INITIATIVE EUROPÄISCHER NETZBETREIBER

IEN · Marienstr. 30 · 10117 Berlin

Per Email an:

Das Bundesministerium des Innern, für Bau und Heimat
CI1@bmi.bund.de

Berlin, 09.12.2020

Entwurf eines Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0)

Stellungnahme der Initiative Europäischer Netzbetreiber

Sehr geehrte Damen und Herren,

das Bundesministerium des Innern, für Bau und Heimat hat am 02.12.2020 den o.g. Diskussionsentwurf des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (Zweites IT-Sicherheitsgesetz – IT-SiG 2.0) veröffentlicht und zur Konsultation gestellt.

Im dazugehörigen Begleittext wurde darauf hingewiesen, dass zu mehreren Themen des Gesetzentwurfs innerhalb der Bundesregierung jedoch bislang noch keine Einigkeit erzielt wurde. Es bestehe noch deutlicher Diskussions- und Anpassungsbedarf und es sei daher davon auszugehen, dass im Laufe der Ressortabstimmung - gegebenenfalls auch deutliche - materielle Veränderungen am Gesetzentwurf auch in bisher nicht adressierten Teilen erfolgen werden.

Dessen ungeachtet wurde die Anhörung jedoch schon zum gegenwärtigen Zeitpunkt mit Frist zur Stellungnahme bis zum 09.12.2020 eingeleitet.

Obgleich die IEN grundsätzlich, wie bereits in der Vergangenheit, eine möglichst schon frühzeitige Beteiligung des Marktes an der Erarbeitung eines Gesetzentwurfs begrüßt, so ist das gegenständliche Vorgehen aus unserer Sicht doch als kritisch zu bewerten.

Eine detaillierte Durchsicht, Abstimmung und Kommentierung eines „Diskussionsentwurfs“ in gerade einmal einer Woche – welcher ausdrücklich noch erhebliche Änderungen erfahren kann - ist als unverhältnismäßig anzusehen. Es fehlt bislang die Klarstellung oder Inaussichtstellung einer wei-

…

teren Anhörungsrunde zum offiziellen Referentenentwurf mit entsprechend angemessener Kommentierungsfrist. Die IEN fordert nachdrücklich die Durchführung eines offiziellen Anhörungsverfahrens mit mindestens vier- bis sechswöchiger Kommentierungsfrist zum Referentenentwurf. Da nicht zu erwarten steht, dass das Gesetzgebungsverfahren noch in diesem Jahr abgeschlossen werden kann, dürfte der Zeitrahmen für ein ordnungsgemäßes Anhörungsverfahren nicht ins Gewicht fallen. Diverse zentrale Punkte der hier erfolgten, weitreichenden Änderung der Regulierung, auch für die TK-Branche, bedürfen einer detaillierten Prüfung und Abstimmung.

Andernfalls ließe das Prozedere erhebliche Zweifel an einem echten Interesse an der Auffassung von Ländern und Branche am Gesetzentwurf aufkommen. Von einer tatsächlichen Beteiligung des Marktes an der Erstellung des ITSiG 2.0 kann jedenfalls unter diesen Umständen nicht ausgegangen werden.

Planungen zufolge intendiert die Bundesregierung, den derzeit noch umstrittenen Gesetzesentwurf zusammen mit anderen wichtigen Vorhaben wie der TKG-Novelle noch in der letzten Kabinettssitzung vor Weihnachten am 16.12.2020 zu beschließen. Diese überstürzte Handlung wäre jedoch für sämtliche Marktbeteiligten fatal. Gerade in einem Land mit erheblicher wirtschaftlicher Relevanz wie Deutschland, sollte ein Gesetzgebungsverfahren von derartiger Relevanz nicht „übers Knie“ gebrochen werden. Die IEN-Mitgliedsunternehmen, die allesamt pan-europäisch ihre Dienstleistungen erbringen und deren Mutterorganisationen häufig im Ausland ihren Sitz haben, sehen sich angesichts dieses Prozederes erheblichen Nachfragen der Muttergesellschaften ausgesetzt, da Vergleichbares in anderen europäischen Mitgliedstaaten nicht stattfindet.

Schließlich gilt auch vor dem Hintergrund der gegenwärtigen Covid-19 Pandemie, in welcher sich die TK-Branche stärker denn je als das zuverlässige Rückgrat für die Wirtschaft, aber insbesondere auch für die Arbeit von Behörden und der Politik erwiesen hat, ist es zwingend erforderlich, neue regulatorische Maßnahmen auch unter Einbeziehung der jüngsten Entwicklungen und Marktgegebenheiten sorgfältig und nachhaltig zu bewerten.

