Stellungnahme

zum Entwurf eines Gesetzes zur Umsetzung der NIS-Richtlinie (EU) 2016/1148

16. Dezember 2016

Bitkom vertritt mehr als 2.400 Unternehmen der digitalen Wirtschaft, davon gut 1.600 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlands-umsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 300 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. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

1. Einleitung und Hintergrund

Am 8. August 2016 trat die Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (ABl. L 194 vom 19. Juli 2016, S. 1; sog. NIS-RL) in Kraft. Mit der Richtlinie wurden ein einheitlicher europäischer Rechtsrahmen für den EU-weiten Aufbau nationaler Kapazitäten für die Cyber-Sicherheit, eine stärkere Zusammenarbeit der Mitgliedstaaten und Mindestanforderungen sowie Meldepflichten für bestimmte Dienste geschaffen. Ziel ist es, einheitliche Maßnahmen festzulegen, mit denen ein hohes Sicherheitsniveau von Netz- und Informationssystemen in der Europäischen Union erreicht werden soll (Artikel 1 Absatz 1 der Richtlinie (EU) 2016/1148). Die Richtlinie ist gemäß Artikel 25 Absatz 1 bis zum 9. Mai 2018 in nationales Recht umzusetzen.

Das Bundesministerium des Innern hat am 9. Dezember 2016 den vorliegenden Referentenentwurf des Gesetzes zukommen lassen, mit dem expliziten Hinweis, dass dieser noch nicht innerhalb der Bundesregierung abgestimmt ist. Die Kommentierungsfrist endet am 16. Dezember 2016. Bitkom nimmt gerne die Gelegenheit wahr, seine Position zum Referentenentwurf nachfolgend darzustellen.

Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Marc Fliehe, CISSP
Bereichsleiter Information Security
T +49 30 27576-242
m.fliehe@bitkom.org

Cornelius Kopke
Bereichsleiter Öffentliche Sicherheit & Wirtschaftsschutz
T +49 30 27576-203
c.kopke@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Thorsten Dirks

Hauptgeschäftsführer
Dr. Bernhard Rohleder

2. Grundsätzliche Anmerkungen zum Referentenentwurf

Bitkom begrüßt daher ausdrücklich die weltweite Debatte um die Verbesserung der Cybersicherheit und kann auch die Intention des Gesetzgebers nachvollziehen, hier eine zeitnahe Umsetzung der Richtlinie in nationales Recht zu forcieren. Ausdrücklich begrüßen wir auch, die – vom Prozess her – sehr frühe Einbindung der Wirtschaft zur regulatorischen Umsetzung der NIS-Richtlinie.

In Anbetracht der ausgesprochen kurzen Kommentierungsfrist ist uns – und vielen der von Bitkom vertretenen Unternehmen – nur eine kursorische Prüfung des Referentenentwurfes möglich gewesen. Es kann nicht davon ausgegangen werden, dass innerhalb von zwei Werktagen eine sach- und interessengerechte Beurteilung des Gesetzesentwurfs unter Einbeziehung der einschlägigen Gremien in den Verbänden möglich ist. Eine angemessene Meinungsbildung in den Verbänden benötigt bei allem nachvollziehbaren politischen Druck ein gewisses Maß an Raum und Zeit für die Auseinandersetzung, Abstimmung und Kommunikation. Damit Anhörungen fundiert vorbereitet und in den Verbänden Branchenmeinungen herbeigeführt werden können, sind entsprechende Kommentierungsfristen einzuräumen. Diese sollten sich am Umfang und der Reichweite der gesetzgeberischen Maßnahmen bemessen. Eine nachträgliche Konkretisierung der hier diskutierten Aspekte behalten wir uns deshalb vor.

Wünschenswert ist über die Möglichkeit der Kommentierung dieses vorliegenden – innerhalb der Bundesregierung noch nicht final abgestimmten – Entwurfes auch eine Kommentierungsmöglichkeit zum finalen Entwurf, bei dem sich noch für die Wirtschaft relevante und signifikante Änderungen gegenüber der hier vorliegenden Version ergeben könnten. Für uns als Bitkom ist es von Bedeutung, insbesondere diese Abweichungen sensibel nachzuverfolgen.

