (272); Pieroth, in: Jarass/Pieroth (Hrsg.), Grundgesetz-Kommentar, 12. Aufl. München 2012, Art. 80 Rn. 1.

9 S. z.B. BVerfGE 48, 210 (221); 76, 130 (143); 123, 39 (80).

10 Roth, (Fn. 7), ZD 2015, 19, erwartet eine „riesige Liste“.

Durch die Verordnungsermächtigung des § 10 Abs. 1 Satz 1 BSIG-E gibt zwar der Gesetzgeber einen großen Entscheidungsspielraum an das Bundesministerium des Innern ab. Es regelt aber wichtige Merkmale des Verfahrens, in dem die Adressaten des Gesetzes festgelegt werden. Das Bundesministerium des Innern soll den Spielraum nämlich nicht allein füllen. Vielmehr hat es zuvor Vertreter der Wissenschaft, der betroffenen Betreiber und der betroffenen Branchenverbände[11] anzuhören und danach die Einrichtungen, Anlagen oder Teile, die als Kritische Infrastrukturen gelten sollen, im Einvernehmen mit neun weiteren Bundesministerien festzulegen. Es ist nachvollziehbar, wenn die Bundesregierung ausführt, dass die Präzisierung des Begriffs der Kritischen Infrastrukturen „der sektor- und branchenspezifischen Einbeziehung aller betroffenen Kreise" bedarf und „nur in einem gemeinsamen Arbeitsprozess mit Vertretern … der Betreiber … und unter Einbeziehung der Expertise von externen Fachleuten erarbeitet werden" kann.[12]

Außerdem hat der Gesetzgeber die beiden Hauptkriterien, die diese Entscheidung leiten sollen, inhaltlich festgelegt. § 10 Abs. 1 Satz 1 BSIG-E bestimmt zum einen, dass die Kritischen Infrastrukturen im Sinne des Gesetzes den sieben Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören müssen. Zum anderen legt er fest, dass die Dienstleistungen im Hinblick auf ihre Bedeutung für das Funktionieren des Gemeinwesens[13] als kritisch und bezogen auf ihren Versorgungsgrads als bedeutend anzusehen sein müssen. Außerdem präzisiert er, zwar nicht im Gesetzestext, aber in seiner Begründung,[14] die Methode der Auswahl und gibt damit dem Bundesministerium des Innern sehr genaue Vorgaben.

Der Gesetzgeber legt nach dem Entwurf also sowohl Kriterien als auch Verfahren ausreichend bestimmt fest, so dass die Vorschrift mit Art. 80 Abs. 1 Satz 2 GG vereinbar ist.

4. Sicherheitsniveau für die Informationstechnik Kritischer Infrastrukturen

Der Entwurf bestimmt für die in der Verordnung nach § 10 Abs. 1 BSIG-E genannten Kritischen Infrastrukturen nach § 8a Abs. 1 Satz 1 BSIG-E, dass ihre Betreiber „angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen" haben, „die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind".

a) Stand der Technik

Nach § 8a Abs. 1 Satz 2 BSIG-E, § 109 Abs. 2 TKG und § 13 Abs. 7 TMG wird bestimmt, dass bei der Gewährleistung des IT-Sicherheit „der Stand der Technik zu berücksichtigen" ist.

Eine Definition, was unter dem „Stand der Technik zu verstehen ist, findet sich in keiner der drei Vorschriften im Text. Dieser Begriff wird nur in der Begründung zu § 8a Abs. 1 Satz 2 BSIG-E definiert, in den Begründungen zu den beiden anderen Vorschriften nicht. Dagegen wird in vielen anderen Gesetzen dieser Begriff definiert und zwar jeweils – entsprechend dem Schutzgut oder der Zielsetzung des Gesetzes – leicht

---

11 S. hierzu die Stellungnahme der Bundesrates, BT-Drs. 18/4096, 81, und die zustimmende Gegenäußerung der Bundesregierung, BT-Drs. 18/4096, 88.

12 Gegenäußerung der Bundesregierung, BT-Drs. 18/4096, 84.

13 Diese wird nach § 2 Abs. 10 Satz 1 Nr. 2 BSIG-E dadurch bestimmt, dass durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.

14 BT-Drs. 18/4096, 52 ff.

unterschiedlich.[15] Was unter dem Stand der Technik im Sinn des BSIG-E, im TMG-E und im TKG-E jeweils zu verstehen ist, sollte im Gesetzestext festgelegt werden.[16] Steht die Definition nur in der Begründung, nimmt sie nicht an der Wortlautauslegung teil, sondern kann höchstens im Rahmen der historischen Auslegung berücksichtigt werden.

Trotz Definition[17] bleibt unklar, was alles für den Stand der Technik berücksichtigt werden soll und auf was sich dieser Stand bezieht. Um in diesen Fragen Rechtssicherheit zu erreichen, wurde z.B. für § 3 Abs. 6 Satz 2 BImSchG ein Verweis aufgenommen, dass bei der Bestimmung des Standes der Technik insbesondere die in der Anlage zum Bundes-Immissionsschutzgesetz aufgeführten Kriterien zu berücksichtigen sind. Nach dieser Anlage sind bei der Bestimmung des Standes der Technik „unter Berücksichtigung der Verhältnismäßigkeit zwischen Aufwand und Nutzen möglicher Maßnahmen sowie des Grundsatzes der Vorsorge und der Vorbeugung, jeweils bezogen auf Anlagen einer bestimmten Art, insbesondere“ 13 im Folgenden genannte „Kriterien zu berücksichtigen“.[18] Eine solche Anlage, die der Gesetzgeber als Teil des Gesetzes formuliert, erhöht die Bestimmtheit der gesetzlichen Sicherheitspflichten und erleichtert die Gewährleistung und Prüfung der IT-Sicherheit.

Der Stand der Technik ist immer „unter Berücksichtigung der Verhältnismäßigkeit zwischen Aufwand und Nutzen möglicher Maßnahmen“ zu bestimmen. Er setzt voraus, dass die Maßnahme technisch möglich und für den durchschnittlichen Betreiber zumutbar ist. Wenn die Maßnahme „mit Erfolg im Betrieb erprobt“ sein muss, dann müssen Unternehmen die Maßnahme seit einer gewissen Zeit unter Berücksichtigung des Verhältnisses von Aufwand und Nutzen im regulären Betrieb nutzen. Mit der Vorgabe des Standes der Technik ist daher die Angemessenheit der Sicherheitsmaßnahme, insbesondere aber, dass sie technisch möglich und zumutbar ist, bereits gefordert. Die Forderung der Angemessenheit, der technischen Machbarkeit und der Zumutbarkeit sind somit überflüssig, wenn bereits der Stand der Technik gefordert wird. In § 13 Abs. 7 TMG-E, in § 109 Abs. 2 TKG-E und in § 8a Abs. 1 Satz 3 BSIG-E können die entsprechenden Passagen als unnötige Verdopplung des Gesetzestextes gestrichen werden.

Nach den Formulierungen in § 8a Abs. 1 Satz 2 BSIG-E, § 109 Abs. 2 TKG-E und § 13 Abs. 7 TMG-E ist der Stand der Technik nur zu „berücksichtigen“,[19] nicht jedoch zu befolgen. „Berücksichtigen“ heißt immer nur, dass eine Forderung zur Kenntnis zu nehmen und ihre Erfüllung zu erwägen, aber gerade nicht, dass sie einzuhalten ist.[20] Nach der Formulierung in den drei Regelungen kann also immer auch von dem Sicherheitsniveau, das der Stand der Technik beschreibt, nach unten abgewichen werden. Welches Sicherheitsniveau durch die drei Regelungen erreicht wird, bleibt somit letztlich der Entscheidung des Betreibers überlassen. Eine Einheitlichkeit im Sicherheitsniveau kann mit dem „Berücksichtigen“ des Standes der Technik gerade nicht erreicht werden. Das Sicherheitsniveau wird auch nicht durch den Begriff der „angemessenen“ Vorkehrungen bestimmt, weil die Angemessenheit sich nicht auf das Sicherheitsziel, sondern nur auf das Verhältnis von Aufwand und Nutzen bezieht. Insgesamt ist daher festzustellen, dass das grundlegende Ziel

---

15 S. z.B. in § 3 Abs. 6 BImSchG, § 3 Abs. 28 KrWG oder § 3 Nr. 11 WHG.

16 Wie in den Vorversionen des Entwurfs.

17 S. BT-Drs. 18/4096, 42.

18 Solche Anlagen zum Stand der Technik enthalten auch das KrWG und das WHG.

19 Ebenso Art. 14 Abs. 1 des Entwurfs der NIS-RL. Die Bestimmungen der NIS-RL stellen jedoch nach Art. 2 nur Mindestanforderungen dar, die die Mitgliedstaaten nicht daran hindern, Bestimmungen zur Gewährleistung eines höheren Sicherheitsniveaus zu erlassen oder aufrechtzuerhalten.

