VDA Verband der Automobilindustrie

Empfehlung

Zweites Gesetz zur Erhöhung der Sicherheit informations-technischer Systeme

IT-SIG 2.0, Oktober 2021

Ansprechpartner

Dr. Joachim Damasky
Geschäftsführung
joachim.damasky@vda.de

Matthias Krähling
Abteilungsleiter
matthias.kraehling@vda.de

Martin Lorenz
Leiter Fachgruppe
martin.lorenz@vda.de

Arbeitskreis Informationssicherheit

Autoren:

Andreas Ebert
Volkswagen

Francisco Rodriguez
Bosch

Martin Lorenz
VDA

Michael Bunzel
BMW

Olaf Strumpf
Magna

Oliver Mann
Daimler

1. Einleitung

Der VDA Arbeitskreis Informationssicherheit[1] empfiehlt die folgenden Hinweise zum Umgang mit dem sogenannten IT-SIG 2.0 für die deutsche Automobilbranche, da die Automobilindustrie als Anbieter digitaler Dienste und als Unternehmen im besonderen öffentlichen Interesse unter diese Regelung fallen. Somit erstreckt sich der Anwendungsbereich dieser Empfehlung auf die Produkte und Dienste der Automobilbranche. Unberührt bleiben branchenfremde Dienstleistungen wie beispielsweise entgeltliche Dienstleistungen für den Zahlungs-, Kredit- und Kapitalverkehr.

Die Handlungsempfehlungen beziehen sich auf die umfängliche IT-Informationssicherheit und beinhalten somit die Begriffe wie Cyber-, IT-Sicherheit und technische Sicherheit.

Diese Empfehlung soll den Umgang mit dem IT-SIG 2.0 erleichtern und innerhalb der deutschen Automobilbranche ein einheitliches Handeln ermöglichen.

Wir empfehlen den Mitgliedsunternehmen, dass sie ihre Maßnahmen und Vorgehensweisen zur Informationssicherheit hinsichtlich der hier erwähnten Punkte prüfen und wenn notwendig Anpassungen vornehmen.

Im Rahmen der geforderten zweijährigen Selbstauskunft an das BSI wird empfohlen, den aktuellen VDA-ISA Katalog als Grundlage heranzuziehen. Ein umfängliches TISAX-Audit (Zertifizierung) durch externe Prüfer ist nicht erforderlich.

Wir empfehlen u.a. aus dem VDA-ISA Katalog den Abschnitt Informationssicherheit im Rahmen der Selbsterklärung. Das Tabellenblatt „Informationssicherheit“ enthält alle Basis-Controls basierend auf der Norm ISO/IEC27001. Die Controls selbst sind als Frage formuliert. Das Ziel des jeweiligen Controls und die Anforderungen zur Erreichung des Ziels sind in den entsprechend benannten Spalten hinterlegt. Jede Control kann hierbei immer anhand des Grades der Erreichung des Ziels bewertet werden. Der VDA-ISA Katalog steht auf der VDA-Webseite zum Download kostenfrei zur Verfügung.

Das am 27.05.2021 im Bundesgesetzblatt veröffentlichte IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) ändert als Artikelgesetz das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG), das Telemediengesetz (TMG) und das Telekommunikationsgesetz (TKG).

Das zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SIG 2.0) dient der Stärkung der Cyber- und Informationssicherheit von Staat, Wirtschaft und Gesellschaft. Das zweite Gesetz folgt dem seit Juli 2015 gültigen Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz), das erstmals größere Änderungen am BSI-Gesetz (BSIG) vornahm.

Das Gesetz erweitert unter anderem die Aufgaben und Befugnisse des BSI. Somit wird das BSI die nationale Behörde für Cybersicherheitszertifizierung (§ 3 Abs. 1 S. 2 Ziff. 5b BSIG). Ferner erhält das BSI eine Kontroll- und Prüfbefugnis gegenüber der Bundesverwaltung (§ 4a BSIG) mit der Pflicht zur Bereitstellung der erforderlichen Informationen der Bundesbehörden. Das BSI ist die allgemeine Meldestelle für die Sicherheit in der Informationstechnik (§ 4b BSIG) und darf Protokolldaten für bis zu 18 Monate speichern (§ 5 Abs. 2 BSIG). Das

1 Autoren: Andreas Ebert (Volkswagen), Francisco Rodriguez (Bosch), Martin Lorenz (VDA), Michael Bunzel (BMW), Olaf Strumpf (Magna), Oliver Mann (Daimler)

BSI erhält die Pflicht, einen Gesamtplan für Reaktionsmaßnahmen des Bundes, im Falle erheblicher Störungen, zu erstellen. Ferner wurde ein Auskunftsrecht gegenüber demjenigen, der geschäftsmäßige Telekommunikationsdienste erbringt (§ 5d BSIG), festgeschrieben. Das BSI erstellt Warnung vor Sicherheitslücken, Schadprogrammen usw. (§ 7 Abs. 1 BSIG) und spricht dazu Empfehlungen von Sicherheitsmaßnahmen aus.

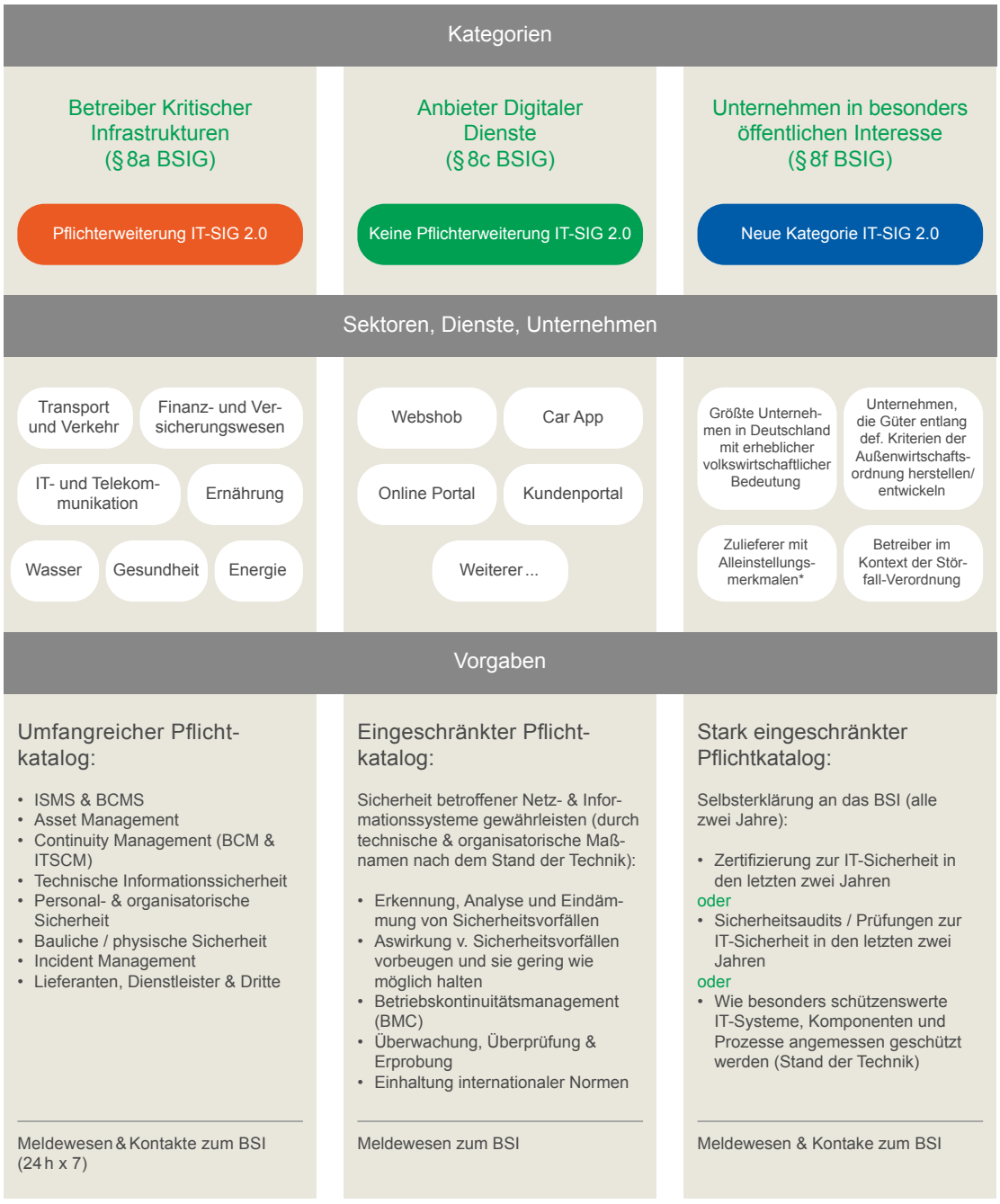
Die Einführung des Begriffs der „Unternehmen im besonderen öffentlichen Interesse“ (UBI), beruht auf der Änderung im § 2 Abs. 14. Nach § 2 Abs. 14 sollen dies unter anderem Unternehmen sein, deren Geschäftstätigkeit unter § 60 Abs. 1 der Außenwirtschaftsverordnung fällt (Nr. 1) oder die aufgrund ihrer volkswirtschaftlichen Bedeutung, bemessen insbesondere an ihrer Wertschöpfung, von besonderem öffentlichem Interesse sind (Nr. 2 Alt. 1). Ebenso fallen Unternehmen, die als Zulieferer wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung sind, unter dieses Gesetz (Nr. 2 Alt. 2).

Eine entsprechende Rechtsverordnung gemäß § 10 Abs. 5, welche die sog. Wirtschafts-UBI nach Nr. 2 genauer definiert, liegt derzeit noch nicht vor. Gleichwohl ist davon auszugehen, dass sowohl Fahrzeughersteller sowie einige Zulieferer unter diese Regelung fallen werden. Für Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 3 besteht die Möglichkeit für eine freiwillige Registrierung beim Bundesamt für Sicherheit in der Informationstechnik (BSI), um ebenfalls von einem vertrauensvollen Austausch profitieren zu können.

Daneben können Geschäftsbereiche der Automobilindustrie unter die bereits vor dem IT-SiG 2.0 bestehende Regelung des § 8c, „Anbieter digitaler Dienste“ (Digital Service Provider, DSP) fallen, wenn beispielsweise eine Car-App, ein Web-Shop oder ein Kundenportal betrieben wird. Bei DSP handelt es sich jedoch um keine neu eingeführte Kategorie im IT-SiG 2.0.

Unternehmen im besonderen öffentlichen Interesse und Anbieter digitaler Dienste sind nicht mit kritischer Infrastruktur (KRITIS) gleichzustellen.

2. Definition zu Anbietern digitaler Dienste (DSP) und Unternehmen im besonderen öffentlichen Interesse (UBI)



*Wird über Merkmale der Rechtsverordnung zum IT-Sicherheitsgesetz 2.0 konkret definiert

Die deutsche Automobilindustrie kann sowohl vom § 8c als auch vom § 8f betroffen sein. Anforderungen für Betreiber kritischer Infrastrukturen (§ 8a) müssen von der Automobilindustrie nicht erfüllt werden.

2.1 Anbieter digitaler Dienste (§8c)

Digitale Dienste im Sinne dieses Gesetzes sind Dienste einer Dienstleistung der Informationsgesellschaft, d. h. jede in der Regel gegen Entgelt elektronisch im Fernabsatz und auf individuellen Abruf eines Empfängers erbrachte Dienstleistung und die

- es Verbrauchern oder Unternehmern im Sinne des Artikels 4 Absatz 1 Buchstabe a beziehungsweise Buchstabe b der Richtlinie 2013/11/EU des Europäischen Parlaments und des Rates vom 21. Mai 2013 über die alternative Beilegung verbraucherrechtlicher Streitigkeiten und zur Änderung der Verordnung (EG) Nr. 2006/2004 und der Richtlinie 2009/22/EG (Richtlinie über alternative Streitbeilegung in Verbraucherangelegenheiten) (ABl. L 165 vom 18.6.2013, S. 63) ermöglichen, Kaufverträge oder Dienstleistungsverträge mit Unternehmern entweder auf der Webseite dieser Dienste oder auf der Webseite eines Unternehmers, die von diesen Diensten bereitgestellte Rechendienste verwendet, abzuschließen (Online-Marktplätze);

- es Nutzern ermöglichen, Suchen grundsätzlich auf allen Webseiten oder auf Webseiten in einer bestimmten Sprache anhand einer Abfrage zu einem beliebigen Thema in Form eines Stichworts, einer Wortgruppe oder einer anderen Eingabe vorzunehmen, die daraufhin Links anzeigen, über die der Abfrage entsprechende Inhalte abgerufen werden können (Online-Suchmaschinen);

- den Zugang zu einem skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglichen (Cloud-Computing-Dienste),

und nicht zum Schutz grundlegender staatlicher Funktionen eingerichtet worden sind oder für diese genutzt werden.