Von besonderer Bedeutung bei der Umsetzung der NIS-Richtlinie ist insbesondere die Frage nach dem Erfüllungsaufwand für die Wirtschaft. Aufgrund der noch nicht vorliegenden Durchführungsrechtsakte der EU-Kommission kann eine konkrete Aufwandsschätzung für die Erfüllung der Verpflichtungen jedoch noch nicht abschließend vorgenommen werden. Überschlägt man den mit der Umsetzung einer Meldung verbundenen Aufwand an Ressourcen und Personal, dürfte der Kostenpunkt von 660 Euro pro Meldung (S. 3, 22 ff. des Entwurfs), aus Sicht einiger Unternehmen, jedoch eher niedrig bemessen sein.

3. Änderungen des Artikel 1 – BSI Gesetz

In Artikel 1 (Änderung des BSI-Gesetzes) zu § 8a Abs. 4 (n.F.) wird eine Unterstützung des BSI angesprochen: Das BSI kann sich bei Überprüfungen und Durchführung der Aufsicht der Hilfe qualifizierter Dritter ("einer qualifizierten Stelle") bedienen. Insbesondere, wenn dieses auch ohne das Einverständnis des Betroffenen geschehen kann, könnte dieses dazu führen, dass Geschäfts- und Firmengeheimnisse einem anderen Wirtschaftsunternehmen (angesichts der Enge des hier in Betracht kommenden Marktes wahrscheinlich ein Wettbewerber) offengelegt werden müssen. Abgesehen vom Schutzbedarf solcher Firmengeheimnisse, erscheint diese Konstellation auch wettbewerbsrechtlich nicht unbedenklich. Eine Konkretisierung des Begriffs „qualifizierte Stelle" sowie eine maßvolle Einschränkung der Befugnisse des BSI, die den vorgenannten Bedenken Rechnung trägt, wird für erforderlich gehalten und deshalb

angeregt. Insbesondere die Beleihung und der Umfang der Befugnisse des Beliehenen müssen hier ausdrücklich geregelt werden, weil sie wesentlich in die Rechte der Betroffenen eingreifen können.

Weiterhin wird in der Begründung zum Gesetzentwurf ausgeführt, die NIS-Richtlinie schreibe für nationale Aufsichtsbehörden die Möglichkeit solcher sog. „ex ante" Kontrollen verpflichtend vor. Tatsächlich wird diese Verpflichtung in der NIS-Richtlinie jedoch nicht konkret eingeführt. Artikel 15 der NIS-Richtlinie bestimmt laut der Gesetzesbegründung (Seite 38) lediglich, „die zuständige Behörde (muss) die Umsetzung der organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der informationstechnischen Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit Kritischer Infrastrukturen maßgeblich sind, überprüfen und von den Betreibern Kritischer Infrastrukturen verlangen können, dass sie die zur Bewertung der Sicherheit ihrer Netz- und Informationssysteme erforderlichen Informationen, einschließlich der dokumentierten Sicherheitsmaßnahmen, zur Verfügung stellen." Diese Anforderung aus der NIS−Richtlinie wird aber bereits mit den gegenwärtigen Bestimmungen des ITSiG erfüllt, wonach KRITIS Betreiber eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen (einschließlich der dabei aufgedeckten Sicherheitsmängel) vorlegen müssen, zumal es sich bei diesen nachzuweisenden Prüfungen um Standards handelt, die wiederum vom BSI anerkannt (und mithin geprüft) sein müssen.

Ferner sehen wir Handlungsbedarf in Hinblick auf die Umsetzung der Meldepflicht (§8b BSI-Gesetz): Durch die geänderte Gesetzgebung erhöht sich der Aufwand für die Meldung von Sicherheitsvorfällen qualitativ und quantitativ. Für die Verpflichteten und für die Empfänger einer Meldung ist eine eindeutige Festlegung der Meldekriterien notwendig, um die Voraussetzung für eine Meldeverpflichtung im Einzelfall prüfen zu können. Die bislang in den FAQ des BSI wohl unverbindlich gegebenen Hinweise zu den Meldekriterien greifen hier zu kurz. Insofern regen wir eine verbindliche Festlegung der Meldekriterien an. Dieses sollte mit den Betreibern im Vorfeld abgestimmt sein, um die Umsetzbarkeit sicherstellen zu können.

