Berlin, 09.12.2020

Stellungnahme
und Handlungsempfehlungen

zum Entwurf des zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme ("IT-Sicherheitsgesetz" / IT-SiG 2.0)

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Ansprechpartner für Rückfragen:

RA Karsten U. Bartels LL.M.
Stellvertretender TeleTrusT-Vorsitzender
Leiter der TeleTrusT-AG "Recht"
bartels@hk2.eu

A. Einleitung

Im Folgenden nimmt der Bundesverband IT-Sicherheit e.V. (TeleTrusT) Stellung zu dem vom Bundesministerium des Innern, für Bau und Heimat am 02.12.2020 vorgelegten Entwurf des zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0-ENT) in der Fassung vom 01.12.2020, 19:55 Uhr.

Die Stellungnahme betrachtet bestimmte Regelungsbereiche des IT-Sicherheitsgesetzes (IT-SiG) und seiner geplanten Änderung. Dem Umstand, Regelungen nicht zu kommentieren, kommt keine ablehnende oder zustimmende Bedeutung zu.

Das Gesetz soll das IT-SiG aus dem Jahr 2015 ändern und somit an neue digitale Herausforderungen anpassen. Das IT-SiG hat erfolgreich mit dazu beigetragen, dass Unternehmen ihre IT-Sicherheit erhöht haben und stellt insgesamt inzwischen einen wichtigen Maßstab für IT-Sicherheit dar. Das Bestreben des Gesetzgebers, den nunmehr gewachsenen Anforderungen an die Sicherheit von IT-Infrastruktur gerecht zu werden, ist zu begrüßen.

Gleichwohl bestehen im Hinblick auf einzelne Regelungen des IT-SiG 2.0-ENT erhebliche Zweifel an der sachgemäßen Umsetzung hinsichtlich vor allem

- des überlimitierten Adressatenkreises des Gesetzes
- der perspektivischen Umsetzung, die allein Deutschland in Bezug nimmt
- der Aufgabenzuordnung zum BSI

- des systematischen Aufbaus von Regelungen
  und
- der tatsächlichen Wirkung der geplanten Regelungen.

B. Adressatenkreis des Gesetzes

Das Maß an IT-Sicherheit in der Wirtschaft kann durchgängig und nachhaltig nur signifikant erhöht werden, wenn die Regelungen des IT-SiG auch für den Mittelstand gelten. Gerade mittelständischen Unternehmen mangelt es noch häufig an einer ausreichend gesicherten IT-Infrastruktur. Die Einbindung in zum Teil weltweite Netzwerke macht sie dabei zu einem erheblichen Sicherheitsrisiko. Gleichzeitig sind sie selbst Ziel von Cyber-Angriffen.

Es bedarf hier angemessener und verständlicher Vorgaben, die den wirtschaftlichen Möglichkeiten von KMU gerecht werden.

Soweit argumentiert wird, das IT-SiG richte sich bewusst nur an KRITIS-Betreiber, darf auf § 13 Abs. 7 Telemediengesetz hingewiesen werden. Die Norm adressiert bereits seit 2015 jeden Telemediendiensteanbieter. Da nahezu jedes Unternehmen auch mindestens ein Telemedium anbietet, sind also bereits Unternehmen jeder Größe adressiert. Warum dies allerdings auf Telemedien beschränkt wurde, ist sachlich nicht nachvollziehbar.

C. Aufgabenzuordnung zum BSI

Der erhebliche Ausbau der Eingriffsbefugnisse des Bundesamts für Sicherheit in der Informationstechnik (BSI) im Rahmen des IT-SiG 2.0-ENT birgt die deutliche Gefahr eines Vertrauensverlustes in das BSI.
Eine derart massive Erweiterung von Befugnissen sollte daher gegebenenfalls an zusätzliche Kontroll- und Transparenzmechanismen geknüpft und insgesamt höchst kritisch hinterfragt werden.

