# Dr. Dennis-Kenji Kipker

# Synopse zum aktuellen Stand des Gesetzgebungsverfahrens für das IT-SiG 2.0

# Stand der Bearbeitung: 03.06.2020

Im Folgenden werden in einer tabellarischen Darstellung die Änderungen zwischen dem ersten Referentenentwurf zum IT-SiG 2.0 aus März 2019 und dem vor Kurzem an die Öffentlichkeit gelangten, überarbeiteten Entwurf aus Mai 2020 aufgezeigt, wobei vereinzelte Änderungen kommentiert und bewertet werden. Aufgegriffen werden in diesem Zusammenhang auch verschiedene Stellungnahmen weiterer Akteure zum neuen Gesetzentwurf. Aufgeführt sind dabei nur Änderungen, bei denen sich der alte von dem neuen Referentenentwurf unterscheidet. Die vorliegende Übersicht fokussiert dabei insbesondere auf diejenigen Änderungsvorschläge, die im Normungskontext relevant sind.

**Kontakt für Hinweise, Anregungen und Verbesserungsvorschläge:**

Dr. Dennis-Kenji Kipker
CERT@VDE
Stresemannallee 15
60596 Frankfurt am Main
E-Mail: dennis-kenji.kipker@vde.com

| Nummer | Gesetz | Aktueller Entwurf Mai 2020 | Entwurf März 2019 | Bewertung/Kommentar |
|---|---|---|---|---|
| 1 | **BSIG** | § 2 Abs. 8a BSIG-E:<br>Protokollierungsdaten sind Aufzeichnungen über die Art und Weise, wie die Informationstechnik genutzt wurde, über technische Ereignisse oder Zustände innerhalb eines informationstechnischen Systems und wie dieses mit anderen kommuniziert hat. Protokollierungsdaten dienen der Erkennung, Eingrenzung oder Beseitigung von Störungen oder Fehlern bei der Kommunikationstechnik oder von Angriffen. | § 2 Abs. 9 BSIG-E:<br>Protokollierungsdaten sind Aufzeichnungen über die Art und Weise, wie die Informationstechnik genutzt wurde, über technische Ereignisse oder Zustände innerhalb eines informationstechnischen Systems und wie dieses mit anderen kommuniziert hat. Protokolldaten nach Absatz 8 sind eine Teilmenge der Protokollierungsdaten. Protokollierungsdaten dienen der Erkennung, Eingrenzung oder Beseitigung von Störungen oder Fehlern bei der Kommunikationstechnik oder von Angriffen. | Minimale Wortlautänderung bezüglich der Definition von Protokollierungsdaten. Protokollierungsdaten sind personenbezogene Daten, sodass sich an dieser Stelle auch Fragen der betrieblichen Mitbestimmung stellen (vgl. § 87 Abs. 1 Nr. 6 BetrVG). |
| 2 | | § 2 Abs. 9a BSIG-E: | § 2 Abs. 9a BSIG-E: | Ausdehnung der Definition gegenüber der alten Fassung. Damit wird |

| | | | | |
|---|---|---|---|---|
| | | IT-Produkte sind Software sowie alle einzelnen oder miteinander verbundenen Hardwareprodukte. | IT-Produkte sind Softwareprodukte sowie alle einzelnen oder miteinander verbundenen Hardwareprodukte und Hardwarekomponenten, inklusive der zur einwandfreien Funktion eingesetzten Software. | der Fokus nicht nur auf den Schutz Kritischer Infrastrukturen, sondern generell auf IT-Produkte gelegt. Der aktuelle Gesetzentwurf geht damit über die europarechtlichen Vorgaben aus der EU NIS-RL hinaus.<br><br>Kritisch zu würdigen: V.a. zu weite Definition, da möglicherweise auch die Zurverfügungstellung von Diensten umfasst ist und das fast voraussetzungslose Auskunftsrecht nach § 7a Abs. 2 BSIG damit auf fast alle digitalen Produkte beziehbar wäre. |
| 3 | | § 2 Abs. 9b BSIG-E:<br>Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch | Keine Definition | Neu eingefügte Definition für „Systeme zur Angriffserkennung“. |

| | | | | |
|---|---|---|---|---|
| | | technische Werkzeuge und organisatorische Einbindung unterstützte Prozesse zur Erkennung von Angriffen auf informationstechnische Systeme. Die Angriffserkennung erfolgt dabei durch Abgleich der in einem informationstechnischen System verarbeiteten Daten mit Informationen und technischen Mustern, die auf Angriffe hindeuten. | | |
| 4 | | § 2 Abs. 13 BSIG-E:<br>Kritische Komponenten im Sinne dieses Gesetzes sind IT-Produkte, die in Kritischen Infrastrukturen eingesetzt werden und die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil Störungen der Verfügbarkeit, Integrität, Authentizität und Vertrau- | § 2 Abs. 13 BSIG-E:<br>Kernkomponenten für Kritische Infrastrukturen (KRITIS-Kernkomponenten) sind IT-Produkte, die zum Betrieb von Kritischen Infrastrukturen im Sinne dieses Gesetzes dienen und für diesen Zweck besonders entwickelt oder geändert werden. KRITIS-Kernkomponenten sind: | Neudefinition der „Kernkomponenten“ als kritische Komponenten. |

| | | | | |
|---|---|---|---|---|
| | | lichkeit dieser IT-Produkte zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können. Die kritischen Komponenten im Sinne dieses Gesetzes werden für Betreiber nach § 8d Abs. 2 Nr. 1 durch den Katalog von Sicherheitsanforderungen nach § 109 Abs. 6 TKG näher bestimmt. Alle übrigen kritischen Komponenten werden in einem Katalog des Bundesamtes näher bestimmt. Das Bundesamt gibt den Betreibern Kritischer Infrastrukturen Gelegenheit zur Stellungnahme. Der Katalog wird vom Bundesamt veröffentlicht. | 1. im Sektor Energie IT-Produkte für die Kraftwerksleittechnik, für die Netzleittechnik oder für die Steuerungstechnik zum Betrieb von Anlagen oder Systemen zur Stromversorgung, Gasversorgung, Kraftstoff- oder Heizölversorgung oder Fernwärmeversorgung,<br>2. im Sektor Wasser IT-Produkte für die Leit-, Steuerungs- oder Automatisierungstechnik von Anlagen zur Trinkwasserversorgung oder Abwasserbeseitigung,<br>3. im Sektor Informationstechnik und Telekommunikation IT-Produkte zum Betrieb von Anlagen oder Systemen zur Sprach- und Datenübertragung oder zur Datenspeicherung und -verarbeitung. Soweit IT-Produkte und deren Einsatz dem Anwendungsbereich des | |

| | | | | |
|---|---|---|---|---|
| | | | TKG unterfallen, gelten diese nur dann als KRITIS-Kernkomponenten im Sinne dieser Vorschrift, wenn sie durch den Sicherheitskatalog nach § 109 Absatz 6 TKG als solche festgelegt sind.<br>4. im Sektor Ernährung IT-Produkte zum Betrieb von Anlagen oder Systemen zur Lebensmittelversorgung.<br>5. im Sektor Gesundheit IT-Produkte zum Betrieb eines Krankenhausinformationssystems, zum Betrieb von Anlagen oder Systemen zum Vertrieb von verschreibungspflichtigen Arzneimitteln sowie zum Betrieb eines Laborinformationssystems,<br>6. im Sektor Finanz- und Versicherungswesen IT-Produkte zum Betrieb von Anlagen oder Systemen | |

| | | | | |
|---|---|---|---|---|
| | | | der Bargeldversorgung, des kartengestützten Zahlungsverkehrs, des konventionellen Zahlungsverkehrs, zur Verrechnung und der Abwicklung von Wertpapier- und Derivatgeschäften oder zur Erbringung von Versicherungsdienstleistungen,<br>7. im Sektor Transport und Verkehr IT-Produkte zum Betrieb von Anlagen oder Systemen zur Beförderung von Personen und Gütern im Luftverkehr, im Schienenverkehr, in der See- und Binnenschifffahrt, im Straßenverkehr, im öffentlichen Personennahverkehr oder in der Logistik,<br>8. im Sektor Entsorgung IT-Produkte zum Betrieb von Anlagen oder Systemen zur Abfallentsorgung. | |

| | | | | |
|---|---|---|---|---|
| 5 | | § 2 Abs. 14 BSIG-E:<br>Unternehmen im besonderem öffentlichen Interesse sind Unternehmen, die nicht Betreiber Kritischer Infrastrukturen nach Absatz 10 sind,<br>1. deren Geschäftstätigkeit unter § 60 Absatz 1 Nummer 1 bis 5 der Außenwirtschaftsverordnung in der jeweils geltenden Fassung fällt,<br>2. die aufgrund ihrer volkswirtschaftlichen Bedeutung und insbesondere ihrer erbrachten Wertschöpfung von besonderem öffentlichen Interesse sind oder<br>3. die einer Regulierung nach der Verordnung zum Schutz vor Gefahrstoffen in der jeweils geltenden Fassung unterliegen | § 2 Abs. 14 BSIG-E:<br>Infrastrukturen im besonderem öffentlichen Interesse sind Anlagen oder Teile davon, die dem Bereich Rüstung angehören und nach § 60 der Außenwirtschaftsverordnung in der jeweils geltenden Fassung wesentlich für die Sicherheitsinteressen der Bundesrepublik Deutschland sind,<br>1. dem Bereich Kultur und Medien angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung eine Gefährdung für die öffentliche Sicherheit eintreten würde, oder | Ersetzen der Infrastrukturen im besonderen öffentlichen Interesse durch Unternehmen im besonderen öffentlichen Interesse. Allgemein formuliert und daher kritisch zu würdigen; allerdings ist wohl anzunehmen, dass die volkswirtschaftliche Bedeutung letztendlich durch gerichtliche Konkretisierung und Auslegung beherrschbar ist.<br><br>Jedoch:<br>- Einführung von „Quasi-KRITIS“-Kategorie, die so aus der EU NIS-Richtlinie nicht bekannt ist.<br>- Zersplitterung der IT-Sicherheitsregulierung in Europa, die gerade |

