STELLUNGNAHME

zum Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat

ENTWURF EINES ZWEITEN GESETZES ZUR ERHÖHUNG DER SICHERHEIT INFORMATIONSTECHNISCHER SYSTEME

(Zweites IT-Sicherheitsgesetz – IT-SiG 2.0)

8. Dezember 2020

BvD e.V.

DATENSCHUTZ GESTALTEN

ÜBERSICHT

1. VORBEMERKUNGEN

Es handelt sich um den Referentenentwurf des Bundesministeriums des Innern, für Bau und Heimat (BMI) mit Stand vom 12. Dezember 2020, welcher innerhalb der Bundesregierung noch nicht abgestimmt wurde. Die Bundesregierung plant die Einbringung eines Entwurfs für die Kabinettsitzung am 16. Dezember 2020, mit grundlegenden Änderungen im Rahmen einer Ressortabstimmung ist innerhalb dieser Zeitspanne nicht zu rechnen. Aus der vom BMI äußerst kurz bemessenen Zeitspanne von nur einer Woche für ein Gesetz, welches die Überwachungsbefugnisse massiv ausweitet, resultiert insbesondere, dass eine adäquate Verbändeanhörung nicht erfolgen kann und ebenfalls keine ausreichende Gelegenheit für die Ressorts besteht, die Rückmeldungen in einer weiteren Ressortabstimmung zu reflektieren.

Aufgrund der kurzen Zeitspanne zur Kommentierung kann in dieser Stellungnahme nur auf die wesentlichen Aspekte der geplanten Regelungen eingegangen werden. Eine fundierte Bewertung im Sinne von konstruktiven Änderungsvorschlägen für das Gesetzesvorhaben ist in diesem Zeitrahmen nicht möglich.

2. ALLGEMEINE HINWEISE

Grundsätzlich sind Bestrebungen zur Erhöhung der IT-Sicherheit zu begrüßen. Dazu gehört insbesondere auch die Anpassung des am 17. Juli 2015 verabschiedeten und am 24. Juli 2015 im Bundesanzeiger veröffentlichten IT-SiG. Inhaltlich greift das IT-SiG 2.0 die Regelungen aus dem IT-SiG 1.0 auf, sodass in gewisser Weise eine ebenfalls zu begrüßende Fortschreibung des IT-SiG 1.0 erfolgt. Jedoch kommt es natürlich auf die Details der Neuregelungen an und hier bestehen unserem Erachten nach erheblicher Anpassungs- und Nachbesserungsbedarf.

3. ERFÜLLUNGSAUFWAND FÜR DIE WIRTSCHAFT

Der Aufwand für die Wirtschaft ist deutlich zu niedrig geschätzt. Das Jahresgehalt eines gut ausgebildeten IT-Sicherheitsfachmannes liegt bei etwa 80.000 Euro zzgl. Sozialabgaben. Jedes Unternehmen hat heute schon entsprechendes Personal, jedoch wird allein durch die bürokratischen Mehraufwände des Referentenentwurfs hier erheblicher Personalbedarf geschaffen. Die Kosten sollten im Referentenentwurf eher von dreistelligen Millionenbeträgen ausgehen. Dies sind erhebliche Mehrbelastungen für die deutsche Wirtschaft, zudem werden aus den untergesetzlichen Ausführungen sicherlich noch deutliche zusätzliche Beträge resultieren.

Dies ist in normalen Zeiten schon kaum zu finanzieren, jedoch gerade angesichts der Corona-Krise und der mit den staatlichen Verordnungen einhergehenden Begrenzung der wirtschaftlichen Aktivitäten wird die Bundesregierung mit diesem Gesetz einige Industrieunternehmen dazu bringen, ihre Unternehmungen in diesen Bereichen einzustellen.

Die enthaltenen Anforderungen gehen zudem deutlich über die europäischen Regelungen hinaus. Weder auf EU-Ebene noch auf Ebene einzelner Mitgliedstaaten sind vergleichbare Regelungen in der Diskussion. Damit haben wir nicht nur ein unterschiedliches Sicherheitsniveau, sondern auch abweichende Wettbewerbsbedingungen innerhalb der EU. Es ist davon auszugehen, dass wir in Deutschland anschließend höhere Anforderungen haben als im (restlichen) EU-Binnenmarkt. Da gerade im EU-Binnenmarkt jedoch Handelshemmnisse nicht gestattet sind, werden Dienstleistungen und Produkte aus dem EU-Binnenland in Deutschland eingesetzt werden: Deutsche Unternehmen bekommen einen massiven Wettbewerbsnachteil.

