Stellungnahme

zum Entwurf des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)
Aktualisierte und ergänzte Version der Stellungnahme vom 12. November 2014

10. Dezember 2014

BITKOM vertritt mehr als 2.200 Unternehmen der digitalen Wirtschaft, davon gut 1.400 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 200 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. Mehr als drei Viertel der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils knapp 10 Prozent kommen aus sonstigen Ländern der EU und den USA, 5 Prozent aus anderen Regionen. BITKOM setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10
10117 Berlin-Mitte
Tel.: +49.30.27576-0
Fax: +49.30.27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Marc Fliehe
Bereichsleiter Sicherheit
Tel.: +49.30.27576-242
Fax: +49.30.27576-5242
m.fliehe@bitkom.org

Präsident
Prof. Dieter Kempf

Hauptgeschäftsführer
Dr. Bernhard Rohleder

1 Einleitung und Hintergrund

Das Bundesministerium des Innern hat am 4. November 2014 einen aktualisierten Referentenentwurf für ein Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vorgelegt und die Verbände aufgefordert, hierzu bis zum 12. November 2014 Stellung zu nehmen. BITKOM nimmt gerne die Gelegenheit wahr, seine Position zum Referentenentwurf darzustellen.

BITKOM unterstützt den Ansatz der Bundesregierung nachdrücklich, den Wirtschaftsstandort Deutschland widerstandsfähiger gegen die Vielzahl von Cyberbedrohungen zu machen. Datensicherheit ist ein hohes Gut und aufgrund seines hohen Niveaus in Deutschland ein Standortvorteil, den es zu bewahren gilt. Das intendierte Ziel, Mindeststandards für IT-Sicherheit bei unterschiedlichen Betreibern kritischer Infrastrukturen zu etablieren, wird daher ausdrücklich begrüßt.

Unumgänglich ist unseres Erachtens dabei eine enge Zusammenarbeit von Staat und Wirtschaft zum verstärkten Aufbau von fachlicher Expertise zur Informationssicherheit in der Privatwirtschaft.

Im Hinblick auf eine erfolgreiche Zusammenarbeit von Staat und Wirtschaft setzt BITKOM auf den Grundsatz der Freiwilligkeit und unterstützt dabei direkt oder durch seine Mitgliedsunternehmen eine Vielzahl von erfolgreichen Initiativen. Insbesondere die von BITKOM mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) initiierte Allianz für Cybersicherheit hat das Potenzial, nachhaltig die Sicherheitskultur in Deutschland zu verändern. Hier wurde beispielsweise ein unkomplizierter und auf Wunsch anonymer Meldeweg geschaffen, um das BSI über aktuelle Angriffe zu unterrichten. Gleichwohl eröffnet eine gesetzliche Verankerung des Themas Informationssicherheit die Chance, Wirtschaft und Staat einen klaren Handlungsrahmen vorzugeben. Dieser sollte für alle Beteiligten Planungs- und Rechtssicherheit erzeugen.

Wir begrüßen ausdrücklich die Vielzahl an Konkretisierungen, die in die neue Fassung des vorliegenden Referentenentwurfes eingeflossen sind, insbesondere im Bereich der KRITIS-Definition sowie im Bereich der Sicherheitsüberprüfungen. Das avisierte Spezialgesetz unterstützen wir insofern, als dass es das berechtigte Bedürfnis der Bundesregierung reflektiert, ein angemessenes Schutzniveau der kritischen Infrastrukturen zu gewährleisten.

BITKOM hat eine erste umfangreiche Stellungnahme zum geplanten IT-Sicherheitsgesetz bereits am 2. April 2013 veröffentlicht und den Gesetzgebungsprozess eng begleitet. Die Veröffentlichung des zweiten Referentenentwurfes vom 18. August 2014 ging dem BITKOM ebenfalls mit der Bitte um Kenntnisnahme zu. In der nun vorliegenden Version des Gesetzesentwurfs ist BITKOM kurzfristig zur Stellungnahme aufgefordert.

2 Grundsätzliche Anmerkungen zum Referentenentwurf

2.1 Ziel des Gesetzes

Auf Seite 1 wird das Ziel dieses Gesetzesvorhaben definiert. Darin heißt es:

„Mit dem Gesetz soll eine signifikante Verbesserung der Sicherheit informationstechnischer Systeme (IT-Sicherheit) in Deutschland erreicht werden. Die vorgesehenen Neuregelungen dienen dazu, die Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität datenverarbeitender Systeme zu verbessern und die Systeme der IT-Sicherheitslage anzupassen. Ziel des Gesetzes ist die Verbesserung der IT-Sicherheit von Unternehmen, der verstärkte Schutz der Bürgerinnen und Bürger im Internet und in diesem Zusammenhang auch die Stärkung von BSI und Bundeskriminalamt (BKA).“

Aus Sicht der Wirtschaft ist die Zielsetzung des Gesetzes begrüßenswert. In den einzelnen Paragraphen schlägt sich diese Zielsetzung aber in unterschiedlicher Art und Weise nieder. Auch berücksichtigt der Entwurf nicht hinreichend, dass bereits jetzt Regelungen über die Sicherheit, vor allem bei Verarbeitung personenbezogener Daten (z.B. Anlage zu § 9 S. 1 BDSG) vorhanden sind. Dieses wird in der entsprechenden Kommentierung der einzelnen Paragraphen gesondert aufgeführt.