| | | | | |
|---|---|---|---|---|
| | | Die Unternehmen im besonderem öffentlichen Interesse nach Nummer 2 werden durch die Rechtsverordnung nach § 10 Absatz 5 näher bestimmt. | 2. nicht von Absatz 10 erfasst sind, aber dennoch von erheblicher Bedeutung sind, weil durch ihren Ausfall oder ihre Beeinträchtigung die Geschäftstätigkeit von Unternehmen mit Zulassung zum Teilbereich des regulierten Marktes mit weiteren Zulassungsfolgepflichten (Prime Standard) nach § 48 Börsenordnung der Frankfurter Wertpapierbörse eingeschränkt und dadurch erhebliche volkswirtschaftliche Schäden eintreten würden. Die Infrastrukturen im besonderem öffentlichen Interesse nach Nummer 2 werden durch die Rechtsverordnung nach § 10 Absatz 5 näher bestimmt. | rechtspolitisch regelmäßig als störend und hinderlich empfunden wird. |

| | | | | |
|---|---|---|---|---|
| 6 | | § 3 Abs. 1 S. 2 Nr. 5a BSIG-E:<br>Erteilung von Befugnissen nach § 1 Absatz 2 des Gesetzes über die Akkreditierungsstelle als Konformitätsbewertungsstelle im Bereich der IT- Sicherheit tätig zu sein, insbesondere durch Anerkennung sachverständiger Stellen zur Durchführung von Prüfungen und Bewertungen im Rahmen der Zertifizierung nach § 9 Absatz 3; | § 3 Abs. 1 S. 2 Nr. 5a BSIG-E:<br>Erteilung der Befugnis nach § 1 Absatz 2 des Gesetzes über die Akkreditierungsstelle, als Konformitätsbewertungsstelle im Bereich der IT-Sicherheit tätig zu sein. Im Bereich der hochwertigen IT-Sicherheitszertifizierung Anerkennung der hierfür erforderlichen Sachkenntnis der Konformitätsbewertungsstelle nach § 9 Absatz 6; | Diese deutliche Befugniserweiterung des BSI dürfte einen Interessenkonflikt innerhalb der Organisation zur Folge haben: So kann das BSI nicht einerseits Ermittlungsbehörde sein, die Schwachstellen aufdeckt, andererseits aber die fraglichen Systeme vorher womöglich selbst zertifiziert haben.<br><br>Nach wie vor ist das BSI überdies keine unabhängige Behörde, sondern durch den Überbau des BMI geprägt, in dessen Zuständigkeit auch eingriffsintensive Behörden wie Nachrichtendienstbehörden und die Strafverfolgung fallen. Fraglich ist deshalb, wie mit solchen Informationen, die im Rahmen von Zertifizierungsverfahren |

| | | | | |
|---|---|---|---|---|
| | | | | erlangt wurden, im Weiteren umgegangen wird.<br><br>Im Hinblick auf die Erarbeitung von neuen Zertifizierungsmaßstäben sollte überdies die Regelung aus Art. 42 EU DS-GVO beachtet werden, soweit partielle Überschneidungen zu Datenschutz/Datensicherheit vorhanden sind, um doppelte Aufwände zu vermeiden. |
| 7 | | § 3 Abs. 1 S. 2 Nr. 5b BSIG-E: Wahrnehmung der Aufgaben und Befugnisse nach Artikel 58 Absatz 7 und 8 der Verordnung (EU) 2019/881 vom 17. April 2019 als nationale Behörde für die Cybersicherheitszertifizierung; | -- | |

| | | | | |
|---|---|---|---|---|
| 8 | | § 3 Abs. 1 S. 2 Nr. 17 BSIG-E:<br>Aufgaben nach den §§ 8a bis 8f als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen, digitaler Dienste, der Unternehmen im besonderen öffentlichen Interesse und der Hersteller von IT-Produkten; | § 3 Abs. 1 S. 2 Nr. 17 BSIG-E:<br>Aufgaben nach den §§ 8a bis 8h als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen, digitaler Dienste, der Infrastrukturen im besonderen öffentlichen Interesse und der Hersteller von IT-Produkten; | |
| 9 | | § 3 Abs. 1 S. 2 Nr. 19 und 20 BSIG-E:<br>19. Empfehlungen für Identifizierungs- und Authentisierungsverfahren und Bewertung dieser Verfahren unter dem Gesichtspunkt der Informationssicherheit;<br>20. Entwicklung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte. | § 3 Abs. 1 S. 2 Nr. 19 und 20 BSIG-E:<br>19. Entwicklung von Anforderungen an Identifizierungs- und Authentisierungsverfahren und Bewertung dieser Verfahren unter dem Gesichtspunkt der Informationssicherheit;<br>20. Entwicklung und Veröffentlichung sicherheitstechnischer Anforderungen an IT-Produkte. | Eventuelle Überschneidungen mit Art. 42 und 57 EU-DSGVO und dem Anwendungsbereich der EU eIDAS-VO sind zu klären. |

| | | | | |
|---|---|---|---|---|
| | | | | |
| 10 | | § 4b BSIG-E: Allgemeine Meldestelle für die Sicherheit in der Informationstechnik<br><br>(1) Das Bundesamt fördert die Sicherheit in der Informationstechnik. Hierzu nimmt es als allgemeine Meldestelle Informationen über Sicherheitsrisiken in der Informationstechnik entgegen und wertet diese aus.<br>(...)<br>(3) Das Bundesamt kann die gemäß Absatz 2 gemeldeten Informationen verarbeiten, um: | § 4b BSIG-E: Meldestelle für die Sicherheit in der Informationstechnik<br><br>(1) Das Bundesamt fördert die Sicherheit in der Informationstechnik. Hierzu sammelt es Informationen über Sicherheitsrisiken in der Informationstechnik und wertet diese aus.<br>(…)<br><br>(3) Das Bundesamt kann die gemäß Absatz 2 gemeldeten Informationen zur Aufgabenerfüllung verarbeiten. Insbesondere kann es die Informationen verarbeiten, um: | Betonung der allgemeinen Meldestellenaufgabe auch durch den Wortlaut des Gesetzes selbst; zudem Aufteilung des bisherigen Absatzes 3.<br><br>In diesem Zusammenhang relevante Fragestellungen:<br>- Umfasst Abs. 3 Nr. 1 auch die Hersteller des Produkts mit (vermeintlicher) Schwachstelle?<br>- Umfasst Abs. 3 Nr. 4 auch die neu eingeführten Unternehmen in besonderem öffentlichen Interesse? Falls nein, was der Wortlaut trotz Verweis auf § 8b Abs. 2 Nr. 4 BSIG-E durch die Bezeichnung „Kritischer Infrastrukturen“ nahe- |

| | | | | |
|---|---|---|---|---|
| | | 1. Dritte über bekanntgewordene Sicherheitslücken, Schadprogramme, erfolgte oder versuchte Angriffe auf die Sicherheit in der Informationstechnik zu informieren, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist,<br>2. im Benehmen mit der zuständigen Aufsichtsbehörde die Öffentlichkeit gemäß § 7 zu warnen,<br>3. Bundesbehörden gemäß § 4 Absatz 2 Nummer 2 über die sie betreffenden Informationen zu unterrichten,<br>4. Betreiber Kritischer Infrastrukturen gemäß § 8b Absatz 2 Nummer 4 Buchstabe a) über die sie betreffenden Informationen zu unterrichten.<br>(4) Eine Weitergabe nach Absatz 3 Nummern 1, 2 und 4 erfolgt nicht, | 1. Dritte über bekanntgewordene Sicherheitslücken, Schadprogramme, erfolgte oder versuchte Angriffe auf die Sicherheit in der Informationstechnik zu informieren, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist,<br>2. die Öffentlichkeit gemäß § 7 zu warnen,<br>3. Bundesbehörden gemäß § 4 Absatz 2 Nummer 2 über die sie betreffenden Informationen zu unterrichten,<br>4. Betreiber Kritischer Infrastrukturen gemäß § 8b Absatz 2 Nummer 4 Buchstabe a) über die sie betreffenden Informationen zu unterrichten. Eine Weitergabe erfolgt nicht, wenn die gemäß Absatz 2 gemeldeten Informationen: | legt, wäre es möglicherweise ratsam, eben jene Unternehmen auch mit aufzunehmen. |

| | | | | |
|---|---|---|---|---|
| | | soweit die gemäß Absatz 2 gemeldeten Informationen:<br>1. Betriebs- und Geschäftsgeheimnisse von Dritten beinhalten und die Maßnahmen nach Absatz 3 Satz 1 nicht ohne Bekanntgabe dieser Betriebs- und Geschäftsgeheimnisse durchgeführt werden können oder<br>2. auf Grund von Vereinbarungen mit Dritten nicht übermittelt werden dürfen. Sonstige gesetzliche Übermittlungshindernisse und Regelungen zum Geheimschutz bleiben unberührt.<br>(5) Erlangt das Bundesamt im Rahmen einer Meldung nach Absatz 2 Kenntnis von der Identität des Meldenden, so kann eine Übermittlung dieser personenbezogenen Daten | 1. Betriebs- und Geschäftsgeheimnisse von Dritten beinhalten und die Maßnahmen nach Absatz 3 Satz 1 nicht ohne Bekanntgabe dieser Betriebs- und Geschäftsgeheimnisse durchgeführt werden können,<br>2. auf Grund von Vereinbarungen mit Dritten nicht übermittelt werden dürfen. Sonstige gesetzliche Übermittlungshindernisse und Regelungen zum Geheimschutz bleiben unberührt.<br>(4) Erlangt das Bundesamt im Rahmen einer Meldung nach Absatz 2 Kenntnis von der Identität eines Dritten, so kann eine Übermittlung dieser personenbezogenen Daten unterbleiben, wenn für das Bundesamt erkennbar ist, dass unter | |

| | | | | |
|---|---|---|---|---|
| | | unterbleiben, wenn für das Bundesamt erkennbar ist, dass unter Berücksichtigung der Schwere einer gemeldeten Sicherheitslücke, eines Schadprogramms, eines erfolgten oder versuchten Angriffs auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweisen sowie der Art und Weise, mittels derer der Meldende diese Erkenntnisse gewonnen hat, die schutzwürdigen Interessen des Meldenden das Allgemeininteresse an der Übermittlung überwiegen. Die Entscheidung nach Satz 1 muss dem oder der behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem oder einer weiteren Bediensteten des Bundesamtes, der | Berücksichtigung der Schwere einer gemeldeten Sicherheitslücke, eines Schadprogramms, eines erfolgten oder versuchten Angriffs auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweisen sowie der Art und Weise, mittels derer der Dritte diese Erkenntnisse gewonnen hat, die schutzwürdigen Interessen des Dritten das Allgemeininteresse an der Übermittlung überwiegen. Die Entscheidung nach Satz 1 muss dem behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem weiteren Bediensteten des Bundesamtes, der die Befähigung zum Richteramt hat, zur vorherigen Entscheidung vorgelegt werden. | |

