VATM e. V. • Frankenwerft 35 • 50667 Köln

Vorab per E-Mail: CI1@bmi.bund.de
Bundesministerium des Inneren,
für Bau und Heimat
Abteilung Cyber- und Informationssicherheit
Alt-Moabit 140
10557 Berlin

Ansprechpartner	E-Mail	Fax	Telefon	Datum
Iris Nolte	in@vatm.de	0221 3767726	0221 3767727	13.01.2021

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

Sehr geehrte Damen und Herren,

am 16.12.2020 hat die Bundesregierung einen Entwurf des „Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme („IT-Sicherheitsgesetz 2.0“) beschlossen. Der VATM hat bereits gemeinsam mit den Verbänden BREKO und BUGLAS bezüglich eines vorläufigen BMI-Entwurfs Stellung genommen. Aufgrund des Verfahrensablaufs, welches durch das BMI vorgegeben wurde, war eine ordentliche Beteiligung der Verbände innerhalb der Frist von einem Tag nach Veröffentlichung des letzten – aber erneut deutlich abgeänderten – Entwurfs nicht möglich. Der VATM möchte daher die Gelegenheit nutzen, auf Basis des Kabinettsbeschlusses einige weitere Punkte aufzuführen, die aufgrund der knappen Frist von VATM-Seite nicht mehr innerhalb der ersten Stellungnahme zur Diskussion gestellt werden konnten. Wir gehen davon aus, dass die von uns vorgetragenen Argumente noch ausreichend Berücksichtigung finden.

Der VATM begrüßt und unterstützt 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. Der Entwurf birgt Unklarheiten, die beseitigt werden müssen, um das Ziel der erhöhten Sicherheit erreichen zu können.

Ebenfalls ist es im Sinne der europäischen Harmonisierung wünschenswert, dass einer nationalen Fragmentierung entgegengewirkt wird und möglichst einheitliche Lösungen gesucht werden. Die „5G-Toolbox“ der EU-Kommission[1] bietet hier gute Ansatzpunkte, die so weit wie möglich im IT-SiG berücksichtigt werden sollten. Da viele Komponenten von TK-Unternehmen in ganz Europa eingesetzt werden, würde eine Harmonisierung zu einer deutlichen Effizienzsteigerung führen.

Darüber hinaus sollte das IT-Sicherheitsgesetz aber auch bereits neue 5G- und 6G-Technologien regulatorisch unterstützen.

I. Kein Aufbau von Wettbewerbsschranken

Das IT-Sicherheitsgesetz stellt hohe Anforderungen an die Verpflichteten. Neben den Betreibern kritischer Infrastrukturen wird der Kreis der Verpflichteten teilweise erweitert. Die Bedeutung der IT-Sicherheit nimmt in Zeiten der stetigen Digitalisierung immer weiter zu. Bei der Auferlegung der Anforderungen an die IT-Sicherheit darf der effektive Wettbewerb nicht aus den Augen verloren werden. Gesetzliche Regelungen wie das IT-Sicherheitsgesetz dürfen nicht als Wettbewerbs- und Markteintrittsschranken fungieren, indem sie Anforderungen aufstellen, die von kleineren und / oder neuen Marktteilnehmern nicht erbracht werden können. So finden sich zwar bereits im Rahmen der BSI-KritisV anhand bestimmter Schwellenwerte entsprechende Berücksichtigungen, die auch mit den Vorgaben des Post- und Telekommunikationssicherstellungsgesetz korrespondieren. Dieser Ansatz sollte auch für den nun neuen Kreis der Verpflichteten „Unternehmen im besonderen öffentlichen Interesse“ gewahrt werden.

Allgemein sollte aber auch überlegt werden, eine Abstufung der Verpflichtungen des IT-SiG 2.0 diesbezüglich in Betracht zu ziehen. Ein solches System könnte bspw. anhand von Größenkriterien beim Pflichtenumfang und / oder bei den Umsetzungsfristen differenzieren, um unter dem Gesichtspunkt von Wettbewerbschancen eine verhältnismäßige Umsetzung zu erreichen. Darüber hinaus könnte es auch sinnvoll sein, wenn insbesondere KMUs in die (vollen) Pflichten des IT-Sicherheitsgesetz mit der Zeit hineinwachsen können.

