Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

ULD · Postfach 71 16 · 24171 Kiel

Bundesministerium des Innern
Staatssekretärin Cornelia Rogall-Grothe
Alt-Moabit 101D
10559 Berlin

Holstenstraße 98
24103 Kiel
Tel.: 0431 988-1200
Fax: 0431 988-1223

Ansprechpartner/in:
Herr Dr. Weichert
Durchwahl: 988-1200

Aktenzeichen:
LD -01.03/10.101

Kiel, 20. Oktober 2014

Stellungnahme zum Referentenentwurf des Bundesministerium des Innern eines Gesetzes zur Erhöhung der Sicherheit informationstechnische Systeme (IT-Sicherheitsgesetz)

Sehr geehrte Frau Staatssekretärin Rogall-Grothe,
sehr geehrte Damen und Herren,

mit Stand vom 18.08.2014 veröffentlichten Sie im Internet den in Betreff genannten Referentenentwurf:

http://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_IT-Sicherheitsgesetz.pdf?__blob=publicationFile

Für die Arbeit des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD) als Datenschutzaufsichtsbehörde des Landes hätte das von Ihnen vorgeschlagene Gesetz weitreichende Konsequenzen. Deshalb erlaube ich mir, Ihnen im Folgenden unsere Stellungnahme hierzu zukommen zu lassen. Ich würde mich freuen, wenn unsere Erwägungen bei der weiteren Entwurfsbearbeitung berücksichtigt würden.

Das mit dem Gesetzentwurf verfolgte Ziel einer Erhöhung der IT-Sicherheit insbesondere im Hinblick auf das Internet und kritischer Infrastrukturen ist aus Sicht des Datenschutzes sehr zu unterstützen. Die **Gewährleistung der Verfügbarkeit, der Integrität und der Vertraulichkeit informationstechnischer Systeme** ist auch ein zentrales Anliegen des Datenschutzes.

Insofern ist es zu begrüßen, das Betreibern von kritischen Infrastrukturen, von Telekommunikationsdiensten und auch von Telemedien Pflichten auferlegt werden, **effektive IT-Sicherheitsmaßnahmen** zu implementieren. Entsprechendes gilt für die vorgesehenen Meldungen an das Bundesamt für die Sicherheit in der Informationstechnik (BSI) sowie die verbesserte Kommunikation von Vorfällen und gewonnenen Erkenntnissen nach außen.

Bei Maßnahmen zur Verbesserung der IT-Sicherheit ist es unter Umständen nötig, personenbezogene Daten von Nutzenden der informationstechnischen Infrastrukturen zu erheben, zu speichern, zu übermitteln und auszuwerten. Hierbei ist aber darauf zu achten, dass die hierzu erlassenen **Regelungen hinreichend bestimmt und verhältnismäßig** sind.

Irritierend ist insofern die Aussage der Begründung des Gesetzentwurfes, die nach dem geplanten IT-Sicherheitsgesetz übermittelnden Daten seien „üblicherweise rein technischer Natur und haben keinen **Personenbezug**“ (S. 40). Bei der Detektion von Sicherheitsvorfällen und deren aussagekräftiger Meldung an zentrale Stellen ist die Verarbeitung der relevanten Daten nicht nur technischer Natur. Zwar sind Einzeldaten wie gescannte Port-Nummer, IP-Adressen, URLs, Routing-Tabellen in BGP-Routern oder Zeitpunkte der Ereignisse zunächst technische Angaben. Handelt es sich hierbei nicht um aggregierte Daten, so enthalten diese Daten zugleich Angaben über die Nutzenden, bei denen es sich in der Regel oder zumindest sehr oft um natürliche Personen handelt. Handelt es sich um Angaben zu Institutionen, so stehen hinter diesen oft natürliche Personen, die den Datensätzen über die Institution i. d. R. zugeordnet werden können. Eventdaten sind somit regelmäßig natürlichen Personen eindeutig zuzuordnen, so dass es sich dann um personenbezogene Daten i. S. d. Datenschutzrechtes handelt (vgl. § 3 Abs. 1 BDSG). Nicht zuletzt das mittlerweile durch die Werbeindustrie vorangetriebene Device-Fingerprinting ermöglicht es, aus „Meta-Daten“ des Internetverkehrs weitreichende Erkenntnisse über Personen abzuleiten. Da es das Ziel des IT-Sicherheitsgesetzes ist, Korrelation von Anomalien festzustellen, müssen zwangsläufig Einzeldaten verarbeitet werden, die vielfach einen Personenbezug haben.

Dass der Regelungsvorschlag personenbezogene Daten erfassen soll, ergibt sich z. B. zwingend aus dem geplanten § 7 Abs. 1 S. 1 b) BSIG-E, wonach sich das BSI bei der **Warnung vor Sicherheitslücken und Schadprogrammen** der Einschaltung Dritter bedienen kann und hierbei „die betroffenen Kreise“ adressiert werden sollen. Im Interesse der Effektivität derartiger Warnungen wie auch im Interesse der Datensparsamkeit müssen solche Warnungen oft personenbezogen erfolgen (so auch die Gesetzesbegründung auf S. 35).

Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat in dem vom Bundesministerium für Bildung und Forschung geförderten Projekt „Monitoring durch Informationsfusion und Klassifikation zur Anomalieerkennung“ (MonIKA) mit Datum von 28.02.2014 eine umfangreiche Ausarbeitung erstellt, in der auf den Vorgängerentwurf des vorliegenden Gesetzentwurfes für ein IT-Sicherheitsgesetz (Stand März 2013)[1] Bezug genommen wird.[2]

[1] Referentenentwurf des Bundesministeriums des Innern, Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme vom 05.03.2013, im Internet: https://www.bmi.bund.de/SharedDocs/Downloads/DE/Gesetzestexte/Entwuerfe/Entwurf_it-sicherheitsgesetz.pdf?__blob=publicationFile.

Darin kommt das ULD zu dem Ergebnis, dass bei der im Bereich von Datensicherheitsmaßnahmen üblichen Anomalieerkennung umfangreich personenbezogene Daten verarbeitet werden. Datensätze haben nicht nur oft einen **Personenbezug**, wenn sie statische oder dynamische IP-Adressen enthalten, sondern auch durch die Speicherung von Portnummern, von autonomen Systeme-Nummern oder von URLs. Zugleich hat sich gezeigt, dass die Konstruktion der Auftragsdatenverarbeitung bei komplexeren Sicherungssystemen kaum noch anwendbar ist und den Gegebenheiten verteilter Systeme nicht mehr gerecht wird und **Verantwortlichkeiten** nicht mehr adäquat abbilden kann (dazu näher s.u.).

Die vom ULD erstellte Studie kommt zu dem zentralen Ergebnis, dass derartige Sicherheitssysteme datenschutzkonform möglich sind, dass dies aber die konsequenten Anwendung des Grundsatzes der **Datensparsamkeit** (vgl. 3a BDSG) bedarf. Diese Erkenntnis wird im vorliegenden Gesetzentwurf nicht reflektiert. Der Entwurf nimmt die Gelegenheit nicht wahr, die Fragen von verbundenen technisch komplexen Monitoring-Netzen tatsächlich und rechtlich anzugehen. Grundlegende Werkzeuge wie Pseudonymisierung und Anonymisierung werden nicht berücksichtig und die daraus folgenden Herausforderungen für die effiziente Umsetzung von derartigen datensparsamen Monitoring-Netzwerken bleiben ungelöst.

Der Regelungsvorschlag hat vorrangig die Datenverarbeitung beim BSI sowie möglicherweise weiteren eingebundenen Behörden (z. B. Bundesnetzagentur) im Blick. Zusätzlich sind Meldepflichten von Betreibern von IT-Systemen vorgesehen. Völlig ausgeblendet wird von dem Entwurf die einer Meldung vorausgehende Datenverarbeitung beim Betreiber, weitgehend auch, welche Folgeverarbeitungen mit erlangten (personenbeziehbaren) Rückmeldungenn zulässig sind. Praktisch alle Regelungen sind als Aufgabenbeschreibungen ausgestaltet, ohne die notwendige **Bestimmtheit von Befugnisnormen** aufzuweisen wie sie für die Legitimation zu Verarbeitung personenbezogener Daten nötig sind.

Ein weiterer genereller Mangel des Gesetzentwurfes besteht darin, dass zwar eine enge Verzahnung zwischen der Telekommunikationsaufsicht und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) vorgesehen ist, nicht aber zwischen der **Datenschutzaufsicht** und dem BSI. Wegen der hohen Datenschutzrelevanz einer Vielzahl von Festlegungen und Verfahren ist eine Einbeziehung der Datenschutzbehörden unabdingbar, um keine Konflikte zwischen IT-Sicherheit und Datenschutz entstehen zu lassen.

Ein weiterer genereller Mangel des Entwurfes besteht darin, dass Betreibern von IT eine Vielzahl sinnvoller Pflichten auferlegt werden, dass aber diese im Nichtbeachtensfall vom BSI nicht sanktioniert werden können. So sollten **Sanktionsmöglichkeiten**, etwa als Ordnungswidrigkeiten oder Anordnungsverfügungen, bei der Verletzung von Meldepflichten oder beim Versäumen der unverzüglichen Beseitigung von Sicherheitsmängeln vorgesehen werden (vgl. § 115 TKG).

Die im Entwurf vorgesehenen Maßnahmen zur Verbesserung der IT-Sicherheit ist weitgehend notwendig, aber bei weitem – angesichts der heute bestehenden technischen Möglichkeiten – nicht hinreichend. So können z. B. die Anbieter von Kommunikationsdiensten verpflichtet werden, eine vertrauliche **Ende-zu-Ende-Verschlüsselung** anzubieten.

---

[2] Engeler/ULD, Ausarbeitung aus Perspektive des Datenschutzes und der Datensicherheit zur Zulässigkeit sowie zum Einsatz und zur Gestaltung von Anomalie erkennenden Verfahren in Internet-Infrastrukturen, Deliverable 5.2, V1.0 v. 28.02.2014.