Was die hohen Kosten sowie das Ungleichgewicht bzgl. der Anforderungen innerhalb des EU-Binnenmarktes für den Industriestandort und insbesondere für die Innovation im Bereich der Informationstechnologie in Deutschland bedeutet, ist natürlich offensichtlich: Die Abhängigkeit von anderen Staaten wird noch stärker als bisher verankert.

4. ZU ARTIKEL 1: ÄNDERUNG DES GESETZES ÜBER DAS BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSIG)

4.1. Kritische Kernkomponenten

4.1.1. Begriffsbestimmung

Ein wesentlicher Punkt, der mit dem im IT-SiG 2.0 enthaltenen BSIG-E adressiert werden sollte, ist die Frage zum Umgang mit den in § 2 Abs. 13 BSIG-E definierten „kritischen Komponenten". Anforderungen hinsichtlich IT-Sicherheit sind durch Betreiber nur umsetzbar, wenn die Hersteller der eingesetzten IT-Systeme diese auch entsprechend sicher (weiter)entwickeln.

Die Regelung in § 2 Abs. 13 BSIG-E enthält leider keine rechtssichere Definition des Begriffes „kritische Komponente", sodass hier Komponenten eher willkürlich zugeordnet werden können. Die Begriffsdarstellung und die nachgelagerten Klarstellungen genügen u. E. nicht dem Bestimmtheitsgebot demokratischer Gesetzgebung. Insbesondere stellt sich die Frage, warum für den TK-Sektor lediglich mittelbar über den Katalog der Sicherheitsanforderungen eine Bestimmung erfolgt, für alle anderen kritischen Komponenten jedoch – richtigerweise – das Parlament über die Notwendigkeit und den Inhalt entsprechender Regelungen entscheidet.

Weiterhin ist zu bedenken, dass die Entscheidung, was eine „kritische Komponente" für einen Betreiber darstellt, tiefes Fachwissen aus dem jeweiligen Sektor benötigt. Dies kann eine Behörde, die selbst entsprechende Sektoren nicht betreibt, allein durch Buchwissen kaum beurteilen; die Infrastruktur bzw. deren Architektur ist aus unserer Sicht bzgl. Der Beurteilung von kritischen Komponenten von herausragender Bedeutung und kann nicht allein vom „grünen Tisch" aus beurteilt werden. Daher raten wir, die Hinzuziehung von Betreibern und Herstellern potenzieller kritischer Komponenten bei der Festlegung den entsprechenden Listen gesetzlich festzulegen.

4.1.2. Regelungen zur kritischen Komponente

Entsprechend § 9b BSIG-E ist der Einsatz dieser Komponenten vorab gegenüber dem BMI anzuzeigen. Das bringt einerseits einen deutlichen Verwaltungsaufwand, andererseits auch entsprechende Verzögerungen bei der Digitalisierung der regulierten Bereiche mit sich. Die politischen Ziele einer raschen Digitalisierung, wie sie beispielsweise im regulierten Sektor des Gesundheitswesens angestrebt sind, dürften sich damit um eine unbekannte, aber sicherlich nicht in Monaten messbaren Zeitraum verschieben.

Positiv festzuhalten ist, dass der Inhalt der in § 9b BSIG-E eingeführten Vertrauenswürdigkeitserklärung vom BMI festgelegt wird und nicht - wie ursprünglich diskutiert - durch die Betreiber selbst. Nur so kann ein einheitlicher Rahmen hinsichtlich der Erfordernisse und damit Rechtssicherheit für die Betreiber geschaffen werden.

Das BMI kann den Einsatz von kritischen Komponenten bestimmter Hersteller ggf. untersagen. Weiterhin kann das BMI in einer weiteren Eskalation auch unter entsprechender Fristwahrung für bereits eingesetzte Technik die Verwendung untersagen. Eine solche Untersagung der Nutzung führt zur faktischen Stilllegung dieser Komponenten. Dies erstreckt sich nicht nur auf eingesetzte kritische Kernkomponenten, sondern auch auf Komponenten desselben Herstellers, deren Funktionen nicht kritisch sind. Dadurch erfolgt ein massiver nachträglicher Eingriff in bereits in der Vergangenheit auf Basis geltenden Rechts getroffene Investitionsentscheidungen.