[1] Siehe hierzu auch den Workshop von ENISA und BEREC: https://berec.europa.eu/eng/events/berec_events_2020/258-joint-enisa-berec-workshop-on-5g-cybersecurity-toolbox-developments-and-ways-forward

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

Präsidium: Martin Witt (Präsident), David Zimmer (Vizepräsident), Valentina Daiber, Michael Jungwirth,
Uwe Nickl, Karsten Rudloff, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Jürgen Grützner

II. Bestandsdatenauskunft (§ 5c BSIG-E)

Gemäß § 5c BSIG-E 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 vom 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 den engen Bereichen des Polizeirechts oder der Landesverteidigung zuzurechnen ist.

Ergänzend zur gemeinsamen Verbände-Stellungnahme möchten wir zusätzlich zu unseren allgemeinen Bedenken ausführen:

Zunächst begrüßen wir die erst kurzfristig aufgenommene Entschädigungsregelung des neuen Absatzes 8, wonach den Verpflichteten eine entsprechende Aufwandsentschädigung nach § 23 und Anlage 3 JVEG zu gewähren ist.

Wir erachten es jedoch vor dem Hintergrund der Bundesverfassungsgerichts-Entscheidung vom Mai letzten Jahres für wichtig, dass ein ergänzender Absatz 9 eingefügt werden sollte. Hierin sollte klargestellt werden, dass die erhobenen Daten nach Behebung der Sicherheitsbeeinträchtigung unverzüglich zu löschen sind.

III. Neue Befugnisse des BSI (§ 7b-d BSIG-E)

Das BSI soll nach den Regelungen der § 7b-d BSIG-E neue Befugnisse erhalten. Insbesondere wird das BSI dazu ermächtigt, aktiv Sicherheitsrisiken aufzudecken und konkrete Anordnung zu erteilen, um Sicherheitsrisiken zu beseitigen. Aus Sicht des Gesetzeszwecks sehen wir diese neuen Befugnisse und die damit zugeordnete Rolle des BSI als „Gefahrenabwehrbehörde“ kritisch. Denn sie ermächtigen das BSI selbst in die IT-Sicherheit einzugreifen. Zur Abwehr der hierdurch potentiell entstehenden Gefahren wären weitere Konkretisierungen für eine tragbare Regelung erforderlich.

Nach § 7b BSIG-E wird das BSI dazu ermächtigt selbst Maßnahmen zu ergreifen, um Sicherheitsrisiken aufzudecken. Das BSI muss hier zumindest den Betreibern die nötige Transparenz

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

Präsidium: Martin Witt (Präsident), David Zimmer (Vizepräsident), Valentina Daiber, Michael Jungwirth,
Uwe Nickl, Karsten Rudloff, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Jürgen Grützner

verschaffen, indem es über den Beginn und die Beendigung der Durchführung der Maßnahmen informiert.

Nach § 7c und d BSIG-E soll das BSI zukünftig gegenüber TK-Diensteanbietern bzw. Telemedien-Anbietern auch befugt sein, konkrete Maßnahmen anzuordnen, um Gefahren für die IT-Sicherheit abzuwenden. Gem. § 7c Abs. 3 BSIG-E kann das BSI anordnen, den Datenverkehr an eine benannte Anschlusskennung umzuleiten. Hier sehen wir dringend weiteren Klarstellungsbedarf, da die Umleitung des Telekommunikationsverkehrs an Dritte eine Verletzung des Fernmeldegeheimnisses darstellt, die es besonders zu begründen gilt. § 7c Abs. 3 BSIG-E bedarf daher der weiteren Konkretisierung, die die Verletzung des Fernmeldegeheimnisses gebührend begründet.

Das BSI erlangt sowohl aus der Ermächtigung zur aktiven Aufdeckung von Sicherheitsrisiken als auch durch die Möglichkeit zur Anordnung konkreter Maßnahmen zu deren Behebung weitreichende Befugnisse, selbst in die IT-Sicherheit der Betreiber einzugreifen. Auch durch einen solchen Eingriff in die IT-Sicherheit können Gefahren entstehen, die geeignet sind, die IT-Infrastrukturen der Unternehmen erheblich zu beeinträchtigen. Dies kann bspw. auch in einem Ausfall der Systeme resultieren. Für die hierdurch entstehenden Schäden bedarf es daher ergänzend einer entsprechenden Kompensationsregelung zugunsten der Betreiber, wenn diese Schäden das Resultat einer, vom BSI vorgenommenen oder angeordneten Handlung sind.

