VERBAND DER INTERNETWIRTSCHAFT E.V.

Stellungnahme zum Referentenentwurf des Bundesministeriums des Innern über den „Entwurf eines Gesetzes zur Umsetzung der 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“

Berlin 16. Dezember 2016

Mit der Verabschiedung der NIS-Richtlinie der Europäischen Union im Juli 2016 stellt sich für Deutschland die Frage, wie die Richtlinie in Deutschland umgesetzt wird. Mit dem IT-Sicherheitsgesetz des Bundes (IT-SiG) und der KRITIS-Verordnung (KRITIS-VO) sind bereits erste Rechtsakte verabschiedet worden, noch bevor die NIS-RL überhaupt in Europa verabschiedet wurde. Die noch offenen Fragen aus der NIS-RL sollen nun ebenfalls geregelt werden.

Das Bundesministerium des Innern hat in diesem Zusammenhang am 9. Dezember 2016 einen Referentenentwurf für den „Entwurf eines Gesetzes zur Umsetzung der 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“ (NIS-Umsetzungsgesetz) vorgelegt. Mit dem als Artikelgesetz angelegten Entwurf soll das BSI-Gesetz maßgeblich erweitert und weitere Rechtsvorschriften angepasst werden.

I. Allgemeine Anmerkungen zum Gesetzentwurf

eco hat die Entwicklung der IT-Sicherheitsgesetzgebung auf europäischer Ebene und in Deutschland begleitet und bereits in der Vergangenheit Stellung dazu bezogen. Im Rahmen des laufenden Kommentierungsverfahrens nimmt eco gerne die Gelegenheit wahr, eine erste Einschätzung zum vorliegenden Referentenentwurf (Stand vom 7. Dezember 2016) abzugeben. eco wird sich dabei aufgrund der sehr kurzen Kommentierungsfrist auf einige für die Internetwirtschaft zentrale Aspekte konzentrieren. Weitergehende Anmerkungen und Kommentare werden wir im Verlauf des Gesetzgebungsverfahrens einbringen.

▪ Anwendungs- und Regelungsbereich

Mit dem vorliegenden Referentenentwurf werden verschiedene Aspekte so genannter digitaler Dienste adressiert. Er bleibt aber sowohl in der Definition als auch in den konkreten Anforderungen für die Anbieter digitaler Dienste unbestimmt. Dies betrifft sowohl die Beschreibung der digitalen Dienste als auch die konkreten Anforderungen an deren Anbieter. Dadurch ist nicht eindeutig, wer letzten Endes mit dem Gesetz konkret adressiert wird und wer

dem Anwendungsbereich des Gesetzes unterliegt. Insbesondere die Frage, wie sich die hier adressierten Anbieter digitaler Dienste von Telemediendiensteanbietern abgrenzen, die bereits durch den § 13 Abs. 7 des Telemediengesetzes im Rahmen des ersten IT-SiG reguliert wurden, bleibt unbeantwortet. Es wird zudem auf zukünftig noch zu erlassende Vorschriften (Durchführungsrechtsakt) durch die Europäische Kommission verwiesen, gleichzeitig aber auch eine Verordnungsermächtigung für das BMI eröffnet, so dass ebenfalls unklar bleibt, welche Auflagen letzten Endes die Anbieter tatsächlich zu erfüllen haben und wie weit der Regelungskreis gezogen wird. Mehrere unbestimmte Rechtsbegriffe sorgen zusätzlich für Unsicherheit.

- **Umsetzungs- und Implementierungsfristen**

Vor dem Hintergrund der vorzunehmenden umfangreichen operativen Implementierungen sowie ggfs. entsprechender Audits wird die Umsetzung der Anforderungen geraume Zeit in Anspruch nehmen. Ein Implementierungszeitraum, der voraussichtlich weniger als ein Jahr betragen wird, ist daher unangemessen. Die Umsetzungsfrist sollte für das vorliegende Gesetz erst dann beginnen, wenn die notwendigen Präzisierungen und Konkretisierungen im Rahmen des Durchführungsrechtsakts und gegebenenfalls zusätzlich durch Rechtsverordnung vorgenommen und verabschiedet sind. Denn diese bilden die Grundlage für die Umsetzung bei den Unternehmen. Auch in diesem Fall ist eine deutlich längere Umsetzungsfrist aus Sicht des eco angezeigt.