Verblüffend ist, dass in der Begründung des Entwurfes neben der Notwendigkeit weiterer 79 Stellen beim Bundeskriminalamt (BKA) ein „zusätzlicher Ressourcenbedarf von 55 Planstellen / Stellen mit Personal und Sachkosten in Höhe von von 4.496 T€ für das Jahr 2015 sowie jeweils ein Haushaltsmittelbedarf in Höhe von 4.170 T€ für die Folgejahre“ zugunsten der „Fachabteilungen des **Bundesamtes für Verfassungsschutz** (BfV)“ angemeldet wird. Hintergrund sei die zusätzliche Zuständigkeit des BfV für die Zusammenarbeit bei der Analyse der Verfügbarkeit der kritischen Infrastrukturen (§ 8b Abs. 2 Nr. 2 BSIG-E). Eine solche Zuständigkeit ergibt sich aber weder aus dem Entwurf noch aus dem Bundesverfassungsschutzgesetz (§ 3 BVerfSchG). Der zusätzliche Ressourcenbedarf wird dadurch noch befremdlicher, dass das BfV eng mit Stellen zusammenarbeitet, die im Verdacht stehen, rechtswidrigen Einfluss auf kritische Infrastrukturen zu nehmen, namentlich die Geheimdienste Großbritanniens und der USA – Government Communications Headquarters (GCHQ) und National Security Agency (NSA). Eine Stärkung der insofern vertrauenswürdigeren Datenschutzaufsichtsbehörden, denen gesetzlich explizit Aufgaben der Datensicherheit zugewiesen sind, wäre in diesem Umfang zweifellos zielführender.

Der Gesetzentwurf berücksichtigt überhaupt nicht, dass Personen und Institutionen in der **Zivilgesellschaft** schon heute einen wertvollen Beitrag der IT-Sicherheit leisten, indem diese Sicherheitslücken aufdecken, veröffentlichen und Schutzkonzepte entwickeln und zugleich ein Korrektiv abgeben bei behördlichem Versagen. Durch das Unterlassen einer Einbindung dieser Kräfte in das gesamtgesellschaftliche Bestreben nach IT-Sicherheit lässt der Entwurf die bestehenden Potenziale ungenutzt.

Zu den einzelnen Regelungsvorschlägen

Artikel 1 – Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik

Zu 1. § 1 BSIG-E

Der Entwurf hält daran fest, dass das BSI als nationale Informationssicherheitsbehörde und Bundesoberbehörde dem Bundesministerium des Innern untersteht. Diese hierarchische Unterordnung hat zur Folge, dass das BSI im Zweifel gezwungen ist, sich dem Ressort unterzuordnen, das auch für die innere Sicherheit im weitesten Sinn zuständig ist und in seiner Politik hiervon bestimmt wird. Viele informationstechnische Sicherungsmaßnahmen sind damit verbunden, dass Daten für Ermittlungsansätze der Sicherheitsbehörden vermieden werden (Pseudonymisierung, Anonymisierung, generell Datenvermeidung, Verschlüsselung). Dadurch sind hausinterne Interessenkonflikte vorprogrammiert, die erfahrungsgemäß in der Vergangenheit im Zweifel für die „innere Sicherheit“ entschieden wurden. Es wäre daher wünschenswert, dem BSI eine **weitergehende Selbständigkeit** zu geben. Auch eine andere Ressortzuordnung ist zu erwägen.

Zu 2. § 2 Abs. 10, 11 BSIG-E – Betreiber kritischer Infrastrukturen

Als Adressat der gesetzlichen Regelungen werden „Betreiber kritischer Infrastrukturen“ benannt, die als „Unternehmen“ gekennzeichnet werden. Diese Terminologie lässt den Eindruck entstehen, dass **öffentliche Stellen** als Betreiber nicht erfasst sein sollen. Hierfür gäbe es keine sachliche Rechtfertigung. Eine Klarstellung, dass diese mit erfasst sind, ist dringend

erforderlich.

Im Entwurf werden insbesondere **Betreiber** kritischer Infrastrukturen angesprochen und mit Pflichten und Aufgaben belegt. Diese Betreiber nehmen im Hinblick auf ihre Informationsverarbeitung generell und die Gewährleistung der IT-Sicherheit im Speziellen eine Vielzahl von Dienstleister in Anspruch, die arbeitsteilig vorgehen und zueinander teilweise in komplexen technischen und rechtlichen Beziehungen stehen. Dabei nehmen diese **Dienstleister** nicht nur Aufgaben nach Weisung wahr, sondern sind in starkem Maße eigenverantwortlich tätig. Dies hat zur Folge, dass eine reine Verantwortungszuweisung, wie sie im Datenschutzrecht durch den Auftraggeber erfolgt (§§ 3 Abs. 7, 11 BDSG), nicht mehr sichergestellt werden kann. Dies gilt erst Recht, wenn man der – nicht rechtskräftigen – Rechtsprechung des OVG Schleswig-Holstein (U. v. 04.09.2014, 4 LB 20/13, https://www.datenschutzzentrum.de/facebook/20140904-OVG-U-FBFanpageAnon.pdf) folgt, die für eine rechtliche Verantwortlichkeit für eine Datenverarbeitung verlangt, dass die tatsächlich Herrschaft über die Datenverarebeitung vorliegt. Es empfiehlt sich daher, die Adressaten der Regelung gemäß der tatsächlich ausgeübten Tätigkeiten im Interesse der Rechtssicherheit weit zu fassen und sicherheitstechnisch relevante Dienstleister mit einzuschließen (ausführlich hierzu siehe die oben zitierte MonIKA-Studie des ULD).