Es bedarf dazu einer breit angelegten und offenen Debatte, die es bislang nicht gegeben hat. Es wurde bereits zum ersten IT-SiG darauf hingewiesen, dass eine umfassende Meldepflicht für Unternehmen, die spiegelbildlich zum Aufbau großer Datenbestände beim BSI führt, dazu verleitet, später gerade aufgrund der gesammelten Erkenntnisse nunmehr auch entsprechende Eingriffsbefugnisse zu fordern.[1]

Um das Vertrauen in das BSI nicht zu beschädigen, muss verhindert werden, dass das BSI sich zu einer kaum zu kontrollierenden Sicherheitsbehörde entwickelt. Einer Behörde, die mit Omnikompetenz alles unternimmt: Beratung, Warnung, Aufsicht, Meldestelle, Informationsstelle, Prüfung, Kriterienaufstellung, Kennzeichen-Ausstellung und Verbraucherschutz u.v.a.m.

Der erhebliche Ausbau der Beratungsleistungen zu IT-Sicherheit im behördlichen Umfeld des BSI tritt in Konkurrenz zum Angebot zahlreicher IT-Sicherheitsunternehmen. Es sollte sichergestellt werden, dass das BSI kein operatives Geschäft der IT-Sicherheitsindustrie übernimmt, um die Innovationskraft des Marktes nicht zu schwächen.

D. Die wichtigsten Regelungen des Entwurfs

I. Neue Kontrollmöglichkeiten für das BSI

§ 4a BSIG n.F.
Das BSI ist hiernach befugt, die Sicherheit der Kommunikationstechnik des Bundes und ihrer Komponenten, einschließlich technischer Infrastrukturen, die zu deren Betrieb erforderlich sind, zu kontrollieren. Dazu kann das BSI zur Abwehr von Gefahren für die Sicherheit der Informationstechnik des Bundes sowie zur Beratung und Warnung betroffener Stellen die Herausgabe von Kopien bzw. die Bereitstellung von Informationen vom Betreiber der jeweiligen Kommunikationstechnik sowie Zutritt zu Betriebsräumen verlangen. Eine Rückausnahme ist nur für das Entgegenstehen von Geheimschutzinteressen oder überwiegenden Sicherheitsinteressen vorgesehen.

[1] Bartels, Bezugspunkte des IT-Sicherheitsgesetzes, ITRB 4/2015, S. 92.

Stellungnahme
Die Bereitstellungspflicht ist im Hinblick auf den Verweis auf § 3 Abs. 1 Nr. 14 BSIG zu weitgehend. Denn so kann das Herausgabeverlangen bereits auf eine bloße Beratungsabsicht gestützt werden. Dadurch könnten sich "Betreiber“ jederzeit und ohne das Vorliegen irgendwelcher Hinweise auf Sicherheitslücken, einem Herausgabeverlangen des BSI ausgesetzt sehen.
Die Begriffe "Betreiber“ und "Dritter“ sind in § 2 zu definieren. Die Verfahren und in Betracht kommenden Schnittstellen sollten konkretisiert werden.

II. Auskunftsanspruch des BSI über Bestandsdaten

§ 5c BSIG n.F.
Nach § 5c BSIG n.F. müssen Telekommunikationsanbieter dem BSI Auskunft über Bestandsdaten geben, um Angriffe auf die Sicherheit und Funktionsfähigkeit informationstechnischer Systeme Kritischer Infrastrukturen oder von Unternehmen im besonderen öffentlichen Interesse zu verhindern oder sonstige erhebliche Schäden vom betroffenen Dritten abzuwenden.

Stellungnahme
Die Tatbestandsalternative gemäß Abs. 1 Ziff. 2 ("sonstige erhebliche Schäden“) stellt zwar als Erheblichkeitsschwelle eine begrüßenswerte Begrenzung des Auskunftsanspruchs dar. Dieser unbestimmte Rechtsbegriff wird aber zu Rechtsunsicherheit führen, welche nur durch eine gefestigte Rechtsprechung beseitigt werden kann. Bis dahin dürften einige Jahre vergehen.

Es bedarf zwingend klarer Vorgaben des Gesetzgebers, wie das BSI mit den erlangten Daten umzugehen hat. Speicherdauer, Zugriffsrechte und Auswertung der Daten müssen für die betroffenen Unternehmen transparent und nachvollziehbar gestaltet sein. Eine Forderung, die auch für die Informationslage nach geltendem IT-SIG gilt.

III. Portscans und Honeypots

§ 7b BSIG n.F.
Gem. § 7b Abs. 1 BSIG n.F. ist das BSI zur Durchführung von Portscans berechtigt, wenn Tatsachen die Annahme rechtfertigen, dass informationstechnische Systeme ungeschützt sind und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sind. Nach Abs. 4 darf das BSI sog. Honeypots nutzen, um den Einsatz von Schadprogrammen oder anderen Angriffsmethoden zu erheben.