- **Problematik der Doppelregulierung**

Der Referentenentwurf birgt aufgrund des unklaren und zu unbestimmten Anwendungs- und Adressatenkreises die Gefahr einer Doppelregulierung für Unternehmen. Es ist nicht eindeutig, wie sich bestehende gesetzliche Verpflichtungen aus dem IT-SiG vom 17. Juli 2015 sowie der KRITIS-VO zu den im vorliegenden Referentenentwurf vorgesehenen Regelungen für die Umsetzung der NIS-Richtlinie verhalten. Insbesondere das Verhältnis der jeweiligen Normadressaten und der ihnen obliegenden Verpflichtungen lassen sich nicht eindeutig voneinander abgrenzen. Damit einher geht die Gefahr einer Doppelregulierung und sich einander überlagernder Verpflichtungen.

- **Mitwirkungspflichten**

Die im Gesetzesentwurf verankerten Mitwirkungspflichten sind in ihrer Tragweite derzeit noch nicht absehbar und bergen eine Vielzahl weiterer Fragen in sich. Daher besteht grundsätzlicher Erörterungsbedarf an der vorgeschlagenen Regelung. Aufgrund der Tragweite und Auswirkungen für die gesamte ITK-Branche bedarf es einer intensiven Diskussion.

II. Zu den einzelnen Regelungen

- **Nummer 1 Referentenentwurf: Änderung § 2 Absatz 9 BSI-Gesetz (Neueinführung von Definitionen für „Digitale Dienste“)**

Die in Nummer 1 angeführte Herleitung der Definition für digitale Dienste ist kritisch zu bewerten. Die NIS-Richtlinie listet zwar im Anhang III „Arten digitaler Dienste“ und darunter Online-Marktplätze, Online-Suchmaschinen und Cloud-Computing-Dienste und definiert diese auch in Artikel 4 Abs. 17-19. Sie verweist aber auch auf die RL (EU) 2015/1535 und führt z.T. abweichende Formulierungen in den Erwägungsgründen 13 bis 15 an.

Das NIS-Umsetzungsgesetz erhöht die Komplexität dieser ohnehin unklaren Konstruktion, indem es die Definitionen aus der NIS-RL Art. 4 Abs. 17-19 noch durch den Bezug auf die EU-Richtlinie 2009/22/EG (Richtlinie über alternative Streitbeilegung in Verbraucherangelegenheiten) erweitert.

Die vorliegenden Definitionen sorgen daher für Unsicherheit bspw. für die Betreiber von Webseiten, die Suchfunktionen auf Ihrem Angebot einbinden und nutzen. Darüber hinaus ist auch offen, inwieweit der vorliegende Gesetzestext die konkreten Dienste adressiert, und inwieweit dann im Rahmen der Anwendung des Gesetzes Verpflichtungen und Beschränkungen für die Infrastrukturdienstleister, z.B. Hosting-Anbieter, solcher Dienste ausgelöst werden. Die Debatte wird parallel auch im BSI geführt, das im Kontext der Umsetzung des IT-SiG bereits Empfehlungen für „Internetdienstleister“ erarbeitet.

Zuletzt bleibt festzuhalten, dass zwar sowohl die NIS-RL, als auch die Gesetzesbegründung Infrastrukturdienstleister von den Verpflichtungen für digitale Dienste ausnehmen, auf der anderen Seite aber durch die unklare Definition diese unmittelbar davon betroffen sein können. In diesem Zusammenhang stellt sich dann zudem die Frage, wie mit den Anbietern der im Gesetzesentwurf genannten Dienste, die gleichzeitig auch der sektorspezifischen Regulierung des TKG unterworfen sind, umgegangen werden soll. eco sieht speziell für solche Anbieter das Risiko paralleler, sich überlagernder Berichtspflichten und einer Doppelregulierung.