| | | | | |
|---|---|---|---|---|
| | | oder die die Befähigung zum Richteramt hat, zur vorherigen Entscheidung vorgelegt werden.<br>(6) Bestehende gesetzliche Meldepflichten und Übermittlungsregelungen bleiben unberührt. | (5) Bestehende gesetzliche Meldepflichten und Übermittlungsregelungen bleiben unberührt. | |
| 11 | | § 5b BSIG-E (bisheriger § 5a):<br>(1) Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Stelle des Bundes oder eines Betreibers einer Kritischen Infrastruktur oder eines Unternehmens im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1, 2 oder 3 um einen herausgehobenen Fall, so kann das Bundesamt auf Ersuchen der betroffenen Stelle oder des betroffenen Betreibers die | § 5b BSIG-E (bisheriger § 5a):<br>(1) Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Stelle des Bundes oder eines Betreibers einer Kritischen Infrastruktur oder eines Betreibers einer weiteren Anlage im besonderen öffentlichen Interesse um einen herausgehobenen Fall, so kann das Bundesamt auf Ersuchen der betroffenen Stelle oder des be- | |

| | | | | |
|---|---|---|---|---|
| | | Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind.<br>(…)<br><br>(7) (…) Ein begründeter Einzelfall liegt in der Regel vor, wenn eine Stelle eines Landes betroffen ist. | troffenen Betreibers die Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind.<br>(…)<br><br>(7) (…) Ein begründeter Einzelfall liegt in der Regel vor, wenn einem Betreiber von Anlagen nach § 8g die Pflichten nach § 8a und § 8b auferlegt wurden oder eine Stelle eines Landes betroffen ist. | |
| 12 | | § 5c BSIG-E:<br>Das Bundesamt stellt im Einvernehmen mit<br>1. dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und | § 5c BSIG-E:<br>Das Bundesamt stellt im Einvernehmen mit<br>1. dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und | Im Wesentlichen vor allem Umbenennung von „Krisenreaktionsplänen“ zu „Gesamtplan für Reaktionsmaßnahmen“. |

| | | | | |
|---|---|---|---|---|
| | | 2. der jeweils zuständigen Aufsichtsbehörde des Bundes einen Gesamtplan für die Reaktionsmaßnahmen des Bundes auf, um die Aufrechterhaltung oder Wiederherstellung der informationstechnischen Systeme, Komponenten oder Prozesse bei Betreibern Kritischer Infrastrukturen oder Unternehmen im besonderen öffentlichen Interesse für den Fall einer erheblichen Störung im Sinne des § 8b Absatz 4 Nummer 2, die zu erheblichen Versorgungsengpässen oder Gefährdungen für die öffentliche Sicherheit führen können, sicherzustellen. Sofern nach Satz 1 keine zuständige Aufsichtsbehörde des Bundes benannt ist, ist das zuständige Ressort zu beteiligen. | 2. der jeweils zuständigen Aufsichtsbehörde des Bundes Krisenreaktionspläne auf, um die Aufrechterhaltung oder Wiederherstellung der informationstechnischen Systeme, Komponenten oder Prozesse bei Betreibern Kritischer Infrastrukturen oder Betreibern weiterer Anlagen im besonderen öffentlichen Interesse für den Fall einer erheblichen Störung im Sinne des § 8b Absatz 4 Nummer 2, die zu erheblichen Versorgungsengpässen oder Gefährdungen für die öffentliche Sicherheit führen können, sicherzustellen. | Problematisch ist vor allem Abs. 4 des neuen § 5c BSIG-E: in bestimmten Konstellationen Weisungsbefugnis des BSI gegenüber privaten Unternehmen und Auskunftsbefugnisse, auch über personenbezogene Daten, und damit jedenfalls Eingriffe in Berufsfreiheit, informationelle Selbstbestimmung und Allgemeines Persönlichkeitsrecht (APR) denkbar. Rechtfertigung dahingehend problematisch, dass augenscheinlich Unternehmen selbst bereits den Anreiz haben, mit IT-Sicherheitskrisen angemessen umzugehen, allerdings zeigt die Praxis, dass es trotzdem regelmäßig zu IT-Sicherheitsvorfällen kommt. |

| | | | | |
|---|---|---|---|---|
| | | (2) Der Gesamtplan soll die an der Krisenreaktion beteiligten Behörden, Betreiber Kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse in die Lage versetzen, im Notfall unverzüglich Entscheidungen zu treffen und die erforderlichen Maßnahmen rechtzeitig durchzuführen.<br><br>(3) Bei der Erstellung und bei wesentlichen Änderungen des Gesamtplans wird das Benehmen mit den Betroffenen hergestellt. Die Krisenreaktionspläne werden regelmäßig unter Berücksichtigung von Erkenntnissen aus bewältigten Krisen im Bereich der Sicherheit in der Informationstechnik sowie den Veränderungen des Stands der | (2) Die Krisenreaktionspläne sollen die an der Krisenreaktion beteiligten Behörden, Betreiber Kritischer Infrastrukturen und Betreiber weiterer Anlagen im besonderen öffentlichen Interesse in die Lage versetzen, im Notfall unverzüglich abgestimmte Entscheidungen zu treffen und die angemessenen Maßnahmen rechtzeitig durchzuführen.<br>(3) Bei der Erstellung und bei wesentlichen Änderungen der Krisenreaktionspläne soll eine Abstimmung mit den Betroffenen sichergestellt werden. Die Krisenreaktionspläne werden regelmäßig unter Berücksichtigung von Erkenntnissen aus bewältigten Krisen im Bereich der Sicherheit in der Informa- | |

| | | | | |
|---|---|---|---|---|
| | | Technik und der Rechtslage überprüft und falls erforderlich angepasst.<br><br>(4) Während einer erheblichen Störung gemäß § 8b Absatz 4 Nummer 2 kann das Bundesamt im Benehmen mit den jeweils im Einzelfall nach § 5 Absatz 5 zu beteiligenden Stellen<br>1. den Betroffenen die zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten übermitteln,<br>2. von den Betroffenen die Herausgabe der zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten verlangen,<br>3. im Benehmen mit dem Bundesamt für Bevölkerungsschutz und | tionstechnik sowie den Veränderungen des Stands der Technik und der Rechtslage überprüft und gegebenenfalls angepasst.<br>(4) Während einer erheblichen Störung gemäß § 8b Absatz 4 Nummer 2 kann das Bundesamt im mit den jeweils im Einzelfall nach § 5 Absatz 5 zu beteiligenden Stellen<br>1. den Betroffenen die zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten übermitteln,<br>2. von den Betroffenen die Herausgabe der zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten verlangen,<br>3. im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe gegenüber den | |

| | | | | |
|---|---|---|---|---|
| | | Katastrophenhilfe gegenüber den Betroffenen die erforderlichen informationstechnischen Maßnahmen für die Wiederherstellung der Sicherheit und der Funktionsfähigkeit ihrer informationstechnischen Systeme anordnen, um erhebliche Versorgungsengpässe oder Gefährdungen für wichtige Rechtsgüter, insbesondere für Leib und Leben sowie für die öffentliche Sicherheit, abzuwenden, wenn der Betroffene die erhebliche Störung nicht unverzüglich selbst beseitigt oder zu erwarten ist, dass der Betroffene die erhebliche Störung nicht selbst unverzüglich beseitigen kann. | Betroffenen die erforderlich informationstechnischen Maßnahmen für die Wiederherstellung der Sicherheit und der Funktionsfähigkeit ihrer informationstechnischen Systeme anordnen, um erhebliche Versorgungsengpässe oder Gefährdungen für andere wichtige Rechtsgüter, insbesondere für Leib und Leben sowie für die öffentliche Sicherheit, abzuwenden, wenn der Betroffene die erhebliche Störung nicht unverzüglich selbst beseitigt oder zu erwarten ist, dass der Betroffene die erhebliche Störung selbst nicht unverzüglich beseitigen kann. | |
| 13 | | § 7 Abs. 1 BSIG-E: | § 7 Abs. 1 BSIG-E: | |

| | | | | |
|---|---|---|---|---|
| | | (…) Das Bundesamt kann zur Wahrnehmung der Aufgaben nach Satz 1 Dritte einbeziehen, wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist. Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung der Warnungen zu informieren. Diese Informationspflicht besteht nicht, wenn hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks gefährdet wird oder wenn berechtigterweise davon ausgegangen werden kann, dass der Hersteller an einer vorherigen Benachrichtigung kein Interesse hat. Soweit entdeckte Sicherheitslücken oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterver- | (…) Das Bundesamt kann zur Wahrnehmung der Aufgaben nach Satz 1 Dritte einbeziehen, wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist. Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung von diese Produkte betreffenden Warnungen zu informieren. Diese Informationspflicht besteht nicht, wenn hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks gefährdet wird oder wenn berechtigter Weise davon ausgegangen werden kann, dass der Hersteller an einer vorherigen Benachrichtigung kein Interesse hat. Soweit entdeckte Sicherheitslücken oder Schadprogramme nicht allgemein bekannt werden sollen, um eine Weiterverbreitung | |

| | | | | |
|---|---|---|---|---|
| | | breitung oder rechtswidrige Ausnutzung zu verhindern oder weil das Bundesamt gegenüber Dritten zur Vertraulichkeit verpflichtet ist, kann es den Kreis der zu warnenden Personen einschränken; Kriterien hierfür sind insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere Zuverlässigkeit des Empfängers. | oder rechtswidrige Ausnutzung zu verhindern oder weil das Bundesamt gegenüber Dritten zur Vertraulichkeit verpflichtet ist, kann es den Kreis der zu warnenden Personen anhand sachlicher Kriterien einschränken; sachliche Kriterien können insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere Zuverlässigkeit des Empfängers sein. | |
| 14 | | In § 7a BSIG-E:<br>(…)<br>(2) Soweit erforderlich kann das Bundesamt für Untersuchungen nach Absatz 1 von Herstellern informationstechnischer Produkte und Systeme alle notwendigen Auskünfte, insbesondere auch zu technischen Details, verlangen. | § 7a BSIG-E:<br>(…)<br>(2) Soweit erforderlich kann das Bundesamt für Untersuchungen nach Absatz 1 von Herstellern informationstechnischer Produkte und Systeme alle notwendigen Auskünfte, insbesondere auch zu technischen Details, verlangen. | Insbesondere die Auskunftspflicht im neuen Abs. 2 ist dahingehend problematisch, dass einzige greifbare Voraussetzung dafür ist, dass das BSI die Auskunft im Rahmen von § 7a BSIG-E für erforderlich hält, wobei von den Auskünften theoretisch auch für die betroffe- |

