VERBAND DER INTERNETWIRTSCHAFT E.V.

Stellungnahme zum Diskussionsentwurf des Bundesministeriums des Innern für Bau und Heimat eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0) (Stand 1.12.2020)

Berlin 9. Dezember 2020

In ihrem Koalitionsvertrag von 2018 kündigten die Regierungsparteien an, das IT-Sicherheitsgesetz fortzuschreiben und dessen Ordnungsrahmen zu erweitern, um neuen Gefährdungen angemessen zu begegnen. Ziel des Gesetzes sollte der Ausbau des BSI zu einer nationalen Cybersicherheitsbehörde sein, das als unabhängige und neutrale Beratungsstelle für Fragen der IT-Sicherheit eine stärkere Rolle bekommen soll. Unterstützung und Beratung für Bund, Länder, Bürger sollten ausgebaut werden und das BIS zur zentralen Zertifizierungs- und Standardisierungsstelle für IT- und Cybersicherheit in Deutschland werden. Mit dem nunmehr vorgelegten Diskussionsentwurf des Bundesministeriums des Innern, für Bau und Heimat möchte die Bundesregierung diesem Auftrag Rechnung tragen.

Die Debatte um das IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) findet auch vor dem Hintergrund einer umfassenden Novellierung des Telekommunikationsgesetzes (TKMoG) sowie weiterer gesetzlicher und untergesetzlicher Regelungen zur Festlegung von Sicherheitsanforderungen, Auskunfts- und Meldepflichten, Zertifizierungsvorgaben sowie Garantieerklärungen über Vertrauenswürdigkeit, statt. Diese zusätzlichen Regelungen erzeugen neben massivem personellen und sachlichen Aufwand für Unternehmen an dortiger Stelle ebenfalls Wechselwirkungen mit dem hier diskutierten Entwurf des IT-SiG 2.0, das aus diesem Grund nicht völlig losgelöst davon betrachtet werden kann. Darüber hinaus wird auf europäischer Ebene derzeit die NIS-Richtlinie evaluiert und es wurde eine Überarbeitung der Richtlinie für das Jahr 2021 in Aussicht gestellt.

eco – Verband der Internetwirtschaft e.V. sieht in dem nun vorliegenden Diskussionsentwurf zahlreiche Aspekte, die problematisch sind. Durch die Regelungen, die das geplante IT-SiG 2.0 vorsieht, werden erhebliche Eingriffe in Netze und Netzinfrastrukturen vorgenommen. Darüber hinaus unterbleiben dringend nötige Anpassungen in der IT-Sicherheitsarchitektur. Unklar sind zudem Wechselwirkungen mit anderen Politikbereichen wie bspw. der Verbraucherschutzpolitik, die das Regulierungsgefüge des IT-SiG 2.0 auseinanderfallen lassen. Im Einzelnen kommentiert eco folgende Aspekte im Diskussionsentwurf für ein IT-SiG 2.0.

Zu Artikel 1 Nr. 1 f

Die neu in das BSI-Gesetz § 2 angefügten Absätze 13 und 14 sollen den Rechtsrahmen für den Einsatz so genannter „kritischer Komponenten“ näher bestimmen. Positiv hervorzuheben ist das Bestreben der Bundesregierung, dass kritische Komponenten im Bereich der Software und der Informationstechnik gesetzlich definiert werden sollen. Dem steht der Katalog von Sicherheitsanforderungen gem. § 109 des Telekommunikationsgesetzes (TKG) gegenüber, der eine vorgesetzliche Regelung darstellt. Hier wäre ein höheres Maß an Kohärenz bei den Regelungen grundsätzlich begrüßenswert gewesen. Allgemein merkt eco hierzu an, dass auch im Rahmen der weiteren Gesetze zur näheren Bestimmung kritischer Komponenten darauf geachtet werden muss, dass keine Doppelregulierung entsteht.

Die in Absatz 14 näher umrissenen Unternehmen von besonderem öffentlichen Interesse sollen nach Ansicht des Gesetzgebers ebenfalls näher beschrieben werden. Als hilfreich ist es zu bewerten, dass hierzu Kriterien und Faktoren genannt und berücksichtigt werden sollen, die eine Methodik bei der Definition entsprechender Unternehmen ermöglicht.

