Per mail: CI1@bmi.bund.de

Bundesministerium des Inneren,
für Bau und Heimat
Abteilung Cyber- und Informationssicherheit
Alt-Moabit 140
10557 Berlin

Berlin/Bonn/Köln 10. Dezember 2020

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

Sehr geehrte Damen und Herren,

das BMI hat einen überarbeiteten Entwurf des „Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme („IT-Sicherheitsgesetz 2.0“) mit Stand vom 09.12.2020 vorgelegt. Die unterzeichnenden Verbände BREKO, BUGLAS und VATM bedanken sich für die Möglichkeit zur Abgabe einer (wenn auch sehr kurzfristig zu erstellenden und deshalb nicht abschließenden) Stellungnahme zum Gesetzentwurf. Vorab möchten wir anmerken, dass aufgrund dieser äußerst kurzen Frist zur Abgabe einer Stellungnahme keine Möglichkeit bestand, hier eine ausgiebige Kommentierung des Gesetzesentwurfs vorzunehmen. Dies gilt leider auch vor dem Hintergrund, dass das BMI bereits am 01.12.2020 einen Vor-Entwurf des Gesetzes veröffentlicht hat. Da auch zwischen diesem Entwurf und dem Entwurf von 09.12.2020 mehrere Änderungen vorgenommen wurden, die zudem nicht entsprechend hervorgehoben wurden, war eine Folgenabschätzung der Änderungen innerhalb der gesetzten Frist von einem Tag leider nicht möglich. Wir gehen davon aus , dass die von uns vorgetragenen Argumente noch im Rahmen der Ressortabstimmung ausreichend Berücksichtigung finden.

Die unterzeichnenden Verbände begrüßen und unterstützen das Ziel, die Sicherheit informationstechnischer Systeme zu erhöhen. Unsere Mitgliedsunternehmen arbeiten intensiv an der Erreichung dieses Ziels. Der Entwurf des IT-Sicherheitsgesetzes 2.0 ist aus unserer Sicht aber nur in Teilen dazu geeignet, das Ziel sachgerecht und effizient zu erfüllen. Für die TK-Unternehmen, die die Basis für die Zukunftsfähigkeit der deutschen Wirtschaft bereitstellen, sind neue Pflichten vorgesehen, die zu großen Belastungen führen und über die Regelungen in §§ 109/109a TKG hinausgehen.

1. Unternehmen von öffentlichem Interesse (§ 2 Abs.14 BSIG-E)

Das BSI-Gesetz, das den Schwerpunkt des IT-Sicherheitsgesetzes bildet, richtet (insbesondere in § 8f BSIG-E) eine Reihe von Verpflichtungen an *„Unternehmen im besonderen öffentlichem Interesse."* Es ist daher zu begrüßen, dass der vorliegende Gesetzentwurf den Begriff des *„Unternehmens im besonderen öffentichen Interesse"* klarer definiert. Soweit der Begriff in § 2 Abs. 14 Nr. 2 an die Unternehmensgröße anknüpft, ist in der entsprechenden Verordnung nunmehr zu regeln, welche wirtschaftlichen Kennzahlen zur Berechnung der inländischen Wertschöpfung heranzuziehen sind, nach welcher Methodik die Berechnung erfolgt und welche Schwellenwerte (vgl. de-minimis-Regelung der KRITIS-VO) dafür maßgeblich sind, dass ein Unternehmen zu den größten Unternehmen in Deutschland gem. § 2 Abs. 14 Nr. 2 gehört.

2. Bestandsdatenauskunft (§ 5c BSIG-E)

Gemäß § 5c des Gesetzentwurfs soll das BSI künftig in den Kreis der berechtigten Stellen aufgenommen werden, die von den TK-Diensteanbietern eine Bestandsdatenauskunft im Wege des manuellen Auskunftsverfahrens nach § 113 Abs.1 TKG anfordern können. Dies ist vor dem Hintergrund der Entscheidungen des Bundesverfassungsgerichts von 27.05.2020 zum manuellen Auskunftsverfahren nicht unkritisch. Während es dem Bundesverfassungsgericht erkennbar darum geht, den Anwendungsbereich des manuellen Auskunftsverfahrens zu konkretisieren und zu beschränken, wird dieses durch § 5c BSIG-E für eine weitere Institution geöffnet, die zudem nicht unmittelbar dem Bereich der Gefahrenabwehr zuzurechnen ist. Immerhin werden Zweck und Voraussetzungen für eine Bestandsdatenauskunft durch das BSI in § 5c Abs.1 Nr.1 und 2 BSIG-E konkret beschrieben.

Es darf allerdings verlangt werden, dass eine Erteilung der Bestandsdatenauskunft durch die TK-Unternehmen an das BSI ausschließlich über die bekannten und in der TR TKÜV beschriebenen Schnittstellen erfolgt.