Der Entwurf sieht die Aufnahme eines § 2 Abs. 11 BSI-Gesetz vor, wonach **Kleinstunternehmen** als Betreiber kritischer Infrastrukturen weitgehend von Meldepflichten befreit werden. Der Europäische Datenschutzbeauftragte (EDPS) wies bereits in einer früheren Stellungnahme[3] vom 14.06.2013 zu Recht darauf hin, dass derartige Kleinstunternehmen in ihrem Marktsegment wesentliche Anbieter sein können und damit wichtige Anbieter der Informationsgesellschaft sein können. Damit werden kleine, aber wichtige Technologie-Unternehmen aus dem Fokus genommen und für Angriffe besonders geeignet gemacht, da dort minimale Verteidigungsfähigkeit auf maximales Schädigungspotenzial trifft. Durch eine geänderte Definition sollte dem Rechnung getragen werden.

Zu 3. § 3 BSIG-E

Der derzeitige § 3 des BSI-Gesetzes wird dahingehend geändert, dass in Abs. 1 Satz 2 Nummer 2 das Wort „andere Stellen“ durch „Dritte“ ersetzt wird. Damit wird der **Empfängerkreis z. B. von Warnmeldungen** noch unbestimmter. In der Begründung (S. 34) wird dies damit gerechtfertigt, dass die vom BSI gewonnenen Erkenntnisse einen „Mehrwert“ für „Wirtschaft und Gesellschaft“ haben. Auch wenn dies zutreffen mag: Zielgerichtetere Informationsflüsse dürften regelmäßig wirkungsvoller sein.

[3] Opinion of the European Data Protection Supervisor on the Joint Communication of the Commission and of the High Representative of the European Union for Foreign Affairs and Security Policy on a 'Cyber Security Strategy of the European Union: an Open, Safe and Secure Cyberspace', and on the Commission proposal for a Directive concerning measures to ensure a high common level of network and information security across the Union, im Internet:
https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-06-14_Cyber_security_EN.pdf.

Zu 5. § 7 BSIG-E

In § 7 soll ein neuer Satz 2 eingefügt werden, der es dem BSI erlaubt, sich zur Erfüllung seiner Warnaufgaben der **Hilfe Dritter** zu bedienen. Dabei wird allerdings nicht klar geregelt, wie dies erfolgen soll, wenn personenbezogene Daten aus den Warnungen ableitbar sind. Eine hinreichend bestimmte Rechtsgrundlage für die Weitergabe und eine spätere Veröffentlichung der in solchen Warnungen enthaltenen personenbezogenen Daten enthält der neue § 7 Abs. 1 S. 2 BSI-Gesetz nicht. Auch der möglicherweise hilfsweise heranzuziehende § 11 BDSG ist vor dem Hintergrund der evtl. sehr weit reichenden Verarbeitungen beim BSI nicht ausreichend konkret, um die „Hilfe Dritter" normenklar zu erfassen. Eine klare Definition dessen, was durch Dritte wahrgenommen werden darf und was ureigene Aufgabe des BSI bleiben muss, wäre wünschenswert.

Zu Nr. 6 Einfügung eines § 7a BSIG-E – Unterstützung der IT-Sicherheit

Der Vorschlag erlaubt dem BSI die Untersuchung von informationstechnischen Produkten, Systemen und Diensten unter Verwendung „**aller geeigneten technischen Mittel sowie der Unterstützung Dritter**". Erneut fehlt eine klare Regelung, welche Mittel eingesetzt werden dürfen, welche Aufgaben ausgelagert werden dürfen und wie die Unterstützung mit welchen Verantwortlichkeiten umgesetzt werden soll.

Zu Nr. 7 § 8 BSIG-E

Es ist zu begrüßen, dass das BSI **Mindeststandards für die Sicherheit** der Informationstechnik des Bundes verbindlich festlegen kann, die vom Bundesministerium des Innern als Verwaltungsvorschrift erlassen werden können. Das Benehmen mit den IT-Beauftragten der Ressorts ist wegen der Relevanz der fachlichen Erfahrung vorgesehen. Mit der Festlegung von Mindeststandards für die informationstechnische Sicherheit werden auch Regeln für die Verarbeitung personenbezogener Daten festgelegt (vgl. § 9 BDSG mit Anlage sowie die entsprechenden Landesdatenschutzgesetze – LDSG). Es ist nicht ersichtlich, weshalb keine verpflichtende **Anhörung der Bundesbeauftragten für den Datenschutz** und die Informationsfreiheit (BfDI) oder eine solche Benehmensregelung geplant ist. Tatsächlich gehört die Datenschutzaufsichtsbehörden neben dem BSI zu den Stellen, die insofern die größte Kompetenz vorweisen können und denen hierbei die Ambivalenz zwischen den Zielen Datensparsamkeit und Datensicherheit bewusst ist.