Dies vorangestellt kommentiert die IEN den Diskussionsentwurf in der möglichen Kürze der Frist wie folgt:

I. Allgemeine Anmerkungen

Mit dem gegenständlichen Diskussionsentwurf soll der im bislang geltenden ITSiG vom 17.07.2015 geschaffene Ordnungsrahmen erweitert werden. Der aktuelle Entwurf basiert auf der dritten Entwurfsfassung vom

01.12.2020 und greift neben den Regelungen, die schon 2015 mit dem ersten ITSiG getroffen wurden, neue technologische und gesellschaftspolitische Entwicklung bei der Nutzung und Vernetzung von IT-Systemen auf.

Unter anderem soll das Bundesamt für Sicherheit in der Informationstechnik (BSI) befugt werden, Kontroll- und Prüfbefugnisse gegenüber der gesamten Bundesverwaltung auszuüben, indem es Informationen über das aktuelle Sicherheitsniveau der überprüften Stelle des Bundes verlangen kann. Außerdem wird der Verbraucherschutz in den Aufgabenkatalog des BSI aufgenommen. Darüber hinaus erhält das BSI die Befugnis zur Untersuchung von IT-Produkten in erheblich erweiterter Form. Hersteller sollen zur Auskunft über ihre Produkte verpflichtet werden. Ferner soll das BSI befugt werden, Sicherheitslücken an den Schnittstellen informationstechnischer Systeme zu öffentlichen TK-Netzen zu detektieren (Portscans) sowie Systeme und Verfahren zur Analyse von Schadprogrammen und Angriffsmethoden einzusetzen (Honeypots). Im Übrigen enthält der Entwurf eine Regelung zur Untersagung des Einsatzes kritischer Komponenten, für die eine Zertifizierungspflicht besteht.

Dabei wurde zu diversen - für eine umfassende Kommentierung jedoch erheblichen - Aspekten innerhalb der Bundesregierung noch keine Einigkeit erzielt und es besteht noch Diskussions- und Anpassungsbedarf.

Die IEN als Verband international tätiger Anbieter von grenzüberschreitendenden Telekommunikationsdienstleistungen für große Unternehmenskunden und Behörden setzt sich bereits seit vielen Jahren für möglichst weitgehende Harmonisierung, insbesondere bei der Identifikation kritischer Infrastrukturen und Komponenten bei gleichzeitiger Berücksichtigung der hohen Anforderungen, welche die Kunden der IEN-Mitgliedsunternehmen an die Dienstleister stellen, ein. Die IEN-Mitgliedsunternehmen haben bereits aufgrund ihres eigenen Geschäftsfokus ein erhebliches Interesse an der Sicherheit ihrer Infrastrukturen und räumen diesem Aspekt im Rahmen ihrer Aktivitäten und Strategien einen erheblichen Stellenwert ein. Da ihre Dienstleistungen überwiegend grenzüberschreitend stattfinden, haben diese Unternehmen zudem insbesondere auch ein erhebliches Interesse daran, dass die internen Sicherheitsprozesse möglichst zentralisiert und länderübergreifend einheitlich durchgeführt werden und dass entsprechende regulatorische Vorgaben diesen Ansatz unterstützen.

Dies dient zudem auch dem Ziel der Erreichung größtmöglicher Harmonisierung im Binnenmarkt, welches erheblich beeinträchtigt würde, wenn die

Mitgliedstaaten jeweils unterschiedliche Kriterien bei Identifikation der kritischen Infrastrukturen zugrunde legen würden. Dies kann aus Sicht der IEN nur durch ein effektives, transparentes und zentralisiertes Gesamtkonzept erreicht werden, welches gerade nicht nur Verpflichtungen für Netzbetreiber vorsieht, sondern als Ende-zu-Ende Konzept auch andere betroffene Marktbeteiligte und regulatorische Vorgaben mitberücksichtigt.