- **Nummer 3 Referentenentwurf: Einführung eines neuen § 5a zur „Wiederherstellung der Sicherheit und Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen“**

In Absatz (5) des neuen § 5a wird darauf verwiesen, dass Unternehmen und Organisationen, die das BSI um Hilfe ersuchen, auch von „qualifizierten Dritten“ entsprechende Hilfe mit ihrem Einverständnis erhalten können. Dies ist insofern relevant, als dass die Kosten für die Inanspruchnahme von qualifizierten Dritten durch das ersuchende Unternehmen zu tragen sind (vgl. auch §5a Absatz (1)). Unklar ist jedoch in welchem Wechselverhältnis dies mit den in Absatz (7) genannten „begründeten Einzelfällen“ steht, in denen das BSI selbst tätig werden darf. Gerade vor dem Hintergrund, dass die

Hinzuziehung von „qualifizierten Dritten“ kleine und mittelständische Unternehmen vor unabsehbare zusätzliche Kosten stellen kann, und diese voraussichtlich verstärkt einer solchen Unterstützung bedürfen, wäre hier eine Klarstellung hilfreich, die eben diese kleinen und mittelständischen Unternehmen vor unverhältnismäßigen Kosten schützt.

Daneben wird in Absatz (6) auch aufgeworfen, dass das Bundesamt für Sicherheit in der Informationstechnik (BSI) „die Mitwirkung an der Wiederherstellung der Sicherheit oder Funktionsfähigkeit“ von den Herstellern „informationstechnischer Systeme“ verlangen kann. Die hier verwendete Formulierung zielt primär auf Drittanbieter von IT.

Mit der im Gesetzentwurf vorgeschlagenen Regelung wird eine Mitwirkungspflicht von Herstellern, Lieferanten oder Zulieferern von IT-Produkten (Hard- oder Software) etabliert. Dem liegt die Überlegung zugrunde, dass die betroffenen Unternehmen zur Beseitigung eines Sicherheitsproblems oftmals auf die Mitwirkung eines Dritten angewiesen sind. Dies mag auf den ersten Blick sinnvoll erscheinen, wirft jedoch bei genauerer Betrachtung eine Vielzahl von Fragestellungen auf, die zunächst einer breiteren Diskussion und Erörterung bedürfen.

So ist beispielsweise aufgrund der breitgefächerten IT-Landschaft mit einer Vielzahl von IT-Produkten mit sehr unterschiedlichen Lebenszyklen fraglich, ob eine solche Forderung nach Mitwirkung überhaupt sinnvoll erbracht werden kann, oder ob sie überhaupt im Sinne des jeweiligen Anbieters eines informationstechnischen Systems liegt, da dieser bspw. den Support für die entsprechende Plattform bereits eingestellt hat. Ein tatsächliches Mitwirken könnte für solche Unternehmen mit enormen Zusatzkosten verbunden sein. Auch ist in diesem Kontext nicht klar, wie mit der Mitwirkung des Herstellers umgegangen werden soll, wenn dieser sich nicht in der EU befindet bzw. wenn er aufgrund der dynamischen Entwicklung der IT-Wirtschaft nicht mehr am Markt verfügbar ist. Die Sorge besteht hier, dass in einem solchen Fall auf Anbieter oder Verkäufer oder gar auf Telekommunikationsdienstleister zurück- bzw. durchgegriffen werden könnte, die evtl. nicht über die nötige Kenntnis der Technologie verfügen und folglich auch keine Möglichkeiten zur Mitwirkung haben. Zwar führt die Gesetzesbegründung auf, dass vor allem Hersteller adressiert sind und diese ggfs. auch zu entschädigen seien, jedoch ändert dies nichts an der grundsätzlichen Problematik, dass eine solche Mitwirkungspflicht nicht immer wie im Gesetzesentwurf dargestellt umgesetzt werden kann. Insbesondere ist problematisch, dass mit der im Gesetzentwurf geplanten Mitwirkungspflicht nicht an ein schuldhaftes Verhalten geknüpft ist.