Zu Nr. 8 Einfügung von den §§ 8a, 8b und 8c BSIG-E

Die neuen §§ 8a, 8b und 8c BSI-Gesetz verlangen einerseits die Schaffung von neuen Schutzmechanismen nach dem Stand der Technik (§ 8a), funktionieren das BSI zur zentralen Meldestelle um (§ 8b) und schaffen ein Auskunftsrecht Dritter über die diesbezüglichen Informationen (§ 8c).

Diese zentralen Normen des vorliegenden Entwurfes eines IT-Sicherheitsgesetzes sind im Ergebnis genauso kritikwürdig wie in einem ersten Entwurf aus dem Jahr 2013. Es **fehlt an einer klaren Rechtsgrundlage** für die Erhebung der Daten bei den meldepflichtigen Stellen und an einer Auseinandersetzung mit dem Konflikt aus technisch möglicher IT-Überwachung und rechtlich zulässiger Verarbeitung personenbezogener Daten. Sie enthalten keine Verfahrensvorgaben hinsichtlich der zentralen Datenfusion beim BSI. Weder die

Zweckbindung noch die Datentrennung werden ausdrücklich festgelegt. Unklar bleiben auch die Rückmeldungen über die Warnung und die Unterrichtung der betroffenen Stellen. Die Gefahr, dass personenbezogene Daten an Unberechtigte übermittelt werden, wird nicht berücksichtigt. Es wird nicht festgelegt, zu welchen Zwecken die so erhaltenen Daten genutzt werden dürfen.

§ 8a BSIG-E – Sicherheit in der Informationstechnik kritischer Infrastrukturen

Anders als noch ein früherer Entwurf aus dem Jahr 2013 verzichtet der aktuelle Entwurf im Rahmen des § 8a auf die **Definition des „Standes der Technik“**. Damit bleibt in einem noch stärkerem Maße als zuvor offen, welche Art von Schutzmaßnahmen im Rahmen des § 8a verlangt werden können. Der aktuelle Entwurf versäumt es so, die ungeklärten Fragen im Rahmen der Überwachung von informationstechnischen System zu beantworten. Es besteht das Risiko, dass Mittel als geeignet und erforderlich angesehen werden, bei denen Fragen des Datenschutzes nicht hinreichend berücksichtigt werden. Basierend auf der nicht zutreffenden Annahme, dass aktuelle Schutzmechanismen keine Daten mit Personenbezug betreffen (s. o. Vorbemerkung), werden zwangsweise Vorgaben zum Einsatz von Firewalls, Spamfilter, Intrusion Detection Systems u. Ä. möglich, ohne dass geklärt wird, wie mit den dabei anfallenden personenbezogenen Daten umgegangen werden kann und darf.

Es ist zu begrüßen, wenn die Betreiber kritischer Infrastrukturen und deren Branchenverbände nach Absatz 2 spezifische **Sicherheitsstandards** vorschlagen können, die vom BSI anerkannt werden können. Es genügt dabei aber nicht, das Benehmen mit den „zuständigen Aufsichtsbehörden und dem Bundesamt für Bevölkerungsschutz und Katastrophenschutz“ zu suchen, wenn damit nur die fachliche und nicht auch die datenschutzrechtliche Aufsicht gemeint ist. Angesichts des Umstandes, dass diese Standards zugleich als technisch-organisatorische Maßnahmen nach § 9 BDSG Wirkung entfalten, muss das **Einvernehmen mit der Datenschutzaufsicht** zur Voraussetzung gemacht werden.

Bei den in Absatz 3 vorgesehenen **Audits, Prüfungen und Zertifizierungen** werden auch eine Vielzahl datenschutzrelevanter Maßnahmen festgelegt oder gar vom BSI abverlangt. Daher sollte zumindest ein Austausch mit der jeweils nach § 38 BDSG zuständigen Datenschutzaufsicht gewährleistet werden. Besser noch wäre eine engere Abstimmung und Kooperation.

§ 8b BSIG-E Zentrale Meldestelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

Der geplante § 8b sieht in Abs. 2 Nr. 1 die Sammlung von **Daten aus Angriffen** gegen informationstechnische Systeme vor. Dass dabei in großem Umfang personenbezogene Daten aus den Systemen der Meldestellen verarbeitet werden, wurde bereits angesprochen. Es stellt sich wie beim geplanten § 8a die Frage, wie der Konflikt aus Sicherheit der Systeme und Schutz der darüber geführten Kommunikation gelöst werden soll. Vor allem aber droht auf diesem Wege eine Speicherung dieser Daten auf Vorrat. Während die Rechtsprechung aktuell eine 7-Tagesfrist für die Speicherung der Verbindungsdaten nach § 100 Abs. 1 TKG akzeptiert (BGH, U. v. 03.07.2014, III ZR 391/13, NJW 2014, 2500), droht durch den neuen Entwurf eine ganz wesentliche Ausweitung der Verarbeitung dieser Daten.