20 S. auch Eckardt, (Fn. 7), ZD 2014, 600.

des Gesetzes, in allen Kritischen Infrastrukturen ein hohes und gleichmäßiges Niveau der IT-Sicherheit zu gewährleisten,[21] durch die Regelung in § 8a Abs. 1 BSIG-E verfehlt wird. Notwendig ist daher, dass der Stand der Technik nicht nur berücksichtigt, sondern erreicht wird.

Dies schließt nicht aus, alternative Lösungen zu wählen, die in einer nationalen oder internationalen technischen Norm nicht enthalten sind. Diese Alternativen müssen aber das gleiche Sicherheitsniveau bieten wie die technischen Normen. Dieses kann aber mit unterschiedlichen Mitteln oder auf anderen Wegen erreicht werden. Soweit der Stand der Technik verbindlich und nicht nur zu berücksichtigen ist, bleibt auch bei Alternativen das Niveau gewahrt und ist für alle Kritische Infrastrukturen gleich.

b) Branchenspezifische Standards

Da die Sicherheitsprobleme in den verschiedenen Sektoren und Branchen unterschiedlich sind, ist es sinnvoll, dass die Betreiber Kritischer Infrastrukturen und ihre Branchenverbände nach § 8a Abs. 2 BSIG-E branchenspezifische Sicherheitsstandards zur Gewährleistung der Anforderungen nach § 8a Abs. 1 BSIG-E vorschlagen können. Diese können die Probleme und Möglichkeiten der Branchen unter Umständen konkreter und wirksamer adressieren.[22] Um bei dieser Selbstregulierung eine „Selbstbedienung" der Regelungsadressaten auszuschließen,[23] ist es notwendig, dass das BSI auf Antrag feststellt, ob diese geeignet sind, die Anforderungen nach § 8a Abs. 1 BSIG-E zu gewährleisten. Dieser feststellende Verwaltungsakt ist inhaltlich nur möglich, wenn der Stand der Technik nach § 8a Abs. 1 Satz 2 BSIG-E verbindlich ist. Ist er nur zu berücksichtigen, hat das BSI keinen festen Maßstab, nach dem es eine gleiche Eignung der branchenspezifischen Sicherheitsstandards bemessen kann. Unklar ist auch, wie repräsentativ der Branchenverband für die Branche sein muss.[24]

c) Nachweise der Sicherheit

Die Betreiber Kritischer Infrastrukturen haben nach § 8a Abs. 3 Satz 1 BSIG-E mindestens alle zwei Jahre die Erfüllung der Anforderungen in § 8a Abs. 1 BSIG-E „auf geeignete Weise nachzuweisen".[25] Welcher Nachweis „geeignet" ist, wird nicht festgelegt. Diese Frage wird aber in der Praxis entscheidend sein. Unklar ist, ob nur Nachweise über das Sicherheitskonzept oder auch seine Umsetzung zu erbringen sind, ob eine Prüfung von Unterlagen genügt oder eine Prüfung vor Ort erforderlich ist, ob eine Besichtigung ausreicht oder eine Kontrolle (wie lange?) des laufenden Betriebs notwendig ist? Muss nur die Sicherheit der eingesetzten Technik (Hard- und Software) nachgewiesen werden oder auch das Bestehen oder Funktionieren eines Sicherheitsmanagementsystems? Genügen Selbstbestätigungen des Betreibers, eines Lieferanten oder eines Herstellers oder müssen alle Bestätigungen von einem Dritten stammen? Welche Qualifikation, Erfahrung und Unabhängigkeit muss dieser Dritte haben? Diese Fragen[26] sind entscheidend dafür, welchen Aufwand der Sicherheitsnachweis beim Regelungsadressaten verursacht und ob er zur Erreichung des gesetzlichen Ziels überhaupt geeignet und ob eine bestimmte Form des Nachweises erforderlich und verhältnismäßig ist. Die Fragen dürfen weder unbeantwortet bleiben noch dem BSI ohne gesetzliche Vorgaben überlassen blei-

---

21 S. BT-Drs. 18/4096, 1.

22 S. auch Roth, (Fn. 7), ZD 2015, 21.

23 S. hierzu Roßnagel, Konzepte der Selbstregulierung, in: ders. (Hrsg.), Handbuch Datenschutzrecht, München 2013, 408f.

24 S. auch Eckardt, (Fn. 7), ZD 2014, 600.

25 Art. 15 Abs. 2 b) des Entwurfs der NIS-RL fordert eine „Sicherheitsüberprüfung …, die von einer qualifizierten unabhängigen Stelle oder einer zuständigen nationalen Behörde durchgeführt wird".

26 S. ansatzweise Antworten hierzu in BT-Drs. 18/4096, 44.

ben. Vielmehr sind diese Fragen wegen des Wesentlichkeits- und Bestimmtheitsprinzips im Grundsatz durch das Gesetz und im Detail durch eine Verordnung zu bestimmen. Insofern ist eine Ergänzung des § 8a BSIG-E erforderlich, in der zumindest die Frage des Gegenstands, des Umfangs, der Tiefe und des Verantwortlichen festgelegt wird, um die Eignung des Nachweises beurteilen zu können. Außerdem ist eine Ergänzung des § 10 BSIG-E erforderlich, die eine Ermächtigung enthält, in einer Rechtsverordnung die Nachweise ausreichender Sicherheit zu regeln. Alternativ könnte eine Regelung wie in § 11 Abs. 1a Satz 6 EnWG-E gewählt werden, dass die Behörde „nähere Bestimmungen zu Format, Inhalt und Gestaltung" des Sicherheitsnachweises trifft.

Soweit für einzelne Aspekte der Sicherheitsgewährleistung Sicherheits-Audits oder -Zertifizierungen angeboten werden, kann nach § 8a Abs. 3 Satz 2 BSIG-E der Nachweis der Sicherheit auch durch die Vorlage der Audit- oder Zertifizierungsdokumente erbracht werden. Dabei ist zu unterscheiden, dass das Sicherheit-Audit nur die Eignung eines Sicherheitsmanagementsystems bestätigen kann und deswegen von Betreiber der Kritischen Infrastruktur in Auftrag gegeben werden muss. [27] Dagegen betrifft das Sicherheits-Zertifikat ein IT-Produkt, einen Prozess oder ein Profil[28] und kann nur vom Hersteller beauftragt werden.[29] Wozu noch Prüfungen, die § 8a Abs. 3 Satz 2 BSIG-E als dritte Möglichkeit erwähnt, hilfreich oder erforderlich sind, ist auch nach der Lektüre der Gesetzesbegründung[30] unklar. Eine Prüfung als solche bestätigt noch kein Ergebnis. Wenn aber das Ergebnis der Prüfung ein Sicherheitsmanagementsystem oder ein Produkt betrifft, kann es auch als Bestätigung eines Audits oder als Zertifikat ausgestellt werden. Für die Akzeptanz des Audits oder des Zertifikats kommt es aber entscheidend darauf an, wer es ausgestellt und nach welcher Methode und in welchem Verfahren er sein Ergebnis festgestellt hat. Auch die Beantwortung dieser Fragen kann nicht ohne gesetzliche Kriterien dem BSI überlassen, sondern muss zumindest dem Grundsatz nach im Gesetz erfolgen. Einzelheiten können einer Rechtsverordnung überlassen werden.

Die Frage, welche Anforderungen an denjenigen zu stellen sind, der ein Sicherheitszertifikat oder ein Datenschutzaudit ausstellt,[31] betrifft dessen Grundrecht auf freie Berufswahl und bedarf daher einer gesetzlichen Regelung. Aus diesem Grund wurde z.B. die Vorschrift des § 18 SigG, die im ersten Signaturgesetz von 1997 noch fehlte, im Jahr 2001 in das neue Signaturgesetz aufgenommen.[32]

Bei der Prüfung der Sicherheitsnachweise und bei der Anordnung nach § 8a Abs. 3 Satz 4 BSIG-E, Sicherheitsmängel zu beseitigen, wird sich in vielen Fällen herausstellen, dass der Betreiber der Kritischen Infrastruktur Verbesserungen der Sicherheit nur im Rahmen der von ihm genutzten Hard- und Software durchführen kann.[33] Mängel dieser technischen Systeme kann er nur beseitigen und Verbesserungen kann er nur erreichen, wenn der Hersteller der Soft- oder Hardware mitwirkt oder diese Maßnahmen selbst durchführt. Soweit für den Hersteller die deutsche Rechtsordnung gilt, könnte das Gesetz für ihn Mitwirkungspflichten vorsehen. Soweit er nicht der deutschen Rechtsordnung unterliegt oder eine Monopolstellung hat, wird auch das nicht weiterführen.