Als Anbieter digitaler Dienste innerhalb der Europäischen Union ist die Sicherheit betroffener Netz- & Informationssysteme mindestens durch folgende Maßnahmen zu gewährleisten (geeignete bzw. verhältnismäßige technische & organisatorische Maßnahmen nach dem Stand der Technik):

- Sicherheit der Systeme und Anlagen

- Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen

- Auswirkungen v. Sicherheitsvorfällen vorbeugen und so gering wie möglich halten

- Betriebskontinuitätsmanagement (BCM)

- Überwachung, Überprüfung und Erprobung

- Einhaltung internationaler Normen

Zusätzlich erforderlich:

- Etablierung eines Meldewesens von / zum BSI

- Meldung von IT-Sicherheitsvorfällen mit erheblicher Auswirkung auf die Bereitstellung eines innerhalb der Europäischen Union erbrachten digitalen Dienstes. Wir sprechen uns für eine strafrechtliche Anzeige bei IT-Sicherheitsvorfällen bzw. Cyberangriffen aus. Neben der Strafanzeige über die zuständige Polizeidienststelle (s. Ziffer 6, Seite 38ff) empfehlen wir die Unterrichtung des BSI auch bei niederschwelligen IT-Sicherheitsvorfällen und ggf. anderer Sicherheitsbehörden wie den örtlich zuständigen Verfassungsschutz.

§ 8c Besondere Anforderungen an Anbieter digitaler Dienste

(1) Anbieter digitaler Dienste haben geeignete und verhältnismäßige technische und organisatorische Maßnahmen zu treffen, um Risiken für die Sicherheit der Netz- und Informationssysteme, die sie zur Bereitstellung der digitalen Dienste innerhalb der Europäischen Union nutzen, zu bewältigen. Sie haben Maßnahmen zu treffen, um den Auswirkungen von Sicherheitsvorfällen auf innerhalb der Europäischen Union erbrachte digitale Dienste vorzubeugen oder die Auswirkungen so gering wie möglich zu halten.

(2) Maßnahmen zur Bewältigung von Risiken für die Sicherheit der Netz- und Informationssysteme nach Absatz 1 Satz 1 müssen unter Berücksichtigung des Stands der Technik ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, dass dem bestehenden Risiko angemessen ist. Dabei ist folgenden Aspekten Rechnung zu tragen:
1. der Sicherheit der Systeme und Anlagen,
2. der Erkennung, Analyse und Eindämmung von Sicherheitsvorfällen,
3. dem Betriebskontinuitätsmanagement,
4. der Überwachung, Überprüfung und Erprobung,
5. der Einhaltung internationaler Normen.

Die notwendigen Maßnahmen werden durch Durchführungsrechtsakte der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 näher bestimmt.

(3) Anbieter digitaler Dienste haben jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die Bereitstellung eines von ihnen innerhalb der Europäischen Union erbrachten digitalen Dienstes hat, unverzüglich dem Bundesamt zu melden. Die Voraussetzungen, nach denen Auswirkungen eines Sicherheitsvorfalls erheblich sind, werden durch Durchführungsakte der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 unter Berücksichtigung insbesondere der folgenden Parameter näher bestimmt:
1. die Zahl der von dem Sicherheitsvorfall betroffenen Nutzer, insbesondere der Nutzer, die den Dienst für die Bereitstellung ihrer eigenen Dienste benötigen,
2. die Dauer des Sicherheitsvorfalls,
3. das von dem Sicherheitsvorfall betroffene geographische Gebiet,
4. das Ausmaß der Unterbrechung der Bereitstellung des Dienstes,
5. das Ausmaß der Auswirkungen auf wirtschaftliche und gesellschaftliche Tätigkeiten.
Die Pflicht zur Meldung eines Sicherheitsvorfalls entfällt, wenn der Anbieter keinen ausreichenden Zugang zu den Informationen hat, die erforderlich sind, um die Auswirkung eines Sicherheitsvorfalls gemessen an den Parametern nach Satz 2 zu bewerten. Für den Inhalt der Meldungen gilt § 8b Absatz 4 entsprechend,

soweit nicht Durchführungsakte der Kommission nach Artikel 16 Absatz 9 der Richtlinie (EU) 2016/1148 etwas anderes bestimmen. Über nach Satz 1 gemeldete Sicherheitsvorfälle, die Auswirkungen in einem anderen Mitgliedstaat der Europäischen Union haben, hat das Bundesamt die zuständige Behörde dieses Mitgliedstaats zu unterrichten.

(4) Liegen Anhaltspunkte dafür vor, dass ein Anbieter digitaler Dienste die Anforderungen des Absatzes 1 in Verbindung mit den Durchführungsrechtsakten der Kommission nach Artikel 16 Absatz 8 der Richtlinie (EU) 2016/1148 und des Absatzes 2 in Verbindung mit den Durchführungsrechtsakten der Kommission nach Artikel 16 Absatz 9 der Richtlinie (EU) 2016/1148 nicht erfüllt, kann das Bundesamt von dem Anbieter digitaler Dienste folgende Maßnahmen verlangen:
1. die Übermittlung der zur Beurteilung der Sicherheit seiner Netz- und Informationssysteme erforderlichen Informationen, einschließlich Nachweisen über ergriffene Sicherheitsmaßnahmen,
2. die Beseitigung von Mängeln bei der Erfüllung der in den Absätzen 1 und 2 bestimmten Anforderungen.
Die Anhaltspunkte können sich auch aus Feststellungen ergeben, die dem Bundesamt von den zuständigen Behörden eines anderen Mitgliedstaats der Europäischen Union vorgelegt werden.

(5) Hat ein Anbieter digitaler Dienste seine Hauptniederlassung, einen Vertreter oder Netz- und Informationssysteme in einem anderen Mitgliedstaat der Europäischen Union, so arbeitet das Bundesamt bei der Erfüllung der Aufgaben nach Absatz 4 mit der zuständigen Behörde dieses Mitgliedstaats zusammen. Diese Zusammenarbeit kann das Ersuchen umfassen, die Maßnahmen in Absatz 4 Satz 1 Nummer 1 und 2 zu ergreifen.

2.2 Unternehmen im besonderen öffentlichen Interesse (§8f)

Mit der Fortschreibung des IT-Sicherheitsgesetzes wurde der Ordnungsrahmen erweitert, um neuen Gefährdungen angemessen begegnen zu können. § 2 Absatz 14 regelt Unternehmen im besonderen öffentlichen Interesse (UBI).

Unter UBI nach Nummer 2 fallen solche, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind. Grund dafür ist, dass auch Ausfall und Störung der Geschäftstätigkeit einzelner Unternehmen, die nicht Betreiber Kritischer Infrastrukturen im Sinne dieses Gesetzes sind, von gesamtgesellschaftlicher Bedeutung sein können. Das ist beispielsweise dann der Fall, wenn die IT-Systeme eines der größten Unternehmen Deutschlands nach inländischer Wertschöpfung durch einen Cyberangriff oder durch anderweitige IT-Störung derart gestört werden, dass das Unternehmen seiner Geschäftstätigkeit für einen längeren Zeitraum nicht nachgehen kann. Die Berechnung der inländischen Wertschöpfung wird dabei in einer Rechtsverordnung im Einzelnen festgelegt.

Die neue Kategorie der Unternehmen im besonderen öffentlichen Interesse hat zwar eine große Bedeutung in Bezug auf die IT-Sicherheit in Deutschland, jedoch ist diese im direkten Vergleich zu Betreibern Kritischer Infrastrukturen (KRITIS) deutlich abgestuft. Sowohl die hier neu eingeführte Definition für Unternehmen im besonderen öffentlichen Interesse als auch die sich daraus ergebenden Rechtsfolgen für die betroffenen Unternehmen sind nicht mit denen von Betreibern Kritischer Infrastrukturen vergleichbar. Die neu eingeführten Verpflichtungen für diese Unternehmen bleiben dementsprechend deutlich hinter den Pflichten für die Betreiber Kritischer Infrastrukturen nach diesem Gesetz zurück. (Quelle: BT-Drucksache 19/26106 S. 57 ff.)

„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 Unternehmen und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit, welche wirtschaftlichen Kennzahlen bei der Berechnung der inländischen Wertschöpfung heranzuziehen sind, wie die Berechnung mit Hilfe der Methodik der direkten Wertschöpfungsstaffel zu erfolgen hat und welche Schwellenwerte maßgeblich dafür sind, dass ein Unternehmen zu den größten Unternehmen in Deutschland im Sinne des § 2 Absatz 14 Satz 1 Nummer 2 gehört. Unter den Voraussetzungen nach Satz 1 kann das Bundesministerium des Innern, für Bau und Heimat durch Rechtsverordnung bestimmen, welche Alleinstellungsmerkmale maßgeblich dafür sind, dass Zulieferer für Unternehmen, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören, von wesentlicher Bedeutung im Sinne des § 2 Absatz 14 Satz 1 Nummer 2 sind.“

Unternehmen von besonderer volkswirtschaftlicher Bedeutung (vgl. § 10 Abs.5) sowie Zulieferer mit Alleinstellungsmerkmal[2] unterliegen folgenden Pflichten:

§ 8f Abs. 5

„Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 und 2 sind verpflichtet, sich gleichzeitig mit der Vorlage der ersten Selbsterklärung zur IT-Sicherheit nach Absatz 1 beim Bundesamt zu registrieren und eine zu den üblichen Geschäftszeiten erreichbare Stelle zu benennen. Die Übermittlung von Informationen durch das Bundesamt nach § 8b Absatz 2 Nummer 4 erfolgt an diese Stelle.“

[2] wird durch eine Rechtsverordnung (RVO) geregelt

- Registrierung beim Bundesamt für Sicherheit in der Informationstechnologie (BSI)
- Benennung einer Kontaktstelle, die zu üblichen Geschäftszeiten erreichbar ist

§ 8f Abs. 7

„Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 und 2 haben ab dem Zeitpunkt, zu dem eine Pflicht zur Vorlage der Selbsterklärung zur IT-Sicherheit nach Absatz 1 besteht, die folgenden Störungen unverzüglich über die nach Absatz 5 benannte Stelle an das Bundesamt zu melden:

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,

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.

Die Meldung muss Angaben zu der Störung, zu den technischen Rahmenbedingungen, insbesondere zu der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und der Art der betroffenen Einrichtung oder Anlage enthalten.“

- Sofortige Meldung von Störung der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit der IT-Systeme. Komponenten oder Prozesse, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Wertschöpfung führen können.

§ 10 Abs. 5 i.V.m. der jeweiligen gültigen Rechtsverordnung (vgl. Seite 2)

- Vorlage einer Selbsterklärung zur IT-Informationssicherheit, Wiederholung alle zwei Jahre

ODER

- IT-Sicherheitszertifizierungen in den letzten zwei Jahren

ODER

- Sonstige IT-Sicherheitsaudits und Prüfungen in den letzten zwei Jahren

ODER

- Information über den Schutz besonders schützenswerter IT-Systeme, Komponenten und Prozesse.

UBI müssen im 2 Jahreszyklus eine Selbsterklärung an das BSI, mit folgenden Mindestinhalten, übersenden:

- Zertifizierungen zur IT-Sicherheit
  Lieferung von entsprechenden Zertifizierungen der letzten zwei Jahre an das BSI, falls vorhanden.

ODER

- Sicherheitsaudits / Prüfungen zur IT-/Informationssicherheit
  Lieferung von entsprechenden Sicherheitsaudits / Prüfungen zur IT-Sicherheit in den letzten zwei Jahren, falls vorhanden.

ODER

Falls vorherige zwei Inhalte nicht existieren bzw. ausreichend sind:

- Schutz besonders schützenswerter Informationen, IT-Systeme, Komponenten und Prozesse
  Lieferung eines Nachweises wie besonders schützenswerte Informationen, IT-Systeme, Komponenten und Prozesse angemessen nach dem Stand der Technik geschützt werden.

Zusätzlich erforderlich:

- Etablierung einer Kontaktstelle & eines Meldewesens von / zum BSI
  Mitteilung einer internen Kontaktstelle an das BSI, die für die Informationssicherheit im Unternehmen operativ zuständig ist. Dies kann eine zentrale interne Meldestelle im Rahmen des Security Incident Management Prozesses sein, z.B. ein SOC (Security Operations Center) oder ein Cyber Security Response Team. Es können aber auch Stellen wie der Information Security Officer (CISO) oder der Chief Security Officer (CSO) sein. Diese Stelle muss zu den üblichen Geschäftszeiten erreichbar sein.

- Meldung von IT-Sicherheitsvorfällen und insbesondere Cyberangriffen mit erheblicher Beeinträchtigung oder einem Ausfall der Erbringung der Wertschöpfung (Störungen der Verfügbarkeit, Integrität und der Vertraulichkeit). Wir sprechen uns für eine strafrechtliche Anzeige bei Cyberangriffen aus. Neben der Strafanzeige über die zuständige Polizeidienststelle empfehlen wir die Unterrichtung des BSI und ggf. anderer Sicherheitsbehörden wie den örtlich zuständigen Verfassungsschutz.

3. Prävention “Three Lines of Defence” – Modell

Eine Ausprägung der Informationssicherheit durch das Modell der drei Verteidigungslinien („Three Lines of Defence“) bietet eine valide Vorgehensweise. Dieses Modell ermöglicht eine klare Rollentrennung in der Realisierung der Informationssicherheit und schafft eine notwenige Resilienz.