| | | | | |
|---|---|---|---|---|
| | | Bei der Versendung des Auskunftsverlangens an einen Hersteller gibt das Bundesamt die Rechtsgrundlage, den Zweck des Auskunftsverlangens und die benötigten Auskünfte an und legt eine angemessene Frist für die Übermittlung der Auskünfte fest. Das Auskunftsverlangen enthält ferner einen Hinweis auf die in § 14 vorgesehenen Sanktionen.<br>(3) Das Bundesamt gibt Auskünfte sowie die aus den Untersuchungen gewonnen Erkenntnisse unverzüglich an die zuständigen Aufsichtsbehörden des Bundes oder sofern keine Aufsichtsbehörde vorhanden ist, an das jeweilige Ressort weiter, wenn Anhaltspunkte bestehen, dass diese sie zur Erfüllung ihrer Aufgaben benötigen. | Bei der Versendung des Auskunftsverlangens an einen Hersteller gibt das Bundesamt die Rechtsgrundlage, den Zweck des Auskunftsverlangens und die benötigten Auskünfte an und legt die Frist für die Übermittlung der Auskünfte fest. Das Auskunftsverlangen enthält ferner einen Hinweis auf die in § 14 vorgesehenen Sanktionen.<br><br>(3) Die Auskünfte und die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 genutzt werden. Das Bundesamt darf seine Erkenntnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung dieser Aufgaben erforderlich ist. Zuvor ist dem Hersteller der betroffenen | nen Unternehmen sensible (Geschäfts-) Informationen umfasst sein können. |

| | | | | |
|---|---|---|---|---|
| | | | Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben. | |
| | | (4) Die Auskünfte und die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 genutzt werden. Das Bundesamt darf seine Erkenntnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 erforderlich ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben.<br>(5) Kommt ein Hersteller der Aufforderung des Bundesamtes nach Absatz 2 Satz 1 nicht oder nur un- | (4) Kommt ein Hersteller der Aufforderung des Bundesamtes nach Absatz 2 Satz 1 nicht oder nur unzureichend nach, kann das Bundesamt hierüber die Öffentlichkeit informieren. Es kann hierbei den Namen des Herstellers sowie die Bezeichnung des betroffenen Produkts oder Systems angeben, und inwieweit der Hersteller seiner Auskunftspflicht nicht nachgekommen ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu gewähren. § 7 Absatz 2 Satz 2 gilt entsprechend. | |

| | | | | |
|---|---|---|---|---|
| | | zureichend nach, kann das Bundesamt hierüber die Öffentlichkeit informieren. Es kann hierbei den Namen des Herstellers sowie die Bezeichnung des betroffenen Produkts oder Systems angeben, und darlegen inwieweit der Hersteller seiner Auskunftspflicht nicht nachgekommen ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu gewähren. § 7 Absatz 2 Satz 2 gilt entsprechend. | | |
| 15 | | § 7b BSIG-E:<br>(1) Das Bundesamt kann zur Erfüllung seiner Aufgaben Maßnahmen zur Detektion von Schadprogrammen, Sicherheitslücken und anderen Sicherheitsrisiken in | § 7b BSIG-E:<br>(1) Das Bundesamt kann zur Erfüllung seiner Aufgaben Maßnahmen zur Detektion und Auswertung von Schadprogrammen, | Befugnis des BSI zur aktiven Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden. „Macht das BSI zur Hackerbehörde.“ |

| | | | | |
|---|---|---|---|---|
| | | öffentlich erreichbaren informationstechnischen Systemen durchführen, wenn Tatsachen die Annahme rechtfertigen, dass diese ungeschützt sind und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können. Erlangt es dabei Informationen, die dem Fernmeldegeheimnis unterliegen, darf es diese nur entsprechend § 5 Absatz 5 und 6 BSIG übermitteln.<br><br>(2) Ein informationstechnisches System im Sinne des Absatzes 1 ist ungeschützt, wenn auf diesem öffentlich bekannte Sicherheitslücken bestehen oder wenn auf Grund sonstiger offensichtlich unzureichender Sicherheitsvorkehrungen unbefugt von Dritten auf | Sicherheitslücken und anderen Sicherheitsrisiken in öffentlich erreichbaren informationstechnischen Systemen durchführen, wenn Tatsachen die Annahme rechtfertigen, dass diese ungeschützt sind und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können. Erlangt es dabei Informationen, die dem Fernmeldegeheimnis unterliegen, darf es diese nur entsprechend § 5 Absatz 5 und 6 BSIG übermitteln.<br>(2) Ein informationstechnisches System ist ungeschützt im Sinne des Absatzes 1, wenn öffentlich bekannte Sicherheitslücken bestehen oder wenn auf Grund offensichtlich unzureichender Sicherheitsvorkehrungen von unbefugten | |

| | | | | |
|---|---|---|---|---|
| | | das System zugegriffen werden kann.<br>(3) Wird durch Maßnahmen gemäß Absatz 1 ein Schadprogramm, eine Sicherheitslücke oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt, sind die für das informationstechnische System Verantwortlichen oder hilfsweise der betreibende Dienstleister des jeweiligen Netzes oder Systems unverzüglich zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßige weitere Ermittlungen möglich ist und überwiegende Sicherheitsinteressen nicht entgegenstehen. Das Bundesamt kann anordnen, dass der Diensteanbieter Maßnahmen gemäß § | Dritten auf das System zugegriffen werden kann.<br>(3) Wird im Falle des Absatzes 1 ein Schadprogramm, eine Sicherheitslücke oder ein anderes Sicherheitsrisiko in einem informationstechnischen System erkannt, sind die hierfür Verantwortlichen oder der betreibende Dienstleister des jeweiligen Netzes oder Systems unverzüglich zu benachrichtigen, wenn sie bekannt sind oder ihre Identifikation ohne unverhältnismäßige weitere Ermittlungen möglich ist und überwiegende Sicherheitsinteressen nicht entgegenstehen. Das Bundesamt kann anordnen, dass der jeweils zuständige Diensteanbieter Maßnahmen gemäß § 109a Absatz 4 des Telekommunikationsgesetzes | |

| | | | | |
|---|---|---|---|---|
| | | 109a Absatz 4 des Telekommunikationsgesetzes ergreift. Das Bundesamt unterrichtet die oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kalenderjährlich jeweils bis zum 30. Juni des Folgejahres über die Anzahl der Vorgänge gemäß Absatz 1. | ergreift. Das Bundesamt unterrichtet die oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit kalenderjährlich jeweils bis zum 30. Juni des Folgejahres über die Anzahl der Vorgänge gemäß Absatz 1. | |
| | | (4) Das Bundesamt darf zur Erfüllung seiner Aufgaben Systeme und Verfahren einsetzen, welche einem Angreifer einen erfolgreichen Angriff vortäuschen, um Schadprogramme und andere Angriffsmethoden zu erheben und auszuwerten. Das Bundesamt darf die hierzu erforderlichen Daten verarbeiten. | (4) Ferner darf das Bundesamt zur Erfüllung seiner Aufgaben Systeme und Verfahren einsetzen, welche einem Angreifer einen erfolgreichen Angriff vortäuschen, um Schadprogramme und andere Angriffsmethoden zu erheben und auszuwerten. Das Bundesamt darf die hierzu erforderlichen Daten verarbeiten. | |

| | | | | |
|---|---|---|---|---|
| 16 | | § 8 BSIG-E:<br>(1) Das Bundesamt legt im Benehmen mit den Ressorts Mindeststandards für die Sicherheit der Informationstechnik des Bundes fest, die von<br><br>1. Stellen des Bundes,<br>2. Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihrer Vereinigungen ungeachtet ihrer Rechtsform auf Bundesebene, soweit von der jeweils zuständigen obersten Bundesbehörde angeordnet, sowie von<br>3. öffentlichen Unternehmen, die mehrheitlich im Eigentum des Bundes stehen und die IT-Dienstleistungen für die Bundesverwaltung erbringen, | § 8 BSIG-E:<br>(1) Das Bundesamt erarbeitet im Benehmen mit den Ressorts Mindeststandards für die Sicherheit der Informationstechnik des Bundes, welche von<br>1. Stellen des Bundes,<br>2. Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihrer Vereinigungen ungeachtet ihrer Rechtsform auf Bundesebene, soweit von der jeweils zuständigen obersten Bundesbehörde angeordnet, sowie von<br>3. öffentlichen Unternehmen, die mehrheitlich in vollem Eigentum des Bundes stehen und die IT-Dienstleistungen für die Bundesverwaltung erbringen, | |

| | | | | |
|---|---|---|---|---|
| | | umzusetzen sind. Abweichungen von den Mindeststandards sind nur in sachlich gerechtfertigten Fällen zulässig, sie sind zu dokumentieren und zu begründen. Das Bundesministerium des Innern, für Bau und Heimat kann im Benehmen mit der Konferenz der IT-Beauftragten der Ressorts bei bedeutenden Mindeststandards die Überwachung und Kontrolle ihrer Einhaltung durch das Bundesamt anordnen. Das Bundesamt teilt das Ergebnis seiner Kontrolle der jeweiligen überprüften Stelle, deren jeweiliger zuständiger Aufsichtsbehörde sowie der Konferenz der IT-Beauftragten der Ressorts mit. Für andere öffentlich- oder privatrechtlich organisierte Stellen dürfen nur | zu berücksichtigen sind. Abweichungen von den Mindeststandards sind nur in sachlich gerechtfertigten Fällen zulässig, sie sind zu dokumentieren und zu begründen. Das Bundesministerium des Innern, für Bau und Heimat kann im Benehmen mit der Konferenz der IT-Beauftragten der Ressorts bei bedeutenden Mindeststandards die Überwachung und Kontrolle ihrer Einhaltung durch das Bundesamt anordnen. Das Bundesamt teilt das Ergebnis seiner Kontrolle der jeweiligen überprüften Stelle sowie der Konferenz der IT- Beauftragten der Ressorts mit. Für andere öffentlich- oder privatrechtlich organisierte Stellen dürfen nur dann Schnittstellen zur | |