Die Aussage in der Begründung, wonach im Fall des Vorliegens eines Personenbezugs sich die Übermittlungsbefugnisse „nach den allgemeinen datenschutzrechtlichen Regelungen oder gegebenenfalls spezialgesetzlichen Regelungen“ richten soll (Begründung S.41), schafft **weder Klarheit noch Rechtssicherheit**. Der Gesetzentwurf muss davon ausgehen, dass bei Meldungen ein Personenbezug vorliegen kann und gewährleisten, dass und wie in diesem Fall bei Meldungen Beeinträchtigungen der informationellen Selbstbestimmung von Betroffenen vermieden werden.

Mit der Pflicht zur Meldung erheblicher IT-Sicherheitsvorfälle an das BSI kann eine **Meldeplicht von Datenpannen** nach § 42a BDSG verbunden sein, etwa wenn bei dem Angriff sensiblen Betroffenendaten offenbart wurden (sog. Breach Notification). Während die BSI-Meldung der Struktursicherung dient, dient die Meldepflicht nach § 42a BDSG vorrangig dem Selbstschutz der Betroffenen. Durch die Einbeziehung der Datenschutzbehörden und wegen der Relevanz des Nutzerverhaltens für die Struktursicherheit von IT-Systemen ist eine Synchronisierung der beiden Regelungen sinnvoll. Diese muss zumindest vorsehen, dass im Fall des Vorliegens der Voraussetzungen des § 42a BDSG eine Unterrichtung der Datenschutzaufsicht durch das BSI erfolgt und umgekehrt die Datenschutzaufsicht das BIS informiert, wenn bei einer Meldung einer Datenpanne die Voraussetzungen einer Meldung nach § 8b BSIG-E gegeben ist.

In Abs. 2 Nr. 2 ist die **Zusammenarbeit mit Bundesbehörden** bei der Analyse der Verfügbarkeit kritischer Infrastrukturen vorgesehen. Es wird davon ausgegangen, dass hier nicht nur an das Bundesamt für Verfassungsschutz (BfV) und das Bundeskriminalamt (BKA) gedacht wird, sondern auch an die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI).

In § 8b Abs. 2 Nr. 4 ist ein **Unterrichtungsrecht** des BSI gegenüber den Betreibern kritischer Infrastrukturen, den zuständigen Aufsichtsbehörden sowie den „sonst zuständigen Bundesbehörden über sie betreffende Informationen“ vorgesehen. Es bleibt unklar, ob mit Aufsichtsbehörden auch die für den Datenschutz zuständigen Aufsichtsbehörden in den Ländern gemeint sind. Sollen bei der Unterrichtung auch personenbezogene Daten übermittelt werden dürfen, so ist die Regelung zu unbestimmt, zumal sie keine datenschutzrechtlichen Schutzvorkehrungen enthält. Es ist weder eine Zweckbindung noch ein Gebot der Datensparsamkeit vorgesehen. Dies gilt auch, wenn „sie betreffende Informationen“ restriktiv in dem Sinne gemeint sein sollte, dass die Unterrichteten über sie betreffende Angriffe unterrichtet werden sollen.

Nach § 8b Abs. 4 ist eine **Meldepflicht** von Betreibern kritischer Infrastrukturen über Beeinträchtigungen vorgesehen, die zu einer Beeinträchtigung (der kritischen Infrastruktur) führen können. Der Gehalt dieser teilweise tautologischen Regelung ist unklar. Die Begründung gibt insofern auch nicht viel mehr Klarheit. Das anscheinend verfolgte Regelungsziel von präventiven Warnmeldungen wird nicht erreicht. Es kann mangels hinreichender Daten auch nicht erreicht werden, wenn bei potenziellen ‚Beeinträchtigungen nicht der Betreiber, sondern nur die Branche gemeldet werden muss bzw. eine pseudonyme Meldung erfolgt.

Die Meldepflicht kommt in gewissem Maße einer Selbstanzeige gleich. Diese mag – manchmal auch zu Recht – mit einem Imageverlust für das betroffene Unternehmen verbunden sein. Insofern ist die Intention des Entwurfes verständlich, die Meldeschwelle

durch die **Nichtnennung des Unternehmens** bei weniger gravierenden Vorfällen zu senken. Es muss aber bezweifelt werden, ob die dadurch eingeschränkten Meldungen geeignet sind, adäquat zu reagieren. Geeigneter dürfte es sein, die Meldebereitschaft durch eine rechtlich abgesicherte Zweckbindung der Meldungen für präventive Maßnahmen des BSI zu gewährleisten (vgl. ähnlich „Breach Notification“ gem. § 42a S. 6 BDSG).