Erste „Verteidigungslinie“ bilden die Fachbereiche mit dem operativen Management. Diese Linie hat, als „Risiko-Eigentümer“, die Verantwortung für die Identifizierung, Analyse der Informationssicherheitsrisiken sowie die Reduzierung Reduktion von Risiken durch Sicherheitsmaßnahmen. Zu dieser Verteidigungslinie gehören neben den Fachbereichen auch die operative IT-Sicherheit mit den Prozessen zum Monitoring der IT-Sicherheit.

Die zweite „Verteidigungslinie“ trägt die Verantwortung für die Steuerung der Risikomanagementfunktion in der Informationssicherheit. Zu dieser Verantwortung gehört auch die Festlegung von Methoden und Verfahren für das Informationssicherheitsrisikomanagement, das Erlassen von Richtlinien und Standards zur Informations-/IT-Sicherheit. Unabdingbar für die zweite Verteidigungslinie ist eine unabhängige Berichtslinie an die Unternehmensleitung über den Status und die Wirksamkeit der Informationssicherheit. Ausprägung der zweiten „Verteidigungslinie“ (2nd Line of Defence).

Die zweite „Verteidigungslinie“ sollte die Verantwortung die für die Informationssicherheit über alle Aspekte der Informationstechnik, die für die Leistungserbringung / Wertschöpfung des Unternehmens notwendig ist, wahrnehmen. Hierzu zählt klassischerweise u.a. die Büro IT, kfm. IT, Produktions-IT. Ausgenommen werden kann beispielsweise, die Informationstechnik die ggf. in eigenen Produkten und Services steckt.

Die möglicherweise vorhandene Struktur des Unternehmens, die Berührungspunkte zur Informationssicherheit haben, einzubeziehen.

Hierzu zählen:

- Chief Information Security Officer (CISO)
- Unternehmenssicherheit und der Chief Security Officer (CSO)
- Beauftragte für den Datenschutz
- Technische IT-Sicherheit
- Rechtsabteilung, die mit Fragen des IT-Rechts beauftragt sind

Eine Operationalisierung der gemeinsamen Verantwortung könnte durch ein entsprechend besetztes Gremium erfolgen. Hierbei fallen den Beteiligten nachstehende Aufgaben zu.

- CISO vertritt die Belange der Informationssicherheit und steht dem Gremium als Leiter und Moderator vor.
- Die Unternehmenssicherheit bildet die Schnittstelle zu den örtlichen bzw. fachlichen zuständigen Sicherheitsbehörden (beispielsweise Polizei, Verfassungsschutz). Sie steuert Lagebilderkenntnisse aus dem Wirtschaftsschutz bei und koordiniert im Falle von Cyberangriffen die Kommunikation mit den Behörden.
- Die technische IT-Sicherheit konkretisiert die Anforderungen der Informationssicherheit und setzt diese für IT bezogene Bedrohungen um.
- Der Datenschutzbeauftragte berät in allen Fragen des Datenschutzes, da Verletzungen der IT-Sicherheit oftmals Belange des Datenschutzes berühren.
- Die Rechtsabteilung berät für alle Fragen betreffend des IT-Rechts.

Die dritte “Verteidigungslinie“ bildet eine unabhängige Prüfungs- und Beratungsinstanz. Diese wird in der Regel durch die interne Revision (Inhouse Audit) abgebildet. Die interne Revision unterstützt in dieser Funktion Unternehmensleitung, bei der Wahrnehmung der Verantwortung zur Implementierung eines geeigneten Risikomanagements.

4. Management der Informationssicherheit (ISMS / VDA-ISA / TISAX)

Zum Management der Informationssicherheit sollte ein entsprechendes System (Information Security Management System, ISMS) aufgebaut, implementiert und kontinuierlich den Risiken entsprechend angepasst werden. Hier empfehlen wir als Grundlage und Nachweis ebenfalls die jeweilige aktuelle Fassung des VDA-ISA Katalogs (Information Security Assessment, VDA-ISA). Der VDA-ISA orientiert sich an der ISO 27001 und geht in Teilen darüber hinaus.

5. Gesetzestext

Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme*

Der Bundestag hat das folgende Gesetz beschlossen:

Artikel 1 Änderung des BSI-Gesetzes

Artikel 1 wird in 3 Vorschriften zitiert und ändert mWv. 28. Mai 2021 BSIG § 1, § 2, § 3, § 5, § 5a, § 5c (neu), § 7, § 7a, § 7b (neu), § 7c (neu), § 7d (neu), § 8a, § 8b, § 8c, § 8d, § 8e, § 8f (neu), § 9, § 9a (neu), § 9b (neu), § 9c (neu), § 10, § 11, § 13, § 14, § 14a (neu), mWv. 1. Dezember 2021 offen

Das BSI-Gesetz vom 14. August 2009 (BGBl. I S. 2821), das zuletzt durch Artikel 73 der Verordnung vom 19. Juni 2020 (BGBl. I S. 1328) geändert worden ist, wird wie folgt geändert:

1. § 1 wird wie folgt gefasst:

„§ 1 Bundesamt für Sicherheit in der Informationstechnik

Das Bundesamt für Sicherheit in der Informationstechnik (Bundesamt) ist eine Bundesoberbehörde im Geschäftsbereich des Bundesministeriums des Innern, für Bau und Heimat. Es ist die zentrale Stelle für Informationssicherheit auf nationaler Ebene. Aufgaben gegenüber den Bundesministerien führt das Bundesamt auf Grundlage wissenschaftlich-technischer Erkenntnisse durch.“

2. § 2 wird wie folgt geändert:

a) Absatz 2 wird wie folgt geändert:

aa) Die folgenden Sätze werden vorangestellt:

* Notifiziert gemäß der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

„Informationen sowie informationsverarbeitende Systeme, Komponenten und Prozesse sind besonders schützenswert. Der Zugriff auf diese darf ausschließlich durch autorisierte Personen oder Programme erfolgen. Die Sicherheit in der Informationstechnik und der damit verbundene Schutz von Informationen und informationsverarbeitenden Systemen vor Angriffen und unautorisierten Zugriffen im Sinne dieses Gesetzes erfordert die Einhaltung bestimmter Sicherheitsstandards zur Gewährleistung der informationstechnischen Grundwerte und Schutzziele."

bb) In dem neuen Satz 4 wird das Wort „Unversehrtheit" durch das Wort „Integrität" ersetzt.

b) Absatz 3 wird wie folgt geändert:

aa) Satz 1 wird wie folgt gefasst:

„Kommunikationstechnik des Bundes im Sinne dieses Gesetzes ist die Informationstechnik, die von einer oder mehreren Bundesbehörden oder im Auftrag einer oder mehrerer Bundesbehörden betrieben wird und der Kommunikation oder dem Datenaustausch innerhalb einer Bundesbehörde, der Bundesbehörden untereinander oder der Bundesbehörden mit Dritten dient."

bb) In Satz 2 werden vor den Wörtern „der Bundesgerichte" die Wörter „des Bundesverfassungsgerichts" und ein Komma eingefügt.

c) Nach Absatz 8 wird folgender Absatz 8a eingefügt:

„(8a) Protokollierungsdaten im Sinne dieses Gesetzes sind Aufzeichnungen über technische Ereignisse oder Zustände innerhalb informationstechnischer Systeme."

d) Nach Absatz 9 werden die folgenden Absätze 9a und 9b eingefügt:

„(9a) IT-Produkte im Sinne dieses Gesetzes sind Software, Hardware sowie alle einzelnen oder miteinander verbundenen Komponenten, die Informationen informationstechnisch verarbeiten.

(9b) Systeme zur Angriffserkennung im Sinne dieses Gesetzes sind durch 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."

e) In Absatz 10 Satz 1 Nummer 1 wird das Wort „sowie" durch ein Komma ersetzt und werden nach dem Wort „Versicherungswesen" die Wörter „sowie Siedlungsabfallentsorgung" eingefügt.

f) Die folgenden Absätze 13 und 14 werden angefügt:

„(13) Kritische Komponenten im Sinne dieses Gesetzes sind IT-Produkte,

1. die in Kritischen Infrastrukturen eingesetzt werden,

2. bei denen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können und

3. die auf Grund eines Gesetzes unter Verweis auf diese Vorschrift

a) als kritische Komponente bestimmt werden oder

b) eine auf Grund eines Gesetzes als kritisch bestimmte Funktion realisieren.

Werden für einen der in Absatz 10 Satz 1 Nummer 1 genannten Sektoren keine kritischen Komponenten und keine kritischen Funktionen, aus denen kritische Komponenten abgeleitet werden können, auf Grund eines Gesetzes unter Verweis auf diese Vorschrift bestimmt, gibt es in diesem Sektor keine kritischen Komponenten im Sinne dieses Gesetzes.

(14) Unternehmen im besonderen öffentlichen Interesse sind Unternehmen, die nicht Betreiber Kritischer Infrastrukturen nach Absatz 10 sind und

1. die Güter nach § 60 Absatz 1 Nummer 1 und 3 der Außenwirtschaftsverordnung in der jeweils geltenden Fassung herstellen oder entwickeln,

2. die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind oder die für solche Unternehmen als Zulieferer wegen ihrer Alleinstellungsmerkmale von wesentlicher Bedeutung sind oder

3. die Betreiber eines Betriebsbereichs der oberen Klasse im Sinne der Störfall-Verordnung in der jeweils geltenden Fassung sind oder nach § 1 Absatz 2 der Störfall-Verordnung diesen gleichgestellt sind.

Die Unternehmen im besonderen öffentlichen Interesse nach Satz 1 Nummer 2 werden durch die Rechtsverordnung nach § 10 Absatz 5 bestimmt, in der festgelegt wird, welche wirtschaftlichen Kennzahlen maßgeblich dafür sind, dass ein Unternehmen zu den größten Unternehmen in Deutschland im Sinne der Nummer 2 gehört und welche Alleinstellungsmerkmale maßgeblich dafür sind, dass Zulieferer für solche Unternehmen von wesentlicher Bedeutung sind.“

3. § 3 Absatz 1 wird wie folgt geändert:

a) Satz 1 wird wie folgt gefasst:

„Das Bundesamt fördert die Sicherheit in der Informationstechnik mit dem Ziel, die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und deren Verarbeitung zu gewährleisten.“

b) In Satz 2 Nummer 2 wird das Wort „oder“ gestrichen.

c) Nach Satz 2 Nummer 5 wird folgende Nummer 5a eingefügt:

„5a. Wahrnehmung der Aufgaben und Befugnisse nach Artikel 58 Absatz 7 und 8 der Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit, Abl. L 151 vom 7.6.2019, S. 15) als nationale Behörde für die Cybersicherheitszertifizierung;“.

d) Nach Satz 2 Nummer 12 wird folgende Nummer 12a eingefügt:

„12a. Beratung und Unterstützung der Stellen des Bundes in Fragen der Sicherheit in der Informationstechnik;“.

e) Satz 2 Nummer 14 wird wie folgt gefasst:

„14. Beratung, Information und Warnung der Stellen des Bundes, der Länder sowie der Hersteller, Vertreiber und Anwender in Fragen der Sicherheit in der Informationstechnik, insbesondere unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;“.

f) Nach Satz 2 Nummer 14 wird folgende Nummer 14a eingefügt:

„14a. Verbraucherschutz und Verbraucherinformation im Bereich der Sicherheit in der Informationstechnik, insbesondere durch Beratung und Warnung von Verbrauchern in Fragen der Sicherheit in der Informationstechnik und unter Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen;“.

g) Satz 2 Nummer 17 wird wie folgt gefasst:

„17. Aufgaben nach den §§ 8a bis 8c und 8f als zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen, digitaler Dienste und der Unternehmen im besonderen öffentlichen Interesse;“.

h) In Satz 2 Nummer 18 wird der Punkt am Ende durch ein Semikolon ersetzt.

i) Dem Satz 2 werden die folgenden Nummern 19 und 20 angefügt:

„19. Empfehlungen für Identifizierungs- und Authentisierungsverfahren und Bewertung dieser Verfahren im Hinblick auf die Informationssicherheit;

20. Beschreibung und Veröffentlichung eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte unter Berücksichtigung bestehender Normen und Standards sowie Einbeziehung der betroffenen Wirtschaftsverbände.“

4. Nach § 4 werden die folgenden §§ 4a und 4b eingefügt:

„§ 4a Kontrolle der Kommunikationstechnik des Bundes, Betretensrechte

(1) Das Bundesamt ist befugt, die Sicherheit der Kommunikationstechnik des Bundes und ihrer Komponenten, einschließlich technischer Infrastrukturen, die zum Betrieb der Kommunikationstechnik des Bundes erforderlich sind, zu kontrollieren. Es kann hierzu die Bereitstellung der zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1 und 14 erforderlichen Informationen, insbesondere zu technischen Details, zu Strategien, Planungen und Regelungen mit Bezug zur Kommunikationstechnik des Bundes einschließlich Aufbau- und Ablauforganisation verlangen sowie Unterlagen und Datenträger des Betreibers der jeweiligen Kommunikationstechnik des Bundes oder eines mit Betriebsleistungen beauftragten Dritten einsehen und die unentgeltliche Herausgabe von Kopien dieser Unterlagen und Dokumente, auch in elektronischer Form, verlangen, soweit nicht Geheimschutzinteressen oder überwiegende Sicherheitsinteressen des Betreibers im Sinne des Satzes 2 entgegenstehen.