| | | | | |
|---|---|---|---|---|
| | | dann Schnittstellen zur Kommunikationstechnik des Bundes eingerichtet werden, soweit die für die Einrichtung verantwortliche Stelle vertraglich sicherstellt, dass die öffentlich- oder privatrechtlich organisierte Stelle sich zur Einhaltung der Mindeststandards verpflichtet. Das Bundesamt kann im Einvernehmen mit dem Dritten die Einhaltung der Mindeststandards überprüfen und kontrollieren. Das Bundesamt berät die unter Satz 1 und 6 genannten Stellen auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards. Für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach diesem Absatz empfehlenden Charakter. | Kommunikationstechnik des Bundes eingerichtet werden, soweit die für die Einrichtung verantwortliche Stelle vertraglich sicherstellt, dass die öffentlich- oder privatrechtlich organisierte Stelle sich zur Einhaltung der Mindeststandards und Duldung der Kontrolle durch das Bundesamt verpflichtet. Das Bundesamt berät die unter Satz 1 und 6 genannten Stellen auf Ersuchen bei der Umsetzung und Einhaltung der Mindeststandards. Für die in § 2 Absatz 3 Satz 2 genannten Gerichte und Verfassungsorgane haben die Vorschriften nach diesem Absatz empfehlenden Charakter.<br><br>(…) | |

| | | | | |
|---|---|---|---|---|
| | | (…)<br>(4) Zur Gewährleistung der Sicherheit in der Informationstechnik bei der Planung und Umsetzung von Digitalisierungsvorhaben des Bundes ist das Bundesamt durch die jeweils verantwortliche Stelle frühzeitig zu beteiligen und dem Bundesamt Gelegenheit zur Stellungnahme zu geben. | (4) Zur Gewährleistung der Sicherheit in der Informationstechnik bei der Planung und Umsetzung von Digitalisierungsvorhaben des Bundes ist das Bundesamt durch die jeweils zuständige Stelle frühzeitig zu beteiligen und dem Bundesamt die Gelegenheit zur Stellungnahme zu geben. | |
| 17 | | § 8a Abs. 1 S. 3 BSIG-E:<br>Zur Umsetzung von Maßnahmen nach Satz 1 können Betreiber Kritischer Infrastrukturen auch geeignete Prozesse vorsehen, um die Vertrauenswürdigkeit der Beschäftigten zu überprüfen, die in Bereichen tätig sind, in denen in besonderem Maße auf die Verfügbarkeit, | | Im Wesentlichen wird Abs. 1a aufgetrennt in verschiedene Absätze. So können KRITIS-Betreiber Prozesse vorsehen, um die Vertrauenswürdigkeit der Beschäftigten zu überprüfen, die in zentralen Bereichen tätig sind. Außerdem wird neuerdings eine Regelung vorgeschlagen, dass solche Daten, die im Rahmen des Einsatzes von |

| | | | | |
|---|---|---|---|---|
| | | Integrität, Authentizität und Vertraulichkeit informationstechnischer Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der Kritischen Infrastruktur maßgeblich sind, eingewirkt werden kann.<br><br>(1a) Die Verpflichtung der Betreiber Kritischer Infrastrukturen, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen nach Absatz 1 Satz 1 zu treffen, umfasst auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung haben dem jeweiligen Stand der Technik zu entsprechen. Die Einhaltung des Standes der Tech- | (1a) Die Verpflichtung der Betreiber Kritischer Infrastrukturen, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind, | Systemen zur Angriffserkennung erhoben wurden, von den Betreibern an die dafür zuständigen Behörden zu übermitteln sind. Ebenso wird eine vom ursprünglichen Entwurf abweichende Änderung von § 8a Abs. 3 BSIG aufgegriffen: So sollen KRITIS-Betreiber dem BSI zusätzlich eine Liste aller IT-Produkte übermitteln, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen von Bedeutung sind. Die Regelung zu KRITIS-Kernkomponenten, die noch in der ersten Entwurfsfassung vorlag, findet sich im aktuellen Entwurf aus Mai 2020 hingegen in dieser Form nicht wieder. Der Regelungsvorschlag aus 2019 sah an dieser Stelle des Ge- |

| | | | | |
|---|---|---|---|---|
| | | nik wird vermutet, wenn die Systeme der Technischen Richtlinie [Bezeichnung] des Bundesamtes in der jeweils geltenden Fassung entsprechen.<br>(1b) Die Betreiber Kritischer Infrastrukturen dürfen die für den Einsatz von Systemen zur Angriffserkennung erforderlichen Daten verarbeiten. Die im Rahmen des Einsatzes von Systemen zur Angriffserkennung verarbeiteten Daten sind unverzüglich zu löschen, wenn sie für die Vermeidung von Störungen nach Absatz 1 Satz 1 nicht mehr erforderlich sind, spätestens jedoch nach zehn Jahren.<br>(1c) Im Rahmen des Einsatzes von Systemen zur Angriffserkennung erhobene Daten, die für den | umfasst auch den Einsatz von Systemen zur Angriffserkennung. Die Betreiber Kritischer Infrastrukturen dürfen die hierzu erforderlichen Daten verarbeiten. Die im Rahmen des Einsatzes von Systemen zur Angriffserkennung erhobenen Daten sind unverzüglich zu löschen, wenn sie nicht für die Vermeidung von Störungen nach Absatz 1 Satz 1 erforderlich sind. Die übrigen Daten dürfen nicht länger als zehn Jahre gespeichert werden. Die Ausgestaltung des Einsatzes von Systemen zur Angriffserkennung legt das Bundesamt in einer Technischen Richtlinie fest. Hierzu muss die oder der Bundesbeauftrage für den Datenschutz und die Informationsfreiheit angehört wer- | setzes vor, dass derlei Komponenten nur von solchen Herstellern bezogen werden dürfen, die eine Vertrauenswürdigkeitserklärung abgegeben haben.<br>Besonders umstritten ist die Meldepflicht von sogenannten kritischen IT-Komponenten, da diese über das BSI letztlich auch dem BMI zur Verfügung stehen. |

| | | | | |
|---|---|---|---|---|
| | | Schutz vor Angriffen auf Informationstechnik oder die Aufklärung und Strafverfolgung eines Angriffs erforderlich sind, haben die Betreiber den dafür zuständigen Behörden zu übermitteln.<br>(3) S. 4: Die Betreiber übermitteln dem Bundesamt dabei zusätzlich eine Liste aller IT-Produkte, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen von Bedeutung sind, weil Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit dieser IT-Produkte zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit einer Kritischen Infrastruktur oder zu einer Gefährdung der öffentlichen Sicherheit und Ordnung führen können. | den. Die Betreiber Kritischer Infrastrukturen müssen der oder dem betrieblichen Datenschutzbeauftragten, dem Bundesamt, der jeweiligen Aufsichtsbehörde und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am Ende eines Quartals detailliert über die Verfahren und Umstände von Maßnahmen nach Satz 1 in diesem Zeitraum schriftlich berichten.<br><br>(6) KRITIS-Kernkomponenten dürfen nur von solchen Herstellern bezogen werden, die vor dem erstmaligen Einsatz der Komponenten eine Erklärung über ihre Vertrauenswürdigkeit gegenüber dem Betreiber der Kritischen Infrastruktur | |

| | | | | |
|---|---|---|---|---|
| | | | abgeben haben (Vertrauenswürdigkeitserklärung). Diese Verpflichtung erstreckt sich auf die gesamte Lieferkette des Herstellers. Das Bundesministerium des Innern, für Bau und Heimat erlässt die Mindestanforderungen für die Vertrauenswürdigkeitserklärung durch Allgemeinverfügung, die im Bundesanzeiger bekannt zu machen ist. Diese Verpflichtung gilt ab der Bekanntmachung der Allgemeinverfügung nach Satz 3. | |
| 18 | | § 8b Abs. 2 BSIG-E:<br>Das Bundesamt hat zur Wahrnehmung dieser Aufgabe<br>(…)<br>3. das Lagebild bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen oder | § 8b Abs. 2 S. 2 BSIG-E:<br>Es regelt die Anspruchsberechtigungen für den Zugang von Betreibern Kritischer Infrastrukturen zu einem einheitlichen Krisenkommunikationssystem, welches eine ge- | |

| | | | | |
|---|---|---|---|---|
| | | Unternehmen im besonderen öffentlichen Interesse kontinuierlich zu aktualisieren und<br>4. unverzüglich<br>a)<br>die Betreiber Kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse über sie betreffende Informationen nach den Nummern 1 bis 3,<br>(…)<br><br>_____<br>Die weiteren Änderungen des § 8b Abs. 2, 3 und 3a BSIG-E entsprechen ansonsten im Wesentlichen dem alten RefE. | eignete Kommunikationsinfrastruktur zur Krisenfrüherkennung, Krisenreaktion und Krisenbewältigung bereitstellt, ohne dass hierdurch Doppelstrukturen zu den Netzinfrastrukturen und Diensten der Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben geschaffen werden. Die zuständigen Aufsichtsbehörden, die sonst zuständigen Behörden des Bundes und die zuständigen Aufsichtsbehörden der Länder haben dem Bundesamt unverzüglich vorliegende Informationen nach Satz 1 Nummer 1 bis 4 zu melden, soweit nicht gesetzliche Regelungen entgegenstehen.<br><br>§ 8b Abs. 3 BSIG-E: | |

| | | | | |
|---|---|---|---|---|
| | | Über den alten RefE hinaus werden nun jedoch weitere Absätze eingeführt.<br><br>§ 8b Abs. 3b BSIG-E:<br>Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1 und 2 sind verpflichtet, sich beim Bundesamt zu registrieren und eine zu den üblichen Geschäftszeiten erreichbare Stelle zu benennen. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Stelle.<br><br>§ 8b Abs. 3c BSIG-E: | Betreiber Kritischer Infrastrukturen sind verpflichtet, die von ihnen betriebenen Kritischen Infrastrukturen im Sinne des § 2 Absatz 10 in Verbindung mit der Rechtsverordnung nach § 10 Absatz 1 beim Bundesamt zu registrieren und eine Kontaktstelle zu benennen. Die Betreiber haben sicherzustellen, dass sie über die benannte Kontaktstelle jederzeit erreichbar sind. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Kontaktstelle.<br><br>§ 8b Abs. 3a BSIG-E:<br>Rechtfertigen Tatsachen die Annahme, dass eine Anlage oder Teile davon nach der Rechtsverordnung nach § 10 Absatz 1 eine | |