In § 9b Abs. 5 BSIG-E werden eine Reihe von Kriterien genannt, anhand derer die Vertrauenswürdigkeit eines Herstellers in Frage gestellt werden kann. Diese können z. T. erst in der Betriebsphase entsprechender Komponenten beurteilt werden, wie beispielsweise ein Verstoß gegen in der Vertrauenswürdigkeitserklärung gegebenen Verpflichtungen oder fehlende Meldungen bekannter bzw. bekannt gewordener Schwachstellen. Hier stellt sich die Frage, ob daraus Pflichten für Betreiber (z. B. Meldepflichten) resultieren. Aber insbesondere ist die Frage, was aus einer nachträglich festgestellten Nichterfüllung in § 9b Abs. 5 BSIG-E genannter Kriterien für ein nachträgliches Verbot derartiger Hersteller bedeuten würde.

Da keine finanziellen Kompensationen formuliert sind, sind die finanziellen Folgen eines nachträglichen Verbotes, die im Extremfall bis zur Insolvenz einzelner Betreiber oder Hersteller reichen können, nicht kalkulierbar und den Betreibern und Herstellern nicht zumutbar. Es ist auch nicht nachvollziehbar, warum derartige Kompensationen im Rahmen des Atom- und/oder Kohleausstiegs gewährt wurden, hier aber weder Bestandsschutz noch Kompensation greifen sollen.

4.2. Unternehmen im besonderen öffentlichen Interesse

Die mit § 2 Abs. 14 BSI-G erfolgte Einbeziehung von weiteren relevanten Unternehmen außerhalb der KRITIS-Betreiber ist grundsätzlich zu begrüßen, dient sie doch der Erhöhung der IT-Sicherheit.

Jede Ausdehnung muss jedoch auch der Prüfung der Rechtssicherheit standhalten. Es bedarf daher klarer Formulierungen auf Gesetzesebene, welche Kriterien für weitere Verpflichtete gelten. Das recht allgemein gehaltene Tatbestandsmerkmal „Verarbeitung staatlicher Verschlusssachen" nach § 60 Außenwirtschaftsverordnung (Nr. 1) muss daher ebenso auf Gesetzesebene konkretisiert werden, wie die Kriterien für die Liste von Unternehmen mit erheblicher volkswirtschaftlicher Bedeutung (Nr. 2).

In der vorliegenden Form stellt sich die Frage, welche Messbarkeitskriterien zur Festlegung eines Unternehmens von erheblicher volkswirtschaftlicher Bedeutung führen. Es existiert zwar das Gutachten der Monopolkommission nach § 44 GWB mit einer Liste der nach inländischer Wertschöpfung 100 größten Unternehmen i Unternehmen[1], jedoch leitet sich auch hieraus nicht deren Bedeutung i.S.v. § 2 Abs. 14 Nr. 2 BSI-G ab.

In der vorliegenden Form sind die Kriterien zu unbestimmt und aufgrund der fehlenden Rechtssicherheit abzulehnen.

4.3. Festlegungen bzgl. des BSI

4.3.1. Aufgaben des Bundesamtes

§ 3 Abs. 1 Ziff. 20 BSI-G legt fest, dass dem BSI die „Entwicklung und Veröffentlichung eines Stands der Technik bei sicherheits-technischen Anforderungen an IT-Produkte" innewohnt. Hier stellt sich die Frage, ob und wenn ja, wie das BSI sich selbst in die Lage versetzt als Nicht-Marktteilnehmer im engeren Sinne einen Stand der Technik festzulegen. Der Stand der Technik ergibt sich aus den jeweiligen branchenüblichen Gepflogenheiten, welche dem BSI – zumindest zeigte sich dies in der Vergangenheit z. B. im Bereich des Gesundheitswesens - regelhaft nicht bekannt sind. Insofern existiert das Risiko, dass die Entwicklung eines Standes der Technik durch das BSI nicht dem realen Stand der Technik entspricht.