(2) Dem Bundesamt ist in den Zeiten, zu denen die Räume normalerweise für die jeweilige geschäftliche oder betriebliche Nutzung zur Verfügung stehen, zu den Grundstücken und Betriebsräumen, einschließlich Datenverarbeitungsanlagen und -geräten, die für die Kommunikationstechnik des Bundes verwendet werden, Zugang zu gewähren, soweit dies zur Erfüllung der Zwecke nach Absatz 1 erforderlich ist.

(3) Bei Einrichtungen eines Dritten, bei dem eine Schnittstelle zur Kommunikationstechnik des Bundes besteht, kann das Bundesamt auf der Schnittstellenseite der Einrichtung nur mit Zustimmung des Dritten die Sicherheit der Schnittstelle kontrollieren. Es kann hierzu mit Zustimmung des Dritten die zur Aufgabenerfüllung erforderlichen Informationen, insbesondere zu technischen Details, zu Strategien, Planungen und Regelungen sowie Unterlagen und Datenträger des Betreibers einsehen und unentgeltlich Kopien, auch in elektronischer Form, anfertigen.

(4) Das Bundesamt teilt das Ergebnis seiner Kontrolle nach den Absätzen 1 bis 3 dem jeweiligen überprüften Betreiber sowie im Falle einer öffentlichen Stelle des Bundes der zuständigen Rechts- und Fachaufsicht mit. Mit der Mitteilung soll es Vorschläge zur Verbesserung der Informationssicherheit, insbesondere zur Beseitigung der festgestellten Mängel, verbinden.

(5) Ausgenommen von den Befugnissen nach den Absätzen 1 bis 3 sind Kontrollen der Auslandsinformations- und -kommunikationstechnik im Sinne des § 9 Absatz 2 des Gesetzes über den Auswärtigen Dienst, soweit sie ausschließlich im Ausland belegen ist oder für das Ausland oder für Anwender im Ausland betrieben wird. Die Bestimmungen für die Schnittstellen der Kommunikationstechnik des Bundes im Inland bleiben davon unberührt. Näheres zu Satz 1 regelt eine Verwaltungsvereinbarung zwischen dem Bundesministerium des Innern, für Bau und Heimat und dem Auswärtigen Amt.

(6) Die Befugnisse nach den Absätzen 1 bis 3 gelten im Geschäftsbereich des Bundesministeriums der Verteidigung nicht für die Kontrolle der Informations- und Kommunikationstechnik, die von den Streitkräften für ihre Zwecke oder dem Militärischen Abschirmdienst genutzt wird. Nicht ausgenommen ist die Informations- und Kommunikationstechnik von Dritten, insbesondere von IT-Dienstleistern, soweit sie nicht ausschließlich für die Zwecke der Streitkräfte betrieben wird. Die Bestimmungen für die Schnittstellen der Kommunikationstechnik des Bundes bleiben von den Sätzen 1 und 2 unberührt. Näheres regelt eine Verwaltungsvereinbarung zwischen dem Bundesministerium des Innern, für Bau und Heimat und dem Bundesministerium der Verteidigung.

§ 4b Allgemeine Meldestelle für die Sicherheit in der Informationstechnik

(1) Zur Wahrnehmung der Aufgaben nach § 3 nimmt das Bundesamt als zentrale Stelle für Meldungen von Dritten Informationen über Sicherheitsrisiken in der Informationstechnik entgegen und wertet diese Informationen aus.

(2) Das Bundesamt nimmt zur Wahrnehmung der Aufgaben nach Absatz 1 Informationen zu Sicherheitslücken, Schadprogrammen, erfolgten oder versuchten Angriffen auf die Sicherheit in der Informationstechnik und der dabei beobachteten Vorgehensweisen entgegen. Das Bundesamt richtet hierzu geeignete Meldemöglichkeiten ein. Die Meldungen können anonym erfolgen. Soweit die Meldung nicht anonym erfolgt, kann der Meldende mit der Meldung oder später verlangen, dass seine personenbezogenen Daten nur anonymisiert weitergegeben werden dürfen. Dies gilt nicht in den Fällen des § 5 Absatz 5 und 6 Satz 1. Eine Übermittlung der personenbezogenen Daten in den Fällen von § 5 Absatz 5 und 6 Satz 1 hat zu unterbleiben, wenn für das Bundesamt erkennbar ist, dass die schutzwürdigen Interessen des Mel-

denden das Allgemeininteresse an der Übermittlung überwiegen. Zu berücksichtigen ist dabei auch die Art und Weise, mittels derer der Meldende die Erkenntnisse gewonnen hat. Die Entscheidung nach Satz 6 muss dem oder der behördlichen Datenschutzbeauftragten des Bundesamtes sowie einem oder einer weiteren Bediensteten des Bundesamtes, der oder die die Befähigung zum Richteramt hat, zur vorherigen Prüfung vorgelegt werden.

(3) Das Bundesamt soll die gemäß Absatz 2 gemeldeten Informationen nutzen, um

1. Dritte über bekannt gewordene Sicherheitslücken, Schadprogramme, erfolgte oder versuchte Angriffe auf die Sicherheit in der Informationstechnik zu informieren, soweit dies zur Wahrung ihrer Sicherheitsinteressen erforderlich ist,

2. die Öffentlichkeit oder betroffene Kreise gemäß § 7 zu warnen und zu informieren,

3. Bundesbehörden gemäß § 4 Absatz 2 Nummer 2 über die sie betreffenden Informationen zu unterrichten,

4. Betreiber Kritischer Infrastrukturen und Unternehmen im öffentlichen Interesse gemäß § 8b Absatz 2 Nummer 4 Buchstabe a über die sie betreffenden Informationen zu unterrichten.

(4) Eine Weitergabe nach Absatz 3 Nummer 1, 2 oder 4 erfolgt nicht, soweit die gemäß Absatz 2 gemeldeten Informationen

1. Betriebs- und Geschäftsgeheimnisse von Dritten beinhalten und die Maßnahmen nach Absatz 3 nicht ohne Bekanntgabe dieser Betriebs- und Geschäftsgeheimnisse durchgeführt werden können oder

2. auf Grund von Vereinbarungen des Bundesamtes mit Dritten nicht übermittelt werden dürfen.

(5) Sonstige gesetzliche Meldepflichten, Regelungen zum Geheimschutz, gesetzliche Übermittlungshindernisse und Übermittlungsregelungen bleiben unberührt.“

5. § 5 wird wie folgt geändert:

a) Absatz 2 wird wie folgt gefasst:

„(2) Protokolldaten nach Absatz 1 Satz 1 Nummer 1 dürfen über den für die automatisierte Auswertung nach Absatz 1 Satz 1 Nummer 1 erforderlichen Zeitraum hinaus, längstens jedoch für 18 Monate, gespeichert werden, soweit tatsächliche Anhaltspunkte dafür bestehen, dass diese im Falle der Bestätigung eines Verdachts nach Absatz 3 Satz 2 zur Abwehr von Gefahren, die von dem gefundenen Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich sein können. Durch organisatorische und technische Maßnahmen ist sicherzustellen, dass eine Auswertung der nach diesem Absatz gespeicherten Daten nur automatisiert erfolgt und dass ein Zugriff auf Daten, die länger als drei Monate gespeichert sind, nur bei Vorliegen tatsächlicher Erkenntnisse über die Betroffenheit des Bundes mit einem Schadprogramm erfolgt. Die Daten sind zu pseudonymisieren, soweit dies automatisiert möglich ist. Eine nicht automatisierte Verarbeitung ist nur nach Maßgabe der nachfolgenden Absätze zulässig. Soweit hierzu die Wiederherstellung pseudonymisierter Protokolldaten erforderlich ist, muss diese durch die Präsidentin oder den Präsidenten des Bundesamtes oder die Vertretung im Amt angeordnet werden. Die Entscheidung ist zu dokumentieren.“

b) Nach Absatz 2 wird folgender Absatz 2a eingefügt:

„(2a) Protokolldaten dürfen vor ihrer Pseudonymisierung und Speicherung nach Absatz 2 zur Sicherstellung einer fehlerfreien automatisierten Auswertung manuell verarbeitet werden. Liegen Hinweise vor, dass die fehlerfreie automatisierte Auswertung wegen eines erheblichen Fehlers erschwert wird, darf der Personenbezug von Protokolldaten zur Sicherstellung der fehlerfreien automatisierten Auswertung wiederhergestellt werden, sofern dies im Einzelfall erforderlich ist. Absatz 2 Satz 3 bis 6 gilt entsprechend.“

6. Nach § 5 wird folgender § 5a eingefügt:

„§ 5a Verarbeitung behördeninterner Protokollierungsdaten

Das Bundesamt darf zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes und ihrer Komponenten, einschließlich technischer Infrastrukturen, die zum Betrieb der Kommunikationstechnik des Bundes erforderlich sind, Protokollierungsdaten, die durch den Betrieb von Kommunikationstechnik des Bundes anfallen, verarbeiten, soweit dies zum Erkennen, Eingrenzen oder Beseitigen von Störungen, Fehlern oder Sicherheitsvorfällen in der Kommunikationstechnik des Bundes oder von Angriffen auf die Informationstechnik des Bundes erforderlich ist und Geheimschutzinteressen oder überwiegende Sicherheitsinteressen der betroffenen Stellen nicht entgegenstehen. Die Bundesbehörden sind verpflichtet, das Bundesamt bei Maßnahmen nach Satz 1 zu unterstützen und hierbei den Zugang des Bundesamtes zu behördeninternen Protokollierungsdaten nach Satz 1 sicherzustellen. Hierzu dürfen sie dem Bundesamt die entsprechenden Protokollierungsdaten übermitteln. § 5 Absatz 1 Satz 5, Absatz 2 bis 4, 8 und 9 gilt entsprechend. § 4a Absatz 6 gilt für die Verpflichtung nach Satz 2 entsprechend.“

7. Der bisherige § 5a wird § 5b und wird wie folgt geändert:

a) In Absatz 1 Satz 1 werden nach den Wörtern „Kritischen Infrastruktur“ die Wörter „oder eines Unternehmens im besonderen öffentlichen Interesse“ eingefügt.

b) Dem Absatz 7 wird folgender Satz angefügt:

„Ein begründeter Einzelfall liegt in der Regel vor, wenn eine Stelle eines Landes betroffen ist.“

c) In Absatz 8 wird die Angabe „§ 5a“ durch die Angabe „§ 5b“ ersetzt.

8. Nach § 5b wird folgender § 5c eingefügt:

„§ 5c Bestandsdatenauskunft

(1) Das Bundesamt darf zur Erfüllung seiner gesetzlichen Aufgabe nach § 3 Absatz 1 Satz 1 Nummer 1, 2, 14, 17 oder 18 von demjenigen, der geschäftsmäßig Telekommunikationsdienste erbringt oder daran mitwirkt, über die nach den §§ 95 und 111 des Telekommunikationsgesetzes erhobenen Daten (§ 113 Absatz 1 Satz 1 des Telekommunikationsgesetzes) Auskunft verlangen. Die Auskunft nach Satz 1 darf nur verlangt werden zum Schutz der Versorgung der Bevölkerung in den Bereichen des § 2 Absatz 10 Satz 1 Nummer 1 oder der öffentlichen Sicherheit, um damit eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme

1. einer Kritischen Infrastruktur oder

2. eines Unternehmens von besonderem öffentlichem Interesse

abzuwenden, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisierten und zeitlich absehbaren Geschehen zulassen, das auf die informationstechnischen Systeme bestimmbarer Infrastrukturen oder Unternehmen abzielen wird, und die in die Auskunft aufzunehmenden Daten im Einzelfall erforderlich sind, um die Betroffenen nach Absatz 4 vor dieser Beeinträchtigung zu warnen, über diese zu informieren oder sie bei deren Beseitigung zu beraten oder zu unterstützen.

(2) Die Auskunft nach Absatz 1 darf auch anhand einer zu einem bestimmten Zeitpunkt zugewiesenen Internetprotokoll-Adresse verlangt werden (§ 113 Absatz 1 Satz 3, § 113c Absatz 1 Nummer 3 des Telekommunikationsgesetzes). Die rechtlichen und tatsächlichen Grundlagen des Auskunftsverlangens sind aktenkundig zu machen.

(3) Der auf Grund eines Auskunftsverlangens Verpflichtete hat die zur Auskunftserteilung erforderlichen Daten unverzüglich und vollständig zu übermitteln.

(4) Nach erfolgter Auskunft weist das Bundesamt den Betreiber der betroffenen Kritischen Infrastruktur oder das betroffene Unternehmen im besonderen öffentlichen Interesse auf die bei ihm drohenden Beeinträchtigungen hin. Nach Möglichkeit weist das Bundesamt den Betreiber der betroffenen Kritischen Infrastruktur oder das betroffene Unternehmen im besonderen öffentlichen Interesse auf technische Mittel hin, mittels derer die festgestellten Beeinträchtigungen durch den Betreiber der betroffenen Kritischen Infrastruktur oder das betroffene Unternehmen im besonderen öffentlichen Interesse selbst beseitigt werden können.