2.2 Erfüllungsaufwand durch die Wirtschaft

Anders als im vorliegenden Gesetzesentwurf angenommen, entstehen der Wirtschaft durchaus Mehraufwände durch die Anforderungen aus dem Gesetz. Hierbei ist das Verhältnis von Aufwand und Nutzen der Meldepflicht zu berücksichtigen.

Bei der Beurteilung des Erfüllungsaufwandes durch die Wirtschaft ist aus BITKOM-Sicht nicht ausreichend berücksichtigt, dass die abgesenkten Meldeschwellen im Rahmen des § 109 Abs. 5 TKG n.F. vermutlich zu einer Erhöhung der zu dokumentierenden Vorgänge führt. Das hat zur Folge, dass (a) adäquate Metriken entwickelt werden müssen, gegen die die Ereignisse innerhalb der Netze gemessen werden können, (b) entsprechende Technologien nicht nur vereinzelt an sicherheitstechnischen „Hot Spots“, sondern flächendeckend

eingeführt werden und (c) die Vielzahl der zu erwartenden Fälle qualifiziert und ggf. an die Behörden weitergegeben und ggf. nachbearbeitet werden müssen.

Der Erfüllungsaufwand für die Wirtschaft wird noch dadurch erweitert, dass die Dokumentations- und Auditaufwände in der Verordnung nach §10 noch zu definierenden KRITIS-Unternehmen vermutlich an Lieferanten und Partner ganz oder in Teilen weitergereicht werden.

Die Feststellung im Entwurf, dies alles müsse gegenwärtig ohnehin getan werden, ist aus der Perspektive des Gesetzes und der derzeit geltenden Schwellen schlicht unzutreffend, zumal die Einhaltung der Meldepflichten bußgeldrelevant ist.

Uns ist daher daran gelegen, dass dieser Mehraufwand der Wirtschaft anerkannt wird. Dieser Mehraufwand wurde auch durch eine von der Wirtschaftsprüfungsgesellschaft KPMG durchgeführte Studie belegt, die unter BITKOM-Beteiligung entstanden ist. Entsprechendes gilt für das Design sowie die Skalierung der Nutzer- und Teilnehmerkommunikationsprozesse und auch für die Anforderungen aus §8a.

2.3 Rolle des BSI

Dem BSI kommt eine Vielzahl von Aufgaben zu, die für die IT-Sicherheit von Staat, Unternehmen und Bürgern von besonderer Bedeutung sind. Beispielsweise seien hier auch die präventiven Aufgaben genannt, die mehr Bewusstsein für IT-Sicherheit schaffen sollen. Die von BITKOM und BSI gemeinsam gegründete Allianz für Cybersicherheit leistet hier einen wichtigen Beitrag.

Gleichzeitig nimmt das Ausmaß und die Qualität der Angriffe auf die IT-Sicherheit insgesamt zu, sodass die Wirtschaft hier einen starken Partner braucht, der sowohl über die entsprechende Expertise von Fachpersonal, als auch über die nötigen finanziellen und personellen Ressourcen verfügen muss. Entgegen der auf Seite 2 als Ziel des IT-Sicherheitsgesetzes beschriebenen Stärkung des BSI, der Ankündigungen aus der Digitalen Agenda und abweichend von Formulierungen aus dem vorherigen Referentenentwurf, findet sich im aktuellen Entwurf das politische Versprechen einer Stärkung des BSI faktisch nicht (mehr) wieder.
Diese Situation ist mit Blick auf die aktuellen Herausforderungen und die zukünftige Aufgabe, die dem BSI auch durch das IT-Sicherheitsgesetz zukommen soll, nicht tragbar. BITKOM fordert hier eine Nachbesserung hinsichtlich der personellen, finanziellen Ressourcen sowie der nötigen Expertise von Fachpersonal, die das BSI samt Nationalem Cyberabwehrzentrum auch langfristig zu einem wirkungsvollen Partner für den Staat, die Wirtschaft und den Bürger werden lässt.

Als Verband nehmen wir positiv zur Kenntnis, dass die Rolle des BSI nicht in der einer bloßen Aufsichtsbehörde besteht, sondern der Gesetzesentwurf weiterhin Raum für eine partnerschaftliche Zusammenarbeit lässt. Der Entwurf lässt allerdings die Frage unbeantwortet, in welchem Verhältnis die Tätigkeit des BSI zu der Tätigkeit der bestehenden Aufsichtsbehörden, vor allem der Datenschutzaufsichtsbehörden, stehen soll. Dabei darf die Rolle des BSI als „Rückkanal“ bekannt gewordener Gefahren nicht aus den Augen verloren werden: BITKOM

erwartet hier eine aktive Position des BSI zur Warnung vor Sicherheitsvorfällen auf Basis des Lagebildes.

2.4 Nachhaltiger Ausfall

Auf Seite 2 des Referentenentwurfes sollen Betreiber Kritischer Infrastrukturen wegen der *„gesellschaftlichen Folgen, die ein nachhaltiger Ausfall oder eine betriebskritische Beeinträchtigung ihrer Infrastrukturen nach sich ziehen kann“*, stärker zur Verantwortung gezogen werden.