1 Monopolkommission: Hauptgutachten XXIII: Wettbewerb 2020 vom 29. Juli 2020. Online, zitiert 2020-12-03.
Abrufbar unter https://www.monopolkommission.de/de/gutachten/hauptgutachten/330-xxiii-gesamt.html
bzw. pdf-Datei unter https://www.monopolkommission.de/images/HG23/HGXXIII_Gesamt.pdf

Wir begrüßen, dass mit § 3 Abs. 5a BSIG-E die Aufgaben und Befugnisse gemäß Verordnung (EU) 2019/881 („EU Cybersecurity Act") an das BSI übertragen wird. Um das Ziel der europäischen Harmonisierung durch das BSIG-E zu unterstützen, müssen jedoch nationale Regelungen unterbleiben, wenn entsprechende europäische Regelungen vorhanden sind.

4.3.2. Kontrolle der Kommunikationstechnik

Die in § 4a Abs. 1 BSIG-E enthaltene Regelung hinsichtlich der unentgeltlichen Vorlagepflicht Dritter gegenüber dem BSI beinhaltet eine Verpflichtung, wobei die daraus resultierenden Aufwendungen bei Dritten nicht abschätzbar: Das damit verbundene Risiko für Verpflichtete kann nicht taxiert werden. Vorzuziehen ist eine Regelung, in welcher Dritten die Kosten ab einem festzulegenden Betrag zu erstatten sind; Bagatellsummen sollten keinen Bürokratieaufwand erzeugen, aber dreistellige Eurobeträge und darüber hinaus sollten ersetzt werden.

Das nach § 4a Abs. 2 BSIG-E zu gewährende Zutrittsrecht ist sicherlich angemessen. Aber gerade im Bereich kritischer Infrastrukturen wie auch bei Herstellern kritischer Komponenten ist aus Gründen der Betriebssicherheit ein geregelter Vorgang, welcher zumindest die Anmeldung eines Zutrittsgesuchs beinhaltet, zwingend erforderlich.

4.3.3. Zentrale Meldestelle

Die Einführung einer zentralen Meldestelle in § 4b BSIG-E ist grundsätzlich begrüßenswert. Aber aktuell werden der Wirtschaft nahezu mit jedem neuen Gesetz neue Meldeadressaten aufgebürdet. Hier bedarf es einer „One-Stop-Shop-Lösung" mit verwaltungsinterner Weiterleitung der Informationen.

4.3.4. Umgang mit detektierten Schwachstellen

Gemäß den Vorgaben in § 7b Abs. 1 BSIG-E kann das BSI Sicherheitslücken und anderen Sicherheitsrisiken wie beispielsweise Schadprogramme an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme detektieren. Diese Regelung ist grundsätzlich sinnvoll, jedoch gilt ein Portscan als ein Angriff. Portscans sind datenschutzrechtlich unzulässig und strafrechtlich sanktioniert. Es ist uns nicht ersichtlich, weshalb das BSI im genannten Zusammenhang davon Gebrauch machen sollte.

Weiterhin löst ein Portscan, der häufig einen Penetrationsversuch ankündigt, entsprechende Aktionen bei Betreibern aus. Die Bewertung derartiger Vorgänge bedarf einer hohen Kompetenz und eines entsprechend hohen Ressourceneinsatzes durch den Betreiber, was zumindest bei vom BSI ausgeführten Portscans zu einen unnötigen Einsatz anderweitig benötigter Ressourcen und natürlich zu entsprechenden Kosten bei den Betreibern führen kann.

Daher sollte das BSI, sofern der Gesetzgeber zwingenden Bedarf für diese Regelung sieht, Portscans grundsätzlich mit den Betreibern absprechen müssen, sodass diese wissen, wann das BSI welche Komponenten prüft. Nur wenn durch vom BSI dokumentierte und bei Bedarf auch vom Betreiber durch Einblick in diese Dokumentation nachvollziehbare, für den jeweiligen Fall existierende spezifische Gründe eine Vorab-Information des Betreibers den Zweck einer Detektion verhindern, sollte das BSI auf eine Vorab-Information verzichtet dürfen.

Alternativ sollte eine Schadensersatzregelung für durch Detektionsbemühungen ausgelöste Schäden eingeführt werden.

§ 7b Abs. 2 BSIG-E enthält die Legaldefinition eines ungeschützten IT-Systems. Diese Definition ist in höchstem Maße unpräzise. Entsprechend der Definition würde faktisch jeder Softwarefehler zu einem gemäß der Definition ungeschützten Zustand führen. Es fehlt zumindest die Einbeziehung der Kritikalität einer öffentlich bekannten Sicherheitslücke.