Allerdings sollte die vorgesehene Möglichkeit, solche Unternehmen von besonderem öffentlichen Interesse zu bestimmen, strikt der geplanten Methodik folgen und keinesfalls zu einer stetigen Ausweitung des entsprechenden Bereichs führen, so dass der Adressatenkreis dieser Norm überschaubar bleibt.

Nach Ansicht des eco ist es problematisch, dass durch die geplante Erweiterung der IT-Sicherheitsregulierung auf Unternehmen von besonderem öffentlichen Interesse und der damit verbundenen faktischen Ausweitung des bislang klar eingegrenzten KRITIS Bereichs eine Vielzahl von Unternehmen, die bislang nicht als Betreiber kritischer Infrastrukturen eingestuft waren, mit den geplanten Regelungen zukünftig erhöhten Anforderungen im Bereich der IT-Sicherheit auf dem Niveau kritischer Infrastrukturen unterliegen werden. Dienstleister und Zulieferbetriebe dieser Unternehmen von besonderem öffentlichen Interesse werden zukünftig aller Voraussicht nach entsprechend Nachweis über ihre IT-Sicherheit zu erbringen und ggf. zertifiziert werden müssen. Für den Bereich der Telekommunikation ist hier eine Ausweitung der KRITIS-Maßgaben für den gesamten Sektor zu erwarten.

Grundsätzlich möchte eco drauf hinweisen, dass durch das komplexe Zusammenspiel der verschiedenen Regelungen und Anforderungen im Bereich der IT-Sicherheit zunehmend Unklarheit über das bereits bestehende und das noch zu erwartende Regulierungsgefüge entsteht. Eine Doppelregulierung aufgrund verschiedener Sicherheitsregime oder bereichsspezifischen Regelungen bspw. im Telekommunikationsgesetz sollte in jedem Fall vermieden werden.

Zu Artikel 1 Nr. 2 g

Das in Punkt 20 angeführte Vorrecht des BSI, einen Stand der Technik zu definieren sollte vor dem Hintergrund, dass das BSI eine nachgelagerte Sicherheitsbehörde des Bundesministeriums des Innern, für Bau und Heimat ist und daher diesem gegenüber weisungsgebunden, kritisch hinterfragt werden. Insbesondere, wenn man in berücksichtigt, dass weitere Sicherheitsbehörden und Stellen im Geschäftsbereich des BMI, namentlich die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) und das Bundesamt für Verfassungsschutz (BfV), zu möglichen Ziel- und Interessenskonflikten führen können. eco plädiert dafür, dass für die Definition eines Standes der Technik die Einbeziehung betroffener Kreise dementsprechend zwingend gesetzlich vorgeschrieben wird.

Zu Artikel 1 Nr. 7

Die im vorliegenden Diskussionsentwurf vorgeschlagene Regelung der Bestandsdatenauskunft für das BSI ist vor dem Hintergrund des Urteils des Bundesverfassungsgerichts vom 27.05.2020 (1 BvR 1873/13) für die zur Auskunft verpflichteten Unternehmen problematisch. Denn sie stellt die Unternehmen vor die Frage, ob sie bei Befolgen der Anforderungen zur Datenbeauskunftung an das BSI gegen das Grundgesetz verstoßen und damit rechtswidrig handeln. Solange keine grundgesetzkonforme Neufassung von § 113 TKG beschlossen und verkündet wurde, sperren die Vorgaben des BVerfG eine Anknüpfung des 5c BSIG-E als neue Abrufregelung i.V.m. § 113 TKG. Die Vorschrift des § 113 TKG ist unvereinbar mit dem Grundgesetz und darf höchstens bis 31.12.2021 angewandt werden. Die neue Abrufregelung des § 5c BSIG-E wäre ein erneuter Verfassungsbruch, und ist nicht gedeckt von der nur ausnahmsweise weiteren Anwendung der Bestehenden, welche das BVerfG zugelassen hat. Ein erster Schritt zur Beseitigung der verfassungswidrigen Rechtslage wurde seitens des Gesetzgebers unternommen und das BMI hat am 24.11.2020 einen eigenen Entwurf hierzu veröffentlicht und zur Konsultation gestellt. eco hat dazu gesondert Stellung genommen.

Unbeschadet von der grundsätzlichen Kritik und den verfassungsrechtlichen Bedenken an der vorgeschlagenen Regelung sollte in jedem Fall eine angemessene Entschädigungsregelung für Bestandsdatenauskünfte einbezogen werden, da diese sich in der Vergangenheit als moderierend auf etwaige Anfragen erwiesen haben, so dass sich die zu erteilenden Auskünfte auf das zwingend notwendige Maß beschränken.