Um hier Klarheit und Erwartungssicherheit für die Unternehmen zu schaffen, ist der Begriff „nachhaltiger Ausfall“ konkret zu definieren. Diese Definition wird über einen kurzzeitigen Ausfall hinausgehen müssen, denn ein kurzer Ausfall gefährdet die Grundversorgung der Gesellschaft nicht. Entgegen dem ursprünglichen Ansatz würde es nach aktueller Fassung des Gesetzentwurfes genügen, dass durch eine Beeinträchtigung auch nur eines Teils einer Kritischen Infrastruktur eine Gefährdung der Grundversorgung der Gesellschaft zu bejahen wäre. Vor diesem Hintergrund ist nicht absehbar, auf welche Bestandteile von Infrastrukturen das Gesetz Anwendung findet, und welche Bestandteile von Infrastrukturen von der Geltung des Gesetzes ausgenommen sind. Dafür ist aus BITKOM-Sicht dringend Klarheit zu schaffen.

2.5 Konformität mit NIS-Richtlinie sicherstellen

Bei der Bewertung des vorliegenden Gesetzesentwurfes ergeben sich eine Vielzahl von Fragestellungen hinsichtlich des Zusammenwirkens des nationalen IT-Sicherheitsgesetzes und der NIS-Richtlinie auf europäischer Ebene. Da die NIS-Richtlinie zwar weit gereift, aber noch nicht beschlossen wurde, ist eine abschließende Bewertung des Zusammenwirkens nicht möglich. Umso mehr ist aus BITKOM-Sicht eine kritische Betrachtung der Anwendungsbereiche des IT-Sicherheitsgesetzes im europäischen Kontext nötig. Die sich daraus ergebenen Rechtsunsicherheiten haben Auswirkungen auf den wirtschaftlichen Betrieb. Darüber hinaus ergeben sich aus den Interpretationsfreiheiten bei der Umsetzung der NIS-Richtlinie wettbewerbliche Bedenken, die durch die Kosten für hohe IT-Sicherheitsstandards den betroffenen Unternehmen im internationalen Umfeld zum Nachteil werden können.

3 Artikel 1 – Änderung des BSI-Gesetzes

3.1 Begriffsdefinition der Kritischen Infrastrukturen

In Artikel 1, Absatz 3 des Gesetzentwurfs wird versucht, eine genauere Begriffsbestimmung der „Kritischen Infrastrukturen“ vorzunehmen.
Es wird seitens BITKOM als notwendig erachtet, dass der sachliche Anwendungsbereich bereits im Gesetz wesentlich konkreter ausgeführt wird. Dazu erscheint es geboten, in Artikel 1 bzw. der Begründung dazu konkrete Kriterien zu benennen, nach denen die Teilsegmente der aufgezählten Sektoren als kritisch eingestuft werden. Die Beschreibung im aktuell vorliegenden Gesetzesentwurf ist dafür nicht ausreichend konkret. BITKOM unterbreitet zur Konkretisierung deshalb folgende Begriffsdefinition:

1) Eine Kritische Infrastruktur betreiben diejenigen gewerblichen und nichtgewerblichen, öffentlichen und nicht-öffentlichen Einrichtungen, welche un-

abhängig von ihrer Rechtsform entgeltliche oder unentgeltliche Leistungen erbringen, die für den Bestand der freiheitlichen, ökonomischen, ökologischen und sozialen Ordnung derart grundlegend sind, dass eine, auch nur kurzfristige, Einschränkung ihrer Verfügbarkeit deshalb zu einer erheblichen Gefahr für die öffentliche Sicherheit für die Versorgung der Allgemeinheit oder schützenswerte Teile davon mit lebenswichtigen Gütern, Leistungen und Informationen für die Allgemeinheit führen kann, weil die jeweilige Leistung jederzeit verfügbar sein muss und anderweitig, d.h. außerhalb der Kritischen Infrastruktur nicht erbracht werden kann. Dazu muss insbesondere der Betreiber von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung nachhaltig wirkende Versorgungsengpässe oder erhebliche Gefährdungen für die öffentliche Sicherheit eintreten würden.

2) Als Betreiber Kritischer Infrastrukturen ist eine Stelle nur dann nach dem Gesetz verpflichtet, wenn sie allein oder als Teil einer Gesamtheit von verpflichteten Stellen einen maßgeblichen Anteil an der Verfügbarkeit der jeweiligen Kritischen Infrastruktur hat.
3) Die Regelungen zur Sicherheit informationsverarbeitender Systeme finden auf verpflichtete Stellen nur insoweit Anwendung, als die verpflichteten Stellen informationsverarbeitende Systeme, einschließlich ihrer Komponenten, zum Zwecke der Unterhaltung von solchen Verfahren betreiben oder in ihrem Auftrage betreiben lassen, welche unmittelbar dem Betrieb und der Verfügbarkeit der Kritischen Infrastruktur dienen.

In diesem Zusammenhang ist zu kritisieren, dass das BMI die Möglichkeit haben soll, verpflichtete Unternehmen in einer Rechtsverordnung zu bestimmen. Dies begegnet nach BITKOM-Einschätzung verfassungsrechtlichen Bedenken, weil der Adressat bereits hinreichend konkret im Gesetz bestimmt werden muss. Es schadet der Rechtssicherheit und trifft auch auf wettbewerbsrechtliche Bedenken. Denn der Verordnungsermächtigung im Gesetzentwurf fehlt es an ausreichender Bestimmtheit, Normklarheit bei der Adressatenbestimmung und an der notwendigen Begrenzung der Ermächtigung. Diese Bedenken sind durch den neuen Gesetzesentwurf noch verstärkt worden. Darüber hinaus besteht ein erhebliches Risiko für die Investitionssicherheit und nimmt den Unternehmen das nötige Maß an Erwartungssicherheit.