In § 7b Abs. 3 BSIG-E sind Verantwortliche bzgl. Sicherheitslücken bzw. Sicherheitsrisiken nur zu informieren, wenn „ überwiegende Sicherheitsinteressen" dem nicht entgegenstehen. Dies bedeutet letztlich, dass es nicht transparent dargelegte Gründe gibt, die es rechtfertigen, dass Sicherheitslücken als Backdoor seitens BSI oder von anderen genutzt werden können. Die Nicht-Information der Betroffenen kann in dieser Form als vorsätzliche Ausnutzung kritisiert werden und dadurch würde das BSI aus unserer Sicht fahrlässig die Sicherheit der betroffenen informationstechnischen Systeme, welche ja kritische Infrastrukturen darstellen, gefährden. Insofern sollte die einschränkende Formulierung des Entwurfs gelöscht werden.

4.3.5. Anordnungen gegenüber Betreibern

In §§ 7c und 7d BSIG-E sind Regelungen enthalten, bei denen nicht ersichtlich ist, auf welcher Basis das BSI sinnhafte konkrete Maßnahmen anordnen kann; letztlich kennen die Betreiber ihre Systeme selbst am besten und nur sie können abschätzen, welche konkreten Maßnahmen erforderlich sind.

Insofern sind konkrete und eindeutige Hinweise auf Schwachstellen immer wünschenswert, ggf. auch mit allgemeinen Hinweisen bzgl. Zielsetzung der Sicherheitsanforderung. Aber die Ergreifung konkreter Maßnahmen zur Beseitigung von Schwachstellen muss die Aufgabe des Betreibers bleiben, u. U. mit Unterstützung des jeweiligen Herstellers der kritischen Komponente.

4.3.6. Sicherheit in der Informationstechnik Kritischer Infrastrukturen

Nach § 8d Abs. 2 BSIG gilt § 8a BSIG nicht für TK-Anbieter oder Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes. § 8a Abs. 1 BSIG verweist auf § 10 Abs. 1 BSIG, welcher wiederum auf § 2 Abs. 10 S. 1 Nr. 2, welcher gerade die in § 8d Abs. 2 BSIG herausgenommenen Sektoren adressiert. Somit ist die bestehende Rechtslage unklar: Gilt § 8a BSIG für TK-Anbieter oder Betreiber von Energieversorgungsnetzen oder Energieanlagen im Sinne des Energiewirtschaftsgesetzes oder nicht?

Hier sollte mit der Neuregelung des BSIG Rechtssicherheit geschaffen, d. h. eine eindeutige Regelung getroffen werden.

Weiterhin ist die nach wie vor fehlende Einbeziehung international anerkannter Standards in § 8a Abs. 1 BSIG zu kritisieren. Etablierte und funktionierende Prozesse nach ISO 27001ff entsprechen dem international anerkannten Stand der Technik, der letztlich auch für Deutschland gelten sollten. Von diesen international anerkannten Standards losgelöste und zusätzliche Anforderungen zu erheben, ist nicht zielführend und führt zu unverhältnismäßigen Mehraufwänden ohne die IT-Sicherheit entsprechend zu fördern.

Die in § 8a Abs. 1b BSIG-E von Betreibern kritischer Infrastrukturen geforderte Speicherung von Protokolldaten in Systemen (ohne personenbezogene Daten) für mindestens 4 Jahre ist eine massive Verpflichtung zur anlasslosen Speicherung, welche aus Sicht der IT-Sicherheit regelhaft nicht erforderlich ist und letztlich einer anlasslosen Vorratsdatenspeicherung nahekommt und daher abzulehnen ist. Wir fordern daher, die Speicherdauer auf ein Jahr zu begrenzen.

4.3.7. Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen

In § 8b Abs. 3 BSIG-E wird Betreibern eine Meldepflicht hinsichtlich der von ihnen betriebenen Kritischen Infrastrukturen beim Bundesamt auferlegt, jedoch fehlen Vorgaben für die Meldung. Es ist unklar, welche Angaben die Meldung enthalten soll. Formal reicht eine Meldung „wir betreiben eine kritische Infrastruktur" aus. Hier müssen Konkretisierungen bzgl. des Detaillierungsgrad erfolgen, z. B. Angaben zum Betreiber, Sektor und eingesetzten System/-en.