Der Entwurf nennt in Abs. 4 S. 2 ein **Mindestmaß an zu übermittelnden Daten** (Angaben zu technischen Rahmenbedingungen, eingesetzte Technik, Branche des Betreibers) ohne aber die Chance für eine klare Normierung zu nutzen, welche Datenkategorien und -arten übermittelt werden dürfen und müssen. Es ist damit vorprogrammiert, dass große Mengen an Informationen über Mitarbeiter, Kunden und Unbeteiligte aus den Protokolldaten der Überwachungssysteme an das BSI weitergegeben werden, ohne dass geklärt ist, ob diese Daten rechtmäßig erhoben und weitergegeben werden durften. Der Entwurf geht damit der zentralen Frage aus dem Weg, wie in Monitoring-Netzwerken die Effektivität der Erkennung von Bedrohungen einerseits und die Wahrung des Rechts auf informationelle Selbstbestimmung miteinander vereinbart werden können.

Auch bei den **obligatorischen namentlichen Meldungen** bei tatsächlich sich direkt auswirkenden Beeinträchtigungen nach Abs. 5 kann ohne Beeinträchtigung des Meldezweckes durch eine Zweckbindung bzw. durch ein Verbot darauf basierender Sanktionen die Meldebereitschaft erhöht werden.

§ 8c BSIG-E Auskunftsverlangen Dritter

Das BSI soll Dritten Auskünfte über Erkenntnisse aus Meldungen geben dürfen, wenn schutzwürdige Interessen der Betreiber kritischer Infrastrukturen nicht entgegenstehen. Die Formulierung lässt offen, ob das Vorliegen **schutzwürdiger Interessen** generell eine Auskunft ausschließt, oder ob hier eine Abwägung vorgenommen werden soll. Zur Klarstellung sollte vor den Begriff schutzwürdige das Wort „überwiegende“ gesetzt werden. Unklar bleibt, wie mit schutzwürdigen sonstigen Interessen, insbesondere von betroffenen Nutzenden umgegangen werden soll. Gemäß der Formulierung bleiben diese unberücksichtigt.

Es ist einsichtig, dass aus Audits nach § 8a Abs. 3 erlangte Daten von Betreibern nur nach deren **Zustimmung** weitergegeben werden dürfen. Nicht verständlich ist aber, weshalb bei realen Beeinträchtigungen kritischer Infrastrukturen der Betreiber als Gefahrenquelle (§ 8b Abs. 5) nur mit dessen Zustimmung genannt werden darf. Eine Anhörung würde in diesen Fällen genügen, wenn die man dann die Weitergabe von einer Interessenabwägung abhängig macht.

Nach S. 3 wird Zugang zu den Akten des BSI in Angelegenheiten nach §§ 8a, 8b nicht gewährt. Diese **ausnahmslose Einschränkung des Informationszugangs**, der grundsätzlich nach dem Informationsfreiheitsgesetz besteht, kann nicht pauschal, wie in der Begründung (S. 44), damit begründet werden, dass „es sich um hochsensible, kumulierte sicherheitskritische Informationen, die einem besonders hohen Schutzbedürfnis unterliegen“, handelt. Statt sämtliche Akten vom Informationszugang auszunehmen, sollte die Auskunftsverweigerung darauf beschränkt werden, dass die Offenlegung der IT-Sicherheit schaden kann.

Zu Nr. 9 (§ 10 BSIG-E Ermächtigung zum Erlass von Rechtsverordnungen)

Das Bundesministerium des Innern soll gemäß dem Vorschlag nach Anhörung von Vertretern der Wissenschaft, betroffener Betreiber usw. und im Einvernehmen mit anderen Ministerien per Verordnung die kritischen Infrastrukturen nach § 2 Abs. 10 BSIG-E näher bezeichnen. Da diese Präzisierung auf Konsequenzen den Umfang und die Qualität personenbezogener Datenverarbeitung hat, sollte vor der Anhörung in jedem Fall die **Anhörung der betroffenen Datenschutzaufsicht** gewährleistet werden.

Zu Artikel 2 (Änderung des Telemediengesetzes – TMG)

Als neuer § 15 Abs. 9 TMG ist eine Erweiterung der Verarbeitungsbefugnisse der anfallenden **Nutzungsdaten** geplant, soweit dies „zum Erkennen, Eingrenzen oder Beseitigen von Störungen seiner für Zwecke seines Telemedienangebotes genutzten technischen Einrichtungen“ erforderlich ist. Derzeit ist nur die Verarbeitung der Nutzungsdaten zu Abrechnungszwecken, zur Erstellung pseudonymer Profile und zur Rechtsverfolgung von Entgeltansprüchen zulässig. Mit § 15 Abs. 9 TMG soll eine Regelung vergleichbar dem § 100 Abs. 1 TKG geschaffen werden, die auch TMG-Anbietern die Verarbeitung von personenbezogenen Daten zu Zwecken der technischen Fehlerbeseitigung erlaubt.