Eine Konsultation mit Branchenvertretern zur Bestimmung der wesentlichen kritischen Infrastrukturen bzw. des Adressatenkreises des geplanten Gesetzes sollte bereits im Vorfeld einer gesetzlichen Regelung stattfinden.
Dieser in Artikel 1 angesprochene Gesetzesabschnitt lässt auch nicht die geografische Reichweite der KRITIS-Definition erkennen. BITKOM schlägt eine Konkretisierung vor, die den Unternehmen mehr Planungssicherheit gibt.

Im Rahmen des geplanten Gesetzes sollte auch berücksichtigt werden, dass sich durch den in internationalen Kooperationen gemeinschaftlich organisierten Betrieb Kritischer Infrastrukturen und in Fällen, in denen Teile Kritischer Infrastrukturen im Ausland liegen, relevante Risiken für die IT-Sicherheit in Deutschlands ergeben können. Dabei muss vermieden werden, dass die Verantwortlichkeiten für diese Risiken nicht ausschließlich beim in Deutschland ansässigen Kooperationspartner liegen, sondern im Sinne der wettbewerblichen Gleichstellung auch über die Landesgrenzen verteilt werden können. Die Verantwortlich-

keiten für den Betrieb Kritischer Infrastrukturen müssen in diesen Fällen gemeinschaftlich geregelt werden bzw. im IT-Sicherheitsgesetz eine gerechte Risikoverteilung berücksichtigt werden.

3.2 Rolle der Datenschutz-Aufsichtsbehörden

Der geplante § 7 Abs. 1 S. 1 Nr. 1 lit. c ist nicht ausreichend von § 42a BDSG abgegrenzt. Diese Vorschrift weist die Zuständigkeit für die Entgegennahme von Meldungen der in § 42a BDSG genannten Art den Datenschutz-Aufsichtsbehörden zu, und er macht nur in den dort genannten Fällen der verantwortlichen Stelle eine Meldung zur Pflicht. Die Meldepflicht und die Veröffentlichungspflicht in § 7 neu scheinen über § 42a BDSG hinauszugehen, und es ist nicht klar, ob eine Meldung allein an die Datenschutz-Aufsichtsbehörden noch ausreicht oder auch in den Fällen des § 42a BDSG eine Meldung an das BSI erforderlich ist. Letzteres erscheint problematisch, da die Zuständigkeit der Datenschutz-Aufsichtsbehörden für die in § 42a BDSG genannten Fälle ausreicht und nicht verunklart werden soll.

3.3 Untersuchung der Sicherheit in der Informationstechnik

In Artikel 1, Absatz 7 des Gesetzentwurfs heißt es:

„(1) Das Bundesamt darf zur Erfüllung seiner Aufgaben auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte, Systeme und Dienste untersuchen. Es darf sich hierbei der Unterstützung Dritter bedienen.
(2) Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Förderung der IT-Sicherheit genutzt werden.
(3) Das Bundesamt darf seine Bewertung der Sicherheit der untersuchten informationstechnischen Produkte, Systeme und Dienste weitergeben und veröffentlichen.“

BITKOM hat Bedenken gegen den § 7a und gegen dessen Einführung wir uns in der jetzigen Beschaffenheit aus folgenden Gründen aussprechen: Die hier gesetzlich verankerte Testkompetenz, die ohne jegliche Einschränkung (etwa auf kritische Infrastrukturen) gelten soll und sogar Produkte umfasst, die noch nicht am Markt verfügbar sind, sieht die BITKOM-Branche kritisch. Eine solche Befugnis steht im Widerspruch zu geltendem Urheber-, Straf- und Kartellrecht in Deutschland. Die Zusammenführung dieser Testergebnisse zusammen mit den Ergebnissen aus den Prüfaudits (§ 8a, Abs.3) an einer zentralen Stelle birgt ein unabschätzbares Sicherheitsrisiko für Angriffe.
Insbesondere kann die Befugnis zur Weitergabe und Veröffentlichung der Informationen ohne angemessene Barrieren und Kontrollen zu einem neuen Sicherheitsrisiko führen oder zu einem erheblichen Reputationsschaden, damit auch wirtschaftlichen Schaden für die betroffenen Unternehmen und ihre Produkte. Daher sollte die Testkompetenz an präzise definierte Voraussetzungen und Verfahrensregeln geknüpft sein. Ebenso sollte klar geregelt sein, wie und zu welchem Zweck die Testergebnisse durch wen verwendet werden dürfen. Die Rechte der Hersteller müssen hierbei gewahrt bleiben. Hier sollte die vorherige Zustimmung des Herstellers verpflichtend sein. Zur Ausgestaltung des Gesetzestextes schlagen wir in diesem Sinne folgende Kriterien vor, die Berücksichtigung finden sollen:

- Es muss nachweislich begründete Zweifel an dem Vorliegen der sicherheitsrelevanten Eigenschaften des Produktes geben
- Es muss sich um bestehende Produkte handeln
- Es werden (nur) Labortests durchgeführt - dementsprechend ist die Befugnis in Bezug auf „Systeme und Dienste“ zu streichen und auf „Produkte“ zu beschränken, da nur diese Labortests zugänglich sind.
- Alle Tests und Testverfahren und alle dabei erlangten Informationen müssen für den Hersteller transparent sein und vertraulich behandelt werden.
- Erkenntnisse aus Tests sollen nur zur anwendungsspezifischen Produktbewertung (in Abhängigkeit vom Einsatzszenario) des Herstellers genutzt werden
- Bestehende, internationale Prüfkriterien und Zertifizierungen dürfen nicht durch die BSI-Bewertung geschwächt werden.