§ 8b Abs. 4 BSIG enthält derzeit zum Teil sehr unscharf gefasst Vorgaben. Die Überarbeitung des BSIG sollte aus unserer Sicht genutzt werden, und die Meldekriterien und -schwellen der Durchführungsverordnung (EU) 2018/151 für die Anwendung der Richtlinie (EU) 2016/1148 in das BSIG-E zu integrieren und somit für den IT-Sektor zur Anwendung bringen, damit hier eine Harmonisierung mit den europäischen Vorgaben erfolgt.

4.3.8. Zertifizierung

In § 9 Abs. 4 BSIG-E fehlt aus unserer Sicht eine Verpflichtung zur schriftlichen Begründung bei Versagung des Zertifikats. Aus Gründen eines effektiven Rechtsschutzes ist eine entsprechende Regelung zwingend erforderlich, da ansonsten kaum eine Möglichkeit gegen den Verwaltungsakt nicht vorgegangen werden kann.

Weiterhin ist in § 9 Abs. 4 BSIG-E zu berücksichtigen, dass die Verordnung (EU) 2019/881 vorsieht, dass bereits vorhandene Zertifizierungsschemata innerhalb der EU wechselseitig anerkannt werden; eine weitere Prüfung bzw. ergänzende lokale Verpflichtungen sind hier nicht vorgesehen. Daher ist zu kritisieren, dass die Bemühungen der ENISA zur begrüßenswerten harmonisierten Durchsetzung durch die Regelungen im BSIG-E konterkariert werden. Dieser Aspekt trifft gleichermaßen auf § 9 Abs. 7 BSIG zu. Es widerspricht fundamental dem Ansatz eines harmonisierten EU-Binnenmarktes, wenn auf der Verordnung (EU) 2019/881 basierende Zertifizierungen in Deutschland nicht anerkannt werden würden.

Die Regelung hinsichtlich des Vetorechts des BMI in § 9 Abs. 4a BSIG-E ist anzulehnen. In § 9 BSIG-E geht es ausschließlich um rein technische Prüfungen, unabhängig der jeweiligen Hersteller. Die im Textentwurf mitschwingende Frage der Vertrauenswürdigkeit sollte ausschließlich in § 9b BSIG-E geregelt werden. § 9 Abs. 4a sowie der gleichlautend § 9 Abs. 6 Nr. 2 BSIG-E sind aus unserer Sicht ersatzlos zu streichen.

4.3.9. Nationale Behörde für die Cybersicherheitszertifizierung

Wie in Abschnitt 4.3.1 auf Seite 5 beschrieben ist die Festlegung des BSI als nationale Zertifizierungsstelle zur Umsetzung der aus der Verordnung (EU) 2019/881 resultierenden Anforderungen des Unionsrechts zu begrüßen.

Allerdings müsste die jeweilige Rechtslage der Nachbarstaaten untersucht werden, um festzustellen, ob eine Vergleichbarkeit mit den Regelungen im BSIG-E und insbesondere § 9a BSIG-E gegeben ist. Andernfalls wäre zu befürchten, dass der Standort Deutschland wegen höherer Anforderungen im Vergleich zu anderen Ländern des EU-Binnenmarktes geschwächt wird.

Zu prüfen ist auch, ob die Ermächtigung nach § 9a Abs. 3 BSIG-E sich auch auf die Prüfung bereits im EU-Ausland zertifizierter Produkte erstreckt bzw. darauf, deren Einsatz zu untersagen.

4.3.10. Freiwilliges IT-Sicherheitskennzeichen

§ 9c BSIG-E enthält Regelungen für ein freiwilliges IT-Sicherheitskennzeichen. Das BSI kann gemäß § 9c Abs. 8 BSIG-G die Einhaltung des IT-Sicherheitskennzeichens prüfen und ggf. die Unterlassung der Nutzung des Kennzeichens regeln. Das klingt auf den ersten Blick nachvollziehbar und vernünftig, jedoch sollte aus der „kann"-Verpflichtung eine „muss"-Regelung werden, zumindest wenigstens bei anlassbezogenen Vorfällen– ein Sicherheitskennzeichen ohne regelmäßige Auditierung der Einhaltung der Vorgaben wird kein Vertrauen erzeugen. Viele Details sollen in einer Rechtsverordnung sowie einer Technischen Richtlinie des BSI geregelt werden. Daher bleiben viele Fragen offen.