Nach Ansicht des eco besteht erheblicher, grundsätzlicher Erörterungsbedarf der vorgeschlagenen Regelung. Es bedarf zunächst einer intensiven Diskussion, bevor Regelungen getroffen werden, deren Tragweite für die gesamte IKT-Branche derzeit unabsehbar sind. eco regt an, dies zunächst mit der Vielzahl der betroffenen Branchen ausführlich zu diskutieren und grundsätzlich zu erörtern.

- **Nummer 5 Referentenentwurf: Änderung des § 8a des BSI-Gesetzes (Auflagen für Betreiber kritischer Infrastrukturen)**

In dem Paragrafen werden durch die Neuformulierung des Satzes 3 zusätzliche Auflagen für die Betreiber kritischer Infrastrukturen geschaffen. Ob dadurch tatsächlich ein bedeutender Beitrag zur Verbesserung von IT-Sicherheit geleistet werden kann, ist jedoch unklar. Der zusätzliche neu eingefügte Absatz (4) ist in der vorliegenden Fassung zu hinterfragen, da zum einen die Aufsichtspflicht an eine „qualifizierte Stelle“ delegiert wird, zum anderen die Kosten einer Überprüfung aufgrund einer nur schwer durchschaubaren Übernahmeregelung dem überprüften Unternehmen aufgebürdet werden. Die Formulierung von „berechtigten Zweifeln“ ist hier nicht ausreichend.

- **Nummer 6 Referentenentwurf: Änderung des § 8b des BSI Gesetzes**

Die Ausweitung der Meldepflicht für Betreiber kritischer Infrastrukturen auch auf „mögliche Auswirkungen“ entspricht nicht der im IT-SiG und der NIS-RL entwickelten Logik, dass beim Auftreten einer Störung die jeweils national betroffene zentrale Kontaktstelle adressiert werden soll. Der erhoffte Erkenntnisgewinn steht in keinem sinnvollen Verhältnis zu dem damit verbundenen Aufwand. Daneben gilt es auch noch zu berücksichtigen, dass möglicherweise hier eine doppelte Meldepflicht ausgelöst wird.

- **Nummer 7 Referentenentwurf: Neueinführung eines § 8c BSI-Gesetz (Besondere Anforderungen an Anbieter digitaler Dienste)**

Der neu eingeführte § 8c stellt zusätzliche Anforderungen an die in Nummer 1 angeführten Anbieter digitaler Dienste. Positiv bleibt hier zunächst festzuhalten, dass sich der Gesetzesentwurf bei den zu berücksichtigenden Faktoren und bei den Kriterien für eine Meldung eines erheblichen IT-Sicherheitsvorfalls nah an der NIS-RL orientiert. Gleichzeitig stellt der Paragraf in seiner vorliegenden Fassung für die Anbieter dieser Dienste eine Herausforderung dar. Wie auch die Betreiber kritischer Infrastrukturen werden sie einer umfassenden Meldepflicht unterworfen. Inwieweit dies für die Anbieter solcher Dienste möglich und machbar ist, bleibt unklar. Stellt diese Anforderung doch personellen und organisatorischen Mehraufwand dar, der auch durch die Einführung der Verhältnismäßigkeitsklausel in Abs. (1) nicht in ein angemessenes Verhältnis von Aufwand und Nutzen gesetzt werden kann. Darüber hinaus ist auch unklar, welche Maßstäbe für die „geeigneten Maßnahmen“ gesetzt werden. Der Gesetzestext verweist an dieser Stelle auf von der EU-Kommission noch zu erlassende „Durchführungsrechtsakte“, deren Inhalte zum heutigen Tag noch nicht bekannt sind. Eine plausible Abschätzung der Angemessenheit und Verhältnismäßigkeit der Anforderung kann an dieser Stelle daher nicht erfolgen. Es ist jedoch bereits jetzt absehbar, dass sich hier enorme

Rechtsunsicherheit für Unternehmen abzeichnet, da sie evtl. Anforderungen unterworfen sind, die derzeit noch nicht absehbar bzw. näher bekannt sind.