IV. Sicherheit in der Informationstechnik kritischer Infrastrukturen (§ 8a BSIG-E)

Nach dem neuen § 8a Abs. 1a BSIG-E sollen Betreiber kritischer Infrastrukturen zukünftig verpflichtet werden, auch Systeme zur Angriffserkennung einzusetzen. Grundsätzlich unterstützen wir den Einsatz von Systemen zur Angriffserkennung, da diese einen wichtigen Beitrag zur IT-Sicherheit leisten können. Allerdings sehen wir eine allgemeine Verpflichtung im Lichte des Systems nach § 8a BSIG-E kritisch. Dieser ist gerade darauf ausgelegt, technische und organisatorische Maßnahmen nach dem jeweils erforderlichen Bedarfsfall auszuwählen und zu implementieren, um einen für diesen Fall zuverlässigen Schutz zu gewährleisten. Eine allgemeine Verpflichtung steht diesem System entgegen.

Darüber hinaus ist die Definition nach § 2 Abs. 9b BSIG-E hier auch zu unbestimmt, wodurch es bereits schwer sein wird zu bestimmen, ob die Betreiber die nötigen Anforderungen überhaupt erfüllt haben. Das BSI soll hierzu ermächtigt werden, durch Richtlinien die Anforderungen zu

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

Präsidium: Martin Witt (Präsident), David Zimmer (Vizepräsident), Valentina Daiber, Michael Jungwirth,
Uwe Nickl, Karsten Rudloff, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Jürgen Grützner

konkretisieren. Die Erstellung und zukünftige Änderungen dieser Richtlinien sollten unter der Beteiligung der Unternehmen erfolgen.

Abschließend halten wir die Verpflichtung der Betreiber nach Abs. 3 S. 1, alle zwei Jahre die Erfüllung der Anforderungen nachzuweisen, für problematisch. Hier sollte ein längeres Zeitintervall, wie bspw. alle fünf Jahre, angesetzt werden.

V. Registrierung kritischer Infrastrukturen (§ 8b Abs. 3 BSIG-E)

Gem. § 8b Abs. 3 BSIG-E sollen Betreiber kritischer Infrastrukturen ihre Anlagen beim BSI registrieren. In dieser Regelung sehen wir im Bereich der Telekommunikationsanbieter erhebliche Probleme, die zu parallelen Strukturen zwischen der BNetzA und dem BSI führen können. Hier bedarf es unbedingt einer Klarstellung, um unnötige Doppelregulierungen und Zuständigkeitsfragen zu vermeiden.

VI. Herausgabe von Informationen (einschließlich personenbezogener Daten) (§ 8b Abs. 4a BSIG-E)

Gem. § 8b Abs. 4a BSIG-E besteht im Falle einer erheblichen Störung die Pflicht zur Herausgabe der notwendigen Informationen (einschließlich personenbezogener Daten) an das Bundesamt, die zur Bewältigung der Störung notwendig sind. Besonders mit Blick auf die Herausgabe personenbezogener Daten sehen wir diese Regelung äußerst kritisch und wünschen uns diesbezüglich weitere Klarstellungen.

VII. Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse (§ 8f BSIG-E)

Der neue § 8f BSIG-E sieht für die „Unternehmen von besonderem öffentlichen Interesse“ insbesondere die Verpflichtung vor, eine Selbsterklärung zur IT-Sicherheit abzugeben. Der Zweck dieser Selbsterklärung ist für uns jedoch nicht nachvollziehbar. Ausgehend von der Definition des Begriffs der „Unternehmen von besonderem öffentlichen Interesse“ verstehen diese Unternehmen die Bedeutung der IT-Sicherheit selbst und werden sie aus eigenem Anreiz gewährleisten. Zudem scheinen einige Regelungen daran anzuknüpfen, die Wertschöpfung dieser Unternehmen aufgrund von Störungen nicht gefährden zu wollen und erlegen diesbezügliche Verpflichtungen