Weiterhin schlagen wir ergänzend zu (1) folgende Klarstellung vor: „Geschäfts und Betriebsgeheimnisse der betroffenen Unternehmen dürfen hierzu nicht herangezogen werden.“

Auch die in § 7a Abs. 2 neu vorgesehene Zweckbindung für bei Untersuchungen gewonnenen Ergebnisse reicht nicht aus. Vielmehr ist es erforderlich, wie in § 42a S. 6 BDSG für die dortigen Pflichtmeldungen bereits geregelt, auch für alle dem BSI gemeldeten Vorfälle eine Regelung aufzunehmen, die eine Verwertung der hieraus gewonnenen Erkenntnisse und der Meldung selbst in Straf- und Ordnungswidrigkeitenverfahren ohne Zustimmung der meldenden Stelle ausschließt.

Artikel (2) bedarf einer Konkretisierung hinsichtlich seiner Zielsetzung (Zweckbestimmung).

3.4 Weitergabe der Ergebnisse eines Sicherheitsaudit

In Artikel 1, Absatz 8 des Gesetzentwurfs heißt es:

„Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel.“

Eine detaillierte Systemkenntnis des BSI ist aus BITKOM-Sicht nicht erforderlich. Wichtiger nach dem Sinn des Gesetzes ist eine Kenntnis von Bedrohungstendenzen. Andernfalls würde über die Audit-Verpflichtung eine Notifikations-Verpflichtung „durch die Hintertür“ eingeführt. Daher ist eine Meldung über die gemeinsame Ansprechstelle ohne Nennung des Betreibers vorzusehen und der Berichtszeitraum auf zwei Jahre anzupassen.

Weiterhin bekommt das BSI folgende Erlaubnis: *„Bei Sicherheitsmängeln kann das Bundesamt die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse (…) verlangen.“*

Eine gesetzliche Verpflichtung zur Detailmeldung der Ergebnisse an das BSI wird von BITKOM als bedenklich erachtet. Das Recht, über die detaillierten Informationen eines Audits oder einer Überprüfung verfügen zu dürfen, sollte prinzipiell ausschließlich dem Betreiber obliegen. Es liegt bereits im Eigeninteresse des Betreibers, diese Informationen zu nutzen, um adäquat auf festgestellte Mängel reagieren zu können und aufgedeckte Sicherheitsmängel schnellstmöglich zu beseitigten. Detaillierte Informationen zu festgestellten Sicherheitsmängeln sollten zudem bereits aus Sicherheitsgründen beim Betreiber verbleiben. Außerdem sollte der Passus nur beim Fortbestehen von Sicherheitsmängeln über einen längeren Zeitraum hinaus relevant werden.

Deshalb schlägt BITKOM folgende Änderung des Gesetzestextes vor: „Bei erheblichen Sicherheitsmängeln, die mit hoher Wahrscheinlichkeit zu einem nachhaltigen Ausfall oder einer betriebskritischen Beeinträchtigung führen werden und im Zeitpunkt der Meldung noch fortbestehen, kann das Bundesamt die Übermittlung der wesentlichen Audit-, Prüfungs- oder Zertifizierungsergebnisse und, soweit erforderlich, im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde, die Beseitigung der Sicherheitsmängel verlangen. Ein Anspruch auf Übermittlung von Geschäftsgeheimnissen besteht nicht."

3.5 Meldepflichtige Ereignisse

In den Erläuterungen zu § 8b (Zentrale Stelle für die Sicherheit in der Informationstechnik der Betreiber Kritischer Infrastrukturen, Seite 40) wird erstmals versucht, meldepflichtige Ereignisse zu definieren:

„Eine Störung im Sinne des BSI-Gesetzes liegt daher vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken. Dazu zählen insbesondere Fälle von Sicherheitslücken, Schadprogrammen und erfolgten, versuchten oder erfolgreich abgewehrten Angriffen auf die Sicherheit in der Informationstechnik sowie außergewöhnliche und unerwartete technische Defekte mit IT-Bezug (z.B. nach Softwareupdates oder ein Ausfall der Serverkühlung). Die Störungen sind dann meldepflichtig, wenn sie bedeutend sind. Eine bedeutende Störung liegt vor, wenn die Funktionsfähigkeit des Betreibers oder die von diesem betriebene Kritische Infrastruktur bedroht sind."

Gemäß dieser Definition liegt bereits dann eine Störung vor, wenn nur versucht wurde, auf die Technik einzuwirken. Ebenso soll eine Störung bereits dann als bedeutend gelten, wenn die Funktionsfähigkeit der Technik nur bedroht wurde. Im Zweifel bedeutet dies eine umfassende, unverzügliche Meldeverpflichtung für jegliche Störungen.
Um Rechtsunsicherheit zu vermeiden, ist hier eine einschränkende Konkretisierung aus BITKOM-Sicht dringend geboten.

In Artikel 1, Absatz 8, 4 (Seite 11) des Gesetzentwurfs heißt es:

„(4) Betreiber Kritischer Infrastrukturen haben bedeutende Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der von ihnen betriebenen Kritischen Infra-

strukturen führen können, über die Kontaktstelle unverzüglich an das Bundesamt zu melden."