Des Weiteren sollen nach dem Referentenentwurf zukünftig „mögliche grenzübergreifende Auswirkungen" bei Störungen gemeldet werden (§8b Abs. 4). Dann sind Meldewege in den einzelnen relevanten Mitgliedsstaaten ggf. zu berücksichtigen, was zu mehrfachen Meldungen nach möglicherweise unterschiedlichen Kriterien führen würde. International agierende Konzerne betreiben meist Dienste in mehreren Staaten der EU, bieten Dienste aus verschiedenen Staaten für verschiedene Staaten an und beziehen Dienste aus verschiedenen Mitgliedsstaaten. Eine nicht harmonisierte Umsetzung der NIS-RL in den einzelnen EU-Mitgliedstaaten führt dann ggf. zu unterschiedlichen oder gar widersprüchlichen Umsetzungen der Anforderungen, die ggf. nicht realisierbar sind. Ein entsprechender Austausch zwecks Harmonisierung in den Mitgliedsstaaten ist wünschenswert.

Das in § 8c Abs. 2 (e) genannte Meldekriterium entspricht dem Meldekriterium in der NIS-Richtlinie. Allerdings ist eine Bewertung der Auswirkung des Vorfalls auf wirtschaftliche und gesellschaftliche Tätigkeiten für die Betreiber in aller Regel mangels entsprechender Informationen nicht durchführbar. Hier regen wir eine praxisnahe Ausgestaltung an.

3.1 Aufsichtsbefugnisse des BSI

Kritisch sehen wir die Anpassung der Aufsichtsbefugnisse des BSI. Im Gesetzentwurf werden zusätzliche, für KRITIS-Betreiber erhebliche Erfüllungsaufwände geschaffen werden, die einer substantiellen Beteiligung und Erörterung bedürfen. Konkret beziehen sich diese Bedenken auf die zusätzliche KRITIS Betreiberverpflichtung zur „Unterstützung des BSI bei der Prüfung der Erfüllung von Sicherheitsanforderungen“:

- Bislang müssen KRITIS-Betreiber dem BSI alle zwei Jahre eine Aufstellung ihrer durchgeführten Überprüfungen sowie festgestellte Mängel melden. Künftig müssen Betreiber demgegenüber sämtliche Ergebnisse dieser Überprüfungen melden.
- Das BSI kann dann zudem die Vorlage der gesamten Dokumentation verlangen.
- Schließlich kann nach Umsetzung der neuen Richtlinie das BSI auch „beim Betreiber die Einhaltung der Anforderungen überprüfen; es kann sich bei der Durchführung der Aufsicht einer qualifizierten Stelle bedienen. Der Betreiber hat dem Bundesamt und den in seinem Auftrag handelnden Personen zu diesem Zweck das Betreten der Geschäfts- und Betriebsräume während der üblichen Betriebszeiten zu gestatten und auf Verlangen die in Betracht kommenden Aufzeichnungen, Schriftstücke und sonstige Unterlagen in geeigneter Weise vorzulegen, Auskunft zu erteilen und die erforderliche Unterstützung zu gewähren.“

Betreiber von KRITIS Anlagen müssen sich folglich künftig darauf einstellen, eine regelmäßige Überprüfung durch BSI-Vertreter vor Ort zu begleiten und zu unterstützen. Mit den jetzt im Gesetzentwurf ausgeweiteten Aufsichtsbefugnissen soll das BSI laut Begründung zwar in die Lage versetzt werden, unabhängig von der Anzeige konkreter Mängel durch einen KRITIS Betreiber zu bewerten, ob dieser seinen Pflichten gemäß ITSiG nachkommt. Dies widerspricht aber völlig dem bislang gewählten kooperativen Ansatz, wonach sich KRITIS-Betreiber in eigener Verantwortung nach dokumentierten Standards schützen und ausdrücklich keine BSI-Überprüfung der einzelnen Anlagen vorgesehen war.

Auch das Argument aus der Begründung, für den Betreiber stelle die „Einsichtnahme vor Ort in der Regel eine geringere Belastung dar“ als die Dokumentation der Sicherheitsmaßnahmen, überzeugt nicht. Tatsächlich bedeutet die ausgeweitete Meldeverpflichtung mit zusätzlicher Vor-Ort-Überprüfung eine erhebliche Mehrbelastung für KRITIS-Betreiber.