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

Präsidium: Martin Witt (Präsident), David Zimmer (Vizepräsident), Valentina Daiber, Michael Jungwirth,
Uwe Nickl, Karsten Rudloff, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Jürgen Grützner

auf. Dieser Ansatz ist mit dem Telos des Gesetzes nur schwer vereinbar. Zumal auch hier wirtschaftlich agierende Unternehmen aus eigenem Anreiz Maßnahmen ergreifen werden, um ihre eigenen Wertschöpfungsprozesse nicht zu gefährden. Auch die weiteren Regelungen des § 8f BSIG-E bauen auf dem angeordneten Selbstbekenntnis zur IT-Sicherheit auf und führen zu hohem bürokratischem Aufwand, ohne dass der Nutzen hierzu ersichtlich ist. § 8f BSIG-E sollte daher gestrichen werden.

VIII. Zertifizierung (§ 9 BSIG)

Nach § 9 Abs. 4 S. 1 Nr. 2 i.V.m. Abs. 4a BSIG-E kann das BMI die Erteilung eines Zertifikats untersagen, wenn überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung entgegenstehen. Das technische Zertifizierungsverfahren, welches sich ausschließlich nach den telekommunikationsrechtlichen Bestimmungen zu richten hat, würde durch eine zusätzliche Überprüfung seitens des BMI um eine sicherheitspolitische Bewertung ergänzt. Unabhängig davon, dass hier eine unbedingt zu vermeidende Doppelprüfung im Raum steht, sollen rein technisch geprägte Zertifizierungsverfahren gerade aufgrund ihrer objektiven Kriterien zur Rechts- und Planungssicherheit beitragen. Mit einer politischen Bewertung, bei der erhebliche Bewertungsspielräume bestehen können, wird diese Rechts- und Planungssicherheit untergraben. Zudem kann sich durch eine zusätzliche (und vor allem sachfremde) Prüfung durch das BMI das Zertifizierungsverfahren erheblich verlängern. Besonders zweckfremd erscheint die Prüfung durch das BMI vor dem Hintergrund der Zertifizierung kritischer Komponenten, die daran anschließend eine erneute Überprüfung anhand sicherheitspolitischer Erwägungen durchlaufen müssen (siehe § 9b BSIG-E). Hiermit käme es praktisch zu einer erneuten Prüfung. Zudem ist dabei zu berücksichtigen, dass im Gegensatz zu dem Verfahren nach § 9b BSIG-E allein das BMI darüber entscheiden darf, ein Zertifikat aus sicherheitspolitischen Bedenken nicht zu erteilen.

Der Regelungsrahmen für die Erteilung eines Zertifikats sollte sich daher rein auf die technischen Fragestellungen begrenzen.

Ebenfalls sollte bedacht werden, dass die Hersteller selbst die Zertifizierungen beantragen, damit diese mit den zuständigen Behörden in die Klärung bestehender (Fach-)Fragen gehen können. Dies darf und sollte nicht über die Netzbetreiber abgehandelt werden. Ansonsten droht nicht nur ein unüberschaubarer bürokratischer Aufwand, sondern auch eine besondere Benachteiligung kleiner TK-Unternehmen, die diesen Aufwand nicht stemmen können.

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

Präsidium: Martin Witt (Präsident), David Zimmer (Vizepräsident), Valentina Daiber, Michael Jungwirth,
Uwe Nickl, Karsten Rudloff, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Jürgen Grützner

Darüber hinaus sollten im Lichte eines harmonisierten EU-Binnenmarkts Zertifizierungen anderer EU-Behörden anerkannt werden, ohne dass eine erneute Zertifizierung vom BSI erforderlich ist (One-Stop-Shop-Prinzip).

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

Es ist richtig, ausschließlich verlässliche Komponenten für den Einsatz in kritischen Infrastrukturen zuzulassen. Dieses Ziel wird auch nachdrücklich unterstützt und begrüßt. Dennoch sehen wir in den hierzu getroffenen Regelungen Verbesserungsmöglichkeiten, um das Ziel des sicheren Betriebs kritischer Infrastrukturen zu gewährleisten.