| | | | | |
|---|---|---|---|---|
| | | Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 3 können eine freiwillige Registrierung beim Bundesamt und Benennung einer zu den üblichen Geschäftszeiten erreichbaren Stelle vornehmen. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Stelle<br><br>§ 8b Abs. 3d BSIG-E:<br>8a Absatz 1 Satz 3 gilt auch für Unternehmen im öffentlichen Interesse nach § 2 Absatz 14 Nummer 1, 2 und 3.<br><br>§ 8b Abs. 4a BSIG-E:<br>Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1 und 2 haben die | Kritische Infrastruktur nach diesem Gesetz ist und der Betreiber seiner Pflicht zur Registrierung nach Absatz 3 nicht erfüllt, so hat der Betreiber dem Bundesamt auf Verlangen die für die Bewertung aus Sicht des Bundesamtes erforderlichen Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorzulegen und Auskunft zu erteilen. Ist eine Anlage oder Teile davon nach der Rechtsverordnung nach § 10 Absatz 1 eine Kritische Infrastruktur im Sinne dieses Gesetzes, kann das Bundesamt die Registrierung auch selbst vornehmen (Ersatzvornahme), wenn der Betreiber seine Pflicht zur Registrierung nicht erfüllt. Rechtfertigen Tatsachen die Annahme, dass im | |

| | | | | |
|---|---|---|---|---|
| | | folgenden Störungen unverzüglich an das Bundesamt zu melden<br>1. Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung geführt haben,<br>2. erhebliche Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung führen können. | Falle einer Registrierung nach Absatz 3 Satz 1 die Anlage oder Teile davon keine Kritische Infrastruktur im Sinne dieses Gesetzes ist, kann das Bundesamt die erfolgte Registrierung eines Betreibers aus tatsächlichen oder rechtlichen Gründen ablehnen. | |

| | | | | |
|---|---|---|---|---|
| | | Die Meldung muss Angaben zu der Störung, zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und der Art der betroffenen Einrichtung oder Anlage enthalten.<br><br>§ 8b Abs. 4b BSIG-E:<br>Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 3 haben die folgenden Störungen unverzüglich an das Bundesamt zu melden:<br>1. Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einer | | |

| | | | | |
|---|---|---|---|---|
| | | erheblichen Gefahr für die öffentliche Sicherheit und Ordnung geführt haben,<br>2. erhebliche Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einer erheblichen Gefahr für die öffentliche Sicherheit und Ordnung führen können.<br>Die Meldung muss Angaben zu der Störung, zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und der Art der betroffenen Einrichtung oder Anlage enthalten | | |

| | | | | |
|---|---|---|---|---|
| 19 | | § 8f BSIG-E:<br>Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse<br><br>(1) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1 sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten dieses Gesetzes ein IT-Sicherheitskonzept beim Bundesamt vorzulegen, aus dem hervorgeht,<br>1. welche Informationstechnischen Systeme, Komponenten und Prozesse für die Erbringung der Wertschöpfung des Unternehmens maßgeblich sind,<br>2. welche organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der | § 8f BSIG-E:<br>Anforderungen für Betreiber von Infrastrukturen im besonderen öffentlichen Interesse<br><br>Anforderungen für Betreiber von Infrastrukturen im besonderen öffentlichen Interesse Die Pflichten nach den §§ 8a und 8b gelten entsprechend für Betreiber von Anlagen oder Teilen davon<br>1. nach § 2 Absatz 14 Nummer 2 spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 5.<br>2. nach § 2 Absatz 14 Nummer 1 und 3 spätestens zwei Jahre nach Inkrafttreten dieses Gesetzes. | |

| | | | | |
|---|---|---|---|---|
| | | Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ebendieser vorgenommen wurden,<br>3. inwieweit bei Vornahme der organisatorischen und technischen Vorkehrungen nach Nummer 2 der Stand der Technik eingehalten wurde.<br>(2) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 2 sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 5 ein IT-Sicherheitskonzept beim Bundesamt vorzulegen, das den in Absatz 1 Nummer 1 bis 3 genannten Voraussetzungen genügt.<br>(3) Das Bundesamt kann auf Grundlage des IT-Sicherheitskonzepts und dessen Anforderungen | | |

| | | | | |
|---|---|---|---|---|
| | | nach Absatz 1 Hinweise zu angemessenen organisatorischen und technischen Vorkehrungen nach Nummer 3 zur Einhaltung des Stands der Technik geben.<br>(4) Unternehmen im besonderen öffentlichen Interesse gemäß § 2 Absatz 14 Nummer 1 und 2 haben das IT-Sicherheitskonzept nach Absatz 1 Nummer 1 bis 3 mindestens alle zwei Jahre vorzulegen. | | |
| 20 | | § 9a BSIG-E:<br>(…)<br>(3) Hersteller ist, wer die Voraussetzungen des § 2 Nummer 14 des Gesetzes über die Bereitstellung von Produkten auf dem Markt erfüllt. Die Herstellererklärung soll sich insbesondere aus einer die Produktkategorie umfassenden | § 9a BSIG-E:<br>(…)<br>(2) (…) Hersteller ist, wer die Voraussetzungen des § 2 Nummer 14 des Gesetzes über die Bereitstellung von Produkten auf dem Markt erfüllt. Die Herstellererklärung soll sich insbesondere aus einer die Produktkategorie umfassenden | Die Einführung des allgemeinen und freiwilligen IT-Sicherheitskennzeichens wurde bereits in der ersten Entwurfsfassung kritisch beurteilt, insb. im Hinblick auf die Unterscheidung von der Zertifizierung gem. EU Cybersecurity Act auf dem Level „niedrig“. Eine Herstel- |

| | | | | |
|---|---|---|---|---|
| | | Technischen Richtlinie ergeben, soweit diese vom Bundesamt bereits veröffentlicht wurde. Branchenabgestimmte IT-Sicherheitseigenschaften können im Rahmen der Herstellererklärung verwendet werden, sofern das Bundesamt feststellt, dass sie geeignet sind, ausreichende IT-Sicherheitseigenschaften für die Produktkategorie abzubilden. Das Verfahren zur Feststellung der Eignung branchenabgestimmter IT- Sicherheitseigenschaften wird durch Rechtsverordnung nach § 10 Absatz 3 bestimmt.<br>(4) Der Antrag auf Freigabe zur Nutzung des IT-Sicherheitskennzeichens ist beim Bundesamt zu stellen. Das Bundesamt bestätigt den Eingang und teilt die Freigabe | Technischen Richtlinie ergeben, soweit diese vom Bundesamt bereits veröffentlicht wurde. Branchenabgestimmte IT-Sicherheitseigenschaften können im Rahmen der Herstellererklärung verwendet werden, sofern das Bundesamt feststellt, dass sie geeignet sind, ausreichende IT-Sicherheitseigenschaften für die Produktkategorie abzubilden. Das Verfahren zur Feststellung der Eignung branchenabgestimmter IT-Sicherheitseigenschaften wird durch Rechtsverordnung nach § 10 Absatz 2a bestimmt.<br>(3) Der Antrag auf Freigabe zur Nutzung des IT-Sicherheitskennzeichens ist beim Bundesamt zu stellen. Das Bundesamt bestätigt den Eingang und teilt die Freigabe | lererklärung sollte nicht als nationaler Alleingang zu einer von der EU unabhängigen Parallelentwicklung führen. |

| | | | | |
|---|---|---|---|---|
| | | zur Nutzung oder die Verweigerung schriftlich innerhalb einer angemessenen Frist, die abhängig von der jeweiligen Produktkategorie in der Rechtsverordnung nach § 10 Absatz 3 bestimmt wird, mit. Die Plausibilitätsprüfung der eingereichten Dokumente des Herstellerversprechens kann auch durch einen qualifizierten Dritten erfolgen. Dem Antrag sind die erklärten IT-Sicherheitseigenschaften über das Produkt, sowie alle Unterlagen aus denen sich diese ergeben, beizufügen. Die Freigabe des IT-Sicherheitskennzeichens nach Satz 1 ist zu verweigern, wenn bekannte Tatsachen die Annahme rechtfertigen, dass die Voraussetzungen des Absatz 7 Satz 2 Nummer 2 bereits bei Antragsstellung vorliegen. | zur Nutzung oder die Verweigerung schriftlich innerhalb einer angemessenen Frist, die abhängig von der jeweiligen Produktkategorie in der Rechtsverordnung nach § 10 Absatz 2a bestimmt ist, mit. Die summarische Prüfung des Herstellerversprechens kann auch durch einen qualifizierten Dritten erfolgen. Dem Antrag sind die erklärten IT-Sicherheitseigenschaften über das Produkt, sowie alle Unterlagen aus denen sich diese ergeben, beizufügen. Den weiteren Ablauf und die notwendigen Informationen regelt die Rechtsverordnung nach § 10 Absatz 2a.<br>(4) Das IT-Sicherheitskennzeichen ist körperlich mit dem jeweiligen Produkt o- der mit dessen Umver- | |

| | | | | |
|---|---|---|---|---|
| | | Den weiteren Ablauf und die notwendigen Informationen regelt die Rechtsverordnung nach § 10 Absatz 3.<br>(5) Das IT-Sicherheitskennzeichen ist körperlich mit dem jeweiligen Produkt oder mit dessen Umverpackung zu verbinden. Das IT-Sicherheitskennzeichen kann vom Hersteller oder Verkäufer zusätzlich auch auf elektronischem Wege veröffentlicht werden. Die Herstellererklärung sowie auch die bestehenden Sicherheitsinformationen nach Absatz 2 Satz 1 werden über einen elektronischen Verweis auf einer Webseite des Bundesamtes abrufbar gemacht. Das genaue Verfahren ist in der Rechtsverordnung nach § 10 Absatz 3 festzulegen. | packung zu verbinden. Das IT-Sicherheitskennzeichen kann vom Hersteller oder Verkäufer auch auf elektronischem Wege veröffentlicht werden. Die Herstellererklärung sowie auch die bestehenden Sicherheitsinformationen nach Absatz 2 Satz 1 werden über einen elektronischen Verweis auf einer Webseite des Bundesamtes abrufbar gemacht. Das genaue Verfahren ist in der Rechtsverordnung nach § 10 Absatz 2a festzulegen.<br>(5) Das IT-Sicherheitskennzeichen darf verwendet werden, wenn das Produkt die Anforderungen für die Verwendung des IT-Sicherheitskennzeichens nach Maßgabe der Regelungen nach den Absätzen 1 bis 4 sowie der Rechtsverordnung nach § 10 Absatz 2a erfüllen. Das | |