3.2 Operative Unterstützung durch das BSI

Eine stärker operativ unterstützende Rolle im Falle schwerwiegender Sicherheitsverletzungen auf Ersuchen des Betroffenen begrüßen wir grundsätzlich. Maßgeblich ist mithin das Anforderungsprinzip, mit dem sichergestellt wird, dass das BSI nur dann tätig wird, wenn der betroffene Anbieter diese Unterstützung für notwendig erachtet, um der eingetretenen Lage Herr zu werden. Als problematisch erweist sich indes, wie auch im bereits geltenden § 8b Abs. 6 BSI-G, die in § 5a Abs. 6 BSI-G-E vorgesehene Ermächtigung zur Einbindung der Hersteller entsprechender Systeme durch das BSI. Hier ist zunächst festzuhalten, dass insoweit für den Betroffenen Hersteller im Gegensatz zum

eigentlichen Anbieter nicht mehr das Anforderungsprinzip gilt, sondern dieser vom BSI verpflichtend herangezogen werden soll, und zwar unabhängig davon, ob Indizien für einen schuldhaften Verursachungsbeitrag vorliegen. Während mithin für den eigentlich betroffenen Betreiber das Anforderungsprinzip greift kann der Hersteller als Dritter verpflichtend herangezogen werden, ohne dass diese Heranziehung qualifizierender Umstände bedarf. Hierin liegt ein Wertungswiderspruch und insoweit auch ein Unterschied zur bereits geltenden Regelung nach § 8b Abs. 6 BSI-G.

Hierbei ist auch zu bedenken, dass die insoweit geplante Befugnis für das BSI in das vertragliche Haftungsgefüge zwischen Hersteller und dem entsprechenden Betreiber eines IT-Systems eingreift. Damit kommt der Norm wie bereits § 8 Abs. 6 BSI-G faktisch eine – öffentlich-rechtliche – Haftungsqualität zu, wobei es sich mangels Regelung qualifizierende Voraussetzungen um eine verschuldensunabhängige Haftung handeln würde.

Aus der Begründung geht zwar hervor, dass der Hersteller nicht generell kostenlos herangezogen werden darf. Jedoch fehlt insoweit zum einen eine klare Regelung im Gesetzestext selbst, zum anderen soll Kostenausgleich nur im Falle des Ablaufs des Supportzeitraumes gewährt werden. Damit aber greift die Regelung gerade auch bzgl. der Kostentragung in das vertragliche Haftungssystem ein. So mögen für entsprechende Serviceleistungen innerhalb des Supportzeitraumes zum einen spezifische Kostenvereinbarungen getroffen worden sein, so dass sich bei Heranziehung nach § 5a Abs. 6 BSI-G-E die Frage des maßgeblichen Kostenmaßstabs stellt. Zum anderen stellt sich auch die Frage, zu welchen konkreten Maßnahmen ein Hersteller überhaupt verpflichtet werden kann, wenn zum Beispiel die Support-Frist gegenüber dem Betreiber für den Betroffenen Dienstes ausgelaufen ist.

Angesichts der faktischen Haftungswirkung und der damit verbundenen Einwirkung in die vertraglichen Beziehungen zwischen Herstellern und Betreibern von IT-Systemen regt Bitkom an, § 5a Abs. 6 BSI-G-E zu streichen.

3.3 Erweiterung der Kontaktstellenpflicht nach ITSiG

Mit der in § 8d Abs. 3 (n.F.) BSI-G-E ins Visier genommenen Änderung, nach der die Bereichsausnahme für bestimmte Sektoren sich nicht mehr auf die Pflicht nach § 8b Abs. 3 und 5 BSI-G beziehen soll, wird die Pflicht zur Benennung einer Kontaktstelle auf Kritis-Betreiber ausgeweitet, die bislang aufgrund spezialgesetzlich vorrangiger Normen insoweit ausgenommen waren, zum Beispiel Telekommunikationsanbieter. Diese Erweiterung der Pflicht zur Etablierung einer Kontaktstelle lehnen wir ab. Die Gründe für die bisherige Regelung des Vorrangs der entsprechenden Spezialgesetze auch für die Meldeprozesse haben weiterhin Bestand. Ziel war, durch das ITSiG keine Doppelregulierungen und vor allem keine Doppelzuständigkeiten in der Aufsicht zu begründen. Genau dies würde aber bewirkt, wenn nunmehr für die Pflicht zur Etablierung der Kontaktstelle dieser Vorrang der spezialgesetzlichen Regelungen durchbrochen wird. Für den Kritis-Sektor „Telekommunikation“ entstünde beispielsweise die Frage, weshalb entsprechende Betreiber künftig gegenüber dem BSI eine Kontaktstelle benennen müssten, während die spezialgesetzliche Meldepflicht sich nach TKG richtet und gegenüber der Bundesnetzagentur zu erfolgen hat.
Von der avisierten Erweiterung der Pflicht zur Benennung einer Kontaktstelle nach § 8b Abs. 3 und 5 BSI-G auf Kritis-Anbieter, die spezialgesetzlichen Vorschriften zur IT-Sicherheit unterliegen ist insofern im Hinblick auf das weiterhin einschlägige Ziel der Vermeidung von Doppelregulierungen und insbesondere Doppelzuständigkeiten abzusehen.