1. Definition „kritischer Komponenten“

Der Begriff der „kritischen Komponenten“ wird in § 2 Abs. 13 BSIG-E definiert. Während aus den früheren Gesetzesbegründungen hierzu noch hervorging, dass die Bestimmung der kritischen Komponenten sich ausschließlich nach den Vorgaben des TK-Sicherheitskatalogs und seiner Anlage 2 ergeben, ließe sich aus der derzeitigen Gesetzesformulierung auch der Schluss ziehen, dass kritische Komponenten auch durch andere Gesetzesvorschriften bestimmt werden können. Vor allem vor dem Hintergrund der Bewertungen durch das BMI und den beteiligten Ressorts im Rahmen der Prüfung nach § 9b Abs. 3 S. 1 BSIG-E bedarf es hier einer Klarstellung, damit sich die kritischen Komponenten abschließend allein aus den telekommunikationsrechtlichen Bestimmungen nach § 109 Abs. 6 TKG i.V.m. Anlage 2 TK-Sicherheitskatalog ergeben.

2. Garantieerklärung

Der neue § 9b BSIG-E möchte das Ziel der IT-Sicherheit im Zusammenhang mit dem Einsatz „kritischer Komponenten“ insbesondere mit der Abgabe einer Garantieerklärung (Vertrauenswürdigkeitserklärung) der Hersteller gegenüber den Betreibern kritischer Infrastrukturen erreichen. Der Entwurf beinhaltet hohe Anforderungen an die eingesetzten Komponenten und Hersteller. So sollen Hersteller versichern, dass und wie sie hinreichend sichergestellt haben, dass die von ihnen hergestellte „kritische Komponente über keine technischen Eigenschaften verfügen, die geeignet sind, missbräuchlich, insbesondere zu Zwecken von Sabotage, Spionage oder Terrorismus auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der kritischen Infrastruktur, einwirken zu können“.

Konkrete Aussagen zu den Bestandteilen der Garantieerklärung lässt die Regelung allerdings vermissen. So ist es bspw. unklar, ob die Zertifikate der Hersteller bereits Bestandteil der

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

Präsidium: Martin Witt (Präsident), David Zimmer (Vizepräsident), Valentina Daiber, Michael Jungwirth,
Uwe Nickl, Karsten Rudloff, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Jürgen Grützner

Erklärung sind oder erst später beizubringen sind. Das Gesetz verweist zum Inhalt der Garantieerklärung auf eine – zu einem späteren Zeitpunkt zu erlassene – Allgemeinverfügung des BMI. Hier sollte eine Klarstellung aufgenommen werden. Aus Gründen der Planungs- und Rechtssicherheit für die betroffenen Unternehmen sollte der Mindestinhalt (z.B. inhaltlich entsprechend der Vertrauenswürdigkeitserklärung betreffend die Logistikkette gemäß Ziffer 3 der Anlage 2 TK-Sicherheitskatalog) bereits in § 9b BSIG-E enthalten sein, der dann anschließend durch eine Allgemeinverfügung weiter konkretisiert werden kann. Die anschließende Allgemeinverfügung muss dann auch den Grundsätzen der Bestimmtheit, Verhältnismäßigkeit und dem Übermaßverbot (vgl. §§ 35 ff VwVfG) genügen.

Weiterhin sollte im Rahmen der Erstellung und ggf. Überarbeitung der Allgemeinverfügung des BMI den beteiligten Stakeholdern hier die Möglichkeit der Anhörung gegeben werden.

3. Prüfprozess

Der Einsatz kritischer Komponenten ist mit einer Prüfung des BMI und den „beteiligten Ressorts“ verbunden. Ein vorheriger Einsatz ist nicht gestattet. Nach § 9b Abs. 3 BSIG-E erfolgt diese Prüfung innerhalb eines Monats. In der Vorschrift wäre eine Klarstellung hilfreich, ob mit Übermittlung der Garantieerklärung an das BMI automatisch der Prüfprozess nach § 9b Abs. 3 BSIG-E eingeleitet wird. Weiterhin ist nach dem bisherigen Gesetzeswortlaut die Frist von einem Monat als nicht verlängerbare Ausschlussfrist zu interpretieren und nach Ablauf selbiger von einer Genehmigung betreffend den Einsatz der Komponenten auszugehen. Aus Gründen der Rechtsklarheit sollte hierzu jedoch eine Klarstellung in einem ergänzenden Satz erfolgen.