Aus BITKOM-Sicht ist eine Meldung über jede Störung, die zu einer „Beeinträchtigung führen könnte" nicht zielführend. Diese Art von Meldungen wäre unangemessen und würde den Blick für das Wesentliche verstellen. Darüber hinaus führt sie in der Umsetzung zu praktischen Problemen, da für den IT-Verantwortlichen nicht in jedem Fall absehbar ist, ob durch ein Vorkommnis eine Beeinträchtigung entstehen könnte. Wir schlagen deshalb eine Änderung wie folgt vor:

„(4) Betreiber Kritischer Infrastrukturen haben bedeutende Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die mit hoher Wahrscheinlichkeit zu einem nachhaltigen Ausfall oder einer betriebskritischen Beeinträchtigung der von ihnen betriebenen Kritischen Infrastrukturen führen werden, über die Kontaktstelle an das Bundesamt zu melden. (…) Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem nachhaltigen Ausfall oder einer betriebskritischen Beeinträchtigung der Kritischen Infrastruktur geführt hat. Ein Anspruch auf Übermittlung von Geschäftsgeheimnissen besteht nicht."

3.6 Festlegung in Rechtsverordnung gerichtlich prüfen

In Artikel 1, Absatz 9 des Gesetzentwurfs sollte folgende Formulierung ergänzt werden:

„Gegen die Festlegungen in der Rechtsverordnung für bestimmte Kritische Infrastrukturen ist für von diesen Festlegungen betroffene Betreiber der Rechtsweg vor die Verwaltungsgerichte eröffnet."

Die Regelung „Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt" geht dann zu weit, wenn sie, wie es der Wortlaut zeigt, auch auf Verwaltungsverfahren angewendet werden würde, in denen betroffene Betreiber gegen die in der Rechtsverordnung getroffene Festlegung Rechtsschutz suchen. Richtiger ist daher eine Regelung

„Für den Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, gilt § 8d Abs. 2 entsprechend."

Die Rechtsverordnung kann nach Anhörung der betroffenen Betreiber erlassen werden. Diese ist eine unzureichende rechtliche Überprüfung, da es dem BMI frei steht, über die Ansichten der Betreiber im Anhörungsprozess hinweg zu gehen, ohne dass eine gerichtliche Überprüfung der Festlegung erfolgen kann. Es besteht zudem das Risiko ständiger Änderungen und dadurch mangelhafter Investitionssicherheit.

4 Artikel 2 – Änderung des Telemediengesetzes

4.1 Erhebung von Nutzungsdaten

Nach Artikel 2, Absatz 2 des Gesetzentwurfs soll folgender Passus in das Telemediengesetz eingefügt werden:

„(9) Soweit erforderlich, darf der Diensteanbieter Nutzungsdaten zum [Erkennen,] Eingrenzen und Beseitigen von Störungen sowie von Missbrauch seiner für Zwecke seines Telemedienangebotes genutzten technischen Einrichtungen erheben und verwenden.“

Um die Prävention oder auch die Erkennung von missbräuchlicher Nutzung oder von IT-Angriffen überwachen und erkennen zu können, ist es nötig, dass „Erkennen“ in den Absatz mit einbezogen wird und die Klammern entfernt werden. Für den sicheren Betrieb von IT-Systemen ist es obligatorisch diese zu überwachen und deren Leistungs- und Nutzungsdaten zu protokollieren. Protokolldaten sind für absolut unerlässlich für die (teil-)automatisierte und manuelle Überwachung der Sicherheit der IT. Deshalb ist an dieser Stelle ist eine Gleichstellung TMG und TKG erforderlich.

BITKOM versteht den vorliegenden Entwurf nicht als Mittel zur Einführung der Vorratsdatenspeicherung. Deshalb bitten wir dringend um Klarstellung, dass diese gespeicherten Daten nicht zu Zwecken der Strafverfolgung eingesetzt werden.

4.2 Erweiterung des Adressatenkreises in § 13 Abs. 7 TMG

Gegenüber der bisherigen Fassung werden nun faktisch alle Diensteanbieter gemäß TMG verpflichtet. Ausgenommen sind nur reine Speicherplatzanbieter (§ 10 Abs. 1 TMG). Betroffen sind also Content-Provider (§ 7 Abs. 1 TMG), Access-Provider und Network-Provider (§ 8 Abs. 1 TMG) sowie reine Caching-Dienstleister(§ 9 Abs. 1 TMG). Für diese Ausweitung des Adressatenkreises ist keinerlei Begründung dargestellt. Es erscheint auch inhaltlich fraglich, ob diese Ausweitung des Adressatenkreises sachlich geboten ist.

4.3 Verschärfung der Pflichten der Adressaten

Die Adressaten sollen nun zur „Sicherstellung“ verpflichtet werden, dass kein unerlaubter Zugriff „möglich“ ist. Das bedeutet eine Garantie für absolute Sicherheit. Diese Verpflichtung ist objektiv nicht erfüllbar, denn absolute Sicherheit kann es nicht geben.

Überdies ist nicht ersichtlich, weshalb hier eine „Zusicherung“ – also eine Garantie – durch jeglichen Diensteanbieter als gesetzliche Pflicht geboten und erforderlich sein soll. Eine solche Garantie könnte zudem zivilrechtlich als „Schutzgesetz“ ausgelegt werden. Dann könnte ein Verstoß den Diensteanbieter zum Schadensersatz gegenüber seinen Kunden verpflichten, selbst wenn ihn keinerlei Verschulden trifft. Das ist wohl seitens des Gesetzgebers nicht gewollt und wird seitens BITKOM strikt abgelehnt.