---

27 S. näher Roßnagel, Datenschutzaudit – Konzeption, Durchführung, Gesetzliche Regelung, Wiesbaden 2000, 56 ff.

28 S. näher § 2 Abs. 7 BSIG.

29 S. zur Unterscheidung von Audit und Zertifikat s. Roßnagel, Das Konzept des Datenschutzaudits, in: ders. (Hrsg.), Handbuch Datenschutzrecht, München 2003, 462 ff.

30 S. BT-Drs. 18/4096, 44.

31 S. hierzu auch BT-Drs. 18/4096, 44.

32 S. näher Roßnagel, in: ders (Hrsg.), Recht der Telemediendienste, München 2013, § 18 SigG, Rn. 9f.

33 Auf die steigende Verantwortung der Hersteller verweist auch BT-Drs. 18/4096, 3.

Daher sind unbedingt Sicherheitszertifizierungen zu forcieren. Hierfür müssen „unwiderstehlich" Anreize geschaffen werden. Ein wichtiger Anreiz könnte sein, wenn die Zertifizierung ein wesentliches Kriterium für die Vergabe von Aufträgen öffentlicher Stellen wäre. Diese Voraussetzung für Aufträge der öffentlichen Hand würde die Kosten für Zertifizierungen bei den Herstellern erträglicher machen. Für privatwirtschaftliche Unternehmen, die Kritische Infrastrukturen betreiben, wäre ein wichtiger Vorteil, wenn bei zertifizierten Produkten unterstellt würde, dass sie die Sicherheitsvoraussetzungen erfüllen, bei nicht-zertifizierten Techniksystemen, diese aber eigens nachgeprüft werden müsste.

d) Ausnahmen von den Sicherheitspflichten

Da die Vorgaben des § 8a BSIG-E nur „Mindestanforderungen"[34] an die IT-Sicherheit von Kritischen Infrastrukturen formulieren wollen, ist es sinnvoll in § 8c Abs. 2 BSIG-E die Betreiber von Kritischen Infrastrukturen auszunehmen, die spezielleren oder weitergehenden Sicherheitsanforderungen unterliegen. Dies wird in § 8c Abs. 2 Nr. 1 bis 3 BSIG-E sehr präzise festgelegt, in Nr. 4 jedoch sehr unbestimmt gehalten, wenn auf „Anforderungen" verwiesen wird, die „nach § 8a vergleichbar oder weitergehend sind". Zwar ist eine gewisse Flexibilität notwendig, weil künftig immer wieder neue Anforderungen auf Unions- oder Bundesebene entstehen können.[35] Dennoch stellt sich die Frage, ob nicht mit wenig gesetzgeberischem Aufwand, die Rechtssicherheit erhöht werden kann.

Die Frage, ob die konkurrierenden Rechtsvorschriften „weitergehend" sind, ist noch relativ leicht zu beantworten, wenn es um die gleichen Themen geht wie in § 8a BSIG. Es wird jedoch immer schwieriger, zu einer klaren Antwort zu gelangen, wenn die Rechtsvorschriften unterschiedliche Themen betreffen. Sind die anderen Rechtsvorschriften weitergehend, wenn sie z.B. die Einhaltung des Standes der Technik fordern, aber nur alle vier Jahre einen Sicherheitsnachweis verlangen und keine Nachbesserungspflichten kennen? Das Problem liegt in der starren Rechtsfolge, dass bei „weitergehenden" Rechtsvorschriften § 8a BSIG-E *insgesamt* nicht anwendbar ist. Daher wird empfohlen, § 8a BSIG-E nur „insoweit" nicht anwendbar zu erklären, als andere Rechtsvorschriften, weitergehend sind.

Schwieriger wird der Vollzug des Gesetzes, wenn es um die Frage geht, ob die anderen Rechtsvorschriften „vergleichbar" sind. Sind die Rechtsvorschriften in dem oben genannten Beispiel „vergleichbar", wenn sie in Bezug auf § 8a BSIG-E unterschiedliche hohe Anforderungen stellen? Auch hier würde eine Flexibilisierung durch eine „Soweit"-Regelung den Vollzug erleichtern.

5. IT-Sicherheits-Informationssystem

Die Vorschriften der § 8b Abs. 3 bis 5 BSIG-E, § 44b AtG-E, § 11 Abs. 1c EnWG-E und § 109 Abs. 5 TKG-E etablieren ein Informationssystem zwischen Betreibern Kritischer Infrastrukturen, dem BSI und den zuständigen Aufsichtsbehörden, um bei Störungen der Sicherheit ein Lagebild zu erstellen und unter den Teilnehmern einen Informationsaustausch zu etablieren, von dem durch die Zusammenführung und Auswertung der Informationen alle profitieren sollen.[36] Ein solches Informationssystem zur Vorsorge und zur Abwehr von Sicherheitsproblemen und -angriffen zu betreiben, ist zum Schutz der Kritischen Infrastrukturen notwendig.

---

34 S. BT-Drs. 18/4096, 2, 29, 42.

35 S. BT-Drs. 18/4096, 50.

36 S. BT-Drs. 18/4096, 45.

a) Meldepflichten der Betreiber von Kritischen Infrastrukturen

Betreiber Kritischer Infrastrukturen haben nach § 8b Abs. 4 Satz 1 BSIG-E „erhebliche" Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen führen können oder bereits geführt haben, unverzüglich an das BSI zu melden.[37] Wann eine Störung „erheblich" ist, wird – trotz der kurzen Erläuterung in der Entwurfsbegründung[38] – zu einer gewissen Unsicherheit führen. Hier wäre ein Leitfaden, mit Kriterien für meldungsrelevante Sicherheitsvorfälle, wie sie die Entwurfsbegründung ankündigt,[39] für die Einschätzung der Erheblichkeit durch die Betreiber hilfreich.[40]

Der Vorschrift könnte gegen das Verbot der Selbstbeschuldigung[41] verstoßen.[42] Dies wäre dann der Fall, wenn eine allein meldepflichtige natürliche Person in die Zwangslage käme, sich selbst einer Straftat oder Ordnungswidrigkeit zu bezichtigen oder gegen die Vorschrift zu verstoßen. Da die Betreiber in der Regel juristische Personen sind und fast immer erklärungsberechtigte Personen verfügbar sind, die die nach der Vorschrift geforderte Meldung durchführen können, dürfte sich in der Praxis diese Zwangslage nie ergeben. Soweit eine solche Zwangslage befürchtet und daher ein Konflikt mit Verbot der Selbstbeschuldigung erwartet wird, würde die Regelung eines Verwendungsverbots wie in § 42a Abs. 6 BDSG eine grundrechtlich sichere Lösung des Problems darstellen.[43]

§ 8b Abs. 4 Satz 2 BSIG-E bestimmt sehr abstrakt, welche Angaben zu melden sind. Aufgeführt werden nur vier Angaben: 1. zur Störung, 2. zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, 3. zur betroffenen Informationstechnik und 4. zur Branche des Betreibers. Diese Angaben sind für einen rechtssicheren Vollzug der Meldung unzureichend.[44] Hilfreich wäre eine Ergänzung des Gesetzestextes, dass das BSI nähere Bestimmungen zu Inhalt und Form der Meldung trifft. Alternativ könnte auch in § 10 BSIG eine Ermächtigung zum Erlass einer Rechtsverordnung aufgenommen werden, um die näheren formalen und inhaltlichen Anforderungen für die Meldung zu konkretisieren. Dann könnte das BSI entscheiden, ob ein Formular oder ein Leitfaden oder eine andere Anleitung die größte Rechtssicherheit für die meldepflichtigen Betreiber bietet.[45]

Hinsichtlich der Nennung des Betreibers regelt § 8b Abs. 4 Satz 2 BSIG-E ein zweistufiges Verfahren: Nach diesem dürfen Meldungen zu Störungen ohne Ausfall oder Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur – über die „gemeinsame übergeordnete Ansprechstelle" des jeweiligen Sektors nach § 8b Abs. 5 BSIG-E – anonym gemeldet werden. Nur wenn die Störung „tatsächlich zu einem Ausfall oder

---

37 Nach Art. 14 Abs. 2 des Entwurfs der NIS-RL sollen die Betreiber „Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die Sicherheit der von ihnen bereitgestellten Kerndienste haben".