Weiterhin sehen wir auch die Notwendigkeit einer Konkretisierung des Prüfverfahrens. Nach § 9b Abs. 3 sind hieran das BMI unter Abstimmung mit den „beteiligten Ressorts“ beteiligt. Leider finden sich weder im Rechtstext noch in den Begründungen entsprechende Ausführungen, welche Ressorts konkret beteiligt sind oder sich beteiligen können. Die Nennung des BMWi erscheint in der Begründung nur beispielhaft erwähnt worden zu sein. Da die Prüfung zu einer Verzögerung des Einsatzes „kritischer Komponenten“ führt, bedarf es hier eines vorab definierten Kreises der beteiligten Behörden, die diese Entscheidung treffen werden. Die Betreiber kritischer Infrastrukturen dürfen nicht zum Spielball eines behörden-internen „Zuständigkeitsgerangel“ werden. Zudem ist zu bedenken, dass der verzögerte Einsatz „kritischer Komponenten“ ebenfalls eine Gefahr für die IT-Sicherheit darstellen kann, die das Gesetz gerade verhindern möchte.

Neben einer Konkretisierung der am Prüfprozess beteiligten Ressorts sehen wir auch das Erfordernis einer Konkretisierung der Prüfungskriterien selbst. So ist nach § 9b Abs. 3 BSIG-E die

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

Präsidium: Martin Witt (Präsident), David Zimmer (Vizepräsident), Valentina Daiber, Michael Jungwirth,
Uwe Nickl, Karsten Rudloff, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Jürgen Grützner

Prüfung anhand „überwiegender öffentlicher Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland“ vorzunehmen.

Der Auf- und Ausbau von Telekommunikationsnetzen, insbesondere der bereits laufende Ausbau des 5G-Netzes, verlangt einen hohen Investitionsaufwand. Auch die Politik und die Kunden erwarten von den Netzbetreibern diese Investitionen. Im Gegenzug muss den Unternehmen eine entsprechende Planungssicherheit zugesprochen werden. Insofern bedürfen die Kriterien der Vertraulichkeitsprüfung einer Konkretisierung, die es den Unternehmen erlaubt, hier eine Risikobewertung bereits im Vorfeld vorzunehmen. Der Bedarf konkreter Bewertungskriterien ist darüber hinaus auch deshalb zwingend, da durch den inländisch politischen Wandel oder personelle Änderungen in den Ressorts die Gefahr einer willkürlichen Entscheidung verstärkt werden, wenn es an diesen Kriterien fehlt. Bei der Konkretisierung der Bewertungskriterien sollte dann schließlich darauf geachtet werden, dass politische Erwägungen sich einzig auf die Schutzziele des IT-Sicherheitsgesetzes wie die Gefahren für die Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität beziehen dürfen. Ziel des Gesetzes ist es nicht, die politische Lage anderer Staaten „durch die Hintertür“ zu sanktionieren, indem Hersteller aus diesen Ländern als nicht vertrauenswürdig angesehen werden. Dies ist nicht der Zweck des IT-Sicherheitsgesetzes und würde andernfalls die Betreiber kritischer Infrastrukturen unverhältnismäßig belasten, wenn diesen bspw. der Einsatz kritischer Infrastrukturen aufgrund von politischen Erwägungen untersagt werden, die außerhalb des Regelungsziels des IT-Sicherheitsgesetzes stehen.

4. Rechtsfolge

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. Das BMI hat seine Entscheidung im Einvernehmen mit den beteiligten Ressorts zu treffen.

a) Nachträgliche Untersagung

Die nachträgliche Untersagung bereits verbauter Komponenten stellt einen erheblichen Eingriff in die Berufs- und Eigentumsfreiheit der beteiligten Unternehmen dar. Ein solcher Eingriff bedarf einer entsprechenden Rechtfertigung. Die Notwendigkeit eines solchen Eingriffs ergibt sich jedoch nicht aus der derzeitigen Regelung. Gerade mit dem vorgeschalteten Prüfungsprozess, bei dem nicht nur die technische Zuverlässigkeit der Komponenten bescheinigt, sondern auch

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

Präsidium: Martin Witt (Präsident), David Zimmer (Vizepräsident), Valentina Daiber, Michael Jungwirth,
Uwe Nickl, Karsten Rudloff, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Jürgen Grützner

zusätzlich die Prüfung nach Abs. 3 durchlaufen wird, lassen einer nachträglichen Untersagung wenig Raum.