Zu Artikel 1 Nr. 8 b

Die Überarbeitung des § 7 des BSI-Gesetzes wirft ein Schlaglicht auf eine zentrale Debatte um das IT-SiG 2.0. Der Umgang mit Informationen über Sicherheitslücken gegenüber betroffenen Unternehmen. Das Gesetz sieht hier unter anderem vor, dass das BSI dazu verpflichtet werden kann, eine Information an die Hersteller zurückzuhalten, sofern das Bundesamt Dritten gegenüber zur Vertraulichkeit verpflichtet ist. Die Gesetzesbegründung legt darüber hinaus dar, dass damit die Interessen von Sicherheitsbehörden über die bestehenden Informationen gemeint sind. Nach Ansicht des eco stellt diese Einschränkung eine erhebliche strukturelle Schwächung der IT-Sicherheit insgesamt dar, die die Vertrauenswürdigkeit des BSI nachhaltig untergräbt. eco fordert daher nachdrücklich eine Streichung dieses Grundes. eco plädiert dafür, dass Sicherheitslücken immer schnellstmöglich geschlossen werden sollten, um eine Gefährdung weiterer Systeme zu vermeiden. Hierfür müssen entsprechende Informationen durch das BSI schnell an die jeweiligen Unternehmen weitergereicht werden. Ein Zurückhalten der Informationen würde diesem Ziel schaden.

Zu Artikel 1 Nr. 9

Die Neufassung des § 7a des BSI-Gesetzes stellt nach Auffassung des eco ein Problem dar, da das für das BSI in § 7a (2)-neu eingeführte Auskunftsverlangen zu weit gefasst ist. Es sollte klargestellt sein, dass Geschäftsgeheimnisse – insbesondere solche mit Bezug auf kryptographische Verfahren – geschützt und keinesfalls weitergereicht werden dürfen. Es ist in jedem Fall sicherzustellen, dass keine sicherheitsrelevanten Informationen auf dem Wege des Auskunftsverlangens i.V.m. § 7a (4)-neu an Sicherheitsbehörden übermittelt werden können, um dort für andere Zwecke eingesetzt zu werden. Darüber hinaus sollte klargestellt sein, dass dementsprechend das Unternehmen, das Ziel einer solchen Anfrage geworden ist, ebenfalls über die in § 7a (3)-neu gewonnen Erkenntnisse zu unterrichten ist.

Zu Artikel 1 Nr. 10

Der neu ins BSI-Gesetz eingeführte § 7b ermöglicht es dem BSI, selbst proaktiv in den öffentlichen Telekommunikationsnetzen nach Sicherheitsrisiken zu suchen. eco erachtet dieses Vorgehen als problematisch. Zum einen sind die tatsächlich durchgeführten Maßnahmen, die das BSI anführt sehr unkonkret. Zum anderen werden als Beispiel für entsprechende Detektionsmaßnahmen so genannte Portscans angeführt, die IT-Systeme unter Umständen beeinträchtigen können und darüber hinaus auch unter strafrechtlichen Aspekten problematisch sein können. Dass das

BSI auch Angriffe vortäuschen darf, sieht eco in diesem Rahmen ebenfalls als problematisch an. Grundsätzlich sollte das BSI bei der Durchführung entsprechender Maßnahmen die Netzbetreiber in geeigneter Weise frühzeitig in Kenntnis setzen, damit mögliche Beeinträchtigungen der Infrastrukturen ausgeschlossen oder zumindest minimiert werden, und um bei Problemen auf Nutzerseite letztere an das Amt weiterverweisen zu können.