38 S. BT-Drs. 18/4096, 46.

39 S. BT-Drs. 18/4096, 48.

40 Nach Art. 14 Abs. 5 des Entwurfs der NIS-RL wird die Kommission ermächtigt, „delegierte Rechtsakte zu erlassen, in denen festgelegt wird, unter welchen Umständen bei Sicherheitsvorfällen für öffentliche Verwaltungen und Marktteilnehmer die Meldepflicht gilt".

41 S. z.B. BVerfGE 38, 105 (113 ff.); 55, 144 (150); 56, 37 (43).

42 So Eckhardt, (Fn. 7), ZD 2014, 600.

43 S. Hornung, in: Roßnagel, Recht der Telemediendienste, München 2013, § 15a TMG, Rn. 43 ff.

44 Ebenso Roth, (Fn. 7), ZD 2015, 21; Roos, (Fn. 7), MMR 2014, 727.

45 Nach Art. 14 Abs. 7 des Entwurfs der NIS-RL kann die Kommission in Durchführungsrechtsakten Formen und Verfahren der Meldungen festzulegen.

einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat", ist die Nennung des Betreibers erforderlich. Die Möglichkeit der gegenüber dem BSI anonymen Meldung ist sinnvoll, um ein vertrauensvolles kooperatives Informationssystem aufzubauen. Die anonymen Meldungen betreffen nur Störungen mit einem *potentiellen* Nachteil für die Kritische Infrastruktur und können dennoch – auch ohne aktuelles Risiko für die Kritische Infrastruktur – leicht zu einem Reputationsschaden des Betreibers führen.

Das Gesetz enthält keine Aufdeckungsregel für die „pseudonymen" Meldungen – wie etwa § 16 DeMailG.[46] Die „gemeinsame übergeordnete Ansprechstelle" des jeweiligen Sektors kennt den meldenden Betreiber und könnte das Pseudonym aufdecken. Hierzu wird sie jedoch nicht verpflichtet, datenschutzrechtlich ist ihr dies aufgrund des Zweckbindungsgrundsatzes untersagt. Das BSI kann also keine Aufdeckung der Identität des Meldenden verlangen, sondern allenfalls Rückfragen an diesen über die „gemeinsame übergeordnete Ansprechstelle" stellen, die dieser wieder über die „gemeinsame übergeordnete Ansprechstelle" vermittelt anonym beantworten kann.[47]

b) Ausnahmen von den Meldepflichten

§ 8c Abs. 3 BSIG-E bestimmt, dass diese Meldepflichten nach Nr. 1 auf Betreiber von öffentlichen Telekommunikationsnetzen und -diensten, nach Nr. 2 auf Betreiber von Energieversorgungsnetzen und Energieanlagen und nach Nr. 3 auf Betreiber von kerntechnischen Anlagen nicht anzuwenden sind. Nach Nr. 4 gilt dies auch für Betreiber, die auf Grund von Rechtsvorschriften „Anforderungen" erfüllen müssen, die „nach § 8b Abs. 3 bis 5 vergleichbar oder weitergehend sind".

Wie für die Ausnahmen von den Sicherheitspflichten[48] gilt auch für Ausnahmen nach § 8c Abs. 3 Nr. 4 BSIG-E, dass sie zu unbestimmt sind. Hier ergeben sich die gleichen Schwierigkeiten festzustellen, ob andere Rechtvorschriften „vergleichbar oder weitergehend" sind. Auch hier würde eine Flexibilisierung durch eine „Soweit"-Regelung den Vollzug erleichtern. Dies gilt umso mehr, als bei den Meldepflichten einzelne Regelungen des § 8b Abs. 3 bis 5 BSIG-E mit anderen Regelungen kombinierbar sind. So könnte eine künftige Pflicht in einer anderen Vorschrift, Sicherheitsvorfälle zu melden, mit der Regelung in § 8b Abs. 4 Satz 3 BSIG-E verbunden werden, dass eine spezifische Gruppe von Meldungen ohne Nennung des Betreibers erfolgen kann, oder mit der Regelung in § 8b Abs. 4 Satz 3 BSIG-E, dass gemeinsame übergeordnete Ansprechstellen gebildet werden können.

c) Meldepflichten der Betreiber von kerntechnischen Anlagen

Betreiber bestimmter kerntechnischer Anlagen werden nach § 8c Abs. 3 Nr. 3 BSIG-E von der Anwendbarkeit der Meldepflichten des § 8b Abs. 3 bis 5 BSIG-E ausgenommen. Für sie gelten spezifische Meldepflichten nach § 44b AtG-E.

Danach haben sie nur „Beeinträchtigungen" ihrer informationstechnischen Systeme, Komponenten oder Prozesse, „die zu einer Gefährdung oder Störung der nuklearen Sicherheit der betroffenen kerntechnischen Anlage oder Tätigkeit führen können oder bereits geführt haben", an das BSI zu melden. Da nicht „erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse" zu melden sind, wie nach § 8b Abs. 4 Satz 1 BSIG-E, sind die Mel-

---

46 S. hierzu Roßnagel, Das De-Mail-Gesetz – Grundlage für mehr Rechtssicherheit im Internet, NJW 2011, 1473 ff.

47 S. hierzu auch BT-Drs. 18/4096, 47.

48 S. 4. d).

depflichten geringer als bei anderen Kritischen Infrastrukturen – angesichts des hohen Schadenspotentials kerntechnischer Anlagen nicht ganz nachvollziehbar.

Der Inhalt der Meldung ist ähnlich unbestimmt wie nach § 8b Abs. 4 Satz 2 BSIG-E, so dass hier die gleichen Überlegungen gelten.

Die Meldung ist unmittelbar an das BSI zu richten, das die Meldung unverzüglich an die für die nukleare Sicherheit und Sicherung zuständigen Genehmigungs- und Aufsichtsbehörden des Bundes und der Länder weiterleitet. Ebenso gut könnte die Meldung an beide gleichzeitig geschickt werden[49] und damit ein Streit zwischen Bundesrat und Bundesregierung beseitigt werden.[50]

Eine anonyme Meldung ist nicht möglich und wäre angesichts der sehr überschaubaren Anzahl der betroffenen kerntechnischer Anlagen auch wenig hilfreich. Auch muss das BSI den Betreiber kennen, um die Meldung der Genehmigungs- und Aufsichtsbehörde des richtigen Landes weiterleiten zu können.

c) Meldepflichten der Betreiber von Energieversorgungsnetzen und Energieanlagen
Betreiber von Energieversorgungsnetzen und Energieanlagen werden nach § 8c Abs. 3 Nr. 2 BSIG-E von der Anwendbarkeit der Meldepflichten des § 8b Abs. 3 bis 5 BSIG-E ausgenommen. Für sie gelten spezifische Meldepflichten des § 11 Abs. 1c EnWG-E.

Die Voraussetzungen eine Meldung sind die gleichen wie für die anderen Betreiber Kritischer Infrastrukturen nach § 8b Abs. 4 Satz 1 BSIG-E. Auch hier verursacht der Begriff der „erheblichen" Störung Rechtsunsicherheit.

Der Inhalt der Meldung ist ebenso unbestimmt wie nach § 8b Abs. 4 Satz 2 BSIG-E, so dass hier die gleichen Überlegungen gelten.

Die Meldung ist unmittelbar an das BSI zu richten, das die Meldung unverzüglich an die Bundesnetzagentur weiterleitet. Dies ist genau umgekehrt organisiert als im Telekommunikationsbereich nach § 109 Abs. 5 TKG-E, obwohl auch dort BSI und Bundesnetzagentur beteiligt sind. Eine gleichzeitige identische Meldung an beide Behörden wäre sinnvoller. Das BSI und die Bundesnetzagentur haben nach § 11 Abs. 1c Satz 5 EnWG-E sicherzustellen, dass die unbefugte Offenbarung, der ihnen durch die Meldung zur Kenntnis gelangten Angaben ausgeschlossen wird.

Die Nennung des Betreibers ist nach § 11 Abs. 1c Satz 3 EnWG-E nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat. Dies ist gegenüber dem BSI aber nur möglich, wenn für den Sektor Energie nach § 8b Abs. 5 BSIG-E eine „gemeinsame übergeordnete Ansprechstelle" geschaffen werden könnte, die die Meldung vermittelt und gegenüber dem BSI anonymisiert. Die Anwendung des § 8b Abs. 5 BSIG-E ist nach § 8c Abs. 3 Nr. 2 BSIG-E für Betreiber von Energieversorgungsnetzen und Energieanlagen aber ausgeschlossen, so dass das Versprechen des § 11 Abs. 1c Satz 3 EnWG-E einer anonymen Meldung faktisch in Leere laufen muss.