Die Möglichkeit einer jederzeitigen – und von dem Betreiber nicht kontrollierbaren oder gar kalkulierbaren – Untersagung, sind vor dem Hintergrund der Rechtssicherheit ein unverhältnismäßiges Mittel. Darüber hinaus fehlt es dem Gesetz auch an entsprechenden Regelungen, die den Rückbau der betroffenen Komponenten regelt. Aufgrund von teils sehr komplexen und / oder quantitativen Faktoren wäre ein Rückbau nach Anordnung der Untersagung rein operativ schwer möglich. Wir sehen die Rechtsfolge der Untersagung daher insgesamt als unverhältnismäßiges Mittel an. § 9 Abs. 4 BSIG-E sollte daher gestrichen werden. Doch selbst wenn an dieser Regelung festgehalten wird, bedarf es unbedingt ergänzender Vorschriften, die es den Unternehmen ermöglichen, die Rechtsfolge in einer angemessenen Zeit umzusetzen.

Die Möglichkeit der nachträglichen Untersagung und ihrer Folgen müssen vor allem auch vor dem Hintergrund der ergänzenden Regelungen der Absätze 6 und 7 betrachtet werden. Danach können auch weitere Komponenten des Herstellers im Falle einer fehlenden Vertrauenswürdigkeit untersagt werden. Unter den bereits oben benannten Aspekten der Planungs- und Rechtssicherheit der Betreiber halten wir diese erweiterte Rechtsfolge für äußerst problematisch. So könnte bereits im Falle des Absatz 6 der erstmalige Verstoß ausreichen, der zur weiteren Untersagung führt. Darüber hinaus fehlt es der Regelung auch an generellen Verfahrensregelungen. Während die Untersagung einer Komponente im direkten Verfahren mit einem Betreiber erfolgt, greift die nachträgliche Untersagung nach den Absätzen 6 und 7 wohl unabhängig von bestimmten Betreibern. Hier stellt sich dann die Frage, woher die Betreiber die nötigen Informationen erhalten, wenn die Entscheidung über die weitere Untersagung „kritischer Komponenten“ nicht innerhalb ihres eigenen Verfahrens getroffen wird. Darüber hinaus bedürfte eine solche Regelung unbedingt entsprechender Vorschriften, die die Umsetzungszeit regeln. Wenn hiermit ggf. betreiber-übergreifend die kritischen Komponenten von Herstellern untersagt werden, muss den Betreibern für die Umsetzung entsprechend Zeit eingeräumt werden. Andernfalls drohen durch diese Vorgaben erhebliche Gefahren für die IT-Sicherheit, wenn alle betroffenen Betreiber innerhalb kürzester Zeit entsprechende Alternativlösungen abwägen und implementieren müssten.

Wir möchten daher darauf hinweisen, dass diese Bedenken im Rahmen einer nachträglichen Untersagung berücksichtigt werden müssen. Zu begrüßen ist, dass der Kabinettsbeschluss jedenfalls die Beteiligung der betroffenen Ressorts in Absatz 7 ergänzt hat.

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

Präsidium: Martin Witt (Präsident), David Zimmer (Vizepräsident), Valentina Daiber, Michael Jungwirth,
Uwe Nickl, Karsten Rudloff, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Jürgen Grützner

b) Recht auf rechtliches Gehör

Bevor das BMI mit der Zustimmung der beteiligten Ressorts den Einsatz von kritischen Komponenten aufgrund fehlender Vertrauenswürdigkeit des Herstellers (nachträglich) untersagen darf, ist es zwingend erforderlich, dass die Betroffenen angehört werden. Dies gebietet das grundrechtlich geschützte Recht auf rechtliches Gehör und ist in Anbetracht der drastischen Folgen einer – vor allem nachträglichen – Untersagung nach dem Verhältnismäßigkeitsgrundsatz für die Betreiber geboten.