Der neu ins BSI-Gesetz eingeführte § 7c sieht eine Anordnungsbefugnis des BSI für die Bekämpfung von Störungen vor. Die hier dargelegten Maßnahmen sind dabei nicht an Vorbedingungen geknüpft, wie etwa die Feststellung der Verletzung gesetzlicher Pflichten der Betreiber. Aus Sicht des eco bedarf es jedoch neben der Störung und Gefährdungslage eines Anordnungsgrundes, um die Anordnungskompetenz des BSI verhältnismäßig auszuüben. Allgemein ist davon auszugehen, dass Betreiber aufgrund ihrer Expertise und Erfahrungen in der Lage sind, Krisensituationen ohne Einschreiten der Aufsichtsbehörde zu bewältigen. Eingriffe in unternehmerische Belange sind daher nur auf Vorfälle zu begrenzen, die sich an klaren Aufgreifschwellen oder Ereignissen orientieren. Zudem muss dringend klargestellt werden, dass bei der Umsetzung einer Anordnung durch das BSI die Betreiber der Infrastrukturen von etwaiger Haftung freizustellen sind. Zudem ist festzuhalten, dass die Möglichkeit zur Anordnung der Umleitung von Verkehren an eine vom BSI benannte Adresse gem. § 7c (3)-neu BSI-Gesetz aus Sicht der Internetwirtschaft zu unpräzise formuliert ist. Die Möglichkeit der Anordnung einer Umleitung von Datenverkehr eines Nutzers muss eindeutig hinsichtlich des Grundes und Zweckes definiert sein. Dabei müssen zwingend auch klare Vorgaben in Bezug auf den Umgang und die Verwendung der umgeleiteten Daten beachtet werden. Hierzu gehört auch, dass eine Verwendung für andere Zwecke als die in § 109a (5) TKG vorgesehenen ausgeschlossen ist.

Zuletzt ist bei der Umsetzung des § 7d-neu BSI-Gesetz darauf zu achten, dass durch die Anordnungen nicht andere Grundrechte, wie bspw. die Pressefreiheit eingeschränkt werden. Auch sollte bei der Anwendung von §7d-neu BSI Gesetz der § 13 Abs. 7 des TMG berücksichtigt werden und sichergestellt sein, dass es die Maßnahmen des BSI wirtschaftlich zumutbar sind.

Zu Artikel 1 Nr. 12

Die mit dem Diskussionsentwurf vorgesehene Ausweitung von Verpflichtungen für Anbieter und Betreiber kritischer Infrastrukturen zur Erkennung von Angriffen nach § 8a-neu BSI-Gesetz ist aus der Sicht von eco nachvollziehbar. Problematisch hingegen sieht eco, dass die

Verpflichtung zur Implementierung dieser Systeme zu unkonkret ist. Eine solche Verpflichtung kann sich technisch gesehen in der Regel nur auf den Schutz und die Integrität der eigenen Systeme beschränken und sich nicht auf die Systeme von Anwenderinnen und Nutzern erstrecken.

Kritisch sieht eco auch die Verpflichtung, nicht-personenbezogene Daten für mindestens vier Jahre zu speichern, wenn sie mit der Angriffserkennung zusammenhängen. Zum einen wird die datenschutzrechtliche gebotene und DSGVO-konforme Trennung von personenbezogenen und nicht personenbezogenen Daten einen erheblichen Mehraufwand darstellen. Darüber hinaus wird eine solche Datenbank unweigerlich vor der Problematik stehen, durch Kombination oder Mustererkennung eine de-Anonymisierung theoretisch zu ermöglichen, so dass dem Datenschutzgedanken und dem Schutz der Grundrechte hier nicht hinreichend Bedeutung beigemessen wird. Zuletzt sei angemerkt, dass die Speicherung dieser Daten aller Voraussicht nach zu enormen Datenbeständen führen, die – entsprechend gesichert – eine erhebliche wirtschaftliche Belastung von Unternehmen darstellen werden.

Zu Artikel 1 Nr. 17

Die gesetzgeberischen Bestrebungen, ein funktionsfähiges IT-Sicherheitsregime über möglichst große Teile der Wirtschaft auszurollen, ist nachvollziehbar. Die Definition von Unternehmen in besonderem öffentlichen Interesse ist dementsprechend ebenfalls nachvollziehbar unter Berücksichtigung und Einbeziehung der Anmerkungen, die eco zu Artikel 1 Abs. 1 f gemacht hatte. Die Vorgabe, Sicherheitskonzepte alle zwei Jahre zu aktualisieren und vorzulegen wie in dem Diskussionsentwurf in § 8f (4)-neu BSI-Gesetz vorgesehen stellt insbesondere für Betreiber kritischer Infrastrukturen, die zusätzlich alle zwei Jahre ihre Konformität mit den geltenden Sicherheitsanforderungen nachweisen müssen (vgl. § 8a (3)-neu BSI-Gesetz), einen zusätzlichen administrativen Aufwand dar. Diesem Aufwand steht aus der Sicht von eco kein tatsächlicher Nutzen gegenüber.