(5) Das Bundesamt kann personenbezogene Daten, die es im Rahmen dieser Vorschrift verarbeitet, entsprechend § 5 Absatz 5 und 6 übermitteln.

(6) In den Fällen des Absatzes 2 ist die betroffene Person über die Auskunft zu benachrichtigen. Im Falle der Weitergabe der Information nach § 5 Absatz 5 oder wenn Tatsachen die Annahme rechtfertigen, dass die Voraussetzungen einer Weitergabe nach § 5 Absatz 5 vorliegen, ergeht darüber keine Benachrichtigung an die betroffene Person, sofern und solange überwiegende schutzwürdige Belange Dritter entgegenstehen. Wird nach Satz 2 die Benachrichtigung zurückgestellt oder wird von ihr abgesehen, sind die Gründe aktenkundig zu machen.

(7) Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres über

1. die Gesamtzahl der Vorgänge, in denen Daten nach Absatz 1 oder Absatz 2 an das Bundesamt übermittelt wurden und

2. die Übermittlungen nach Absatz 5.

(8) Das Bundesamt hat den Verpflichteten für ihm erteilte Auskünfte eine Entschädigung zu gewähren. Der Umfang der Entschädigung bemisst sich nach § 23 und Anlage 3 des Justizvergütungs- und -entschädigungsgesetzes; die Vorschriften über die Verjährung in § 2 Absatz 1 und 4 des Justizvergütungs- und -entschädigungsgesetzes finden entsprechende Anwendung.“

9. § 7 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

aa) Satz 1 wird wie folgt geändert:

aaa) In dem Wortlaut vor Nummer 1 werden nach den Wörtern „§ 3 Absatz 1 Satz 2 Nummer 14“ die Wörter „und 14a“ eingefügt.

bbb) Nummer 1 wird wie folgt gefasst:

„1. Die folgenden Warnungen und Informationen an die Öffentlichkeit oder an die betroffenen Kreise richten:

a) Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten,

b) Warnungen vor Schadprogrammen,

c) Warnungen bei einem Verlust oder einem unerlaubten Zugriff auf Daten und

d) Informationen über sicherheitsrelevante IT-Eigenschaften von Produkten.“

bb) Die Sätze 3 und 4 werden aufgehoben.

b) Nach Absatz 1 wird folgender Absatz 1a eingefügt:

„(1a) Die Hersteller betroffener Produkte sind rechtzeitig vor Veröffentlichung der Warnungen zu informieren. Diese Informationspflicht besteht nicht,

1. wenn hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks gefährdet wird oder

2. 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 Weiterverbreitung 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 für die Auswahl des zu warnenden Personenkreises nach Satz 3 sind insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere Zuverlässigkeit des Empfängers.“

c) Absatz 2 Satz 1 wird wie folgt gefasst:

„Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 und 14a kann das Bundesamt die Öffentlichkeit unter Nennung der Bezeichnung und des Herstellers des betroffenen Produkts und Dienstes vor Sicherheitslücken in informationstechnischen Produkten und Diensten und vor Schadprogrammen warnen, wenn hinreichende Anhaltspunkte dafür vorliegen, dass Gefahren für die Sicherheit in der Informationstechnik hiervon ausgehen, oder Sicherheitsmaßnahmen sowie den Einsatz bestimmter informationstechnischer Produkte und Dienste empfehlen.“

10. § 7a wird wie folgt gefasst:

„§ 7a Untersuchung der Sicherheit in der Informationstechnik

(1) Das Bundesamt kann zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14, 14a, 17 oder 18 auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen. Es kann sich hierbei der Unterstützung Dritter bedienen, soweit berechtigte Interessen des Herstellers der betroffenen Produkte und Systeme dem nicht entgegenstehen.

(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. In dem Auskunftsverlangen 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.

(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.

(4) Die Auskünfte und die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14, 14a, 17 und 18 genutzt werden. Das Bundesamt darf seine Erkenntnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung der Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14, 14a, 17 und 18 erforderlich ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben.

(5) 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 darlegen, inwieweit der Hersteller seiner Auskunftspflicht nicht nachgekommen ist. Zuvor ist dem Hersteller mit angemessener Frist Gelegenheit zur Stellungnahme zu gewähren. § 7 Absatz 2 Satz 2 gilt entsprechend.“

11. Nach § 7a werden die folgenden §§ 7b bis 7d eingefügt:

„§ 7b Detektion von Sicherheitsrisiken für die Netz- und IT-Sicherheit und von Angriffsmethoden

(1) Das Bundesamt kann im Rahmen seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 2, 14 oder 17 zur Detektion von Sicherheitslücken und anderen Sicherheitsrisiken bei Einrichtungen des Bundes oder der in § 2 Absatz 10, 11 und 14 genannten Unternehmen Maßnahmen an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen (Portscans) durchführen, wenn Tatsachen die Annahme rechtfertigen, dass diese ungeschützt im Sinne des Absatzes 2 sein können und dadurch in ihrer Sicherheit oder Funktionsfähigkeit gefährdet sein können. Die Maßnahmen müssen sich auf einen vorher bestimmten Bereich von Internet-Protokolladressen, die regelmäßig den informationstechnischen Systemen

1. des Bundes oder

2. Kritischer Infrastrukturen, digitaler Dienste und der Unternehmen im besonderen öffentlichen Interessezugeordnet sind (Weiße Liste), beschränken. Die Weiße Liste ist stetig durch geeignete Überprüfungen anzupassen, um Änderungen bei der Zuordnung von Internetprotokoll-Adressen zu den in den Nummern 1 und 2 bezeichneten Stellen zu berücksichtigen. Erlangt das Bundesamt dabei Informationen, die durch Artikel 10 des Grundgesetzes geschützt sind, darf es diese nur zum Zwecke der Übermittlung nach § 5 Absatz 5 und 6 verarbeiten. Sofern die Voraussetzungen des § 5 Absatz 5 und 6 nicht vorliegen, sind Informationen, die nach Artikel 10 des Grundgesetzes geschützt sind, unverzüglich zu löschen. Maßnahmen nach Satz 1 dürfen nur durch eine Bedienstete oder einen Bediensteten des Bundesamtes mit der Befähigung zum Richteramt angeordnet werden.

(2) Ein informationstechnisches System ist ungeschützt im Sinne des Absatzes 1, wenn in diesem öffentlich bekannte Sicherheitslücken bestehen oder wenn auf Grund sonstiger offensichtlich unzureichender Sicherheitsvorkehrungen unbefugt von Dritten auf das System zugegriffen werden kann.

(3) Wird durch Maßnahmen gemäß Absatz 1 eine Sicherheitslücke oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt, sind die für das informationstechnische System Verantwortlichen unverzüglich darüber zu informieren. Das Bundesamt soll dabei auf bestehende Abhilfemöglichkeiten hinweisen. Sind dem Bundesamt die Verantwortlichen nicht bekannt oder ist ihre Identifikation nur mit unverhältnismäßigem Aufwand oder über eine Bestandsdatenabfrage nach § 5c möglich, ist hilfsweise der betreibende Dienstleister des jeweiligen Netzes oder Systems unverzüglich zu benachrichtigen, wenn überwiegende Sicherheitsinteressen nicht entgegenstehen. Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Anzahl der gemäß Absatz 1 ergriffenen Maßnahmen. Das Bundesamt legt die Weiße Liste nach Absatz 1 Satz 3 der Bundesbeauftragten oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit vierteljährlich zur Kontrolle vor.

(4) Das Bundesamt darf zur Erfüllung seiner Aufgaben Systeme und Verfahren einsetzen, welche einem Angreifer einen erfolgreichen Angriff vortäuschen, um den Einsatz von Schadprogrammen oder andere Angriffsmethoden zu erheben und auszuwerten. Das Bundesamt darf dabei die zur Auswertung der Funktionsweise der Schadprogramme und Angriffsmethoden erforderlichen Daten verarbeiten.

§ 7c Anordnungen des Bundesamtes gegenüber Diensteanbietern

(1) Zur Abwehr konkreter erheblicher Gefahren für die in Absatz 2 genannten Schutzziele kann das Bundesamt gegenüber einem Anbieter von Telekommunikationsdiensten im Sinne des Telekommunikationsgesetzes (Diensteanbieter) mit mehr als 100.000 Kunden anordnen, dass er

1. die in § 109a Absatz 5 oder 6 des Telekommunikationsgesetzes bezeichneten Maßnahmen trifft oder

2. technische Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene informationstechnische Systeme verteilt,

sofern und soweit der Diensteanbieter dazu technisch in der Lage ist und es ihm wirtschaftlich zumutbar ist. Vor der Anordnung der Maßnahmen nach Satz 1 Nummer 1 oder 2 durch das Bundesamt ist Einvernehmen mit der Bundesnetzagentur herzustellen. Vor der Anord-

nung der Maßnahme nach Satz 1 Nummer 2 durch das Bundesamt ist zusätzlich Einvernehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit herzustellen. Die Daten, auf die mit der Maßnahme nach Satz 1 Nummer 2 zugegriffen werden soll, sind in der Anordnung zu benennen. § 5 Absatz 7 Satz 2 bis 8 gilt entsprechend. Widerspruch und Anfechtungsklage gegen die Anordnungen nach Satz 1 haben keine aufschiebende Wirkung.

(2) Schutzziele gemäß Absatz 1 Satz 1 sind die Verfügbarkeit, Unversehrtheit oder Vertraulichkeit

1. der Kommunikationstechnik des Bundes, eines Betreibers Kritischer Infrastrukturen, eines Unternehmens im besonderen öffentlichen Interesse oder eines Anbieters digitaler Dienste,

2. von Informations- oder Kommunikationsdiensten oder

3. von Informationen, sofern deren Verfügbarkeit, Unversehrtheit oder Vertraulichkeit durch unerlaubte Zugriffe auf eine erhebliche Anzahl von telekommunikations- oder informationstechnischen Systemen von Nutzern eingeschränkt wird.

(3) Ordnet das Bundesamt eine Maßnahme nach Absatz 1 Satz 1 Nummer 1 an, so kann es gegenüber dem Diensteanbieter auch anordnen, den Datenverkehr an eine vom Bundesamt benannte Anschlusskennung umzuleiten.

(4) Das Bundesamt darf Daten, die von einem Diensteanbieter nach Absatz 1 Satz 1 Nummer 1 und Absatz 3 umgeleitet wurden, verarbeiten, um Informationen über Schadprogramme oder andere Sicherheitsrisiken in informationstechnischen Systemen zu erlangen. Die übermittelten Daten dürfen durch das Bundesamt so lange gespeichert werden, wie dies für die Erfüllung des in Satz 1 genannten Zwecks erforderlich ist, längstens jedoch für drei Monate. § 5 Absatz 7 Satz 2 bis 8 gilt entsprechend. Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Gesamtzahl der angeordneten Datenumleitungen.

§ 7d Anordnungen des Bundesamtes gegenüber Anbietern von Telemediendiensten

Das Bundesamt kann in begründeten Einzelfällen zur Abwehr konkreter, erheblicher Gefahren für informationstechnische Systeme einer Vielzahl von Nutzern, die von Telemedienangeboten von Diensteanbietern im Sinne des § 2 Satz 1 Nummer 1 des Telemediengesetzes ausgehen, die durch ungenügende technische und organisatorische Vorkehrungen im Sinne des § 13 Absatz 7 des Telemediengesetzes unzureichend gesichert sind und dadurch keinen hinreichenden Schutz bieten vor

1. unerlaubten Zugriffen auf die für diese Telemedienangebote genutzten technischen Einrichtungen oder

2. Störungen, auch soweit sie durch äußere Angriffe bedingt sind,

gegenüber dem jeweiligen Diensteanbieter im Sinne des § 2 Satz 1 Nummer 1 des Telemediengesetzes anordnen, dass dieser die jeweils zur Herstellung des ordnungsgemäßen Zustands seiner Telemedienangebote erforderlichen technischen und organisatorischen Maßnahmen ergreift, um den ordnungsgemäßen Zustand seiner Telemedienangebote herzustellen. Die Zuständigkeit der Aufsichtsbehörden der Länder bleibt im Übrigen unberührt.“

12. § 8 wird wie folgt geändert:

a) Absatz 1 wird durch die folgenden Absätze 1 und 1a ersetzt:

„(1) Das Bundesamt legt im Benehmen mit den Ressorts Mindeststandards für die Sicherheit der Informationstechnik des Bundes fest, die von

1. Stellen des Bundes,

2. Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts sowie ihren Vereinigungen ungeachtet ihrer Rechtsform auf Bundesebene, soweit von der jeweils zuständigen obersten Bundesbehörde angeordnet, sowie

3. öffentlichen Unternehmen, die mehrheitlich im 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 und sind zu dokumentieren und zu begründen. Das Bundesamt berät die in Satz 1 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 Satz 1 empfehlenden Charakter. Für die Verpflichtung nach Satz 1 gilt die Ausnahme nach § 4a Absatz 6 entsprechend.