ABER: Grundsätzlich stellt sich jedoch auch hier die Frage, warum Deutschland hier einen Sonderweg geht, wenn Verordnung (EU) Nr. 526/2013 entsprechende Zertifizierungen berücksichtigt. ErwGr. 67 der Verordnung (EU) Nr. 526/2013 beschreibt ja gerade, dass nationale Regelungen kein kohärentes und ganzheitliches Konzept entstehen lassen, und folgert völlig zu Recht in ErwGr. 69 der Verordnung (EU) Nr. 526/2013, dass es notwendig ist, „einen gemeinsamen Ansatz zu verfolgen und einen europäischen Rahmen für die Cybersicherheitszertifizierung aufzubauen". Dies wird mit § 9c BSIG-E konterkariert. Daher empfehlen wir, § 9c BSIG-E ersatzlos zu streichen.

4.4. Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse

Die Einbeziehung weiterer Unternehmen in § 8f BSIG-E ist grundsätzlich zu begrüßen, da dies ein weiterer sinnvoller Schritt zur Erhöhung der IT-Sicherheit ist. Wir verweisen jedoch auf die im Abschnitt 4.2 auf Seite 4 dargestellte fehlende Rechtssicherheit bei der Bestimmung der Unternehmen, für welche die Regelungen gelten sollen.

4.5. Untersagung des Einsatzes kritischer Komponenten

Positiv hervorzuheben ist die inhaltliche Weiterentwicklung der in § 9b BSIG-E enthaltenen Regelungen zum Umgang mit der politischen Vertrauenswürdigkeit im Vergleich zu den Vorentwürfen zum IT-SiG 2.0.

Jedoch enthält der Entwurf nach wie vor diverse Schwachstellen. Gemäß § 8b Abs. 3 BSIG-E sind Betreiber Kritischer Infrastrukturen „verpflichtet, die von ihnen betriebenen Kritischen Infrastrukturen beim Bundesamt zu registrieren und eine Kontaktstelle zu benennen". Die in § 9b BSIG-E geforderte zusätzliche Meldung beim BMI erzwingt eine Doppelmeldung. Dies bedingt für Betreiber die Auseinandersetzung mit zwei Organen (BSI und BMI), bzw. in Anbetracht der Zuständigkeit der BNetzA im Sektor der Telekommunikation sogar zu dreifacher Regulierung mit entsprechendem Verwaltungsaufwand beim Betreiber. Hier sollte behördenintern eine Kommunikation möglich sein und § 9b Abs. 1 BSIG-E ersatzlos gestrichen werden.

In § 9b Abs. 2 BSIG-E sind die Anforderungen nicht ausreichend hinsichtlich der erforderlichen Inhalte formuliert. Zur Wahrung der Rechtssicherheit muss der erwartete Inhalt der Garantieerklärung vollumfänglich vorab festgelegt werden. Die Anforderungen müssen angemessen gestaltet werden und nicht über das Maß hinausgehen, welches auch inländische Hersteller leisten könnten.

§ 9 Abs. 3 BSIG-E trifft den Begründungen nach Regelungen zum Erstbetrieb, § 9 Abs. 4 BSIG-E zum Weiterbetrieb. Hier sollte in § 9 Abs. 3 BSIG-E eine Klarstellung erfolgen, da dies aus dem Wortlaut von § 9 Abs. 3 BSIG-E nicht eindeutig hervorgeht.

Bzgl. des Entzugs der Vertrauenswürdigkeit verweisen wir auf die in Abschnitt 4.1.2 auf Seite 3 beschriebene erforderliche finanzielle Kompensation, welche bei nachträglichem Entzug der Betriebserlaubnis für Betreiber aus unserer Sicht erforderlich ist.