3. Anordnungsbefugnis gegenüber TK-Diensteanbietern (§ 7c BSIG-E)

§ 7c BSIG-E begründet eine umfangreiche und im Vergleich zum Entwurf vom Mai 2020 neue Anordnungsbefugnis des BSI gegenüber TK-Diensteanbietern mit mehr als 100.000 Kunden. Die darin liegende Umgestaltung des BSI (auch) zur Gefahrenabwehrbehörde ist insgesamt nicht unkritisch. Das BSI kann den Diensteanbieter dazu verpflichten, die in § 109a Abs.5 und 6 TKG bezeichneten Maßnahmen einzuleiten, also insbesondere die Nutzung von TK-Diensten und Datenverkehre zu Störungsquellen einzuschränken, zu unterbinden und umzuleiten, sofern dies zur Vermeidung von Störungen an Telekommunikations- und Datenverarbeitungssystemen erforderlich ist. Darüber hinaus kann das BSI nach § 7c Abs.3 BSIG-E die Umleitung der betroffenen Datenverkehre an eine vom BSI benannte Anschlusskennung verlangen.

Vermitteln § 109a Abs.5 und 6 TKG dem Diensteanbieter allerdings lediglich entsprechende Berechtigungen, verwandelt § 7c BSIG die Vorschrift in eine Ermächtigungsgrundlage für das BSI, die Einleitung entsprechender Maßnahmen zu verlangen. Auch wenn entsprechende Anordnungen nur zur Abwehr von Gefahren für die in § 7c Abs.2 BSIG-E angeführten Schutzziele getroffen werden dürfen, halten die unterzeichnenden Verbände dies weder für erforderlich noch für verhältnismäßig.

4. Datenspeicherung zur Angriffserkennung (§ 8a Abs. 1b BSIG-E)

Gem. § 8a Abs. 1b BSIG-E werden Betreiber kritischer Infrastrukturen dazu verpflichtet, relevante nicht personenbezogene Daten für die Angriffserkennung und Angriffsnachverfolgung mindestens vier Jahre zu speichern. Eine Speicherfrist von vier Jahren halten wir für unverhältnismäßig. Zudem sehen wir hier erhebliche Datenschutzprobleme. Zwar spricht der Entwurf nur von *nicht personenbezogenen* Daten. Der Personenbezug kann jedoch nicht immer oder nur unter erheblichem Aufwand entfernt werden. Dies gilt vor allem bei einem weiten Verständnis des Begriffs der personenbezogenen Daten. Aufgrund dieser Gefahr und der sehr langen Speicherfrist sehen wir erhebliche Gefahren für die Rechte der betroffenen Personen.

5. Untersagung des Einsatzes kritischer Komponenten (§ 9b BSIG-E)

Es ist richtig, ausschließlich Komponenten vertrauenswürdiger Hersteller für den Einsatz in kritischen Infrastrukturen zuzulassen. Der ausschließliche Einsatz von Komponenten vertrauenswürdiger Hersteller soll durch die Abgabe einer Garantieerklärung (Vertrauenswürdigkeitserklärung) gegenüber dem Betreiber abgesichert werden. Der Entwurf beinhaltet hohe Anforderungen an Komponenten und Hersteller. Dies wird im Sinne der IT-Sicherheit von den unterzeichnenden Verbänden nachdrücklich unterstützt. Es ist jedoch darauf zu achten, dass die angeforderte Nachweisführung der Umsetzung der sicherheitstechnischen Maßnahmen nicht dazu führt, dass sichere und innovative Komponenten nicht mehr eingesetzt werden können. Hier ist deswegen eine angemessene Frist für die Nachweisführung erforderlich. Außerdem ist es dringend erforderlich, dass die Hersteller selbst mit den zuständigen (zertifizierenden) Behörden in die Klärung technischer Fragen gehen können und dies nicht über die Netzbetreiber abgehandelt wird. Hier droht sonst nicht nur ein unüberschaubarer bürokratischer Aufwand, sondern auch eine besondere Benachteiligung kleiner TK-Unternehmen, die diesen Aufwand nicht stemmen können.

Gemäß § 9b Abs.4 BSIG-E kann das BMI den weiteren Betrieb einer kritischen Komponente gegenüber dem Betreiber einer kritischen Infrastruktur untersagen, wenn der Hersteller der kritischen Komponente sich als nicht vertrauenswürdig im Sinne des Abs.5 erwiesen hat, also insbesondere gegen die dem Betreiber der kritischen Infrastruktur gegenüber abzugebende Garantieerklärung verstoßen hat.