(1a) 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 zuständiger Aufsichtsbehörde sowie der Konferenz der IT-Beauftragten der Ressorts mit. Für andere öffentlich-rechtlich oder privatrechtlich organisierte Stellen dürfen nur 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.“

b) In Absatz 3 Satz 4 wird das Wort „Bundesbehörden“ durch die Wörter „Stellen des Bundes oder von ihnen beauftragte Dritte“ ersetzt.

c) Folgender Absatz 4 wird angefügt:

„(4) Zur Gewährleistung der Sicherheit in der Informationstechnik bei der Planung und Umsetzung von wesentlichen Digitalisierungsvorhaben des Bundes soll die jeweils verantwortliche Stelle das Bundesamt frühzeitig beteiligen und dem Bundesamt Gelegenheit zur Stellungnahme geben.“

13. § 8a wird wie folgt geändert:

a) In Absatz 1 Satz 1 werden die Wörter „spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1“ durch die Wörter „spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten,“ ersetzt.

b) Nach Absatz 1 wird folgender Absatz 1a eingefügt:

„(1a) Die Verpflichtung nach Absatz 1 Satz 1, angemessene organisatorische und technische Vorkehrungen zu treffen, umfasst ab dem 1. Mai 2023 auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen. Absatz 1 Satz 2 und 3 gilt entsprechend."

c) In Absatz 2 Satz 1 und 2 wird jeweils die Angabe „Absatz 1" durch die Wörter „den Absätzen 1 und 1a" ersetzt.

d) In Absatz 2 Satz 3 Nummer 2 werden die Wörter „oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde" gestrichen.

e) Absatz 3 Satz 1 wird wie folgt gefasst:

„Betreiber Kritischer Infrastrukturen haben die Erfüllung der Anforderungen nach den Absätzen 1 und 1a spätestens zwei Jahre nach dem in Absatz 1 genannten Zeitpunkt und anschließend alle zwei Jahre dem Bundesamt nachzuweisen."

f) In Absatz 4 Satz 1 und 3 wird jeweils die Angabe „Absatz 1" durch die Wörter „den Absätzen 1 und 1a" ersetzt.

14. § 8b wird wie folgt geändert:

a) Absatz 2 wird wie folgt geändert:

aa) In Nummer 3 werden nach den Wörtern „Kritischen Infrastrukturen" die Wörter „oder der Unternehmen im besonderen öffentlichen Interesse" eingefügt.

bb) Nummer 4 Buchstabe a wird wie folgt gefasst:

„a) die Betreiber Kritischer Infrastrukturen und die Unternehmen im besonderen öffentlichen Interesse über sie betreffende Informationen nach den Nummern 1 bis 3,".

b) Absatz 3 wird wie folgt gefasst:

„(3) Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Betreiber einer Kritischen Infrastruktur nach der Rechtsverordnung nach § 10 Absatz 1 gelten, die von ihnen betriebenen Kritischen Infrastrukturen beim Bundesamt zu registrieren und eine Kontaktstelle zu benennen. Die Registrierung eines Betreibers einer Kritischen Infrastruktur kann das Bundesamt auch selbst vornehmen, wenn der Betreiber seine Pflicht zur Registrierung nicht erfüllt. Nimmt das Bundesamt eine solche Registrierung selbst vor, informiert es die zuständige Aufsichtsbehörde des Bundes darüber. Die Betreiber haben sicherzustellen, dass sie über die benannte oder durch das Bundesamt festgelegte Kontaktstelle jederzeit erreichbar sind. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Kontaktstelle."

c) Nach Absatz 3 wird folgender Absatz 3a eingefügt:

„(3a) Rechtfertigen Tatsachen die Annahme, dass ein Betreiber seine 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, soweit nicht Geheimschutzinteressen oder überwiegende Sicherheitsinteressen entgegenstehen."

d) Nach Absatz 4 wird folgender Absatz 4a eingefügt:

„(4a) Während einer erheblichen Störung gemäß Absatz 4 Satz 1 Nummer 2, § 8f Absatz 7 Satz 1 Nummer 2 oder Absatz 8 Satz 1 Nummer 2 kann das Bundesamt im Einvernehmen mit der jeweils zuständigen Aufsichtsbehörde des Bundes von den betroffenen Betreibern Kritischer Infrastrukturen oder den Unternehmen im besonderen öffentlichen Interesse die Herausgabe der zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten verlangen. Betreiber Kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse sind befugt, dem Bundesamt auf Verlangen die zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten zu übermitteln, soweit dies zur Bewältigung einer erheblichen Störung gemäß Absatz 4 Satz 1 Nummer 2, § 8f Absatz 7 Satz 1 Nummer 2 oder Absatz 8 Satz 1 Nummer 2 erforderlich ist."

e) Absatz 6 wird wie folgt geändert:

aa) In Satz 1 werden nach den Wörtern „Störung nach Absatz 4" ein Komma und die Wörter „oder § 8f Absatz 7 oder 8" eingefügt.

bb) In Satz 2 wird die Angabe „§ 8c Absatz 3" durch die Angabe „§ 8d Absatz 3" ersetzt.

15. In § 8c Absatz 3 Satz 4 wird die Angabe „Absatz 3" durch die Angabe „Absatz 4" ersetzt.

16. § 8d wird wie folgt geändert:

a) In Absatz 1 Satz 1 wird die Angabe „2003/361/EC" durch die Angabe „2003/361/EG" ersetzt.

b) Nach Absatz 1 wird folgender Absatz 1a eingefügt:

„(1a) § 8f ist nicht anzuwenden auf Kleinstunternehmen und kleine Unternehmen im Sinne der Empfehlung 2003/361/EG. Artikel 3 Absatz 4 des Anhangs zu der Empfehlung ist nicht anzuwenden."

c) In Absatz 3 in dem einleitenden Satzteil wird die Angabe „§ 8b Absatz 4" durch die Wörter „§ 8b Absatz 4 und 4a" ersetzt.

17. § 8e wird wie folgt geändert:

a) Die Absätze 1 und 2 werden wie folgt gefasst:

„(1) Das Bundesamt kann Dritten auf Antrag Auskunft zu den im Rahmen von § 8a Absatz 2 und 3, § 8c Absatz 4 und § 8f erhaltenen Informationen sowie zu den Meldungen nach § 8b Absatz 4, 4a und 4b sowie § 8c Absatz 4 nur erteilen, wenn

1. schutzwürdige Interessen des betroffenen Betreibers einer Kritischen Infrastruktur, des Unternehmens im besonderen öffentlichen Interesse oder des Anbieters digitaler Dienste dem nicht entgegenstehen und

2. durch die Auskunft keine Beeinträchtigung von Sicherheitsinteressen eintreten kann.

Zugang zu personenbezogenen Daten wird nicht gewährt.

(2) Zugang zu den Akten des Bundesamtes in Angelegenheiten nach den §§ 8a bis 8c und 8f wird bei Vorliegen der Voraussetzungen des § 29 des Verwaltungsverfahrensgesetzes nur gewährt, wenn

1. schutzwürdige Interessen des betroffenen Betreibers einer Kritischen Infrastruktur, des Unternehmens im besonderen öffentlichen Interesse oder des Anbieters digitaler Dienste dem nicht entgegenstehen und

2. durch den Zugang zu den Akten keine Beeinträchtigung von Sicherheitsinteressen eintreten kann.“

b) Folgender Absatz 4 wird angefügt:

„(4) Informationsansprüche nach dem Umweltinformationsgesetz bleiben von dieser Vorschrift unberührt.“

18. Nach § 8e wird folgender § 8f eingefügt:

„§ 8f Sicherheit in der Informationstechnik bei Unternehmen im besonderen öffentlichen Interesse

(1) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 und 2 sind verpflichtet, spätestens bis zum ersten Werktag, der darauf folgt, dass diese erstmalig oder erneut als Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 oder 2 gelten, und danach mindestens alle zwei Jahre eine Selbsterklärung zur IT-Sicherheit beim Bundesamt vorzulegen, aus der hervorgeht,

1. welche Zertifizierungen im Bereich der IT-Sicherheit in den letzten zwei Jahren durchgeführt, welche Prüfgrundlage und welcher Geltungsbereich hierfür festgelegt wurden,

2. welche sonstigen Sicherheitsaudits oder Prüfungen im Bereich der IT-Sicherheit in den letzten zwei Jahren durchgeführt, welche Prüfgrundlage und welcher Geltungsbereich hierfür festgelegt wurden oder

3. wie sichergestellt wird, dass die für das Unternehmen besonders schützenswerten informationstechnischen Systeme, Komponenten und Prozesse angemessen geschützt werden, und ob dabei der Stand der Technik eingehalten wird.

(2) Das Bundesamt kann für die Selbsterklärung nach Absatz 1 zu verwendende Formulare einführen.

(3) Das Bundesamt kann auf Grundlage der Selbsterklärung nach Absatz 1 Hinweise zu angemessenen organisatorischen und technischen Vorkehrungen nach Absatz 1 Nummer 3 zur Einhaltung des Stands der Technik geben.

(4) Für Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 gilt die Pflicht nach Absatz 1 nicht vor dem 1. Mai 2023. Für Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 2 gilt diese Pflicht frühestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 5.

(5) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 und 2 sind verpflichtet, sich gleichzeitig mit der Vorlage der ersten Selbsterklärung zur IT-Sicherheit nach Absatz 1 beim Bundesamt zu registrieren und eine zu den üblichen Geschäftszeiten erreichbare Stelle zu benennen. Die Übermittlung von Informationen durch das Bundesamt nach § 8b Absatz 2 Nummer 4 erfolgt an diese Stelle.

(6) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 3 können eine freiwillige Registrierung beim Bundesamt und die Benennung einer zu den üblichen Geschäftszeiten erreichbaren Stelle vornehmen. Die Übermittlung von Informationen durch das Bundesamt nach § 8b Absatz 2 Nummer 4 erfolgt an diese Stelle.

(7) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 1 und 2 haben ab dem Zeitpunkt, zu dem eine Pflicht zur Vorlage der Selbsterklärung zur IT-Sicherheit nach Absatz 1 besteht, die folgenden Störungen unverzüglich über die nach Absatz 5 benannte Stelle an das Bundesamt zu melden:

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,

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.

Die Meldung muss Angaben zu der Störung, zu den technischen Rahmenbedingungen, insbesondere zu der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und der Art der betroffenen Einrichtung oder Anlage enthalten.

(8) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 3 haben spätestens ab dem 1. November 2021 die folgenden Störungen unverzüglich an das Bundesamt zu melden:

1. Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Störfall nach der Störfall-Verordnung in der jeweils geltenden Fassung geführt haben,

2. erhebliche Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Störfall nach der Störfall-Verordnung in der jeweils geltenden Fassung führen können.

Die Meldung muss Angaben zu der Störung, zu den technischen Rahmenbedingungen, insbesondere zu der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und der Art der betroffenen Einrichtung oder Anlage enthalten.

(9) Rechtfertigen Tatsachen die Annahme, dass ein Unternehmen ein Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 2 ist, aber seine Pflichten nach Absatz 5 nicht erfüllt, so kann das Bundesamt verlangen:

1. eine rechnerische Darlegung, wie hoch die vom Unternehmen erbrachte inländische Wertschöpfung nach der in der Rechtsverordnung nach § 10 Absatz 5 festgelegten Berechnungsmethode ist, oder

2. eine Bestätigung einer anerkannten Wirtschaftsprüfungsgesellschaft, dass das Unternehmen nach der in der Rechtsverordnung nach § 10 Absatz 5 festgelegten Berechnungsmethode kein Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Satz 1 Nummer 2 ist.“

19. § 9 Absatz 4 wird durch die folgenden Absätze 4 und 4a ersetzt:

„(4) Das Sicherheitszertifikat wird erteilt, wenn

1. informationstechnische Systeme, Komponenten, Produkte oder Schutzprofile den vom Bundesamt festgelegten Kriterien entsprechen und

2. das Bundesministerium des Innern, für Bau und Heimat die Erteilung des Zertifikats nicht nach Absatz 4a untersagt hat.

Vor Erteilung des Sicherheitszertifikats legt das Bundesamt den Vorgang dem Bundesministerium des Innern, für Bau und Heimat zur Prüfung nach Absatz 4a vor.

(4a) Das Bundesministerium des Innern, für Bau und Heimat kann eine Zertifikatserteilung nach Absatz 4 im Einzelfall untersagen, wenn überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung entgegenstehen.“

20. Nach § 9 werden die folgenden §§ 9a bis 9c eingefügt:

„§ 9a Nationale Behörde für die Cybersicherheitszertifizierung

(1) Das Bundesamt ist die nationale Behörde für die Cybersicherheitszertifizierung im Sinne des Artikels 58 Absatz 1 der Verordnung (EU) 2019/881.

(2) Das Bundesamt kann auf Antrag Konformitätsbewertungsstellen, die im Anwendungsbereich der Verordnung (EU) 2019/881 sowie des § 9 dieses Gesetzes tätig werden, eine Befugnis erteilen, als solche tätig zu werden, wenn die Voraussetzungen des maßgeblichen europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 der Verordnung (EU) 2019/881 oder des § 9 dieses Gesetzes erfüllt sind. Ohne eine Befugniserteilung durch das Bundesamt dürfen Konformitätsbewertungsstellen im Anwendungsbereich der Verordnung (EU) 2019/881 nicht tätig werden.