Darüber hinaus wirkt die im NIS-Umsetzungsgesetz unter § 8c Abs. 2 formulierte Meldepflicht in einer Art geregelt, die für Anbieter von Infrastruktur oder Technologie die für die Bereitstellung digitaler Dienste genutzt wird, z.B. Host-Provider, vor die Frage stellt, inwieweit diese in die Meldepflicht einbezogen werden. Es sollte in jedem Fall sichergestellt werden, dass die hier aufgeworfene Meldepflicht, sofern diese überhaupt statthaft ist, keine weiteren Rechtsfolgen für diese Dienstleister z.B. im Bereich der Haftung hat und dass konkrete Sicherheitsmaßnahmen im Rahmen der Bearbeitung meldepflichtiger Ereignisse nur mit deren Einverständnis erfolgt. Es muss ausgeschlossen sein, dass durch etwaige Sicherheitsmaßnahmen in die Infrastruktur des Anbieters eingegriffen und deren Funktionsfähigkeit beeinträchtigt wird.

Auch wird nicht klar, welche Dienste bspw. aufgrund anderer gesetzlicher Regelungen bereits eigene Meldepflichten etabliert haben und sinnvollerweise aus der hier formulierten Verpflichtung ausgenommen werden sollten. eco sieht hier den Bedarf für eine stärkere Differenzierung in der Herangehensweise. Auch ist die in Ausnahme von Kleinstbetrieben von entsprechenden Verpflichtungen gem. Nummer 8 des vorliegenden Gesetzesentwurfes aus Sicht des eco an dieser Stelle nicht ausreichend, um speziell kleine und mittelständische Anbieter digitaler Dienste vor der enormen Last einer solchen Meldepflicht adäquat zu schützen. Dies wird durch die dort formulierte Ausnahme für die Bereitstellung von digitalen Diensten innerhalb der Europäischen Union weiter verschärft.

- **Nummer 8 Referentenentwurf: Überführung des § 8c in den § 8d**

Die in Absatz (4) formulierte Regelung für den Geltungsbereich des § 8c für die Anbieter digitaler Dienste ist aus Sicht des eco nicht eindeutig. Grundsatz der NIS-RL ist, dass sich die gerichtliche Zuständigkeit nach dem Land des Hauptsitzes eines solchen Anbieters bestimmt. Dies wird grundsätzlich auch ins Gesetz überführt. Allerdings wird mit der Formulierung „Für Anbieter nach Satz 2 gilt § 8c Absatz 3 nur, soweit diese in der Bundesrepublik Deutschland Netz- und Informationssysteme betreiben, die sie im Rahmen der Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen.“ dieses Prinzip ausgehöhlt. Es besteht das Risiko doppelter Berichts- und Meldepflichten mit entsprechenden Rechtsfolgen. Die Einführung des Begriffs „Netz- und Informationssysteme“ schafft Unsicherheit, da der Begriff nicht mit den sonst verwandten Definitionen harmoniert und als solcher ein unbestimmter Rechtsbegriff ist.

- **Nummer 9 Referentenentwurf: Überführung des § 8d BSI-Gesetz in einen § 8e**

Die zu Nummer 7 aufgeführten problematischen Aspekte können analog für den unter Nummer 9 zusammengefassten Formulierungen zum Auskunftsverlangen des BSI festgehalten werden.

- **Nummer 10 Referentenentwurf: Ergänzung des § 10 BSI-Gesetz (zusätzliche Verordnungsermächtigung für das BMI)**

Die im neuen Absatz (4) des Gesetzesentwurfs verankerte Verordnungsermächtigung für das BMI zur näheren Bestimmung der Anforderungen an die Betreiber digitaler Dienste verschärft die Rechtsunsicherheit für deren Anbieter weiter. Wie bereits im IT-SiG Bund besteht nun die Situation, dass Unternehmen im Rahmen einer nachgelagerten Rechtsverordnung Regelungen unterworfen werden, die weiter ausgeführt, anders ausgelegt oder gar im Vergleich zur Intention der Richtlinie deutlich verschärft werden könnten.