c) Regress gegenüber dem Staat

§9b BSIG-E führt zu erheblichen Rechts- und Planungsunsicherheiten bei den Betreibern kritischer Infrastrukturen. Wie gezeigt fehlt es an nachprüfbaren Kriterien woran das BMI und die beteiligten Ressorts die fehlende Vertrauenswürdigkeit der Hersteller festmachen können und dürfen. Ergänzend fehlt es an konkretisierten Instrumenten der Betreiber sich vor der Entscheidung im Wege des einstweiligen Rechtsschutzes zu schützen. Die Folgen für die Betreiber, aber auch für die Sicherheit der Netze aufgrund fehlender Umsetzungszeiten sind groß. Es besteht die Gefahr, dass Hersteller aus unberechtigten Gründen als nicht vertrauenswürdig eingestuft werden und den Betreibern hieraus erhebliche Schäden entstehen können. Sofern es an entsprechenden Schutzinstrumenten fehlt, die den Schadenseintritt verhindern, muss der Staat entsprechend haftbar gemacht werden können.

d) Bestandsschutz

Abschließend sollte auch klargestellt werden, dass die Verpflichtungen keine Auswirkungen auf bereits langjährig erprobte und zuverlässig eingesetzte Komponenten haben. Es bedarf eines Schutzes der derzeitigen Bestandsnetze, weshalb sich die Pflichten nur auf Komponenten beziehen dürfen, die seit Inkrafttreten des neuen Gesetzes (bzw. nach Geltung der Verordnung zur Konkretisierung kritischer Komponenten) eingebaut wurden. Andernfalls droht den Verpflichteten hier ein erheblicher Investitionsaufwand, der bei der damaligen Auswahl der entsprechenden Komponenten nicht berücksichtigt werden konnte. Dies kann nicht nur zu erheblichen Investitionen führen, sondern beeinflusst auch direkt den zukünftigen Ausbau der Infrastrukturnetze.

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

Präsidium: Martin Witt (Präsident), David Zimmer (Vizepräsident), Valentina Daiber, Michael Jungwirth,
Uwe Nickl, Karsten Rudloff, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Jürgen Grützner

X. Offenlegungspflicht (§ 10 Abs. 6 BSIG-E)

Der neue § 10 Abs. 6 BSIG-E sieht vor, dass das BMI unter Beteiligung von Verbänden und des BMWi durch Rechtsverordnung die Offenlegung von Schnittstellen und die Einhaltung etablierter technischer Standards bestimmen kann. Eine derart allgemeine Anordnungsbefugnis zur Offenlegung von Schnittstellen, Einhaltung etablierter technischer Standards und Interoperabilität halten wir aus europarechtlichen Gründen für äußerst problematisch. Noch dazu, weil generell von Komponenten und Prozessen gesprochen wird, anstatt den Fokus auf kritische Komponenten zu begrenzen und keine Konkretisierung „etablierter" technischer Standards erfolgt. Hiermit wird das BMI ermächtigt, Komponenten über die „kritischen Komponenten nach § 2 Abs. 13 BSIG-E" hinaus zu regulieren, ohne dass der Zweck dieser Ermächtigung erkennbar ist. Die Offenlegung von Schnittstellen dient jedenfalls nicht der Erreichung der Schutzziele des IT-SiG, also der Gewährleistung der Cyber- und Informationssicherheit. Im Gegenteil: Durch die Offenlegung wird ein Sicherheitsrisiko dergestalt geschaffen, dass sensible, für den Schutz der Netzwerke relevante Informationen, in die Hände böswilliger Akteure fallen könnten. § 10 Abs. 6 sollte damit ersatzlos gestrichen werden.

XI. Bußgelder (§ 14 BSIG-E)

Abschließend möchten wir erneut darauf hinweisen, dass die Bußgelder aufgrund des Verweises auf § 30 Absatz 2 Satz 3 OWiG unverhältnismäßig hoch ausfallen können. Der Verweis auf das OWiG sollte daher unbedingt gestrichen werden.

Wir bitten um die Berücksichtigung der aufgezeigten Erwägungen und stehen für Rückfragen gerne zur Verfügung.

VATM Verband der Anbieter von Telekommunikations- und Mehrwertdiensten e. V.
Frankenwerft 35 • 50667 Köln • Tel.: 0221 3767725 • Fax: 0221 3767726 • E-Mail: vatm@vatm.de

Präsidium: Martin Witt (Präsident), David Zimmer (Vizepräsident), Valentina Daiber, Michael Jungwirth,
Uwe Nickl, Karsten Rudloff, Rickmann von Platen, Norbert Westfal, Peter Zils • Geschäftsführer: Jürgen Grützner