3.4 Umsetzung der Regelungen zu digitalen Diensten

Hier ist insbesondere die Umsetzung der Regelungen zu digitalen Diensten nach § 8c BSI-G-Entwurf und Regelungen zum Anwendungsbereich nach § 8d Abs. 4 (n.F.) BSI-G-Entwurf angesprochen: Wir begrüßen zunächst prinzipiell die wortlautnahe Implementierung der Richtlinienvorgaben im Hinblick auf die damit verbundene europäische Harmonisierung der entsprechenden Vorgaben für digitale Dienste.

Im Hinblick auf die Tatsache, dass digitale Dienste im Sinne der NIS-Richtlinie heute überwiegend länderübergreifend innerhalb der EU angeboten werden, kommt der Regelung der örtlichen Zuständigkeit der Aufsichtsbehörden eine besondere praktische Bedeutung zu.
Wir begrüßen daher die mit § 8d Abs. 4 Satz 2 und Satz 3 BSI-G-Entwurf erfolgte Klarstellung, dass sowohl für die Meldepflicht nach § 8c Abs. 2 als auch die Nachweispflicht nach § 8c Abs. 3 BSI-G-Entwurf grundsätzlich auf die Hauptniederlassung des Anbieters abzustellen ist, womit die entsprechende Vorgabe der Richtlinie umgesetzt wird.

Bezüglich der in § 8d Abs. 4 Satz 3 BSI-G-Entwurf hinterlegten Präzisierung, dass die Nachweispflicht ggü. dem BSI auch dann gelten soll, soweit die jeweiligen Anbieter „in der Bundesrepublik Deutschland Netz- und Informationssysteme betreiben, die sie im Rahmen der Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen“ besteht allerdings noch dringender Klarstellungsbedarf.

Da die Begrifflichkeiten des „Netz- und Informationssystems“ nicht legal definiert sind und von der Richtlinie als Überbegriff für alle erfassten Diente verwendet werden, stellt sich die Frage, auf welche Fälle diese Einschränkung der örtlichen Anwendbarkeit bzw. Zuständigkeit der Verpflichtungen nach § 8c Abs. 3 BSI-G-Entwurf zielt. Soweit hier auf den „Betrieb“ entsprechender Systeme abgestellt wird, besteht die Gefahr, dass die an sich als Grundprinzip gedachte Regelung der Maßgeblichkeit des Hauptsitzes in der Praxis obsolet wird, weil z.B. beim europaweiten Angebot eines Dienstes immer (auch) vom Betrieb des Netz- und Informationssystems in Deutschland ausgegangen werden müsste.

Die NIS-Richtlinie ist im Falle des Sitzlandprinzips für Digitale Dienste eindeutig. Die vorgeschlagene Umsetzung in Deutschland würde diesen Ansatz praktisch aushebeln. Wir regen daher an, die Gegenausnahme des § 8d Abs. 4 Satz 3 BSI-G-Entwurf zu streichen, um klarzustellen, dass auch in Bezug auf die Nachweispflicht nach § 8c Abs. 3 uneingeschränkt das Sitzlandprinzip gilt. Jedenfalls aber bedarf es ggf. einer Klarstellung und Qualifizierung, wann im Sinne dieser Vorschrift von einem „Betrieb eines Netz- und Informationssystems in Deutschland“ auszugehen ist. Andernfalls droht die Gefahr, dass für die Nachweispflicht nach § 8c Abs. 3 das als Regel gedachte Sitzlandprinzip praktisch zum Ausnahmefall wird und die betroffenen Diensteanbieter gegenüber mehreren Behörden (im EU-Sitzland und in Deutschland) berichtspflichtig wären.