Stellungnahme
Die Detektionsmaßnahmen sind grundsätzlich geeignet, Sicherheitsrisiken und deren Ursache zu erkennen und zu untersuchen. Es ist richtig und rechtsstaatlich nicht anders zulässig, diese Maßnahmen dem Angemessenheitsvorbehalt unterzuordnen.

Unklar lässt der Entwurf allerdings, wie vermieden werden soll, dass es bei diesen Maßnahmen zu Schäden kommt, die der Betreiber gegebenenfalls nicht zu verantworten hat oder die Maßnahmen unangemessen sind. Das betroffene Unternehmen sollte deshalb vorab über die Portscans informiert werden, wenn nicht zu erwarten ist, dass die Information das Ergebnis verfälschen wird. Jedenfalls ist das betroffene Unternehmen unverzüglich nach der Maßnahme über den Umfang und mögliche Folgen zu informieren.

IV. Anordnungs-, Auskunfts- und Untersuchungsbefugnisse des BSI gegenüber TK-Anbietern

§ 7a BSIG n.F.
Zur Erfüllung seiner Aufgaben kann das BSI für die Untersuchung informationstechnischer Systeme alle notwendigen Auskünfte verlangen.

Stellungnahme
Der Auskunftsanspruch ist zu weitgehend. Jedenfalls sind die Limitierungen durch die Erforderlichkeit und die Notwendigkeit nicht geeignet, die Unternehmen mit einer hinreichenden Rechtssicherheit auszustatten. Es ist

insbesondere unklar, wie die Unternehmen ihre Geschäftsgeheimnisse tatsächlich und rechtlich schützen können sollen. Ein Abgleich mit den Anforderungen des seit 2019 geltenden Geschäftsgeheimnisschutz-Gesetz (GeschGehG) sollte vorgenommen werden.
Ebenfalls sehr kritisch wird der gesetzlich nicht differenzierte Einsatz Dritter zur Unterstützung bewertet. Hier erhöht sich noch einmal das oben dargestellte Problem um die Dimension des Dritten. Eine Eingrenzung und Klarstellung sind hier höchst wünschenswert.

§§ 7c, 7d BSIG n.F.
Zur Abwehr konkreter erheblicher Gefahren, insbesondere für die Verfügbarkeit und Vertraulichkeit der Informations- oder Kommunikationsdienste, kann das BSI gegenüber einem Anbieter von Telekommunikationsdiensten mit mehr als 100.000 Kunden anordnen, dass er Maßnahmen zur Abwehr spezifischer Gefahren trifft, sofern er dazu technisch in der Lage und ihm dies wirtschaftlich zumutbar ist.
Ferner kann das BSI Daten umleiten, um Informationen über Schadprogramme oder andere Sicherheitsrisiken erlangen. Diese Daten dürfen durch das BSI höchstens drei Monate gespeichert werden.

Stellungnahme
Die Möglichkeit des BSI, Daten an eine bestimmte Anschlussstelle umzuleiten, ist höchst kritisch. Die Einschränkung, dass diese nur für drei Monate gespeichert werden und die Regelungen nur für Unternehmen mit mehr als 100.000 Kunden gelten sollen, verbessert den Regelungsgehalt nicht. Hier bedarf es mindestens klarer Präzisierungen und Ausnahmeregelungen sowie eine eindeutige Transparenz bei einem derartigen Vorgehen.

Dies gilt auch für die Anhörung der benannten Stellen in § 7c Abs. 1 BSIG n.F. Andernfalls sind durch ein solches Vorgehen sowohl Daten nach dem GeschGehG als auch personenbezogene Daten einer Willkür ausgesetzt, die zu einem deutlichen Vertrauensverlust führt.

V. Ausweitung von Meldepflichten und Mindeststandards

§§ 8, 8f BSIG n.F.
Die bestehenden Meldepflichten und verpflichtenden Mindeststandards für Betreiber Kritischer Infrastruktur werden auf weitere Teile der Wirtschaft ausgeweitet. Neben den KRITIS-Betreibern sind nunmehr auch Unternehmen im besonderen öffentlichen Interesse (§ 8f BSIG n.F.) erfasst sowie IT-Dienstleister, die Dienstleistungen für die Kommunikationstechnik des Bundes erbringen.