---

[49] S. hierzu auch 5. d).

[50] Eine parallele Meldung hält auch die Bundesregierung für möglich – s. Gegenäußerung der Bundesregierung zu § 44b AtG, BT-Drs. 18/4096, 87.

d) Meldepflichten der Betreiber von Telekommunikationsnetzen und diensten

Für Betreiber von öffentlichen Telekommunikationsnetzen und -diensten sind nach § 8c Abs. 3 Nr. 1 BSIG-E die Meldepflichten des § 8b Abs. 3 bis 5 BSIG-E nicht anwendbar. Für sie gelten stattdessen die spezifischen Meldepflichten nach § 109 Abs. 5 TKG-E.

Nach Satz 1 dieser Vorschrift haben die Anbieter nur „Beeinträchtigungen" von Telekommunikationsnetzen und -diensten an das BSI zu melden, die „zu beträchtlichen Sicherheitsverletzungen führen oder … führen können". Insofern sind – wie bei kerntechnischen Anlagen – die Meldepflichten geringer als bei anderen Kritischen Infrastrukturen. Andererseits haben sie nach § 109 Abs. 5 Satz 2 TKG-E die Meldungen auch auf „Störungen" zu erstrecken, „die zu einer Einschränkung der Verfügbarkeit der über diese Netze erbrachten Dienste oder einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können". Insoweit sie nicht nur potentielle Einschränkungen ihrer Netze und Dienste, sondern auch mögliche Auswirkungen auf ihre Nutzer melden müssen, sind ihre Meldepflichten weiter als bei anderen Kritischen Infrastrukturen. Diese erweiterten Meldepflichten werden von der Entwurfsbegründung mit der besonderen Bedeutung der Telekommunikation für die digitale Vernetzung („Schlüsselrolle für die Sicherheit des Cyberraums",[51] „Rückgrat unserer Informationsgesellschaft"[52]) begründet. Diese besonders hohe Verantwortung der Betreiber von öffentlichen Telekommunikationsnetzen und -diensten rechtfertigt die erweiterten Meldepflichten.

Der Inhalt der Meldung ist nach § 109 Abs. 5 Satz 3 TKG-E ähnlich unbestimmt wie nach § 8b Abs. 4 Satz 2 BSIG-E, so dass hier die gleichen Überlegungen gelten.

Im Gegensatz zu allen anderen Meldungen, insbesondere auch im Gegensatz zu den Meldungen nach § 11 Abs. 1c Satz 1 EnWG-E sind die Meldung der Telekommunikationsanbieter nicht an das BSI zu richten, sondern an die Bundesnetzagentur. Diese hat dann die Meldungen zu Sicherheitsverletzungen, die die Informationstechnik betreffen, nach § 109 Abs. 5 Satz 5 TKG-E an das BSI weiter zu leiten. Das BSI benötigt aber nicht nur Meldungen zu „Sicherheitsverletzungen", sondern zu allen Beeinträchtigungen der Kritischen Infrastruktur, um ein vollständiges Lagebild erzeugen zu können. Warum in Fall der Telekommunikationsanbieter die Meldungen zuerst der Bundesnetzagentur gemeldet und im Fall der Energienetze und -anlagen zuerst an das BSI geschickt werden sollen, ist unverständlich. Warum werden nicht die Meldungen direkt beiden Behörden gleichzeitig geschickt?[53] In der E-Mail, die die Meldung enthält, würde dies nur einen zusätzlichen Eintrag im Header erfordern. Das gilt auch für die Genehmigungs- und Aufsichtsbehörden kerntechnischer Anlagen.

Eine anonyme Meldung ist nicht vorgesehen. Warum die Betreiber von öffentlichen Telekommunikationsnetzen und -diensten in dieser Frage schlechter gestellt werden als sonstige Betreiber Kritischer Infrastrukturen, ist nicht nachvollziehbar. Allerdings müsste für eine Gleichstellung § 8c Abs. 3 BSIG geändert werden.

e) Aufgaben des BSI

Nach § 8b Abs. 2 BSIG-E hat das BSI die gemeldeten „wesentlichen" Informationen zu sammeln und auszuwerten, hinsichtlich ihrer potentielle Auswirkungen auf die Verfügbarkeit der Kritischen Infrastrukturen zu

---

51 S. BT-Drs. 18/4096, 2.

52 S. BT-Drs. 18/4096, 62.

53 So auch die Gegenäußerung der Bundesregierung zu § 44b AtG, BT-Drs. 18/4096, 87.

analysieren, das Lagebild bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen kontinuierlich zu aktualisieren und unverzüglich die Betreiber Kritischer Infrastrukturen und die Aufsichtsbehörden über die erforderlichen Informationen zu unterrichten. Diese Aufgaben zu erfüllen, ist für das Erreichen des Gesetzesziels notwendig und hilfreich

Ungeregelt bleiben jedoch Anforderungen, wie das BSI mit diesen Informationen jenseits ihrer inhaltlichen Bearbeitung umzugehen hat.[54] Es hat nur die „wesentlichen" Daten zu sammeln. Es sollte festgelegt werden, wie die eventuell riesige Menge an Rohdaten der Meldungen gesichert und wann sie gelöscht werden.[55] Auch sollte festgelegt werden, dass das BSI diese Rohdaten ausschließlich für die in § 8b Abs. 2 BSIG-E genannten Auswertungen und Analysen verwenden und an niemanden weitergeben darf. Eine Klausel wie etwa die in § 11 Abs. 1c Satz 5 EnWG-E, dass die unbefugte Offenbarung, der dem BSI durch die Meldung zur Kenntnis gelangten Angaben auszuschließen ist, fehlt. Warum in dieser Hinsicht die Betreiber von Energieversorgungsnetzen und Energieanlagen besser behandelt werden als andere Betreiber Kritischer Infrastrukturen ist unverständlich.

Schließlich wäre zu klären, ob korrespondierend zu den Kontaktstellen der Betreiber Kritischer Infrastrukturen, die nach § 8b Abs. 3 Satz 2 BSIG-E „jederzeit erreichbar" sein müssen, auch die Kontaktstelle des BSI jederzeit erreichbar sein muss.[56]

f) Information Betroffener und der Öffentlichkeit

Der Schutzpflicht des Staates kann es erfordern, die Öffentlichkeit oder einzelne Nutzer zu informieren, um sie vor Schäden zu schützen oder ihnen zu ermöglichen ihre informationstechnische Sicherheit zu erhöhen. Dies kann es auch erforderlich machen, über Sicherheitsvorfälle zu informieren, vor Sicherheitslücken zu warnen oder Sicherheitsmaßnahmen zu empfehlen.

Dies ist nach § 3 Abs. 1 Satz 2 Nr. 14 BSIG auch Aufgabe des BSI. Es konnte auch bisher schon nach § 7 BSIG Warnungen und Empfehlungen aussprechen. Nach der Neufassung des § 7 Abs. 1 Satz 1 BSIG-E wird diese Befugnis noch ausgeweitet und präzisiert. Dies ist im Interesse der allgemeinen Sicherheit in der Informationstechnik zu begrüßen. Als Adressaten der Informationen sollten auch die Anbieter von IT-Dienstleistungen genannt werden.[57] Auch die allgemeinen Erkenntnisse aus der Tätigkeit als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen (§ 3 Abs. 1 Satz 2 Nr. 17 BSIG-E) müssen auch in diese Öffentlichkeits- und Aufklärungsarbeit eingehen. Dies bedeutet nicht, dass die einzelnen Sicherheitsinformationen oder Meldungen nach §§ 8a und 8b BSIG-E mitgeteilt werden sollten oder dürfen.