(3) Soweit dies zur Erfüllung seiner Aufgaben nach Artikel 58 Absatz 7 der Verordnung (EU) 2019/881 und nach § 9 dieses Gesetzes erforderlich ist, kann das Bundesamt von Konformitätsbewertungsstellen, denen eine Befugnis nach Absatz 2 erteilt wurde, von Inhabern europäischer Cybersicherheitszertifikate und von Ausstellern von EU-Konformitätserklärungen im Sinne von Artikel 56 Absatz 8 der Verordnung (EU) 2019/881 die erforderlichen Auskünfte und sonstige Unterstützung, insbesondere die Vorlage von Unterlagen oder Mustern, verlangen. § 3 Absatz 1 Satz 1 und 3 des Akkreditierungsstellengesetzes gilt entsprechend.

(4) Das Bundesamt kann Untersuchungen in Form von Auditierungen nach Artikel 58 Absatz 8 Buchstabe b der Verordnung (EU) 2019/881 bei Konformitätsbewertungsstellen, denen eine Befugnis nach Absatz 2 erteilt wurde, bei Inhabern europäischer Cybersicherheitszerti-

fikate und bei Ausstellern von EU-Konformitätserklärungen im Sinne von Artikel 56 Absatz 8 der Verordnung (EU) 2019/881 durchführen, um die Einhaltung der Bestimmungen des Titels III der Verordnung (EU) 2019/881 zu überprüfen. § 3 Absatz 1 Satz 1 bis 3 des Akkreditierungsstellengesetzes gilt entsprechend.

(5) Das Bundesamt ist befugt, Betriebsstätten, Geschäfts- und Betriebsräume von Konformitätsbewertungsstellen, denen eine Befugnis nach Absatz 2 erteilt wurde, und von Inhabern europäischer Cybersicherheitszertifikate im Sinne von Artikel 56 Absatz 8 der Verordnung (EU) 2019/881 in den Zeiten, zu denen die Räume normalerweise für die jeweilige geschäftliche oder betriebliche Nutzung zur Verfügung stehen, zu betreten, zu besichtigen und zu prüfen, soweit dies zur Erfüllung seiner Aufgaben nach Artikel 58 Absatz 7 der Verordnung (EU) 2019/881 sowie nach § 9 dieses Gesetzes erforderlich ist. § 3 Absatz 1 Satz 1 bis 3 des Akkreditierungsstellengesetzes gilt entsprechend.

(6) Das Bundesamt kann von ihm ausgestellte Cybersicherheitszertifikate oder durch eine Konformitätsbewertungsstelle, der eine Befugnis nach Absatz 2 erteilt wurde, nach Artikel 56 Absatz 6 der Verordnung (EU) 2019/881 ausgestellte Cybersicherheitszertifikate widerrufen oder EU-Konformitätserklärungen im Sinne der Verordnung (EU) 2019/881 für ungültig erklären,

1. sofern diese Zertifikate oder EU-Konformitätserklärungen die Anforderungen nach der Verordnung (EU) 2019/881 oder eines europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 der Verordnung (EU) 2019/881 nicht erfüllen oder

2. wenn das Bundesamt die Erfüllung nach Nummer 1 nicht feststellen kann, weil der Inhaber des europäischen Cybersicherheitszertifikats oder der Aussteller der EU-Konformitätserklärung seinen Mitwirkungspflichten nach Absatz 3 nicht nachgekommen ist oder weil dieser das Bundesamt bei der Wahrnehmung seiner Befugnisse nach Absatz 4 oder im Falle eines Inhabers eines europäischen Cybersicherheitszertifikats auch nach Absatz 5 behindert hat.

(7) Das Bundesamt kann von ihm erteilte Befugnisse nach Absatz 2 widerrufen,

1. sofern die Voraussetzungen des maßgeblichen europäischen Schemas für die Cybersicherheitszertifizierung nach Artikel 54 Verordnung (EU) 2019/881 oder des § 9 dieses Gesetzes nicht erfüllt sind oder

2. wenn das Bundesamt die Erfüllung dieser Voraussetzungen nicht feststellen kann, weil die Konformitätsbewertungsstelle ihren Mitwirkungspflichten nach Absatz 3 nicht nachgekommen ist oder weil diese das Bundesamt bei der Wahrnehmung seiner Befugnisse nach den Absätzen 4 und 5 behindert hat.

§ 9b Untersagung des Einsatzes kritischer Komponenten

(1) Der Betreiber einer Kritischen Infrastruktur hat den geplanten erstmaligen Einsatz einer kritischen Komponente gemäß § 2 Absatz 13 dem Bundesministerium des Innern, für Bau und Heimat vor ihrem Einsatz anzuzeigen. In der Anzeige sind die kritische Komponente und die geplante Art ihres Einsatzes anzugeben. Satz 1 gilt für einen Betreiber einer Kritischen Infrastruktur nicht, wenn dieser den Einsatz einer anderen kritischen Komponente desselben Typs für dieselbe Art des Einsatzes bereits nach Satz 1 angezeigt hat und ihm dieser nicht untersagt wurde.

(2) Das Bundesministerium des Innern, für Bau und Heimat kann den geplanten erstmaligen Einsatz einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur im Benehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt bis zum Ablauf von zwei Monaten nach Eingang der Anzeige nach Absatz 1 untersagen oder Anordnungen erlassen, wenn der Einsatz die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt. Bei der Prüfung einer voraussichtlichen Beeinträchtigung der öffentlichen Ordnung oder Sicherheit kann insbesondere berücksichtigt werden, ob

1. der Hersteller unmittelbar oder mittelbar von der Regierung, einschließlich sonstiger staatlicher Stellen oder Streitkräfte, eines Drittstaates kontrolliert wird,

2. der Hersteller bereits an Aktivitäten beteiligt war oder ist, die nachteilige Auswirkungen auf die öffentliche Ordnung oder Sicherheit der Bundesrepublik Deutschland oder eines anderen Mitgliedstaates der Europäischen Union, der Europäischen Freihandelsassoziation oder des Nordatlantikvertrages oder auf deren Einrichtungen hatten, oder

3. der Einsatz der kritischen Komponente im Einklang mit den sicherheitspolitischen Zielen der Bundesrepublik Deutschland, der Europäischen Union oder des Nordatlantikvertrages steht.

Vor Ablauf der Frist von zwei Monaten nach Anzeige nach Absatz 1 ist der Einsatz nicht gestattet. Das Bundesministerium des Innern, für Bau und Heimat kann die Frist gegenüber dem Betreiber um weitere zwei Monate verlängern, wenn die Prüfung besondere Schwierigkeiten tatsächlicher oder rechtlicher Art aufweist.

(3) Kritische Komponenten gemäß § 2 Absatz 13 dürfen nur eingesetzt werden, wenn der Hersteller eine Erklärung über seine Vertrauenswürdigkeit (Garantieerklärung) gegenüber dem Betreiber der Kritischen Infrastruktur abgeben hat. Die Garantieerklärung ist der Anzeige nach Absatz 1 beizufügen. Aus der Garantieerklärung muss hervorgehen, wie der Hersteller sicherstellt, dass die kritische Komponente nicht über technische Eigenschaften verfügt, die spezifisch geeignet sind, missbräuchlich, insbesondere zum Zwecke von Sabotage, Spionage oder Terrorismus auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können. Das Bundesministerium des Innern, für Bau und Heimat legt die Einzelheiten der Mindestanforderungen an die Garantieerklärung im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt durch Allgemeinverfügung fest, die im Bundesanzeiger bekannt zu machen ist. Die Einzelheiten der Mindestanforderungen an die Garantieerklärung müssen aus den Schutzzielen der Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur folgen und die Vermeidung von Gefahren für die öffentliche Sicherheit und Ordnung, insbesondere im Sinne von Absatz 2 Satz 2, adressieren, die aus der Sphäre des Herstellers der kritischen Komponente, insbesondere dessen Organisationsstruktur, stammen. Die Sätze 1 und 2 gelten erst ab der Bekanntmachung der Allgemeinverfügung nach Satz 5 und nicht für bereits vor diesem Zeitpunkt eingesetzte kritische Komponenten. Soweit Änderungen der Allgemeinverfügung erfolgen, sind diese für bereits nach diesem Absatz abgegebene Garantieerklärungen unbeachtlich.

(4) Das Bundesministerium des Innern, für Bau und Heimat kann den weiteren Einsatz einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen oder Anordnungen erlassen, wenn der weitere Einsatz die öffentliche

Ordnung oder Sicherheit der Bundesrepublik Deutschland voraussichtlich beeinträchtigt, insbesondere, wenn der Hersteller der kritischen Komponente nicht vertrauenswürdig ist. Absatz 2 Satz 2 gilt entsprechend.

(5) Ein Hersteller einer kritischen Komponente kann insbesondere dann nicht vertrauenswürdig sein, wenn hinreichende Anhaltspunkte dafür bestehen, dass

1. er gegen die in der Garantieerklärung eingegangen Verpflichtungen verstoßen hat,

2. in der Garantieerklärung angegebene Tatsachenbehauptungen unwahr sind,

3. er Sicherheitsüberprüfungen und Penetrationsanalysen an seinem Produkt und in der Produktionsumgebung nicht im erforderlichen Umfang in angemessener Weise unterstützt,

4. Schwachstellen oder Manipulationen nicht unverzüglich, nachdem er davon Kenntnis erlangt, beseitigt und dem Betreiber der Kritischen Infrastruktur meldet,

5. die kritische Komponente auf Grund von Mängeln ein erhöhtes Gefährdungspotenzial aufweist oder aufgewiesen hat, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können oder

6. die kritische Komponente über technische Eigenschaften verfügt oder verfügt hat, die spezifisch geeignet sind oder waren, missbräuchlich auf die Sicherheit, Vertraulichkeit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können.

(6) Wurde nach Absatz 4 der weitere Einsatz einer kritischen Komponente untersagt, kann das Bundesministerium des Innern, für Bau und Heimat im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt

1. den geplanten Einsatz weiterer kritischer Komponenten desselben Typs und desselben Herstellers untersagen und

2. den weiteren Einsatz kritischer Komponenten desselben Typs und desselben Herstellers unter Einräumung einer angemessenen Frist untersagen.

(7) Bei schwerwiegenden Fällen nicht vorliegender Vertrauenswürdigkeit nach Absatz 5 kann das Bundesministerium des Innern, für Bau und Heimat den Einsatz aller kritischen Komponenten des Herstellers im Einvernehmen mit den in § 10 Absatz 1 aufgeführten jeweils betroffenen Ressorts sowie dem Auswärtigen Amt untersagen.

§ 9c Freiwilliges IT-Sicherheitskennzeichen

(1) Das Bundesamt führt zur Information von Verbrauchern über die IT-Sicherheit von Produkten bestimmter vom Bundesamt festgelegter Produktkategorien ein einheitliches IT-Sicherheitskennzeichen ein. Das IT-Sicherheitskennzeichen trifft keine Aussage über die den Datenschutz betreffenden Eigenschaften eines Produktes.

(2) Das IT-Sicherheitskennzeichen besteht aus

1. einer Zusicherung des Herstellers oder Diensteanbieters, dass das Produkt für eine festgelegte Dauer bestimmte IT-Sicherheitsanforderungen erfüllt (Herstellererklärung), und

2. einer Information des Bundesamtes über sicherheitsrelevante IT-Eigenschaften des Produktes (Sicherheitsinformation).

(3) Die IT-Sicherheitsanforderungen, auf die sich die Herstellererklärung bezieht, ergeben sich aus einer Norm oder einem Standard oder aus einer branchenabgestimmten IT-Sicherheitsvorgabe, die die jeweilige Produktkategorie umfasst, sofern das Bundesamt in einem Verfahren, das durch Rechtsverordnung nach § 10 Absatz 3 geregelt wird, festgestellt hat, dass die Norm oder der Standard oder die branchenabgestimmte IT-Sicherheitsvorgabe geeignet ist, ausreichende IT-Sicherheitsanforderungen für die Produktkategorie abzubilden. Ein Anspruch auf diese Feststellung besteht nicht. Liegt keine Feststellung nach Satz 1 vor, ergeben sich die IT-Sicherheitsvorgaben aus einer vom Bundesamt veröffentlichten Technischen Richtlinie, die die jeweilige Produktkategorie umfasst, sofern das Bundesamt eine solche Richtlinie bereits veröffentlicht hat. Wird ein Produkt von mehr als einer oder einem bestehenden, als geeignet festgestellten Norm, Standard, branchenabgestimmten IT-Sicherheitsvorgabe oder Technischen Richtlinie umfasst, richten sich die Anforderungen nach der oder dem jeweils spezielleren bestehenden, als geeignet festgestellten Norm, Standard, branchenabgestimmten IT-Sicherheitsvorgabe oder Technischen Richtlinie.

(4) Das IT-Sicherheitskennzeichen darf nur dann für ein Produkt verwendet werden, wenn das Bundesamt das IT-Sicherheitskennzeichen für dieses Produkt freigegeben hat. Das Bundesamt prüft die Freigabe des IT-Sicherheitskennzeichens für ein Produkt auf Antrag des Herstellers oder Diensteanbieters. Dem Antrag sind die Herstellererklärung zu dem Produkt sowie alle Unterlagen beizufügen, die die Angaben in der Herstellererklärung belegen. Das Bundesamt bestätigt den Eingang des Antrags und prüft die Plausibilität der Herstellererklärung anhand der beigefügten Unterlagen. Die Plausibilitätsprüfung kann auch durch einen vom Bundesamt beauftragten qualifizierten Dritten erfolgen. Für die Antragsbearbeitung kann das Bundesamt eine Verwaltungsgebühr erheben.