Auch wenn die unterzeichnenden Verbände Verständnis für die starken öffentlichen Sicherinteressen haben, die das Motiv dieser Regelung sind, so ist doch festzuhalten, dass die Betreiber einer kritischen Infrastruktur in dieser Dreieckskonstellation mit einem ganz erheblichen Risiko belastet werden, das sie selbst weder verursacht haben, noch abmildern können. Es entspricht daher dem Grundsatz der Verhältnismäßigkeit, dass dieses Risiko für die Betreiber kritischer Infrastrukturen gesetzgeberisch soweit wie möglich abgesichert wird. So ist ein Eingriff in die Bestandsnetze nur bei Sicherheitsrisiken von einiger Erheblichkeit gerechtfertigt. Zudem muss die Durchsetzung etwaiger zivilrechtlicher Regressansprüche gegen nicht vertrauenswürdige Hersteller im Sinne des § 9b Abs.5 BSIG-E soweit wie möglich erleichtert werden. Dies kann dadurch geschehen, dass es sich insbesondere ein Verstoß gegen die Kriterien des § 9b Abs.5 BSIG-E als Verletzung einer wesentlichen Vertragspflicht festgelegt wird, bei der die Haftung nicht durch AGB beschränkt oder ausgeschlossen werden kann. Zudem sollte zumindest in der Gesetzesbegründung klargestellt werden, dass § 9b Abs.5 BSIG-E auch eine Schutznorm zugunsten der Betreiber einer kritischen Infrastruktur im Sinne des § 823 Abs.2 BGB darstellt.

Schließlich ist klarzustellen, dass der nach § 109 Abs.6 TKG von der BNetzA im Einvernehmen mit dem BSI zu erstellende Sicherheitskatalog die Anforderungen an kritische Komponenten in Telekommunikationsnetzen umfassend beschreibt und Anhang 2 des Sicherheitskataloges 2.0 in Verbindung mit den Durchsetzungsbefugnissen der BNetzA nach dem TKG die Rechtmäßigkeit des Einsatzes kritischer Komponenten in TK-Netzen als sektorspezifisches „lex specialis“ abschließend regelt.

6. IT-Sicherheitskennzeichen

Nach § 9c BSIG-E führt das BSI ein freiwilliges IT-Sicherheitskennzeichen ein. Dieses enthält ausdrücklich keine Aussagen den Datenschutz betreffend. Das IT-Sicherheitskennzeichen soll aus einer Herstellererklärung und der BSI-Sicherheitsinformation bestehen. Die Anforderungen an das IT-Sicherheitskennzeichen ergeben sich aus einer Technischen Richtlinie des BSI, das die Einhaltung der Anforderungen auch kontrolliert.

Positiv hervorzuheben ist die Freiwilligkeit einer Nutzung des IT-Sicherheitskennzeichens. Allerdings stellt sich die Frage, inwieweit das Sicherheitskennzeichen in das bereits bestehende Gefüge des europäischen IT-Sicherheits-Zertifizierungsrahmens einfügt. Es wäre daher sinnvoll, darauf hinzuweisen, dass das geplante IT-Sicherheitskennzeichen im Einklang mit dem durch den EU-Cybersecurity Act gesetzten Zertifizierungsrahmen entwickelt und umgesetzt wird.

7. Bußgelder (14 BSIG-E)

Für die TK-Unternehmen hat das Thema IT-Sicherheit einen enorm hohen Stellenwert. Aus eigenem Antrieb werden Sicherheitsvorschriften meist nicht nur eingehalten, sondern deutlich übertroffen. Vor diesem Hintergrund halten wir die Ausgestaltung von möglichen Bußgeldern ebenfalls für diskussionswürdig. Anzumerken ist, dass der Bußgeldrahmen in § 14 Abs.2 BSI-G im Verhältnis zum Entwurf vom Mai 2020 zwar deutlich beschränkt wurde, aber gerade durch den Verweis auf § 30 Absatz 2 Satz 3 OWiG immer noch zu hoch ist, was Verhältnismäßigkeitsfragen aufwirft.

Zudem berühren die im BSI-Gesetz geregelten Sachverhalte und die daran anknüpfenden Bußgeld-tatbestände auch die Regelungsgegenstände anderer Gesetze, wie des TKG oder des Datenschutzrechts. Auch dort gibt es umfangreiche Bußgeldtatbestände, so dass grundsätzlich das Konkurrenzverhältnis der verschiedenen Bußgeldregelungen zu klären wäre, um eine unverhältnismäßige Mehrfach-Sanktionierung zu vermeiden.

8. Zu Artikel 2: Änderungen des Telekommuikationsgesetzes

Aus Gründen der Effizienz, Transparenz und der Eineheitlichkeit der Gesetzegebung sollten Änderungen des Telekommunikationsgesetzes, hier der §§ 109, 109a TKG, ausschließlich im Rahmen der laufenden Novellierung des TKG und nicht zusätzlich oder parallel durch das IT-Sicherheitsgesetz erfolgen. Inhaltlich würden wir die betreffenden Punkte dann im Rahmen der Verbändetellungnahmen zur TKG-Novellierung kommenieren.

Wir bitten um die Berücksichtigung der hier angesprochenen Punkte im weiteren Gesetzgebungsverfahren und stehen für einen weiteren Austausch sehr gerne zur Verfügung.