Ferner wollen wir anregen, dass die Anbieter digitaler Dienste sowie die Betreiber kritischer IT-Infrastrukturen das Recht erhalten, die bei der Nutzung der Dienste entstehenden Daten der Nutzer zu erheben und zu verwenden, um Störungen oder Fehler an Telekommunikationsanlagen zu erkennen, einzugrenzen oder beseitigen zu können.

4 Anregungen zur Konkretisierung

Angesichts des bereits mit dem IT-Sicherheitsgesetz etablierten regulatorischen Rahmens, der neben neuen Regelungen zu spezifischen kritischen Infrastrukturen auch Änderungen im TMG (§ 13 Abs. 7 TMG) für Telemedien umfasst hat, begrüßen wir prinzipiell die grundlegende Herangehensweise einer wortlautnahen Umsetzung der Richtlinie, wie sie dem vorgelegten Referentenentwurf zugrunde liegt. Gleichzeitig ergeben sich aus dem Zusammenspiel der bereits geschaffenen Regelungen und den durch die NIS-Richtlinie notwendig gewordenen Änderungen indes Fragestellungen im Hinblick auf den Anwendungsbereich der entsprechenden Normen und etwaiger Überschneidungen.

4.1 Cloud-Dienste

Mit der jetzt von der Richtlinie übernommenen Definition der Cloud-Dienste, die bislang so im deutschen Recht nicht existiert, entsteht ein Überschneidungsbereich mit den nach IT-Sicherheitsgesetz und der darauf aufbauenden Verordnung erfassten Betreibern von Rechenzentren, die auch der entsprechenden Meldepflicht unterliegen. Hier ergeben sich Fragen in Bezug auf etwaige Doppelregulierungen. Bitkom regt deshalb zur Vermeidung von Doppelregulierungen eine Klarstellung derart an, dass die im Zuge der Umsetzung der NIS-Richtlinie geschaffenen Verpflichtungen (etwa Meldepflichten) nicht gelten, wenn entsprechende oder strengere Pflichten für den konkreten Anbieter bereits aus Regelungen für die Betreiber kritischer Infrastrukturen folgen. Ferner sollte die deutsche Umsetzung einen enge Interpretation des Begriffs der „Cloud Dienste“ vornehmen – konkret: eine Fokussierung auf die Infrastruktur-Ebene und eben nicht die Applikationsebene – welches sich mit Ansatz im ITSiG/VO decken würde.

Die Definition für Cloud Computing Dienste (§2 Abs. 9 BSI-Gesetz) ist wenig griffig und sollte sich noch stärker an der Definition der NIS-Richtlinie (Ziff.17) orientieren. Andernfalls ist der Geltungsbereich nicht hinreichend bestimmt. In Bezug auf § 2 Abs. 9 regen wir an, die zahlreichen Verweise auf Richtlinien und Verordnungen der EU durch dem EU-Recht entsprechende Formulierungen zu ersetzen und so in nationales Recht umzusetzen. Dies dürfte auch die Lesbarkeit und Anwendbarkeit erheblich verbessern.

4.2 Verhältnis der Regelungen zu Diensten zu § 13 Abs. 7 TMG

Hier stellt sich auch die Frage nach dem Verhältnis zu § 13 Abs. 7 TMG (relevant für Begründung, S. 29 oder S. 41 ff. des Entwurfs): Es wäre wünschenswert, wenn in der Gesetzesbegründung die Anwendungsbereiche von § 13 Abs. 3 TMG und von § 8c BSIG-Entwurf klar voneinander abgegrenzt werden. Es besteht ggf. Gesetzeskonkurrenz insbesondere zu den in § 2 Abs. 9 definierten Diensten. Zur Schaffung von Rechtssicherheit für die betroffenen Unternehmen bedürfen diese einer stärkeren Konkretisierung. Es wäre deshalb wünschenswert, wenn in der Gesetzesbegründung die Anwendungsbereiche von § 13 Abs. 3 TMG und von § 8c BSIG-Entwurf klar voneinander abgegrenzt werden und insbesondere zu der Durchsetzung von Sanktionen Stellung genommen würde. Dies stützt sich auf die Erwägung, dass aus dem Entwurf nicht ersichtlich wird, wie sich die neuen, bußgeldbewehrten Pflichten

für Anbieter digitaler Dienste (§ 8c BSIG-Entwurf, § 14 Abs. 1 Nr. 5-7 BSIG-Entwurf) zum bisherigen § 13 Abs. 7 TMG verhalten.