Zu Artikel 1 Nr. 18

Der aus § 9 (4)-alt BSI Gesetz abgeleitete § 9 (4a) soll klarstellen, dass das Bundesministerium des Innern die Erteilung eines Zertifikats untersagen kann. Nach Ansicht des eco wäre es hier wünschenswert, wenn neben der Untersagung auch die Gründe für die Versagung ausführlich dargelegt werden müssen, damit die Unternehmen nicht nur mit der Verweigerung des Zertifikats konfrontiert sind, sondern auch tatsächlich Abhilfe schaffen können.

Zu Artikel 1 Nr. 19

Der neu eingefügte § 9a-neu BSI Gesetz regelt die Struktur der Zertifizierung und stellt klar, dass das BSI als Zertifikatevergeber fungiert, während entsprechende unabhängige Stellen die Bewertung der Konformität mit den BSI-Vorgaben vornehmen. eco befürwortet diesen marktlichen Ansatz bei der Zertifikatevergabe ausdrücklich. Gleichwohl bleiben Fragen an die Zertifizierung und Konformitätsbewertung, die im weiteren Verlauf der Debatte gelöst werden müssen. Hierzu gehören insbesondere Fragen nach dem Umgang mit quelloffener Software bzw. quelloffenen Softwarekomponenten (Open Source) und automatisiert angepasster Software und selbst entwickelter Software.

Sehr problematisch ist der neu ins BSI-Gesetz eingefügte § 9b-neu. Dieser gibt vor, dass der Einsatz kritischer Komponenten dem BSI gegenüber durch die Betreiber kritischer Infrastrukturen anzuzeigen ist. Die Regelung ist – anders als die übrigen Regelungen im geplanten IT-SiG 2.0 – ohne eine entsprechende Übergangsfrist und stellt daher für Unternehmen eine deutliche Anpassungshürde an das neue IT-Sicherheitsregime dar. Darüber hinaus steht zur Debatte, dass die vorgesehene Regelung eine Allgemeinverfügung des BMI für die Abgabe von Garantierklärungen vorsieht, die in dieser Form nicht dem sonst üblichen Vorgehen wie bspw. bei § 109 TKG entspricht. Eine Anhörung betroffener Kreise und Verbände hält eco bei einem so sensiblen Thema mit entsprechend weitreichenden Konsequenzen für dringend angebracht. Die im Diskussionsentwurf vorgelegte Regelung zur Abgabe von Garantieerklärungen lehnt er ab. Auch die Untersagung des Einsatzes kritischer Komponenten gem. § 9b (3)-neu des BSI-Gesetzes sieht eco in diesem Zusammenhang kritisch. Der Möglichkeit zur Untersagung fehlt es an Transparenz und Nachvollziehbarkeit. Es ist nicht nachvollziehbar, welche Ressorts in welchen Fällen mit einzubeziehen sind und welche Aspekte zu einer Untersagung des Einsatzes führen. Umgekehrt ist davon auszugehen, dass diese Regelung zu Investitionshemmnissen und Einschnitten beim Ausbau digitaler Infrastrukturen führen wird. Vor diesem Hintergrund ist auch die Regelung in § 9b (6)-neu zur Ausweitung des Einsatzes kritischer Komponenten auf weitere Komponenten desselben Herstellers als zu weitgehend und zu unkonkret abzulehnen. Aus der Formulierung im Tatbestand geht weiter nicht hervor, welche Ressorts unter welchen Voraussetzungen jeweils konkret zu beteiligen sind.

Unklar ist bei diesen Regelungen zudem, wie die Vertrauenswürdigkeit gem. § 9b (2)-neu BSI Gesetz in der Praxis tatsächlich nachzuweisen ist oder inwieweit hier generell Probleme in IT-Lieferketten für bestimmte Bauteile zementiert werden, ohne, dass sich dadurch eine Lösung im Markt finden lässt. Es ist davon auszugehen, dass entsprechende Garantien bzw. Erklärungen von Lieferanten, sofern diese tatsächlich durch einen anderen

Staat zur Implementierung entsprechender Sicherheitslücken verpflichtet sein sollten, nicht eingeholt werden können bzw. die Erklärungen wertlos sind, da diese im Zweifelsfall entsprechende Sicherheitslücken gerade deshalb nicht offenbaren dürfen. Letztlich sollten die Betreiber im Falle einer nachträglichen und aufgrund späterer Erkenntnisse erfolgten Untersagung des Einsatzes von Komponenten aufgrund des damit verbundenen Eingriffs in das Eigentumsrecht entschädigt werden. Vor diesem Hintergrund wäre eine entsprechende Ausgleichsregelung für die von der Untersagung betroffenen Unternehmen dringend zusammen mit dem IT-SiG 2.0 auf den Weg zu bringen.