4.6. Einschränkung von Grundrechten

Insgesamt erfolgt eine deutliche Erweiterung der Anwendungsfälle erfolgter Grundrechtseinschränkungen. Diese sind jedoch nur zum Teil dem erweiterten Anwendungsbereich geschuldet. Beispielsweise ist für den in § 9a Abs. 5 BSIG-E geregelten Zutritt zu Betriebsstätten, Geschäfts- und Betriebsräume keine Einschränkung i.S.v. Art. 13 GG benötigt. § 20 BMG definiert eine Wohnung als „umschlossene Raum, der zum Wohnen oder Schlafen benutzt wird", Betriebsstätten, Geschäfts- und Betriebsräume stellen keine Wohnungen dar, der Grundrechtseingriff ist also nicht erforderlich und daher abzulehnen.

Kritisch anzumerken ist, dass die Regelungen an den entsprechenden Stellen eine richterliche Kontrolle nicht vorsehen.

4.7. Bußgeldvorschriften

Die konkrete Bußgeldbewährung einzelner Vorschriften des BSIG-E ist zu begrüßen, da die Regelungen für den Rechtsanwender Klarheit schaffen, wenn im materiellen Teil des BSIG-E ein angemessener Pflichtenkatalog etabliert wird, hier verweisen wir auf unsre Anmerkungen bzgl. fehlender Rechtssicherheit bei verschiedenen Regelungen.

5. ZU ARTIKEL 6: ÄNDERUNG DES ZEHNTEN BUCHES SOZIALGESETZBUCH

In § 67 Abs. 3 SGB X-E erfolgt durch die Ergänzung eine Verletzung des Sozialdatenschutzes. § 67 regelt die Zweckbindung für den Verantwortlichen, das Bundesamt für Sicherheit in der Informationstechnik ist sowohl aus Sicht des Sozialdatenschutzes als auch der Verordnung (EU) 2016/679 ein Dritter. D. h. bei Zugriffen auf Sozialdaten i. S. d. § 67 Abs. 3 SGB X-E erfolgt regelhaft eine Übermittlung, für welche Verantwortliche, d. h. die Stellen i.S.v. § 35 Abs. 1 SGB I, einen Erlaubnistatbestand benötigen. Jedoch wird mit der Regelung in § 67 Abs. 3 SGB X-E kein Erlaubnistatbestand für den Verantwortlichen zur Übermittlung der Sozialdaten an das BSI geschaffen.

In der vorliegenden Form müssen die in § 67 Abs. 3 SGB X-E enthaltenen Änderungen abgelehnt werden. Aus unserer Sicht ist die Regelung in dieser Form zu streichen.

Ggf. könnte in § 71 SGB X ein Erlaubnistatbestand zur Übermittlung von Sozialdaten aufgenommen werden, jedoch verlangt der hohe Schutzbedarf von Sozialdaten eine konkrete Benennung, welche rechtliche Pflicht eine Übermittlung durch den Verantwortlichen an den Empfänger erfordert. D. h. im BSIG-E müsste eine Rechtsgrundlage geschaffen werden, in § 71 SGB X-E könnte dann darauf verwiesen werden.

Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.

Mit mehr als 30 Jahren Erfahrung ist der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. die älteste Interessenvertretung für betriebliche und behördliche Datenschutzbeauftragte und -berater. BvD-Mitglieder sind in allen Branchen vertreten, insbesondere IT und IKT, Industrie/Produktion, Handel/Vertrieb, Beratung und Gesundheitsund Sozialwesen. Als erster Ansprechpartner der Betroffenen sind die BvD-Mitglieder Anlaufstelle für etwa fünf Millionen ArbeitnehmerInnen sowie einen Großteil der BürgerInnen/KonsumentInnen. Zudem sind sie als konstruktiv lösungsorientierte Datenschutzexperten ein wichtiger Partner für die verantwortliche Unternehmensleitung. Alle Vorstände, alle Leiter von Arbeitskreisen, Ausschüssen und Regionalgruppen des BvD bringen ihre praktische Erfahrung unentgeltlich in die Verbandsarbeit ein. Mit der Gründung des Europäischen Dachverbandes EFDPO hat der BvD zuletzt die Weichen für verstärkte Vernetzung und Kommunikation auf EU-Ebene gestellt.

BvD e.V.
DATENSCHUTZ GESTALTEN

IMPRESSUM

Herausgeber
Berufsverband der Datenschutzbeauftragten
Deutschlands (BvD) e. V.
Budapester Straße 31
10787 Berlin

T 030 . 26 36 77 60
F 030 . 26 36 77 63

bvd-gs@bvdnet.de

Stand
8. Dezember 2020

www.bvdnet.de