| | | | | |
|---|---|---|---|---|
| | | (6) Das IT-Sicherheitskennzeichen darf verwendet werden, wenn das Produkt die Anforderungen für die Verwendung des IT-Sicherheitskennzeichens nach Maßgabe der Regelungen nach den Absätzen 1 bis 4 sowie der Rechtsverordnung nach § 10 Absatz 3 erfüllt. Das IT-Sicherheitskennzeichen darf auch für die Werbung für die Produkte genutzt werden, soweit die Darstellung den Vorgaben der Absatz 1 bis 4 sowie der Rechtsverordnung nach § 10 Absatz 3 entspricht.<br>(7) Das Bundesamt soll in regelmäßigen Abständen sowie anlassbezogen prüfen, ob die Vorgaben des IT-Sicherheitskennzeichens eingehalten werden. Werden bei einem das IT-Sicherheitskennzeichen tragenden Produkt | IT-Sicherheitskennzeichen darf auch für die Werbung für die Produkte genutzt werden, soweit die Darstellung den Vorgaben der Absatz 1 bis 4 sowie der Rechtsverordnung nach § 10 Absatz 2 a entspricht.<br>(6) Das Bundesamt soll in regelmäßigen Abständen sowie anlassbezogen prüfen, ob die Vorgaben des IT-Sicherheitskennzeichens eingehalten werden. Werden bei einem das IT-Sicherheitskennzeichen tragenden Produkt Abweichungen vom abgegeben Herstellerversprechen oder Sicherheitslücken festgestellt, kann das Bundesamt die geeigneten Maßnahmen treffen, insbesondere<br>1. Informationen über den elektronischen Verweis in geeigneter | |

| | | | | |
|---|---|---|---|---|
| | | Abweichungen vom abgegeben Herstellerversprechen oder Sicherheitslücken festgestellt, kann das Bundesamt die geeigneten Maßnahmen treffen, insbesondere<br>1. Informationen über den elektronischen Verweis in geeigneter Weise darstellen (BSI-Sicherheitsinfo),<br>2. die Freigabe zur Nutzung des IT-Sicherheitskennzeichens widerrufen und die Werbung mit dem IT-Sicherheitskennzeichen sowie die Nutzung des IT- Sicherheitskennzeichens untersagen.<br>(8) Wird das IT-Sicherheitskennzeichen ohne Freigabe genutzt, kann das Bundesamt die Nutzung untersagen. Dem Hersteller ist vor einer Maßnahme nach Absatz 7 | Weise darstellen (BSI-Sicherheitsinfo),<br>2. die Freigabe zur Nutzung des IT-Sicherheitskennzeichens widerrufen und die Werbung mit dem IT-Sicherheitskennzeichen sowie die Nutzung des IT- Sicherheitskennzeichens untersagen.<br>(7) Wird das IT-Sicherheitskennzeichen ohne Freigabe genutzt, kann das Bundesamt die Nutzung untersagen. Dem Hersteller ist vor einer Maßnahme nach Absatz 6 Satz 2 die Gelegenheit einzuräumen, die Nichterfüllung der Herstellererklärung oder der weiteren Anforderungen des IT-Sicherheitskennzeichens innerhalb eines angemessenen Zeitraumes abzustellen oder Sicherheitslücken zu beseitigen, es sei denn, gewichtige | |

| | | | | |
|---|---|---|---|---|
| | | Satz 2 die Gelegenheit einzuräumen, die Nichterfüllung der Herstellererklärung oder der weiteren Anforderungen des IT-Sicherheitskennzeichens innerhalb eines angemessenen Zeitraumes abzustellen oder Sicherheitslücken zu beseitigen, es sei denn, gewichtige Gründe der Sicherheit der Produkte erfordern eine sofortige Maßnahme. | Gründe der Sicherheit der Produkte erfordern eine sofortige Maßnahme. | |
| 21 | | § 9b BSIG-E:<br>Untersagung des Einsatzes kritischer Komponenten nicht vertrauenswürdiger Hersteller<br>(1) Der Einsatz einer kritischen Komponente (§ 2 Absatz 13), für die auf Grund einer spezialgesetzlichen Regelung eine Zertifizierungspflicht besteht, ist durch den | -- | Zwar Entfall des Tatbestands der Cyberkritikalität aus der ersten Entwurfsfassung, es finden sich aber wesentliche der ursprünglichen Regelungsgedanken im neuen Regelungsvorschlag § 9b BSIG-E wieder, so z.B. die „Garantieerklärung“. |

| | | | | |
|---|---|---|---|---|
| | | Betreiber einer Kritischen Infrastruktur dem Bundesministerium des Innern, für Bau und Heimat vor Einbau anzuzeigen. In der Anzeige ist die kritische Komponente und die Art ihres Einsatzes anzugeben. (2) Kritische Komponenten nach Absatz 1 dürfen nur von solchen Herstellern eingesetzt werden, die eine Erklärung über ihre Vertrauenswürdigkeit gegenüber dem Betreiber der Kritischen Infrastruktur abgeben haben (Garantieerklärung). Diese Erklärung erstreckt sich auf die gesamte Lieferkette des Herstellers. Die Garantieerklärung des Herstellers der kritischen Komponente ist der Anzeige nach Absatz 1 beizufügen. Das Bundesministerium des Innern, für | | |

| | | | | |
|---|---|---|---|---|
| | | Bau und Heimat legt die Mindestanforderungen für die Garantieerklärung unter Berücksichtigung überwiegender öffentlicher Interessen, insbesondere sicherheitspolitischer Belange, durch Allgemeinverfügung fest, die im Bundesanzeiger bekannt zu machen ist. Aus der Garantieerklärung muss hervorgehen, ob und wie der Hersteller hinreichend sicherstellen kann, dass die kritische Komponente über keine technischen Eigenschaften verfügt, die geeignet sind, missbräuchlich auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur (etwa Sabotage, Spionage oder Terrorismus) einwirken zu können. Die Verpflichtung in Satz 1 | | |

| | | | | |
|---|---|---|---|---|
| | | gilt ab der Bekanntmachung der Allgemeinverfügung nach Satz 5.<br>(3) Ist der Anwendungsbereich des § 9b eröffnet, ist eine Feststellung nach § 9 Absatz 4 Nr. 2 entbehrlich. Zum Zwecke der Gewährleistung der nationalen Sicherheitsinteressen der Bundesrepublik Deutschland prüft das Bundesministerium des Innern, für Bau und Heimat stattdessen den Einsatz der kritischen Komponente nach Absatz 1 in Hinblick auf die Vertrauenswürdigkeit des Herstellers und kann gegenüber dem Betreiber der Kritischen Infrastruktur im Einvernehmen mit dem jeweils betroffenen Ressort den Einsatz untersagen, wenn der Hersteller der kritischen Komponente nicht vertrauenswürdig ist. | | |

| | | | | |
|---|---|---|---|---|
| | | (4) Ein Hersteller einer kritischen Komponente ist nicht vertrauenswürdig, wenn<br>1. er gegen die in der Garantieerklärung eingegangen Verpflichtungen und Versicherungen verstoßen hat,<br>2. seine in der Garantieerklärung angegebenen Tatsachen unwahr sind<br>3. er Sicherheitsüberprüfungen und Penetrationsanalysen nicht im erforderlichen Umfang an seinem Produkt und in der Produktionsumgebung in angemessener Weise unterstützt,<br>4. er bekannte bzw. bekannt gewordene Schwachstellen oder Manipulationen nicht unverzüglich | | |

| | | | | |
|---|---|---|---|---|
| | | dem Betreiber der Kritischen Infrastruktur meldet und solche nicht beseitigt,<br>5. die kritische Komponente über technische Eigenschaften verfügt, die geeignet sind, missbräuchlich auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können. Dies gilt nicht, wenn der Hersteller nachweisen kann, dass er die technische Eigenschaft nicht implementiert hat und er diese jeweils ordnungsgemäß beseitigt hat.<br>(5) Ist eine Untersagung nach Absatz 3 erfolgt, kann das Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit dem betroffenen Ressort ohne erneute | | |

| | | | | |
|---|---|---|---|---|
| | | Prüfung der Vertrauenswürdigkeit eines Herstellers nach Absatz 3<br>1. den angezeigten Einsatz weiterer kritischer Komponenten desselben Typs und desselben Herstellers untersagen und<br>2. die Nutzung im Einsatz befindlicher kritischer Komponenten desselben Typs und desselben Herstellers innerhalb einer verhältnismäßigen Frist untersagen.<br>(6) Bei wiederholten Verstößen nach Absatz 4 Nummer 1 bis 3 kann der Einsatz aller kritischen Komponenten des Herstellers untersagt werden. | | |
| 22 | | § 10 BSIG-E:<br>(…) | § 10 BSIG-E:<br>(…) | |

| | | | | |
|---|---|---|---|---|
| | | (3) Das Bundesministerium des Innern, für Bau und Heimat wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie und dem Bundesministerium der Justiz und für Verbraucherschutz, Einzelheiten der Gestaltung und Verwendung des IT-Sicherheitskennzeichens nach § 9a Absatz 1 Satz 1 zu regeln, um eine einheitliche Gestaltung des Kennzeichens und eine eindeutige Erkennbarkeit der gekennzeichneten informationstechnischen Produkte zu gewährleisten, sowie die erfassten | (2a) Das Bundesministerium des Innern, für Bau und Heimat wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie und dem Bundesministerium der Justiz und für Verbraucherschutz, Einzelheiten der Gestaltung und Verwendung des IT-Sicherheitskennzeichens nach § 9a Absatz 1 Satz 1 zu regeln, um eine einheitliche Gestaltung des Kennzeichens und eine eindeutige Erkennbarkeit der gekennzeichneten informationstechnischen Produkte zu gewährleisten, sowie die erfassten | |

| | | | | |
|---|---|---|---|---|
| | | Produktkategorien und das Verwaltungsverfahren zur Sicherstellung der Anforderungen im Zusammenhang mit der Verwendung des Kennzeichens festzulegen.<br>(…)<br>(5) Das Bundesministerium des Innern, für Bau und Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem | Produktkategorien und das Verwaltungsverfahren zur Sicherstellung der Anforderungen im Zusammenhang mit der Verwendung des Kennzeichens festzulegen.<br>(…)<br>(5) Das Bundesministerium des Innern, für Bau und Heimat bestimmt durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem | |

| | | | | |
|---|---|---|---|---|
| | | Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, bei welchen Unternehmen ein besonderes öffentliches Interesse nach § 2 Absatz 14 Nummer 2 besteht | Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit, bei welchen Anlagen oder Teilen davon ein besonderes öffentliches Interesse nach § 2 Absatz 14 Nummer 2 besteht und ob die Betreiber nach § 8f Nummer 2 den Pflichten der §§ 8a und 8b unterfallen. | |
| 23 | **TKG** | In der Inhaltsübersicht werden bei der Angabe zu § 109 hinter dem Wort „technische“ die Wörter „und organisatorische“ eingefügt. | -- | |
| 24 | | § 109 TKG-E:<br><br>(…) | § 109 TKG-E:<br><br>(2a) Maßnahmen nach Absatz 2 Satz 2 umfassen auch den Einsatz | |