Zu Artikel 2

In Anbetracht der Tatsache, dass die Beratungen zum TKMoG derzeit noch nicht abgeschlossen sind, ist es schwierig, eine vollständige Einschätzung zu den geplanten Änderungen im TKG vorzunehmen. Mehrere Aspekte in dem Gesetzesvorhaben verweisen auf das BSI-Gesetz und auf Regelungen, die auch im IT-SiG 2.0 ihre Wirkung entfalten wie bspw. der § 162 und § 164 TKMoG-Entwurf. Die dort getroffenen Regelungen könnten unter Umständen dazu führen, dass der hier im IT-SiG 2.0 geregelte Parlamentsvorbehalt, den Einsatz kritischer Komponenten jeweils gesetzlich zu regeln, untergraben wird. Konkret geht es dabei um die elementaren Fragestellungen, welche Maßgaben für kritische Komponenten gelten sollen und was unter einem Telekommunikationsnetz mit erhöhtem Gefährdungspotential zu verstehen ist. Grundsätzlich wäre es begrüßenswert, den Adressatenkreis der Norm zu konkretisieren. Die Möglichkeit, besonders strikte Sicherheitsanforderungen, die derzeit nur für 5G-Mobilfunkanbieter gelten, ohne parlamentarische Kontrolle auf alle Anbieter von Telekommunikation auszudehnen, wirft die Frage nach der Verhältnismäßigkeit und damit auch nach der Verfassungskonformität der hier vorgeschlagenen Regelungen auf.

Auch ist die Möglichkeit der doppelten Prüfung einerseits auf Anordnung der BNetzA durch eine qualifizierte unabhängige Stelle oder durch das BSI nach § 162 (8) 1 TKMoG-Entwurf und andererseits durch die BNetzA selbst gem. § 163 (4) und 163 (5) nicht erforderlich und unverhältnismäßig. Dies gilt erst recht für die zwingend vorgesehene Prüfung der Netzbetreiber mit erhöhtem Gefährdungspotenzial. Bei den entsprechenden Auflagen im IT-SiG 2.0 ist dies zu berücksichtigen, um Doppelregulierung zu vermeiden.

Zu Artikel 3 Nr. 1

Die vorgeschlagene Änderung im Telemediengesetz sieht eine neue Meldepflicht für Betreiber von Telemediendiensten vor. Konkret erfasst werden dadurch die Straftatbestände der §§ 202a bis 202d des

Strafgesetzbuches. Nach Auffassung des eco ist die Notwendigkeit einer Meldepflicht nicht ausreichend dargelegt, insbesondere, da durch die Übermittlung auch personenbezogene Daten dem BKA mitgeteilt werden sollen. Die Anforderungen und Voraussetzungen der Meldepflicht, neben der Annahme des Vorliegens einer Straftat nach §§ 202a bis 202d StGB, wie „der Abfluss eines Datenbestands von großem Ausmaß“, sind aus der Sicht von eco nicht präzise genug, um proaktive Meldepflichten gegenüber den Betreibern von Telemediendiensten zu rechtfertigen. Die darüber hinaus nach § 15d TMG-E geforderte Schnittstelle zur Ausleitung entsprechender Informationen bei mehr als 100.000 Kunden ist zudem mit Blick auf die Vielzahl unterschiedlicher Telemediendienste sehr unpräzise und ungeeignet und dürfte – je nach Szenario – eine große Menge an Anbietern betreffen. Fraglich ist auch, inwieweit sich eine solche Schnittstelle technisch überhaupt in den jeweiligen Dienst integrieren lässt.

Zu Artikel 5

Die vorgesehene Schaffung einer Nr. (2) des § 55 Abs. 1 der Außenwirtschaftsverordnung i. V. m. § 2 (13) BSIG-E verletzt nach Ansicht des eco den Parlamentsvorbehalt. Über § 2 (13) i. V. m. § 109 (8) TKMoG-Entwurf sollen kritische Komponenten für den Bereich der Telekommunikation im Sicherheitskatalog festgelegt werden. Demgegenüber soll in allen anderen Branchen diese Festlegung vom Gesetzgeber und im Rahmen einer gesetzlichen Regelung erfolgen. Aus der Begründung wird diese Ungleichbehandlung nicht nachvollziehbar erläutert und verwehrt der betroffenen Branche somit die Gelegenheit, eine angemessene parlamentarische Debatte über diese Themen führen zu können.