Gerade vor dem Hintergrund, dass sich die betreffenden TK-Infrastrukturanbieter, deren Dienstleistungen überwiegend grenzüberschreitend erbracht werden, im Fall der Festlegung von nationalen Einzelregelungen häufig unterschiedlichen Vorgaben für ein und dieselbe Dienstleistung für ein und denselben Kunden gegenübersehen. Deren Erfüllung dürfte häufig wegen konträrer Vorgaben, etwa zur Art der Meldung oder Schnittstelle, überhaupt nicht rechtskonform möglich sein, obgleich die TK-Unternehmen sich rechtstreu verhalten wollen und erheblichen Wert auf die Sicherheit ihrer Infrastrukturen legen. Es ist essenziell, dass die im gegenständlichen Entwurf gemachten Verpflichtungen, etwa hinsichtlich Zertifizierungen und Auskunftserteilungen, keine Vorgaben machen, welche in anderen europäischen Ländern anders, oder gar konträr geregelt sind. Marktbeteiligte dürfen durch nationale Vorgaben nicht gezwungen werden, sich gegenüber einem anderen EU-Mitgliedstaat möglicherweise rechtswidrig zu verhalten.

Aus Sicht der IEN besteht weiterhin Bedarf, europaweit einheitliche Mindestregelungen, welche insbesondere auch internationalen Standards entsprechen, für die betroffenen Unternehmen in den Mitgliedstaaten unter der Beteiligung von ENISA festzulegen, um in der Branche verstärkt für harmonisierte Rechts- und Planungssicherheit zu sorgen.

II. Im Einzelnen

1. Zu § 2 Absatz 14 BSIG-E in Verbindung mit §§ 2 Absatz 3 Satz 2, 8, 8f und 10 Absatz 5 BSIG-E „Unternehmen im besonderen öffentlichen Interesse“

Die politischen Forderungen der Einbeziehung von Unternehmen in den Regelungsbereich des ITSIG, die zwar keine „kritischen Infrastrukturen“ als solche darstellen, bei denen ein Ausfall jedoch erhebliche volkswirtschaftliche Beeinträchtigungen zur Folge haben, existieren bereits seit einiger Zeit. Im gegenständlichen Entwurf erfolgte nunmehr die Einbeziehung von „Unternehmen im besonderen öffentlichen Interesse“.

Dies ist aus Sicht der IEN zu kritisieren, da keine genaue Abgrenzung zu anderen, möglichen Adressaten erreicht wird. Zunächst bleibt unklar, nach welchen Kriterien die „erhebliche volkswirtschaftliche Bedeutung“ bewertet wird. Darüber hinaus bleibt unklar, in welchem Verhältnis diese Unternehmen zu den „Institutionen im besonderen staatlichen Interesse" (INSI) nach den Vorgaben des BSI[1] oder zu den „Unternehmen im besonderen öffentlichen Interesse" nach § 8f BSIG-E stehen. Auch die EU NIS-Richtlinie oder das entsprechende Umsetzungsgesetz[2] geben über die Abgrenzung keinen klaren Aufschluss. Derartige Ungenauigkeiten bei der Verwendung neuer Begrifflichkeiten führen bei den betroffenen Unternehmen zu Rechts- und Planungsunsicherheiten und wirken der mit der NIS-Richtlinie intendierten Harmonisierung entgegen. Die IEN rät dringend davon ab, bei der Implementierung neuer unbestimmter Begrifflichkeiten von den EU-Vorgaben abzuweichen. Zudem stellt sich auch die Frage nach dem Sinn einer solchen weiteren Kategorie. Soweit Unternehmen als kritisch erachtet werden, werden diese unter die KRITIS-Regulierung eingeordnet, um sie bzgl. IT-Sicherheit zu regulieren. Falls sie als nicht relevant genug angesehen werden, um bzgl. IT-Sicherheit reguliert zu werden, könnten sie dann noch unter den bestehenden, unbestimmten Rechtsbegriff der „Institutionen im besonderen staatlichen Interesse“ fallen. Die entsprechende Differenzierung kann bei Aufnahme in die KRITIS-Regulierung über die branchenspezifischen Sicherheitsstandards stattfinden.