Diese Unternehmen müssen beim BSI eine Selbsterklärung vorlegen, aus der u. a. hervorgeht, ob das Unternehmen beim Schutz seiner IT-Systeme den Stand der Technik einhält.

Stellungnahme
Die Ausweitung ist erheblich und wird die betroffenen Unternehmen vor große Herausforderungen stellen. Die in § 2 Abs.14 BSIG n.F. vorgesehene Rechtsverordnung zur Konkretisierung sollte dies bei der Festlegung der Schwellenwerte berücksichtigen.

Mit den derzeitigen Schwellenwerten der BSI-KRITIS-Verordnung muss bezweifelt werden, ob in dünn besiedelten Regionen kritische Dienstleistungen bei gravierenden Cyberangriffen aufrechterhalten werden können. Vor allem IT-Sicherheitsvorfälle mit Kaskadeneffekten, ausgelöst durch Sicherheitslücken bei einer Mehrzahl von Unternehmen oder einer Mehrzahl von getrennten IT-Einheiten können zu Szenarien führen, die bislang nicht gesetzlich berücksichtigt sind. Deshalb wäre eine Absenkung der Schwellenwerte grundsätzlich zu begrüßen, auch wenn dies keine hinreichende Maßnahme wäre. Eine umfassende Betrachtung und Verbesserung der IT-Sicherheit in Deutschland sollte die KMU nicht ausklammern.

Die sektorale Erweiterung der Unternehmen auf solche aus der Rüstungsindustrie sowie mit Bezug zu staatlich relevanter IT ist zu begrüßen. Insbesondere die Erweiterung auf volkswirtschaftlich bedeutsame Unternehmen (§ 2 Abs. 14 Nr. 2 BSIG) stellt eine Neuerung dar, da erstmals die wirtschaftliche Leistung ausschlaggebend ist. Hierfür sind zeitnah Rechtsverordnungen zu erlassen, um die benötigten Kennzahlen und Schwellen für betroffene Unternehmen festzulegen, damit diesen eine schnelle und effektive Umsetzung ermöglicht wird. Darüber hinaus sind weitere Präzisierungen hinsichtlich der Begrifflichkeiten notwendig, um eine klare und begründete Abgrenzung zu gestatten und somit langfristig ein einheitliches europäisches Vorgehen zu ermöglichen.

Im Hinblick auf das wesentliche Merkmal zum Technologieniveau "Stand der Technik“ bleibt unklar, wie sich dieses bestimmt. Insoweit bleibt nach dem derzeitigen Entwurf ein erhebliches Maß an Rechtsunsicherheit

bestehen. Keinesfalls sollte der Stand der Technik innerhalb einer Verordnung oder Technischen Richtlinie statisch beschrieben werden. Die Regelung sollte dynamisch und zugleich hinreichend konkret sein. Es wäre höchst wünschenswert und gewissermaßen überfällig, auf die in Praxis und Wissenschaft ausgearbeiteten und bewährten Definitionen und Methoden zurückzugreifen. Es bietet sich die inzwischen auch von der ENISA aufgegriffene Definition des TeleTrusT an (Handreichung zum Stand der Technik[2]).

Es ist wesentlich, den objektiv-technisch festzustellenden Stand der Technik sehr klar zu trennen von den subjektiven Tatbestandsmerkmalen, die die Frage beantworten, inwieweit der Stand der Technik im Einzelfall umzusetzen ist. Hier liegen inzwischen Methoden[3] vor, die es aufzugreifen gilt.

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) begrüßt es ausdrücklich und hält es für richtig, dass der vorliegende Entwurf von einer gesetzlichen Fiktion zur Einhaltung des Stands der Technik in § 8a Abs. 1a BSIG n.F. absieht. Der Entwurf vom 07.05.2020 hatte dies noch so vorgesehen[4]. Eine Festlegung des Stands der Technik in Technischen Richtlinien und/ oder entsprechende Fiktionen zum Stand der Technik widersprechen systematisch dem Wesen des Stands der Technik.