Da die Informationsaufgabe des BSI keine „Wohltat" gegenüber den Unternehmen und Bürgern ist, sondern Ausfluss der grundrechtlichen Schutzpflicht des Staates, sollte dies auch in der Ausgestaltung der Informationspflichten des BSI zum Ausdruck kommen. Ob das BSI über Sicherheitslücken, Sicherheitsrisiken oder Sicherheitsmaßnahmen informiert, sollte nicht in seinem freien Ermessen („kann") stehen, sondern seinem gebundenen Ermessen („soll") unterliegen. Um berechtigte Sicherheits- und Geheimhaltungsinteressen zu schützen, sollte es vor seinen Informationen eine Abwägung mit entgegenstehenden Interessen durchfüh-

---

54 S. Bundesrat, BT-Drs. 18/4096, 74f.

55 S. hierzu für personenbezogene Daten auch 9.

56 S. hierzu auch Eckardt, (Fn. ##), ZD 2014, 601.

57 Bundesrat, BT-Drs. 18/4096, 76 und Gegenäußerung der Bundesregierung, BT-Drs. 18/4096, 85.

ren. Durch die gesetzliche Regelung der Informationsaufgaben muss zum Ausdruck kommen, dass die Information der Öffentlichkeit oder einzelner besonders Betroffener die Regel ist und die Verweigerung aus entgegenstehenden Interessen die Ausnahme – nicht wie bisher umgekehrt. Auch darf die Information nicht davon abhängig gemacht werden, dass sie im öffentlichen Interesse liegt.[58] Der Schutz der Grundrechte ist dem Staat nicht nur im öffentlichen Interesse aufgegeben, sondern im Interesse jedes Grundrechtsträgers.

Die Öffentlichkeit oder einzelne Nutzer sind zwar nicht Teil des Informationssystems, das nach § 8b BSIG-E aufgebaut werden soll. Dennoch können sie die Erkenntnisse, die das BSI durch die branchenspezifischen Sicherheitsstandards und die betreiberbezogenen Sicherheitsnachweise gewonnen hat, existenziell betreffen. Daher sieht § 8d Abs. 1 Satz 1 BSIG-E vor, dass das BSI auch „Dritten" auf Antrag Auskunft zu diesen Informationen erteilen „kann". Es darf nach § 8d Abs. 1 Satz 2 BSIG-E diese Auskunft jedoch nur erteilen, „wenn schutzwürdigen Interessen des betroffenen Betreibers Kritischer Infrastrukturen dem nicht entgegenstehen und durch die Auskunft keine Beeinträchtigung wesentlicher Sicherheitsinteressen zu erwarten ist". Diese Regelung kennt keine Abwägung zwischen den Sicherheitsinteressen des Antragstellers und den Interessen des Betreibers, sondern lässt diese vollständig vorgehen. Zugespitzt sind nach dem Wortlaut dieser Regelung geringe schutzwürdigen Interessen des betroffenen Betreibers gewichtiger als noch so große Sicherheitsinteressen eines antragstellenden Unternehmens, das sich besser schützen will. Diese starre Regelung wird der gebotenen Abwägung der beteiligten Grundrechte, die durch das Handeln des BSI geschützt werden sollen, nicht gerecht. Angemessener wäre es, dem BSI grundsätzlich aufzugeben, auf berechtigte Anfragen hin Auskünfte zu erteilen, diese aber im Einzelfall von eine Abwägung der widerstreitenden Interessen abhängig zu machen. Auch sollte es versuchen, durch die Art der Auskunftserteilung beiden Interessen gerecht zu werden.

Neben dem BSI wird durch § 109 Abs. 5 Satz 7 TKG-E auch die Bundesnetzagentur als Stelle, die dem Schutz der Öffentlichkeit und einzelner Dritter verpflichtet ist, angesprochen. Sie „kann" nach dieser Regelung die Öffentlichkeit unterrichten oder die nach zu Meldungen verpflichteten Telekommunikationsanbieter zu dieser Unterrichtung auffordern, „wenn sie zu dem Schluss gelangt, dass die Bekanntgabe der Sicherheitsverletzung im öffentlichen Interesse liegt".[59] Eine solche Unterrichtung kann aber auch im berechtigten Interesse einzelner oder Gruppen von Unternehmen oder Nutzern liegen. Daher sollte auch diese Auskunft dem genannten Regel-Ausnahme-Prinzip folgen und bei entgegenstehenden Interessen eine Abwägungspflicht bestehen. Auch sollte die Bundesnetzagentur die Mitteilung in einer Form durchführen, die möglichst allen beteiligten Interessen gerecht wird.

Mit dem neuen § 109a Abs. 4 TKG-E werden neue Informationspflichten der Telekommunikationsanbieter begründet. Sie haben, wenn ihnen Störungen bekannt werden, die von Datenverarbeitungssystemen der Nutzer ausgehen, diese darüber zu benachrichtigen, soweit sie ihnen bereits bekannt sind. Soweit ihnen dies technisch möglich und zumutbar ist, haben sie die Nutzer außerdem „auf angemessene, wirksame und zugängliche technische Mittel hinzuweisen, mit denen sie diese Störungen erkennen und beseitigen können". Mit dieser Informationspflicht werden den Telekommunikationsanbietern Belastungen auferlegt, die von anderen Betreibern Kritischer Infrastrukturen nicht zu tragen sind. Dies sehen manche als ungerechtfertigt an. [60] Die Entwurfsbegründung[61] verweist für diese Sonderbelastung zum einen darauf, dass der

---

58 S. BT-Drs. 18/4096, 64.

59 Dies entspricht Art. 14 Abs. 4 des Entwurfs einer NIS-RL.

60 S. z.B. Eckardt, (Fn. 7), ZD 2014, 604f.

61 So aber BT-Drs. 18/4096, 46.

Betreiber für diesen Zweck keine Nutzerdaten sammeln muss und auch nicht sammeln darf, sondern nur solche Nutzer benachrichtigen muss, die ihm ohnehin bekannt sind. Außerdem muss er keine individuelle Beratung durchführen, sondern kann – notfalls nur die Teilnehmer – seine Hinweise in einer Massenmail mitteilen oder – soweit dies von der Sicherheitslage empfehlenswert ist – seiner Informationspflicht auch dadurch genügen, dass er die Information auf seiner Webseite bekannt gibt.[62] Diese doch geringe Belastung wird gerechtfertigt durch die besondere Bedeutung, die Telekommunikation für die Sicherheit in der digitalen Gesellschaft hat, und die besondere Verantwortung, die ein privates Unternehmen trifft, das diese öffentliche Aufgabe übernimmt. Nur so kann der Nutzer in die Lage versetzt werden, „selbst Maßnahmen gegen die auf ihren Systemen vorhandene Schadsoftware zu ergreifen" und damit die allgemeine Sicherheitslage zu verbessern.[63]

6. Mangelnde Sanktionsbefugnisse

Die Pflichten der Betreiber Kritischer Infrastrukturen in §§ 8a und 8b BSIG-E sind nicht sanktionsbewehrt. Damit fehlt eine Möglichkeit, die Sicherheitspflichten der Betreiber und den vom Entwurf verfolgten kooperativen Ansatz eines Informationssystems auch durchzusetzen.[64]

Nach § 8a Abs. 1 Satz 1 BSIG-E trifft den Betreiber einer Kritischen Infrastruktur eine Pflicht zu *Sicherheitsvorkehrungen*, nach § 8a Abs. 3 Satz 1 BSIG-E eine periodische Pflicht zum Nachweis seiner Sicherheitsvorkehrungen und nach § 8a Abs. 3 Satz 4 BSIG-E eine Pflicht zur Beseitigung von Sicherheitsmängeln. Alle drei Pflichten kann das BSI theoretisch mit den Mitteln des Verwaltungszwangs nach § 11 Verwaltungsvollstreckungsgesetz durch Zwangsgeld durchsetzen. Dieses Verfahren setzt aber einen Verwaltungsakt voraus, der die fehlende Handlung genau beschreibt, eine Androhung des Zwangsgelds, seine Festsetzung und seine Eintreibung. Gegen alle Schritte des BSI stehen dem Betreiber Rechtsmittel zu. Dieses Verfahren ist zu umständlich und zu zeitraubend, um praktisch hilfreich zu sein. Wenn tatsächlich ein einheitliches Sicherheitsniveau bei *allen* Betreibern Kritischer Infrastrukturen – nicht nur den Gutwilligen – erreicht werden soll, muss das BSI eine Möglichkeit haben, dieses Sicherheitsniveau auch durchzusetzen. Verstöße gegen die genannten drei Betreiberpflichten müssen daher mit einer Bußgelddrohung bewehrt werden. Das Gesetz muss durch einen Ordnungswidrigkeitentatbestand ergänzt werden, der für Verstöße gegen diese drei Pflichten empfindliche Bußgelder vorsieht. Ohne eine Bußgeldbewehrung des Verstoß gegen Sicherheitspflichten würde der Entwurf gegen Art. 3 Abs. 1 GG verstoßen, weil § 149 Nr. 21 TKG eine entsprechende Regelung für Telekommunikationsanbieter und § 16 Abs. 2 Nr. 3 TMG eine Ordnungswidrigkeitenvorschrift für Telemedienanbieter vorsehen, selbst wenn sie keine Kritischen Infrastrukturen betreiben.