Fazit

Gut über ein Jahr, nachdem der erste Entwurf des IT-Sicherheitsgesetzes inoffiziell an die Öffentlichkeit gelangt ist und von eco scharf kritisiert wurde, liegt nunmehr ein neuer Diskussionsentwurf vor. Es ist erkennbar, dass zahlreiche Aspekte im Laufe der Beratungen nachgebessert und klargestellt wurden, so dass der nun vorliegende Entwurf eine deutlich höhere Qualität aufweist, als die zuvor bekannt gewordenen. Gleichzeitig weist auch dieser Entwurf zahlreiche Aspekte auf, die aus der Sicht von eco nach wie vor grundlegende Kritikpunkte darstellen.

Damit IT-Sicherheit in Deutschland effektiv reguliert wird und sich in im europäischen digitalen Binnenmarkt sinnvoll weiterentwickeln und gestärkt werden kann, müssen diese Probleme adressiert und gelöst werden. An erster Stelle wäre hier die Harmonisierung der Überlegungen des Bundesinnenministeriums mit den Plänen der europäischen Kommission zur

Novelle der NIS-Richtlinie zu nennen. Eine vorschnelle nationale Regulierung könnte das Risiko in sich bergen, anschließend noch einmal gesetzgeberisch tätig werden zu müssen und durch erneute nationale gesetzliche Anpassungen eine Harmonisierung mit den europäischen Regeln anzustreben. Für Unternehmen sind diese Nachbesserungen oft mit zusätzlichen Kosten verbunden, um bereits implementierte Systeme und Lösungen nochmals anzupassen. Insbesondere die Klarstellung der Rolle des BSI als nationale Oberbehörde für IT-Sicherheit – losgelöst von Weisungspflichten und u.U. im Interessengeflecht von Sicherheitsbehörden gefangen – sollte dabei oberste Priorität genießen. Auch sollten die Möglichkeiten für den Einsatz von kritischen Komponenten bzw. deren Untersagung möglichst europäisch adressiert und behandelt werden. Nationale Sonderregelungen sollten ausschließlich für eng umgrenzte Bereiche mit klaren gesetzlichen Definitionen vorgesehen werden. Neue Befugnisse für das BSI müssen, vor dem Hintergrund dessen unklarer Funktion im IT-Sicherheitsgefüge und der deutschen Sicherheitsarchitektur, enge und konkrete Grenzen gesetzt werden. Die an verschiedenen Stellen vorgesehenen Maßnahmen sollten für einen jeweils konkret umgrenzten und eindeutig definierten Adressatenkreis gelten sowie klar festgelegte Aufgreifschwellen haben. Anderenfalls steht zu befürchten, dass unpräzise Regelungen bei Unternehmen zu Rechtsunsicherheit führen.

Grundsätzlich sollte insbesondere auch IT-Anbietern, Netzbetreibern und Anbietern von Telemediendiensten mehr Vertrauen in ihre IT-Kompetenz zugestanden werden. Auch Nutzerinnen und Nutzer sind in diese Überlegungen mit einzubeziehen und deren Bewusstsein für IT-Sicherheit ist zu stärken. Nach Ansicht des eco sollten diese Probleme im weiteren Gesetzgebungsverfahren behoben werden können, so dass für Deutschland ein sinnvoller nationaler IT-Sicherheitsrahmen geschaffen wird, der sich gut in die europäische IT-Sicherheitsregulierung einfügt.

Über eco

Mit über 1.100 Mitgliedsunternehmen ist eco der größte Verband der Internetwirtschaft in Europa. Seit 1995 gestaltet eco maßgeblich das Internet, fördert neue Technologien, schafft Rahmenbedingungen und vertritt die Interessen seiner Mitglieder gegenüber der Politik und in internationalen Gremien. Die Zuverlässigkeit und Stärkung der digitalen Infrastruktur, IT-Sicherheit und Vertrauen sowie eine ethisch orientierte Digitalisierung bilden Schwerpunkte der Verbandsarbeit. eco setzt sich für ein freies, technikneutrales und leistungsstarkes Internet ein.