Nach dem jetzigen Entwurf ist schließlich davon auszugehen, dass die Vorgabe der Prüfkriterien und die Überprüfung derselbigen einheitlich in der Hand des BSI liegt. Diese Kompetenzkonzentration sollte vom Gesetzgeber mit Transparenz- und Kontrollmechanismen flankiert werden. Nur so kann sichergestellt werden, dass für die betroffenen Unternehmen jederzeit nachvollziehbar ist, nach welchen Kriterien das BSI prüft.

VI. Untersagungsmöglichkeit für kritische Komponenten

§ 9b BSIG n.F.
Für sog. kritische Komponenten besteht eine Prüfmöglichkeit durch das Bundesministerium des Innern, für Bau und Heimat (BMI). Der Einsatz kann untersagt werden, wenn überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange dem entgegenstehen. Über eine verpflichtende Garantieerklärung werden von den Herstellern bestimmte Maßnahmen eingefordert, welche den laufenden Betrieb der Komponenten betreffen (§ 9b Abs. 2 n.F.). Dadurch soll sichergestellt werden, dass die kritischen Komponenten über keine technischen Eigenschaften verfügen, die geeignet sind, auf die Integrität der Kritischen Infrastruktur missbräuchlich einwirken zu können.

Stellungnahme
Auf das pauschale Ausschließen bestimmter Anbieter ist verzichtet worden. Das ist zu begrüßen. Es erscheint nicht sachgerecht, Hersteller allein wegen ihrer Herkunft auszuschließen. Vielmehr müssen effektive, prüfbare und auch tatsächlich geprüfte Sicherheitsanforderungen an die betreffenden Anbieter gestellt werden.

Es erscheint völlig offen, wie diese Sicherheitsanforderungen praktisch mittels der geplanten Garantieerklärungen umgesetzt werden sollen. Es wird bestritten, dass die Prüfungen des BMI geeignet sind, um die Integrität der Komponenten abschließend zu beurteilen. Es gilt, hier einen wirkungslosen Formalismus zu vermeiden, der allein einem politischen Kompromiss geschuldet ist.

Die vorgesehene Untersagungsmöglichkeit für kritische Komponenten birgt ein großes Unsicherheitspotenzial. Der neue § 9b BSIG legt zumindest nahe, dass auch der nachträgliche Ausbau von solchen Komponenten durch das BSI gefordert werden kann. Dadurch besteht die Gefahr, dass bereits im Aufbau befindliche Großprojekte, wie z.B. der Ausbau des 5G-Netzes, ins Stocken geraten.
Es ist darauf hinzuweisen, dass kritische Komponenten im Sinne der Norm technisch komplexe Systeme mit Bauteilen/ -gruppen unterschiedlichster Herkunft sein werden. Um einer Pauschalbewertung vorzubeugen, müssten die Inhalte der kritischen Komponenten aufgeführt, analysiert und bewertet werden. Es ist nicht er-

[2] Der Stand der Technik kann als die im Waren- und Dienstleistungsverkehr verfügbaren Verfahren, Einrichtungen oder Betriebsweisen, deren Anwendung die Erreichung der jeweiligen gesetzlichen Schutzziele am wirkungsvollsten gewährleisten, bezeichnet werden, vgl. TeleTrusT-Handreichung Stand der Technik in der IT-Sicherheit, S. 11; Bartels/Backer, Die Berücksichtigung des Stands der Technik in der DSGVO, DuD 4-2018, 214; Bartels/Backer/Schramm, Der „Stand der Technik" im IT-Sicherheitsrecht, Tagungsband zum 15. Deutschen IT-Sicherheitskongress 2017, Bundesamt für Sicherheit in der Informationstechnik, 503.
[3] TeleTrusT-Handreichung Stand der Technik in der IT-Sicherheit, S. 12 f.
[4] § 8a Abs. 1a S. 3 BSIG-ENT vom 07.05.2020: „Die Einhaltung des Standes der Technik wird vermutet, wenn die Systeme der Technischen Richtlinie [Bezeichnung] des Bundesamtes in der jeweils geltenden Fassung entsprechen".

kennbar, wie sich diese Komplexität mit den im Rahmen von § 2 Abs. 13 BSIG n.F. vorgesehenen Festlegungen abbilden lassen soll. Betroffene Unternehmen sollten frühzeitig die Möglichkeit erhalten, die in § 9b Abs. 2 BSIG n.F. geforderten Garantieerklärungen vorzubereiten bzw. einzuholen.