Hinsichtlich des *IT-Sicherheits-Informationssystems* ist der Ansatz des Gesetzentwurfs, dieses in einer kooperativen Weise zusammen mit den Betreibern der Kritischen Infrastrukturen zu betreiben,[65] zu unterstützen. Die Hoffnung der Autoren des Gesetzentwurfs, dass dieses Angebot eines kooperativen Informationssystems von der Betreiberseite auch angenommen wird, stellt jedoch nicht sicher, dass tatsächlich auch *jeder* Betreiber einer Kritischen Infrastruktur sich an seine gesetzlichen Pflichten aus § 8b BSIG-E hält. Sollten sich – mangels drohender Sanktionen[66] – auch nur wenige verweigern, wird das gesamte Konzept eines

---

62 S. hierzu auch Roos, (Fn. 7), MMR 2014, 727.

63 S. BT-Drs. 18/4096, 64.

64 S. hierzu auch Roos, (Fn. 7), MMR 2014, 729.

65 S. BT-Drs. 18/4096, .

66 Zwangsmittel nach dem Verwaltungsvollstreckungsgesetz scheiden schon mangels eines Verwaltungsakts aus.

kooperativen Informationssystems misslingen, weil es darauf angewiesen ist, dass die Teilnahme an ihm nicht zu Wettbewerbsnachteilen führt. Solange sich aber einzelne ohne Konsequenzen verweigern können, wird dies genau dazu führen, dass auch die Kooperationswilligen nicht einsehen, warum sie wirtschaftliche Nachteile in Kauf nehmen sollen, die ihre Konkurrenz sich erspart. Das Konzept des kooperativen Informationssystems ist daher gerade darauf angewiesen, dass Pflichtverletzungen als Ordnungswidrigkeit mit einem spürbaren Bußgeld sanktioniert werden können. Fehlt eine Bußgeldbewehrung für die Verletzung der Meldepflichten, würde der Entwurf gegen Art. 3 Abs. 1 GG verstoßen, da er selbst in dem neuen § 149 Nr. 21a TKG eine entsprechende Regelung für Telekommunikationsanbieter vorsieht. Dies muss auch für andere Betreiber von Kritischen Infrastrukturen gelten.

Auch der Entwurf der NIS-RL fordert in Art. 17 Abs. 1, für Verstöße sowohl gegen die Sicherheitspflichten als auch gegen die Meldepflichten Sanktionen zu erlassen, die „wirksam, angemessen und abschreckend" sind.

Diese Sanktion kann jedoch – dem kooperativen Ansatz entsprechend – differenziert geregelt werden und zum Ansatz kommen. Keine Ordnungswidrigkeit sollte vorgesehen werden, wenn die erforderliche Meldung nach § 8b Abs. 4 Satz 1 BSIG-E eine Störung betrifft, die tatsächlich zu keinem Ausfall und zu keiner Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat. Eine solche Störung zu erkennen und einem Betreiber nachzuweisen, ist extrem schwierig. Eine solche Meldung kann nach § 8b Abs. 4 Satz 3 BSIG-E ohne Nennung des Betreibers erfolgen. Dieser Anreiz und die hohe Schwierigkeit des Nachweises einer Rechtsverletzung könnten dazu führen, von einem Bußgeldtatbestand abzusehen. Auch soweit eine Ordnungswidrigkeit für den Fall vorgesehen ist, dass die unterbliebene Meldung eine Störung betrifft, die tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der Kritischen Infrastruktur geführt hat, gilt das Opportunitätsprinzip. Das BSI kann somit das Sanktionsinstrument unter Berücksichtigung des kooperativen Ansatzes gezielt einsetzen, wo dies motivationssteigernd wirkt.

7. Überprüfung von Produkten

Nach dem neuen § 7a Abs. 1 BSIG-E darf das BSI informationstechnische Produkte und Systeme untersuchen, soweit dies dazu dient, seine Aufgaben nach § 3 Abs. 1 Satz 2 Nr. 1 (Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes), Nr. 14 (Beratung und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender) und Nr. 17 (zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen) zu erfüllen. Da Bund, Länder, Hersteller, Vertreiber und Anwender auf solche Überprüfungen der informationstechnischen Sicherheit von Produkten und Systemen dringend angewiesen sind, ist es sehr zu begrüßen, dass durch diese Regelung das BSI rechtssicher solche Prüfungen durchführen kann.[67]

Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nach § 7a Abs. 1 BSIG-E vom BSI und von anderen Stellen nur zu den in § 7a Abs. 1 Satz 1 BSIG-E genannten Zwecken genutzt werden. Zu diesen Zwecken darf das BSI seine Erkenntnisse weitergeben und veröffentlichen, soweit die für diese Zwecke erforderlich ist. Sowohl diese Zweckbegrenzung als auch die Möglichkeit, die Erkenntnisse zu diesen Zwecken weitergeben zu können, ist zu begrüßen. Diese Regelungen verhindern Missbrauch, ermöglichen aber auch einen Gebrauch der Erkenntnisse zur Steigerung der Sicherheit in der Informationstechnik. Allerdings sollte für diese Informationen das bereits angesprochene, aus der staatlichen Schutzpflicht abgeleitete Regel-Ausnahme-Prinzip gelten.

---

[67] S. BT-Drs. 18/4096, 40f.

8. Vorratsdatenspeicherung

Der Entwurf sieht vor, in § 100 TKG an den nur sprachlich umgestalteten Satz 1 einen neuen Satz 2 anzuhängen, nach dem auch Störungen den Umgang mit Bestandsdaten und Verkehrsdaten rechtfertigen, „die zu einer Einschränkung der Verfügbarkeit von Informations- und Kommunikationsdiensten oder zu einem unerlaubten Zugriff auf Telekommunikations- und Datenverarbeitungssysteme der Nutzer führen können".

Durch diese Ergänzung werden die Befugnisse der Telekommunikationsanbieter nicht erweitert. Der Gesetzentwurf erweitert nur den Begriff der Störung.[68] Dies entspricht der Auslegung dieses Begriffs durch den Bundesgerichtshof.[69] Diese Rechtsprechung wird jetzt vom Entwurf in den Gesetzestext übernommen und dadurch der Begriff präzisiert. Eine Rechtsänderung gegenüber der durch den Bundesgerichtshof gefundenen Interpretation tritt nicht ein.[70] Wenn man eine Prävention von Störungen will, ist es sinnvoll, unter dem Begriff der Störung auch Beeinträchtigungen der Funktionsfähigkeit zu verstehen.

Von dieser Frage zu unterscheiden ist jedoch die Frage, ob nach der Rechtsprechung des Bundesverfassungsgerichts und des Europäischen Gerichtshofs zum Schutz des Fernmeldegeheimnisses und insbesondere zur Grundrechtswidrigkeit der Vorratsdatenspeicherung nach §§ 113a und 113b TKG[71] die Vorschrift des § 100 Abs. 1 TKG geändert werden müsste. Ob durch diese Vorschrift „im Kern … eine weitreichende Vorratsdatenspeicherung"[72] zulässt oder in der Auslegung der Erforderlichkeit, die sie durch den Bundesgerichtshof erfahren hat, gerade keine „kleine Vorratsdatenspeicherung" erlaubt,[73] ist heftig umstritten.

Der Bundesgerichtshof hat zu § 100 Abs. 1 TKG festgestellt, dass das Urteil des Europäischen Gerichtshofs zur Vorratsdatenspeicherung[74] den Fall des § 100 Abs. 1 TKG nicht berühre, weil „die Speicherung … nicht für die Zwecke der Strafverfolgungsbehörden, sondern im Interesse des Netzbetreibers" erfolge.[75] Diese Schlussfolgerung verkennt die Tragweite der Auslegung der Art. 7 und 8 GrCh durch den Europäischen Gerichtshof. Der Schutz dieser Grundrechte verlangt „jedenfalls, dass sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken müssen".[76] Daher muss eine einschränkende Regelung „klare und präzise Regeln für die Tragweite und die Anwendung" des Eingriffs vorsehen und „Mindestanforderungen aufstellen, so dass" die Betroffenen „über ausreichende Garantien verfügen, die einen wirksamen Schutz ihrer personenbezogenen Daten vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglichen". [77] Jedenfalls ist der Eingriff nicht auf das „absolut Notwendige" beschränkt, wenn er eine alle um-

---

68 S. Gegenäußerung der Bundesregierung, BT-Drs. 18/4096, 89; Roos, (Fn. 7), MMR 2014, 727.

69 S. BGH, NJW 2014, 2500 (2501).

70 S. hierzu z.B. Roos, (Fn. 7), MMR 2014, 728.

71 S. zu diesen Roßnagel, in: Geppert/Schütz (Hrsg.), Beck'scher TKG-Kommentar, 4. Aufl. 2014, §§ 113a und 113b.

72 S. Bundesrat, BT-Drs. 18/4096, 82.

73 S. auch Eckardt, (Fn. 7), ZD 2014, 604.

74 S. EuGH, NJW 2014, 2169; s. hierzu näher Roßnagel, Neue Maßstäbe für den Datenschutz in Europa. Folgerungen aus dem Urteil des EuGH zur Vorratsdatenspeicherung, MMR 2014, 372 ff.