2. Zu § 5c- Verarbeitung von Protokolldaten und Bestandsdatenauskunft

Neu werden im Diskussionsentwurf umfassende Speichermöglichkeiten für Protokoll- und Bestandsdaten inklusive IP-Adressen festgelegt. Dies ist aus Sicht der IEN, gerade im Hinblick auf die gegenwärtige Rechtslage zur Bestandsdatenauskunft, abzulehnen. Der Gesetzgeber hat nach wie vor die Vorgaben des Bundesverfassungsgerichts vom Mai 2020 zur Ausgestaltung des manuellen Bestandsdatenauskunftsverfahrens nicht umgesetzt. Dies ist bislang auch nicht im aktuellen Diskussionsentwurf des TKModG vom 06.11.2020 erfolgt. Sowohl die Übermittlung von Daten durch Telekommunikationsdiensteanbieter als auch der Abruf durch berechtigte Stel-

[1] https://www.allianz-fuer-cybersicherheit.de/ACS/DE/Registrierung/registrierung.html

[2]https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl117s1885.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s1885.pdf%27%5D__1607070631436

len (z.B. Staatsanwaltschaften) bedürfen jeweils einer verhältnismäßigen und normenklaren Grundlage, welche die aktuelle Fassung des § 113 TKG und die Abrufnormen auf Seiten der Empfängerkreise nicht erfüllen. Dies wird seit Ergehen der Entscheidung der Branche, aber auch von anderen Institutionen, wie etwa zuletzt der Bundesdatenschutzkonferenz gefordert[3]. So lange hier keine verfassungskonforme Ausgestaltung der Regulierung erfolgt, darf nicht einfach eine stetige Ausweitung der - rechtswidrigen – Befugnisse auf andere Behörden erfolgen.

3. Zu § 9b - Untersagung des Einsatzes kritischer Komponenten

Der Diskussionsentwurf sieht vor, dass der Einsatz solcher Komponenten, für die aufgrund einer gesetzlichen Regelung eine Zertifizierungspflicht besteht, durch den Betreiber einer Kritischen Infrastruktur gegenüber dem BMI vor dem Einsatz anzeigepflichtig ist. Dabei wurde die auch in früheren Entwürfen vorgesehene Garantieerklärung (inkl. Lieferkettennachweis) des Herstellers von kritischen Komponenten beibehalten. Die weite Definition von „kritischen Komponenten“ in Verbindung mit der Garantieerklärung über die „gesamte Lieferkette des Herstellers“ auf Basis einer nicht näher definierten späteren Allgemeinverfügung des BMI lässt eine Prüfung dieser Vorgabe derzeit nicht möglich erscheinen. Aus Sicht der IEN wird vorliegend jedoch über Aspekte der technischen IT- und Cybersicherheit hinausgegangen, für die das BSI und letztlich der vorliegende Gesetzentwurf zuständig sind. Dies wird bereits daran deutlich, dass vorliegend eine Kompetenz des BMI und gerade nicht des BSI definiert wird. Gleichzeitig sollen sowohl die Inhalte der Garantieerklärung als auch die Risikobewertung des Herstellers der kritischen Komponente „im Einvernehmen mit den jeweils betroffenen Ressorts“ und zur Unterstützung ein fortlaufender Austausch durch einen „interministeriellen Jour Fixe“ erfolgen.

Die IEN weist darauf hin, dass „kritische Komponenten“ bei 5G-basierten Netzen meist Softwarekomponenten sein dürften, deren Funktionalität zügig angepasst werden kann. Wenn es lediglich einen engen Fokus auf Zertifizierung kritischer Komponenten gibt, werden sämtliche anderen Faktoren für den sicheren Betrieb eines Telekommunikationsnetzes in ein Missverhältnis gesetzt.

[3] https://www.datenschutzkonferenz-online.de/media/pm/20202711_pm_100_dsk.pdf

3. Zu § 9c - Einführung neuer IT-Sicherheitskennzeichen

Der Diskussionsentwurf des ITSiG 2.0 überträgt in § 9a die Aufgaben und Befugnisse entsprechend dem EU Cybersecurity Act (VO EU 2019/881) an das BSI damit diese die Aufgaben als nationale Cybersicherheitszertifizierungsbehörde übernimmt. Dieser Schritt wird insoweit von der IEN auch nicht kritisiert – allerdings hat die IEN bereits in den allgemeinen Anmerkungen darauf hingewiesen, dass die Entwicklung und Veröffentlichung eines Stands der Technik für sicherheitstechnische Anforderungen an IT-Produkte, insbesondere aber das „freiwillige IT-Sicherheitskennzeichen" nach § 9c weit über diesen Ansatz der Harmonisierung hinausgehen. Nach Auffassung der IEN sind vorliegend keine zusätzlichen, nationalen Alleingänge erforderlich. Ein solches nationales Gütesiegel auf einer niedrigen Stufe ist nicht geeignet, einen Mehrwert gegenüber einer EU-Cybersicherheitszertifizierung - die für das B2C-Segment gelten dürfte – zu generieren. Ein weiteres Gütesiegel dürfte beim Verbraucher eher für Verwirrung sorgen und bedeutet letztlich nur einen Mehraufwand bei den betroffenen Unternehmen.