Es ist nicht ersichtlich, weshalb für beliebige Webangebote ein höherer Sicherheitsstandard gelten soll als für den Schutz auch sensibelster personenbezogener Daten nach BDSG. Es ist auch nicht ersichtlich, weshalb eine verschuldensunabhängige Verpflichtung des Diensteanbieters bestehen sollte. Die Regelungen des BDSG (dort Verpflichtung zur Datensicherheit nach § 9 BDSG) werden seit Jahrzehnten allgemein anerkannt. Insoweit können allenfalls Vollzugsdefizite bestehen.

Daneben besteht nach dem Regelungsvorschlag – anders als seit vielen Jahren im BDSG bewährt – keinerlei Zusammenhang zwischen den Risiken und den zur Risikovermeidung angemessenen Aufwänden. Die Regelung erscheint auch daher als unangemessen. Selbst kleinste Diensteanbieter (z.B. die reine Image-Homepage des „Kaninchenzüchter-Vereins“) würden über ein so geändertes

TMG zu umfassender Sicherheitsmaßnahmen verpflichtet und müssten absolute Sicherheit garantieren.
Hinsichtlich der Informationspflicht über die Erhebung und Verwendung der Nutzungsdaten nach §15 Abs. 9 nF TMG sollte im Gesetzeswortlaut klargestellt werden, dass ein Hinweis in den AGB- oder Datenschutzbestimmungen ausreichend ist, da diese Informationspflicht sonst zu einem unzumutbaren Aufwand für den betroffenen Telemedienanbieter führen würde.

4.4 Bußgeldandrohung für Verstöße gegen § 3 Abs. 7 S. 1 TMG

Mit dieser Änderung werden Verstöße gegen die nun geschaffene und praktisch nicht durchführbare „Zusicherung absoluter Sicherheit“ (siehe oben Ziffer 4.3) nun durch Bußgeld von bis zu 50.000 Euro bedroht.
Die Bußgeldandrohung besteht völlig unabhängig davon, ob und inwieweit der Verstoß gegen die „Zusicherung absoluter Sicherheit“ einen Einfluss auf tatsächlich bestehende, konkrete Risiken hat oder tatsächlich zu irgendwelchen Folgen geführt hat. Schon dies erscheint als unangemessen.
Daneben gelten die Aspekte der Unangemessenheit gemäß § 13 Abs. 7 TMG (neu) erst recht für die Bußgeldandrohung.

5 Artikel 3 – Änderung des Telekommunikationsgesetzes

5.1 Konkretisierung der IT-Schutzziele

BITKOM begrüßt die in Artikel 3, Abs. 2 vorgesehene Erweiterung des § 100 Abs. 1 TKG zur Nutzung von Daten für die genannten Zwecke. Sie trägt wesentlich zur Effizienz und Effektivität der Gefahrenabwehr bei. Zusätzlich schlagen wir vor, dass auch die weiteren Schutzziele der Informationssicherheit in § 100 Abs. 1 TKG wie folgt Aufnahme finden:

„…Störungen, die zu einer Einschränkung der Verfügbarkeit, Integrität oder Vertraulichkeit von Informations- und Kommunikationsdiensten oder zu einem …“

Hiermit werden insbesondere auch konkrete Fälle von Sicherheitsverletzungen, z.B. Hacking / APTs, besser erfasst.

5.2 Konkretisierung der Speicherdauer

Zudem geht es in Artikel 3, Absatz 2 um die Konkretisierung der Speicherdauer. Anbietern wird gemäß TKG das Recht eingeräumt, zum Erkennen, Eingrenzen oder Beseitigen von Störungen bzw. zum Erkennen und Beseitigen von Schadprogrammen und entsprechender Infrastruktur, bzw. Bestands- und Verkehrsdaten zu verwenden, folglich diese auch zu speichern.

Eine Konkretisierung der rechtlich zulässigen Dauer dieser Gestattung wird hingegen – anders als unter § 15 Abs. 9 TMG-neu – nicht vorgenommen. Eine solche Klarstellung könnte zumindest in der Gesetzesbegründung vorgenommen werden, um den Anbietern Rechtssicherheit gegenüber Dritten zu garantieren.

5.3 Einheitliche Legaldefinition von „Störung“

Innerhalb des §15 Abs. 9 TMG einerseits und §100 Abs. 1 TKG sowie des BSI-Gesetzes andererseits kommen unterschiedlich detaillierte Störungsbegriffe vor.

Zugunsten von Rechtsklarheit und Rechtssicherheit regt BITKOM an, diese Störungsbegriffe zu vereinheitlichen.