Der Entwurf ist zu **unbestimmt**. Die Auslegung des Begriffs der „Störungen“ wird in das Belieben des Anbieters gelegt, zumal in der Begründung (S. 51) ausgeführt wird, dieser Begriff sei „umfassend zu verstehen als jede vom Dienstanbieter nicht gewollte Veränderung der von ihm für sein Telemedienangebot genutzten technischen Einrichtungen“. Eine maximal zulässige Speicherdauer wird nicht genannt. Letztlich handelt es sich bei der Speicherungsbefugnis um eine Art Vorratsdatenspeicherung, für die die Rechtsprechung enge verfassungsrechtliche Anforderungen definiert hat (EuGH, U. v. 08.04.2014, C-293/12 u. C-594,12, DVBl 2014, 708 ff., NVwZ 2014, 709 ff.; BVerfG, U. v. 02.03.2010, 1 BvR 256/08 u. a., NJW 2010, 833 ff., DVBl 2010, 503 ff., JZ 2010, 611 ff.) Eine Präzisierung ist verfassungsrechtlich geboten, etwa durch Anonymisierungspflichten, Maximalspeicherfristen (z. B. eine Woche, vgl. BGH, U. v. 03.07.2014, III ZR 391/13, NJW 2014, 2500) sowie explizite, sanktionierte Verbote der Verwendung zu anderen Zecken und der personenbezogenen diensteübergreifenden Datenzusammenführung.

In Abs. 9 S. 2 ist vorgesehen, dass § 15 Abs. 8 S. 2 TMG entsprechend gelten soll. Dies bedeutet, dass Daten nicht gelöscht werden müssen, wenn diese „**für die Rechtsverfolgung**“ benötigt werden. Anders wie im in Absatz 8 geregelten Fall der Leistungserschleichung werden nach Absatz 9 Daten von anderen Personen als diejenigen, die eine (Leistungs-) Störung verursachen, gespeichert. Der Regelungsvorschlag findet auch keine Entsprechung in § 100 Abs. 1 TKG. Er lässt sich leicht zur Rechtfertigung von unbefristeten Datenspeicherungen verwenden. Seine Notwendigkeit ist nicht dargetan, weshalb er zu streichen ist.

Zu Artikel 3 (Änderung des Telekommunikationsgesetzes – TKG)

Zu 1. Änderung des § 100 Abs. 1 TKG

Durch eine Konkretisierung des § 100 Abs. 1 TKG wird die Rechtsgrundlage für die Verwendung personenbezogener Daten zur Störungsabwehr dahingehend geändert, dass auch **Einschränkungen der Verfügbarkeit** als Störung eingeordnet werden. Laut der Begründung des Entwurfs (S. 52) soll damit auch die Bekämpfung von Bot-Netzen ermöglicht werden. Unklar bleibt, in welchem Umfang auch Spam-Mail und damit zusammenhängend die Spam-Filterung von E-Mails von der Konkretisierung erfasst werden soll. Gerade die Detektion von Spam-Kampagnen kann als Werkzeug zur Erkennung von Botnetzen genutzt werden, setzt aber die Verarbeitung gewaltiger Mengen an personenbezogenen Daten voraus. Unklar bleibt z. B., wie in Fällen zu entscheiden ist, in denen zwar Bots erkannt werden, diese aber die Verfügbarkeit der eigenen Netze und Anlagen nicht beeinträchtigen. Offen bleibt weiterhin, ob der Schutz von Netzen anderer Anbieter mit erfasst werden soll. Die vorgelegte Formulierung scheint diesen Schutz auszuschließen. Die Formulierung „führen können“ eröffnet einen sehr weiten Anwendungsspielraum, mit dem anlasslos die Aufzeichnung jedweden Netzwerkverkehrs gerechtfertigt werden kann, ohne dass die Norm angemessene Grenzen aufzeigt.

Auf die **Ausführungen zu § 15 Abs. 9 TMG-E** (oben) wird verwiesen.

Zu 6. Einfügung eines § 109a Abs. 4 TKG (Daten- und Informationssicherheit)

Der Regelungsvorschlag sieht eine **Informationspflicht des Diensteanbieters** gegenüber dem Nutzer bei von seinen Datenverarbeitungssystemen ausgehenden Störungen vor. Es soll auf „technische Mittel hingewiesen werden, mit deren Hilfe die Nutzer Störungen, die von ihren Datenverarbeitungssystemen ausgehen, erkennen und beseitigen können“. Die Frage, wie dieser Informationspflicht entsprochen werden soll, beantwortet der Entwurf nicht. In der Begründung wird insofern auf mögliche Hinweisseiten verwiesen. Dies kann nur als ein Beispiel verstanden werden. Andere, möglichst wirksame Wege, müssen auch möglich und sollten im Zweifelfall verpflichtend sein (E-Mail, Post, Telefonanruf). Dies darf aber zugleich nicht dazu führen, dass vor Eintritt einer Störung präventiv zusätzliche Erreichbarkeitsdaten erhoben werden.

Die Informationspflicht trifft gemäß dem Wortlaut ausschließlich den Diensteanbieter, nicht aber dessen **Dienstleister**, denen in der äußerst arbeitsteiligen Telekommunikation oft wesentliche Funktionen zukommen. Um diese mit zu erfassen, ist es sinnvoll, in Absatz 1 S. 1 (für den gesamten Paragraph geltend), hinter dem Wort „erbringt“ aufzunehmen: „oder an der Erbringung solcher Dienste mitwirkt“.

Für Rückfragen und Erläuterungen der oben gemachten Ausführungen stehe ich gerne zur Verfügung.

Mit freundlichen Grüßen

Dr. Thilo Weichert