Beide Regelungsmechanismen können mit "Diensteanbietern" (§ 2 Nr. 1 TMG) und "Digitalen Diensten" (§ 2 Abs. 9 BSIG-Entwurf) als verpflichtete Normadressaten praktisch dieselben Unternehmen erfassen. So würden nach dem Gesetzesentwurf etwa Cloud Anbieter gleichermaßen unter das BSIG-Entwurf und das TMG fallen. Sowohl § 8c Abs. 1 BSIG-Entwurf als auch § 13 Abs. 7 TMG sehen eine Pflicht zur Implementierung technischer und organisatorischer Vorkehrungen bzw. Maßnahmen vor, um "Sicherheitsvorfällen" "vorzubeugen" oder sie "gering zu halten" (§ 8c Abs. 1 BSIG-Entwurf) und "unerlaubte Zugriffe" oder "Störungen" (§ 13 Abs. 7 TMG) der Dienste zu verhindern. Beide Vorschriften sehen jeweils im Falle der Verletzung die Möglichkeit der Verhängung einer Geldbuße bis zu 50.000 Euro vor (§ 16 Abs. 2 Nr. 3, Abs. 3 TMG und §§ 14 Abs. 1 Nr. 5-7, Abs. 2 BSIG-Entwurf). Da die Schutzzwecke des TMG und des BSIG sich jedenfalls überschneiden und die Vorschriften entsprechend in Normkonkurrenz treten, sollte eine Klarstellung zum Verhältnis der relevanten Normen aus dem TMG und BSIG erfolgen, sofern ein Unternehmen in den Anwendungsbereich beider Gesetze fallen sollte.

Im Rahmen des IT-Sicherheitsgesetzes wurde mit § 13 Abs. 7 erstmals auch eine IT-Sicherheitsregulierung für geschäftsmäßig erbrachte Telemediendienste eingeführt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat diese Pflicht durch eine entsprechende Empfehlung mittlerweile konkretisiert, wobei der Begriff des „Standes der Technik“ die maßgebliche Leitlinie bildet. Das Empfehlungspapier geht dabei explizit auf die verschiedenen Providertypen ein, wie sie dem TMG prinzipiell zugrunde liegen, womit prinzipiell zwischen Content-, Host-, Access- und Cache-Providern unterschieden wird. Auch hier ergeben sich Fragen zum Überschneidungsbereich des § 13 Abs. 7 TMG im Verhältnis zu den nun für Dienste geplanten Normen im BSI-G. Sowohl Online-Marktplätze, als auch Suchmaschinen und Cloud-Dienste unterfallen auch den entsprechenden Regelungen des TMG, inklusive des § 13 Abs. 7 TMG.

Der nunmehr geplante § 8c BSI-G schafft in Umsetzung der NIS-Richtlinie eine im Kern ähnliche Regelung zu technischen und organisatorischen Vorkehrungen wie § 13 Abs. 7 TMG, wenn auch die Anforderungen auf gesetzgeberischer Ebene entsprechend der Vorgaben der Richtlinie detaillierter hinterlegt sind als im TMG. Auch hier bildet indes der „Stand der Technik die grundlegende Leitlinie“. Damit entsteht eine Doppelregulierung nach BSI-G und TMG für die nach § 8 c BSI-G erfassten Dienstegruppen, da diese auch als Telemedien zu qualifizieren sind.

Zur Vermeidung von Doppelregulierungen und Rechtsunsicherheiten empfiehlt Bitkom daher, die Regelung des § 13 Abs. 7 TMG generell auf Regelungsnotwendigkeit & Regelungsgehalt zu überprüfen und entsprechend anzupassen oder zumindest klarzustellen, sodass § 8c BSI-G für die hier erfassten Dienste der Vorschrift des § 13 Abs. 7 TMG als spezialgesetzliche Norm vorgeht.