5.4 Informationen zur Identifikation von Störungen

Insbesondere dann, wenn es um die Erkennung von Störungen in Form von Angriffen auf Nutzerendgeräte oder auf TK-Infrastrukturen geht, werden diese Störungen anhand von Mustern erkannt („Pattern“). Diese Pattern setzen sich jedoch ggf. nicht nur aus Bestands- oder Verkehrsdaten zusammen, sondern insbesondere im IP-Verkehr auch aus Protokollinformationen höherer Protokollebenen, die von den Aufsichtsbehörden nicht mehr als Verkehrsdaten, sondern ausschließlich als Inhaltsdaten angesehen werden, die dem exklusiven Schutz des Fernmeldegeheimnisses nach § 88 TKG unterliegen. Wichtig ist es daher, in die Gesetzesbegründung aufzunehmen, dass mit der Erweiterung des Pflichtenkreises des TK-Anbieters und den in § 100 Abs. 1 TKG definierten Rechten bzw. Pflichten in diesem Lichte auch eine erweiterte Auslegung des in § 88 Abs. 3 TKG definierten Begriffs der *geschäftsmäßigen Erbringung von Telekommunikationsdiensten* zu erfolgen hat. Damit würde anerkannt, dass dem Fernmeldegeheimnis unterliegende Informationen zum Erkennen und Beseitigen von Angriffen genutzt werden können, auch wenn es sich bei diesen Daten nicht um Verkehrsdaten im engen Sinne handelt. Andernfalls werden sich die TK-Anbieter schwer tun, diesen Pflichten rechtssicher nachzukommen.

5.5 Senkung der Meldeschwelle in § 109 Abs. 5 TKG

Kritisch anzumerken ist, dass die Meldeschwelle bei Sicherheitsverstößen in § 109 Abs. 5 TKG in dreierlei Weise spürbar gesenkt wird.

- Einerseits werden bereits (simple) „Störungen, die zu einer Einschränkung der Verfügbarkeit“ führen können, als eine Ausprägung der „beträchtlichen Sicherheitsverletzung“ verstanden. Hierbei wird übersehen, dass sich geringfügige Verfügbarkeitsbeeinträchtigungen innerhalb von TK-Netzen generell nicht ausschließen lassen, weshalb seit Jahren entsprechende Klauseln in den Allgemeinen Geschäftsbedingungen üblich und von den Gerichten auch bestätigt sind. Es sollte insbesondere sichergestellt werden, dass wartungsbedingte Störungen der Verfügbarkeit, die nicht über das übliche Maß hinausgehen, nicht einen Meldetatbestand auslösen, da Wartungsarbeiten der Systemerhaltung dienen und nahezu täglich routinemäßig stattfinden müssen. Diese bergen stets das abstrakte Risiko einer Einschränkung der Verfügbarkeit.

- Andererseits erscheint es unverhältnismäßig, dass auch solche Fälle darunter fallen sollen, bei denen sich eine Störung noch gar nicht verwirklicht hat („können“). Da der tatsächliche Verlauf eines Vorfalls zu Beginn gar nicht sicher prognostiziert werden kann, müsste ggf. aus Compliance-Gründen eine Meldung in jedem Fall erfolgen.

- Schließlich sollte im Vergleich mit der Entwurfsfassung vom August 2014 der gestrichene Passus „von denen der Netzbetreiber oder der Telekommunikationsdiensteanbieter Kenntnis erlangt“ wieder ergänzt werden, um den Unternehmen Handlungssicherheit zu geben und die Meldegrenze anwendbarer festzulegen.

Durch sämtliche Faktoren würde die Meldeschwelle substanziell sinken und damit die Anzahl meldepflichtiger Vorfälle deutlich erhöht.
Daher bleibt festzuhalten, dass entgegen der Gesetzesbegründung in jedem Fall Mehrkosten anfallen, und nicht nur dann, wenn bisher keine Meldewege existieren. Soweit die Schwelle für eine Meldepflicht entsprechend niedrig gelegt wird, steigt die Anzahl der meldepflichtigen Vorgänge automatisch und damit die Notwendigkeit, diese durch personellen und organisatorischen Einsatz zu verarbeiten, bewerten und zu administrieren. Im Übrigen sind dies Ressourcen, die dann ggf. nicht für die Schließung der potenziellen Sicherheitslücke zur Verfügung stehen. In gleichem Maße dürfte der Aufwand seitens der BNetzA bzw. BSI für die Administration der deutlich höheren Zahl von Meldefällen spürbar steigen.

5.6 Anonyme Übermittlung von Meldungen

Artikel 3 Absatz 3 des Gesetzentwurfs zu § 109 Abs. 8 TKG verpflichtet die Bundesnetzagentur zur unverzüglichen Unterrichtung des BSI über die im Rahmen von Audits aufgedeckten IT-Sicherheitsmängel sowie die in diesem Zusammenhang von der BNetzA geforderten Abhilfemaßnahmen.
Hier gilt es, die in Artikel 1 eingeräumte Möglichkeit der anonymen Übermittlung aufzugreifen. Die BNetzA darf die vertraulich und anonym übermittelten Informationen ihrerseits lediglich in anonymer Form weiterreichen.
Darüber hinaus sollte ein Mechanismus geschaffen werden, der es ermöglicht, anonyme Meldungen abzugeben (ggf. durch gesicherte, anonyme Web-Formulare). Eine anonyme Meldung darf nicht mit erhöhten Kosten oder Aufwand bei den Unternehmen verbunden sein, da mit einer solchen Erschwerung das Recht einer anonymen Meldung faktisch entwertet würde.

5.7 Definition der Rechtsbegriffe

Angesichts der weitreichenden Rechtsfolgen des § 115 erscheinen die Rechtsbegriffe der „organisatorischen Struktur“ und „aus rechtlichen Gründen“ zu unbestimmt, um das gewünschte Ziel der Norm (die erhöhte Sicherheit) diskriminierungsfrei zu erreichen.