| | | | | |
|---|---|---|---|---|
| | | (2) (…) Insbesondere sind Maßnahmen zu treffen, um Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern und Auswirkungen von Sicherheitsverletzungen für Nutzer, für Dienste oder für zusammengeschaltete Netze so gering wie möglich zu halten.<br>(…)<br>Der Umfang der Maßnahmen nach Satz 1 und 2 richtet sich nach dem jeweiligen Gefährdungspotenzial des öffentlichen Telekommunikationsnetzes oder öffentlich zugänglichen Telekommunikationsdienstes. Sicherheitsrelevante Netz- und Systemkomponenten, die kritische Funktionen erfüllen, (kritische Komponenten) dürfen nur eingesetzt werden, wenn sie von einer | von Systemen zur Angriffserkennung - nach Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik. Details legt das Bundesamt in einer Technischen Richtlinie im Benehmen mit der Bundesnetzagentur fest. Die Diensteanbieter und das Bundesamt dürfen die hierzu erforderlichen Daten verarbeiten. Soweit erforderlich, dürfen Diensteanbieter und das Bundesamt insoweit Kenntnisse über Tatsachen, die dem Fernmeldegeheimnis nach § 88 Absatz 2 unterliegen, für diesen Zweck verarbeiten. Daten, die für die Aufklärung des Angriffs, den Schutz der Informationstechnik und die Strafverfolgung der Angreifer erforderlich sind, haben die Diensteanbieter von sich aus und | |

| | | | | |
|---|---|---|---|---|
| | | anerkannten Prüfstelle überprüft und von einer anerkannten Zertifizierungsstelle zertifiziert wurden. Die Einzelheiten der nach den Satz 1 bis 4 zu treffenden Maßnahmen sowie Einzelheiten der Festlegung kritischer Funktionen und der Bestimmung der kritischen Komponenten nach Satz 5 legt die Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit im Katalog von Sicherheitsanforderungen nach Absatz 6 fest.<br>(…)<br>§ 62 Absatz 1 des Bundesdatenschutzgesetzes gilt entsprechend.<br>(…) | auf Anforderung den dazu zuständigen Behörden zu übermitteln. Die im Rahmen des Einsatzes von Systemen zur Angriffserkennung erhobenen Daten sind unverzüglich zu löschen, wenn sie nicht für die Vermeidung von Störungen im Sinne von Absatz 1 Satz 1 erforderlich sind. Die übrigen Daten dürfen nicht länger als zehn Jahre gespeichert werden. Hierzu muss die oder der Bundesbeauftrage für den Datenschutz und die Informationsfreiheit angehört werden. Die Diensteanbieter müssen der oder dem betrieblichen Datenschutzbeauftragten, dem Bundesamt für Sicherheit in der Informationstechnik, der Bundesnetzagentur und der oder dem | |

| | | | | |
|---|---|---|---|---|
| | | (4) (…) Insbesondere ist im Sicherheitskonzept darzustellen, auf welche Weise die verbindlichen Vorgaben des Katalogs von Sicherheitsanforderungen nach Absatz 6 umgesetzt sind. Sofern der Katalog Sicherheitsziele vorgibt, die auf unterschiedliche Weise erreicht werden können, ist im Sicherheitskonzept darzulegen, dass mit den ergriffenen Maßnahmen das jeweilige Sicherheitsziel vollumfänglich erreicht wird.<br>(5) (…) Erforderlichenfalls unterrichtet die Bundesnetzagentur die nationalen Regulierungsbehörden der anderen Mitgliedstaaten der Europäischen Union und die Agentur der Europäischen Union für Cybersicherheit über die Sicherheitsverletzungen. | Bundesbeauftragten für den Datenschutz und die Informationsfreiheit am Ende eines Quartals detailliert über die Verfahren und Umstände von Maßnahmen nach Satz 1 in diesem Zeitraum schriftlich berichten. | |

| | | | | |
|---|---|---|---|---|
| | | (…)<br>Die Bundesnetzagentur legt der Europäischen Kommission, der Agentur der Europäischen Union für Cybersicherheit und dem Bundesamt für Sicherheit in der Informationstechnik einmal pro Jahr einen zusammenfassenden Bericht über die eingegangenen Meldungen und die ergriffenen Abhilfemaßnahmen vor.<br><br>(6) (…) Die im Katalog festgelegten Anforderungen sind verbindlich.<br>Die Bundesnetzagentur gibt den Herstellern, den Verbänden der Betreiber öffentlicher Telekommunikationsnetze und den Verbänden der Anbieter öffentlich zugänglicher Telekommunikationsdienste Gelegenheit zur Stellungnahme. | | |

| | | | | |
|---|---|---|---|---|
| | | Der Katalog wird von der Bundesnetzagentur durch öffentliche Bekanntmachung zugestellt.<br>Die öffentliche Bekanntmachung wird dadurch bewirkt, dass der Katalog, die Rechtsbehelfsbelehrung und ein Hinweis auf die Veröffentlichung auf der Internetseite der Bundesnetzagentur im Amtsblatt der Bundesnetzagentur bekannt gemacht werden. Der Katalog gilt mit dem Tag als zugestellt, an dem seit dem Tag der Bekanntmachung im Amtsblatt der Bundesnetzagentur zwei Wochen verstrichen sind; hierauf ist in der Bekanntmachung hinzuweisen. Die nach Absatz 1, 2 und 4 Verpflichteten haben die Anforderungen des Katalogs spätestens ein Jahr nach dessen Inkrafttreten zu erfüllen, es sei denn, in | | |

| | | | | |
|---|---|---|---|---|
| | | dem Katalog ist eine davon abweichende Umsetzungsfrist festgelegt worden.<br>(7) (…) Unbeschadet von Satz 1 haben sich Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial alle zwei Jahre einer Überprüfung durch eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde zu unterziehen, in der festgestellt wird, ob die Anforderungen nach Absatz 1 bis 3 erfüllt sind. Die Bundesnetzagentur legt den Zeitpunkt der erstmaligen Überprüfung nach Satz 2 fest.<br>Der nach Satz 1 und 2 Verpflichtete hat eine Kopie des Überprüfungsberichts unverzüglich an die Bun- | | |

| | | | | |
|---|---|---|---|---|
| | | desnetzagentur und an das Bundesamt für Sicherheit in der Informationstechnik, sofern dieses die Überprüfung nicht vorgenommen hat, zu übermitteln.<br>(…)<br>Die Bewertung der Überprüfung sowie eine diesbezügliche Feststellung von Sicherheitsmängeln im Sicherheitskonzept erfolgt durch die Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik. | | |
| 25 | **TMG** | § 13 TMG-E:<br>(…)<br>(7a) Das Bundesamt für Sicherheit in der Informationstechnik kann zur Abwehr von Gefahren für die Kom- | § 13 TMG-E:<br>(…)<br>(7a) Das Bundesamt für Sicherheit in der Informationstechnik kann zur Abwehr von Gefahren für die Kom- | |

| | | | | |
|---|---|---|---|---|
| | | munikationstechnik des Bundes oder eines Betreibers einer Kritischen Infrastruktur oder für eine Infrastruktur im besonderen öffentlichen Interesse gegenüber Diensteanbietern in begründeten Ausnahmefällen die Umsetzung erforderlicher technischer und organisatorischer Vorkehrungen zur Sicherstellung der Schutzgüter nach Absatz 7 Satz 1 anordnen, wenn hierdurch eine konkrete Gefahr für Datenverarbeitungssysteme einer Vielzahl von Nutzern durch unzureichend gesicherte Telemedienangebote beseitigt werden kann.<br>(…)<br>(9) Liegen tatsächliche Anhaltspunkte für eine unrechtmäßige Er- | munikationstechnik des Bundes oder eines Betreibers einer Kritischen Infrastruktur oder für eine Infrastruktur im besonderen öffentlichen Interesse gegenüber Diensteanbietern in begründeten Ausnahmefällen die Umsetzung erforderlicher technischer und organisatorischer Vorkehrungen zur Sicherstellung der Schutzgüter nach Absatz 7 Satz 1 anordnen, wenn hierdurch eine konkrete Gefahr für Datenverarbeitungssysteme einer Vielzahl von Nutzern durch unzureichend gesicherte Telemedienangebote beseitigt werden kann.<br>(…) | |

| | | | | |
|---|---|---|---|---|
| | | langung oder Verbreitung personenbezogener Daten oder Daten, die Geschäftsgeheimnisse beinhalten, vor, so ist der Zugang zu diesen Daten durch den Diensteanbieter zu sperren. Der betroffene Nutzer ist zu benachrichtigen.<br>(10) Im Falle der unrechtmäßigen Erlangung oder Verbreitung von Geschäftsgeheimnissen können die zuständigen Stellen unter den Voraussetzungen des Absatz 9 eine Sperrung der Daten anordnen. Zuständige Stellen sind die für die Abwehr von Gefahren für die öffentliche Sicherheit oder Ordnung zuständigen Behörden. Der Diensteanbieter hat die unverzügliche Umsetzung der Anordnung sicherstellen. | | |

| | | | | |
|---|---|---|---|---|
| 26 | **AWV** | § 55 Abs. 1 S. 2 Nr. 2 AWV-E:<br>Eine Gefährdung der öffentlichen Ordnung oder Sicherheit kann insbesondere vorliegen, wenn das inländische Unternehmen<br>(…)<br>2. kritische Komponenten nach § 2 Absatz 13 des BSI-Gesetzes in der jeweils geltenden Fassung besonders entwickelt oder ändert, die branchenspezifisch zum Betrieb von Kritischen Infrastrukturen im Sinne des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik dient,<br>(…)<br>--<br>Überdies ist vorgesehen, § 55 Abs. 1 S. 3 AWV zu streichen. | § 55 Abs. 1 S. 2 Nr. 2 AWV-E:<br>Eine Gefährdung der öffentlichen Ordnung oder Sicherheit kann insbesondere vorliegen, wenn das inländische Unternehmen<br>(…)<br>2. KRITIS-Kernkomponenten nach § 2 Absatz 13 des BSI-Gesetzes in der jeweils geltenden Fassung besonders entwickelt oder ändert, die branchenspezifisch zum Betrieb von Kritischen Infrastrukturen im Sinne des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik dient,<br>(…)<br>-<br>Überdies ist vorgesehen, § 55 Abs. 1 S. 3 AWV zu streichen. | |