Die Lösung der konkreten Anforderungen an Dienste über eine Verordnung entspricht zwar der bisherigen Praxis aus dem IT-SiG. Allerdings sollte bei der Erarbeitung der Rechtsverordnung ein kooperativer und pragmatischer Ansatz verfolgt werden. Dies setzt voraus, dass die Erarbeitung der Rechtsverordnung in Abstimmung mit den betroffenen Unternehmen und deren Verbänden erfolgt und auch eine entsprechende Anhörung der beteiligten Kreise durchgeführt wird.

In diesem Zusammenhang stellt sich auch die Frage, inwieweit für Cloud-Dienste, Online-Marktplätze und Suchmaschinen überhaupt branchenspezifische Standards formuliert werden können und ob diese nicht so tief in die Dienste eingreifen, dass sie evtl. die Bereitstellung des Dienstes oder das dem Dienst zu Grunde liegende Geschäftsmodell gefährden. In diesem Kontext sind auch die in § 8c des NIS-Umsetzungsgesetzes formulierten Anforderungen an die Berücksichtigung des "Stands der Technik" problematisch. Aufgrund der unklaren Situation kann hier keine valide Aussage über die tatsächlichen Auswirkungen dieses Paragrafen getroffen werden, es besteht jedoch das Risiko, dass neben der zusätzlichen bürokratischen Belastung auch in den Bereich der Normung digitaler Dienste und Angebote eingegriffen wird, die sich als innovationsschädlich erweisen könnte.

Die zu Absatz (4) getroffenen Aussagen lassen sich in Bezug auf die Nichteinbeziehung der Internetwirtschaft auch auf den Absatz (5) übertragen.

- **Nummer 14 Referentenentwurf: Neueinfügung eines § 15 Übergangsvorschriften**

Der Gesetzgeber setzt den 10. Mai 2018 als Datum, ab dem die Anbieter digitaler Dienste die Vorschriften umzusetzen haben. Mit Blick auf die Vielzahl der zunächst einer weiteren Konkretisierung bedürftigen Fragen, die

erst im weiteren Verlauf beispielsweise durch einen Durchführungsrechtsakt der EU-Kommission und/oder Rechtsverordnung offenbar werden, insbesondere zu den konkreten Anforderungen an die digitalen Dienste, ist diese Umsetzungsfrist zu kurz bemessen und sollte verlängert werden – insbesondere unter dem Gesichtspunkt, dass die einschlägigen europäischen Durchsetzungsrechtsakte noch nicht erarbeitet sind, und unklar ist, ob das BMI von seiner Möglichkeit, eine Verordnung zu erlassen, Gebrauch machen wird. Vor diesem Hintergrund ist die Stichtagsregelung im Referentenentwurf mehr als unglücklich und sollte zugunsten einer Fristenregelung ersetzt werden, die sich am Inkrafttreten der Durchführungsrechtsakte der EU-Kommission und der sich voraussichtlich daran anschließenden Verordnung orientiert. Bei der Bemessung der Frist sollte berücksichtigt werden, dass die Etablierung und Implementierung von Sicherheitsstandards, sowie unter Umständen deren Zertifizierung, längere Zeit in Anspruch nehmen. Die Umsetzungsfrist nach Inkrafttreten der entsprechenden Normen sollte daher deutlich länger sein als dies im derzeitigen Referentenentwurf vorgesehen ist.

Über eco
eco - Verband der Internetwirtschaft e.V. ist Interessenvertreter und Förderer aller Unternehmen, die mit oder im Internet wirtschaftliche Wertschöpfung betreiben. Der Verband vertritt derzeit mehr als 900 Mitgliedsunternehmen. Hierzu zählen unter anderem ISP (Internet Service Provider), Carrier, Hard- und Softwarelieferanten, Content- und Service-Anbieter sowie Kommunikationsunternehmen. eco ist der größte nationale Internet-Service-Provider-Verband Europas.