VII. BSI als neutrale Beratungsstelle für Fragen der IT-Sicherheit/ IT-Sicherheitskennzeichen

§ 9c BSIG n.F.
Das BSI übernimmt den Verbraucherschutz im Bereich der Informationssicherheit als zusätzliche Aufgabe (Art. 1 Nr. 2 d IT-SiG 2.0). In diesem Zusammenhang soll ein freiwilliges IT-Sicherheitskennzeichen geschaffen werden, welches die IT-Sicherheit von Produkten erstmals sichtbar macht, § 9c BSIG n.F.

Stellungnahme
Das Hervorheben der Perspektive des Verbraucherschutzes ist im Zusammenhang mit IT-Sicherheit grundsätzlich zu begrüßen. Inwieweit das geplante IT-Sicherheitszeichen als freiwillige Selbstverpflichtung (mit reiner Plausibilitätsprüfung durch das BSI) gegenüber Verbrauchern einen spürbaren Effekt zeitigen kann, lässt sich noch nicht bewerten. Der Erfolg hängt von der Akzeptanz auf Seiten der Hersteller und der Kunden ab. Dessen ungeachtet ist die Konzeption als nationalstaatliches Kennzeichen nicht überzeugend. Die diversen politischen und rechtlichen Aufträge an europäische Stellen, IT-Sicherheitskennzeichen auf der EU-Ebene zu schaffen, wurden nicht erkennbar berücksichtigt. Dies wäre aber wünschenswert. Ebenso wie die Gestaltung des IT-Sicherheitskennzeichens in Form einer Zertifizierung.

Durch die in diesem Zusammenhang vorgeschlagene Befugnis des BSI, eigenständige Technische Richtlinien zu erlassen, wird der europäische Marktzugang fragmentiert und erschwert. Dies kann nicht im Sinne der Strategie eines einheitlichen digitalen EU-Binnenmarktes sein und gerade für KMU wird es zunehmend schwieriger, einen Überblick über den Regulierungsdschungel zur IT-Sicherheit zu behalten.

VIII. Neues Bußgeldregime

§ 14 BSIG n.F.
Der Bußgeldrahmen wird deutlich erhöht. In der aktuellen Fassung von § 14 BSIG liegt die Höchstgrenze bei 100.000 Euro. Im vorliegenden Entwurf soll sie auf bis zu EUR 2 Millionen angehoben werden, wobei verschiedene Abstufungen vorgesehen sind.

Stellungnahme
Die DSGVO hat gezeigt, dass spürbare Bußgeldandrohungen und tatsächlich erhobene Bußgelder einen erheblichen Anteil daran haben, dass Unternehmen Regelungen zur Informationssicherheit u.a. befolgen. Die Erhöhung des Bußgeldrahmens kann daher als positiv bewertet werden.
Gleichwohl wird in Frage gestellt werden, ob die Höchstgrenze von EUR 2 Millionen tatsächlich ausreicht, um die gewünschte Wirkung zu erzielen.

IX. § 13 Abs. 7 TMG

Im Zusammenhang mit der Bewertung des IT-SiG 2.0-ENT ist eine Evaluierung des § 13 Abs. 7 TMG angezeigt. Die Vorschrift ist 2015 mit dem IT-SiG eingeführt worden.

Die bereits im Zuge der Einführung verlautbarten Befürchtungen, wonach das Fehlen von Mindeststandards sowie die fehlende Konkretisierung durch Branchenverbände letztlich zu einem Leerlaufen der Vorschrift führen könnten, haben sich für die Telemediendiensteanbieter bewahrheitet. Fünf Jahre nach Einführung der Vorschrift ist nüchtern festzustellen, dass die Norm in der Praxis weder der Unternehmen noch der Aufsichtsbehörden irgendeinen Widerhall gefunden haben. Die Norm ist unbekannt, wird nicht umgesetzt und bis heute ist unklar, ob die Landesmedienaufsicht oder / und die Landesdatenschutz-Aufsichtsbehörden zuständig sind.[5]

Das IT-SiG 2.0 sollte § 13 Abs. 7 TMG auf den Prüfstand stellen und entweder nachjustieren oder aufheben.

[5] Bartels/ Backer, ITSiG-konforme Telemedien – Technische und organisatorische Vorkehrungen nach § 13 Abs. 7 Telemediengesetz, DuD, 40(1), 22.