4. Zu den §§ 7a, 7b Untersuchungs- und Detektionsrechte des BSI

Zunächst enthält die Rechtseinräumung zur Untersuchung der Sicherheit in der Informationstechnik nach § 7a kaum Einschränkungen dahingehend, welche informationstechnischen Produkte und Systeme das BSI untersuchen darf und in diesem Zusammenhang auch „alle notwendigen Informationen" von den Herstellern einfordern kann. Aus Sicht der IEN ist eine derart breite Berechtigung zur Untersuchung aller informationstechnischen Produkte und Systeme mit einer zusätzlichen Befugnis, externe Informationen anzufordern, kritisch zu bewerten. Dies gilt umso mehr, als es an Regelungen fehlt, welche dem BSI den Umgang mit diesen vertraulichen Informationen auferlegen, wie etwa das Verbot der Weitergabe, etc.

Diese breite Befugnis wird flankiert von der Berechtigung zur Vornahme von Detektionsmaßnahmen nach § 7b. Auch hier ist nach Auffassung der IEN zu fordern, dass derartige Maßnahmen, die sich auf die IT des Bundes oder von kritischen Infrastrukturen, digitalen Diensten oder Unternehmen im besonderen öffentlichen Interesse beziehen können, einen beschränkten Rahmen haben müssen.

5. Zu den Bußgeldvorschriften

Der aktuelle Diskussionsentwurf geht mit seinen Bußgeldvorschriften weit über die Vorgaben anderer vergleichbarer Regelungen, wie etwa der

…

DSGVO, hinaus. Der frühere Entwurf dieses Gesetzes lag mit den Vorgaben noch gleich. Aus Sicht der IEN wird mit der aktuellen Fassung ein unübersichtliches Geflecht geschaffen, dass wieder in Richtung des vorhergehenden Entwurfs überarbeitet werden sollte. So sind derzeit für bestimmte Fälle Geldbußen bis zu 2 Millionen Euro vorgesehen mit Abstufungen auf 1 Million Euro und 100.000 Euro. Gleichzeitig wurde der Verweis auf § 30 OWiG eingeführt, der eine maximale Geldbuße von bis zu 20 Millionen Euro vorsieht.

Gerade auch vor dem Hintergrund der Erreichung größtmöglicher Harmonisierung zwecks Schaffung von Rechts- und Planungssicherheit bei der Erbringung grenzüberschreitender TK-Dienstleistungen sollte sich an EU einheitlichen Vorgaben, wie denen der DSGVO, orientiert werden.

****

Diese Stellungnahme enthält keine Betriebs- und Geschäftsgeheimnisse. Für Rückfragen stehen die IEN-Mitgliedsunternehmen sowie die Unterzeichnerin zur Verfügung.

Malini Nanda, Rechtsanwältin
Geschäftsführerin der IEN

Über die IEN

Die IEN vertritt seit 2003 in Deutschland ansässige, pan-europäisch tätige Anbieter von Telekommunikationsdienstleistungen für große, überregional oder international agierende Geschäftskunden und Behörden. Obgleich nur ein sehr geringer Prozentsatz von Unternehmen in Deutschland als multinationale Konzerne und sogenannte „Multi-Site-Kunden“ der IEN-Unternehmen bezeichnet werden können, bilden diese gleichwohl einen wesentlichen Anteil der deutschen Wirtschaft ab. Sie zeichnen sich für eine Vielzahl von Arbeitsplätzen verantwortlich und repräsentieren einen erheblichen Teil der Geschäftsumsätze und damit der jährlichen Gesamtwirtschaftsleistung in Deutschland. Die Größe und wirtschaftliche Ausrichtung dieser Unternehmen, sowie ihr Bedarf an überregionalen oder sogar globalen Kommunikationslösungen, führt dazu, dass große Geschäftskunden oder auch manche staatliche Behörden detaillierte und umfangreiche Produktanforderungen an TK-Dienstleistungen stellen, die stets das Angebot maßgeschneiderter TK-Produkte erfordern.

Vor diesem Hintergrund setzt sich die IEN bereits seit vielen Jahren für harmonisierte Marktbedingungen ein.