75 S. BGH, NJW 2014, 2500 (2503).

76 S. EuGH, NJW 2014, 2169, Rn. 52.

77 S. EuGH, NJW 2014, 2169, Rn. 54.

fassende, flächendeckende und anlasslose Sicherungsmaßnahme erlaubt – „ohne irgendeine Differenzierung, Einschränkung oder Ausnahme“ anhand des verfolgten Ziels.[78]

Daher ist ein umgekehrter Erst-Recht-Schluss, wie ihn der Bundesgerichtshof angestellt hat, erforderlich: Wenn schon „die Bekämpfung schwerer Kriminalität zur Gewährleistung der öffentlichen Sicherheit“[79] keine anlasslose, ausnahmslose und flächendeckende Speicherung auf Vorrat erlaubt, kann dies für erheblich weniger gewichtige Interessen des Netzbetreibers nicht zulässig sein.

Der Bundesgerichtshof hat sich auch nicht mit den Anforderungen des Bundesverfassungsgerichts an Gesetze, die Eingriffe in das Fernmeldegeheimnis und die informationelle Selbstbestimmung erlauben,[80] auseinandergesetzt. Dann hätte er nämlich festgestellt, dass § 100 Abs. 1 TKG außer der Erforderlichkeit[81] und der Zweckbestimmung keine Begrenzungen der Datenverarbeitung fordert. Er enthält weder Vorgaben zur Eingriffsschwelle (Tatsachen, die einen Anlass für die Maßnahme bieten, und deren Dkumentation), zum Zeitraum der Speicherung,[82] zu Schutzvorkehrungen gegen Missbrauch, zu Zweckbegrenzungen in der Verwendung der Daten, zu Ausnahmen für Träger von Berufsgeheimnissen, zur Information der Betroffenen und zu Löschverpflichtungen.[83] Solange diese Anforderungen des Bundesverfassungsgerichts für Eingriffsregelungen ignoriert werden, muss davon ausgegangen werden, dass die Eingriffsermächtigung verfassungswidrig ist.[84]

9. Datenschutz

Der Datenschutz wird im Entwurf des Gesetzestextes nur in § 8b Abs. 6 BSIG-E angesprochen. Die Begründung geht davon aus, dass die „im Rahmen von § 8b übermittelten Informationen … üblicherweise rein technischer Natur“ sind.[85] Sollte im Einzelfall doch ein Personenbezug gegeben sein, stellt § 8b Abs. 6 BSIG-E klar, dass personenbezogene Daten nur zu den in dieser Vorschrift vorgesehenen Zwecken erhoben, verarbeitet oder genutzt werden dürfen. Eine darüber hinausgehende Verarbeitung und Nutzung zu anderen Zwecken ist unzulässig. Da außerdem die allgemeinen datenschutzrechtlichen Regelungen gelten, ist auch der Grundsatz der Datensparsamkeit nach § 3a BDSG anzuwenden. Daher müssen alle Beteiligten die Möglichkeiten zur Datensparsamkeit etwa durch Anonymisierung, Pseudonymisierung, frühzeitiges Löschen und Abschotten anwenden.[86] Außerdem ordnet die Vorschrift an, die Datenschutzregelungen des § 5 Abs. 7 Satz 3 bis 8 BSIG zum Schutz des Kernbereichs privater Lebensgestaltung entsprechend anzuwenden. Diese Datenschutzregelungen gelten sowohl für den Datenumgang der Betreiber Kritische Infrastrukturen für den Zweck der Meldungen als auch für das BSI für den Zweck der Sammlung, Auswertung und Weitergabe der Daten. Die Daten sind nach §§ 20 Abs. 2 und 35 Abs. 2 BDSG zu löschen, wenn sie nicht mehr für

---

78 S. EuGH, NJW 2014, 2169, Rn. 57.

79 S. EuGH, NJW 2014, 2169, Rn. 42, 51.

80 S. z.B. BVerfGE 65, 1; 78, 77; 84, 192; 96, 171; 103, 21; 100, 313; 107, 299; 109, 279; 110, 33; 113, 348; 113, 348; 115, 166; 115, 320; 118, 168; 120, 274; 125, 260.

81 Die der Bundesgerichtshof gerade nicht im Sinn des EuGH auslegt.

82 S. hierzu auch den Leitfaden des BfDI und der BNetzA für eine datenschutzgerechte Speicherung von Verkehrsdaten: max. sieben Tage.

83 S. zu diesen und weiteren grundrechtlich gebotenen Differenzierungen Roßnagel/Moser-Knierim/Schweda, Interessenausgleich in der Vorratsdatenspeicherung, 2013.

84 S. z.B. Leisterer/Schneider, (Fn. 7), CR 2014, 577f.

85 S. BT-Drs. 18/4096, 48.

86 S. hierzu auch Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. und 19. März 2015.

die genannten Zwecke erforderlich sind. Um diese Löschpflicht zu präzisieren, sollte eine Frist vorgesehen werden, nach der sie im Regelfall nicht mehr benötigt werden und zu löschen sind.[87]

Aus der Vorschrift des § 8b Abs. 6 BSIG-E kann der Rückschluss gezogen werden, dass die Regelungen in §§ 8a und 8b BSIG-E keine Erlaubnistatbestände zum Umgang mit personenbezogenen Daten darstellen.[88] Soweit für die Sicherheitsvorkehrungen oder die Sicherheitsmeldungen und ihre Bearbeitung mit personenbezogenen Daten umgegangen werden muss, ist dies durch andere Erlaubnistatbestände zu rechtfertigen.

Ein Erlaubnistatbestand ist allerdings in § 7 Abs. 1 BSIG-E „versteckt". Satz 2 dieser Vorschrift ermöglicht es dem BSI, bei Warnungen Dritte als Informationsintermediäre einzubeziehen, sofern dies für eine wirksame und rechtzeitige Warnung erforderlich ist, insbesondere um Betroffene schnellstmöglich zu erreichen. Die damit verbundene Datenübertragung wird durch diese Regelung erlaubt. Sie dient nach der Begründung „auch zur Klarstellung unter Datenschutzgesichtspunkten". „Satz 2 eröffnet aber nicht die Möglichkeit, zusätzliche Daten bei den Dritten zu erheben."[89]

Die Betreiber Kritischer Infrastrukturen können auch nach § 42a BDSG, § 15a TMG und § 109a TKG verpflichtet sein, Datenschutzverletzungen an die Bundesnetzagentur und die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit zu melden. Da Datenschutzverletzungen und Sicherheitsverletzungen gemeinsam auftreten können, ist es notwendig, dies bei den Meldewegen und dem Umgang mit Doppelmeldungen zu berücksichtigen.[90]

Schließlich ist die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit bei der Erstellung von Leitlinien, Katalogen und ähnlichen untergesetzlichen Vorgaben zu beteiligen, um bei der Abwägung zwischen Informationssicherheit, klassischer Gefahrenabwehr und Strafverfolgung sowie Fernmeldegeheimnis und informationeller Selbstbestimmung mit dem Ziel mitwirken zu können, zu einer angemessen Berücksichtigung dieser Grundrechte beizutragen.[91] Bei der Erstellung des Sicherheitskataloges nach § 109 Abs. 6 TKG wird die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit schon einbezogen. Nach der Neufassung dieser Vorschrift ist mit ihr sogar ein Einvernehmen herzustellen.

(Prof. Dr. Alexander Roßnagel)

---

87 S. hierzu auch 5. e).

88 S. auch Eckardt, (Fn. 7), ZD 2014, 602f.

89 S. BT-Drs. 18/4096, 40.

90 S. hierzu Erwägungsgrund 31 des Entwurfs der NIS-RL; s. auch Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. und 19. März 2015; Roos, (Fn. ##), MMR 2014, 727.

91 S. auch Entschließung der 89. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 18. und 19. März 2015.