(5) Das Bundesamt erteilt die Freigabe des IT-Sicherheitskennzeichens für das jeweilige Produkt, wenn

1. das Produkt zu einer der Produktkategorien gehört, die das Bundesamt durch im Bundesanzeiger veröffentlichte Allgemeinverfügung bekannt gegeben hat,

2. die Herstellererklärung plausibel und durch die beigefügten Unterlagen ausreichend belegt ist und

3. die gegebenenfalls erhobene Verwaltungsgebühr beglichen wurde.

Die Erteilung der Freigabe erfolgt schriftlich und innerhalb einer angemessenen Frist, die in der Rechtsverordnung nach § 10 Absatz 3 bestimmt wird. Den genauen Ablauf des Antragsverfahrens und die beizufügenden Unterlagen regelt die Rechtsverordnung nach § 10 Absatz 3.

(6) Hat das Bundesamt die Freigabe erteilt, ist das Etikett des IT-Sicherheitskennzeichens auf dem jeweiligen Produkt oder auf dessen Umverpackung anzubringen, sofern dies nach der Beschaffenheit des Produktes möglich ist. Das IT-Sicherheitskennzeichen kann auch elektronisch veröffentlicht werden. Wenn nach der Beschaffenheit des Produktes das Anbringen nicht möglich ist, muss die Veröffentlichung des IT-Sicherheitskennzeichens elektronisch erfolgen. Das Etikett des IT-Sicherheitskennzeichens verweist auf eine Internetseite des Bundesamtes, auf der die Herstellererklärung und die Sicherheitsinformationen abrufbar sind. Das genaue Verfahren und die Gestaltung des Verweises sind in der Rechtsverordnung nach § 10 Absatz 3 festzulegen.

(7) Nach Ablauf der festgelegten Dauer nach Absatz 3 Satz 5 oder 6 oder nach Rücknahmeerklärung des Herstellers oder Diensteanbieters gegenüber dem Bundesamt erlischt die Freigabe. Das Bundesamt nimmt einen Hinweis auf das Erlöschen der Freigabe in die Sicherheitsinformation auf.

(8) Das Bundesamt kann prüfen, ob die Anforderungen an die Freigabe des IT-Sicherheitskennzeichens für ein Produkt eingehalten werden. Werden bei der Prüfung Abweichungen von der abgegebenen Herstellererklärung oder Sicherheitslücken festgestellt, kann das Bundesamt die geeigneten Maßnahmen zum Schutz des Vertrauens der Verbraucher in das IT-Sicherheitskennzeichen treffen, insbesondere

1. Informationen über die Abweichungen oder Sicherheitslücken in geeigneter Weise in der Sicherheitsinformation veröffentlichen oder

2. die Freigabe des IT-Sicherheitskennzeichens widerrufen.

Absatz 7 Satz 2 gilt entsprechend.

(9) Bevor das Bundesamt eine Maßnahme nach Absatz 8 trifft, räumt es dem Hersteller oder Diensteanbieter Gelegenheit ein, die festgestellten Abweichungen oder Sicherheitslücken innerhalb eines angemessenen Zeitraumes zu beseitigen, es sei denn, gewichtige Gründe der Sicherheit der Produkte erfordern eine sofortige Maßnahme. Die Befugnis des Bundesamtes zur Warnung nach § 7 bleibt davon unberührt.“

21. § 10 wird wie folgt geändert:

a) Nach Absatz 2 wird folgender Absatz 3 eingefügt:

„(3) Das Bundesministerium des Innern, für Bau und Heimat bestimmt 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 die Einzelheiten der Gestaltung, des Inhalts und der Verwendung des IT-Sicherheitskennzeichens nach § 9c, um eine einheitliche Gestaltung des Kennzeichens und eine eindeutige Erkennbarkeit der gekennzeichneten informationstechnischen Produkte zu gewährleisten, sowie die Einzelheiten des Verfahrens zur Feststellung der Eignung branchenabgestimmter IT-Sicherheitsvorgaben und des Antragsverfahrens auf Freigabe einschließlich der diesbezüglichen Fristen und der beizufügenden Unterlagen sowie das Verfahren und die Gestaltung des Verweises auf Sicherheitsinformationen.“

b) Folgender Absatz 5 wird angefügt:

„(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 Unternehmen und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie, dem Bundesministerium der Justiz und für Verbraucherschutz, dem Bundesministerium für Gesundheit, dem Bundesministerium für Verkehr und digitale Infrastruktur, dem Bundesministerium der Verteidigung und dem Bundesministerium für Umwelt, Naturschutz und nukleare Sicherheit, welche wirtschaftlichen Kennzahlen bei der Berechnung der inländischen Wertschöpfung heranzuziehen sind, wie die Berechnung mit Hilfe der Methodik der direkten Wertschöpfungsstaffel zu erfolgen hat und welche Schwellenwerte maßgeblich dafür sind, dass ein Unternehmen

zu den größten Unternehmen in Deutschland im Sinne des § 2 Absatz 14 Satz 1 Nummer 2 gehört. Unter den Voraussetzungen nach Satz 1 kann das Bundesministerium des Innern, für Bau und Heimat durch Rechtsverordnung bestimmen, welche Alleinstellungsmerkmale maßgeblich dafür sind, dass Zulieferer für Unternehmen, die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören, von wesentlicher Bedeutung im Sinne des § 2 Absatz 14 Satz 1 Nummer 2 sind."

22. § 11 wird wie folgt gefasst:

„§ 11 Einschränkung von Grundrechten

Das Fernmeldegeheimnis (Artikel 10 des Grundgesetzes) wird durch die §§ 4a, 5 bis 5c, 7b und 7c eingeschränkt."

23. § 13 wird wie folgt geändert:

a) Absatz 2 Satz 2 wird wie folgt gefasst:

„§ 7 Absatz 1a ist entsprechend anzuwenden."

b) Nach Absatz 2 wird folgender Absatz 3 eingefügt:

„(3) Das Bundesministerium des Innern, für Bau und Heimat unterrichtet kalenderjährlich jeweils bis zum 30. Juni des dem Berichtsjahr folgenden Jahres den Ausschuss für Inneres und Heimat des Deutschen Bundestages über die Anwendung dieses Gesetzes. Es geht dabei auch auf die Fortentwicklung des maßgeblichen Unionsrechts ein."

c) Die bisherigen Absätze 3 bis 5 werden die Absätze 4 bis 6.

24. § 14 wird wie folgt gefasst:

„§ 14 Bußgeldvorschriften

(1) Ordnungswidrig handelt, wer entgegen § 8a Absatz 3 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 einen Nachweis nicht richtig oder nicht vollständig erbringt.

(2) Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig

1. einer vollziehbaren Anordnung nach

a) § 5b Absatz 6, § 7c Absatz 1 Satz 1, auch in Verbindung mit § 7c Absatz 3, § 7d, oder § 8a Absatz 3 Satz 5,

b) § 7a Absatz 2 Satz 1 oder

c) § 8b Absatz 6 Satz 1, auch in Verbindung mit Satz 2, oder § 8c Absatz 4 Satz 1

zuwiderhandelt,

2. entgegen § 8a Absatz 1 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 eine dort genannte Vorkehrung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig trifft,

3. entgegen § 8a Absatz 3 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 einen Nachweis nicht oder nicht rechtzeitig erbringt,

4. entgegen § 8a Absatz 4 Satz 2 oder § 8b Absatz 3a das Betreten eines dort genannten Raums nicht gestattet, eine dort genannte Unterlage nicht oder nicht rechtzeitig vorlegt, eine Auskunft nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig erteilt oder Unterstützung nicht oder nicht rechtzeitig gewährt,

5. entgegen § 8b Absatz 3 Satz 1 in Verbindung mit einer Rechtsverordnung nach § 10 Absatz 1 Satz 1 oder entgegen § 8f Absatz 5 Satz 1 eine Registrierung nicht oder nicht rechtzeitig vornimmt oder eine dort genannte Stelle nicht oder nicht rechtzeitig benennt,

6. entgegen § 8b Absatz 3 Satz 4 nicht sicherstellt, dass er erreichbar ist,

7. entgegen § 8b Absatz 4 Satz 1, § 8c Absatz 3 Satz 1 oder § 8f Absatz 7 Satz 1 oder Absatz 8 Satz 1 eine Meldung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig macht,

8. entgegen § 8c Absatz 1 Satz 1 eine dort genannte Maßnahme nicht trifft,

9. entgegen § 8f Absatz 1 eine Selbsterklärung nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig vorlegt,

10. entgegen § 9a Absatz 2 Satz 2 als Konformitätsbewertungsstelle tätig wird oder

11. entgegen § 9c Absatz 4 Satz 1 das IT-Sicherheitskennzeichen verwendet.

(3) Ordnungswidrig handelt, wer eine in Absatz 1 bezeichnete Handlung fahrlässig begeht.

(4) Ordnungswidrig handelt, wer gegen die Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit) (Abl. L 151 vom 7.6.2019, S. 15) verstößt, indem er vorsätzlich oder fahrlässig

1. entgegen Artikel 55 Absatz 1 eine dort genannte Angabe nicht, nicht richtig, nicht vollständig oder nicht binnen eines Monats nach Ausstellung zugänglich macht oder

2. entgegen Artikel 56 Absatz 8 Satz 1 eine Information nicht, nicht richtig, nicht vollständig oder nicht unverzüglich nach Feststellung einer Sicherheitslücke oder Unregelmäßigkeit gibt.

(5) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 2 Nummer 1 Buchstabe a mit einer Geldbuße bis zu zwei Millionen Euro sowie in den Fällen der Absätze 1, 2 Nummer 2 und 3 mit einer Geldbuße bis zu einer Million Euro geahndet werden. Die Ordnungswidrigkeit kann in den Fällen des Absatzes 2 Nummer 1 Buchstabe c, Nummer 5 und 7 bis 11 und des Absatzes 4 mit einer Geldbuße bis zu fünfhunderttausend Euro sowie in den Fällen des Ab-

satzes 2 Nummer 1 Buchstabe b, Nummer 4 und 6 und des Absatzes 3 mit einer Geldbuße bis zu einhunderttausend Euro geahndet werden. In den Fällen des Satzes 1 ist § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten anzuwenden.

(6) Verwaltungsbehörde im Sinne des § 36 Absatz 1 Nummer 1 des Gesetzes über Ordnungswidrigkeiten ist das Bundesamt.“

25. Nach § 14 wird folgender § 14a eingefügt:

„§ 14a Institutionen der sozialen Sicherung

Bei Zuwiderhandlungen gegen eine in § 14 Absatz 1 bis 4 genannte Vorschrift, die von Körperschaften gemäß § 29 des Vierten Buches Sozialgesetzbuch, Arbeitsgemeinschaften gemäß § 94 des Zehnten Buches Sozialgesetzbuch sowie der Deutschen Post AG, soweit sie mit der Berechnung oder Auszahlung von Sozialleistungen betraut ist (Institutionen der sozialen Sicherung), begangen werden, finden die Sätze 2 bis 4 Anwendung. Bei einer in Satz 1 genannten Zuwiderhandlung von Institutionen der sozialen Sicherung in Trägerschaft des Bundes stellt das Bundesamt das Einvernehmen über die zu ergreifenden Maßnahmen mit der für die Institution der sozialen Sicherung zuständigen Aufsichtsbehörde her. Bei einer in Satz 1 genannten Zuwiderhandlung von Institutionen der sozialen Sicherung in Trägerschaft der Länder informiert das Bundesamt die zuständige Aufsichtsbehörde und schlägt geeignete Maßnahmen vor. Die jeweils zuständige Aufsichtsbehörde informiert das Bundesamt über die Einleitung und Umsetzung von Aufsichtsmitteln und sorgt für deren Durchsetzung.“

Artikel 2 Änderung des Telekommunikationsgesetzes

Artikel 2 wird in 1 Vorschrift zitiert und ändert mWv. 28. Mai 2021 TKG § 109, § 113

Das Telekommunikationsgesetz vom 22. Juni 2004 (BGBl. I S. 1190), das zuletzt durch Artikel 6 des Gesetzes vom 19. April 2021 (BGBl. I S. 771) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht werden in der Angabe zu § 109 nach dem Wort „Technische“ die Wörter „und organisatorische“ eingefügt.

2. § 109 wird wie folgt geändert:

a) In der Überschrift werden nach dem Wort „Technische“ die Wörter „und organisatorische“ eingefügt.

b) Absatz 2 wird wie folgt geändert:

aa) In Satz 2 werden nach dem Wort „Nutzer“ ein Komma und die Wörter „für Dienste“ eingefügt.

bb) Nach Satz 3 wird folgender Satz eingefügt:

„Kritische Komponenten im Sinne von § 2 Absatz 13 des BSI-Gesetzes dürfen von einem Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotential nur eingesetzt werden, wenn sie vor dem erstmaligen Einsatz von einer anerkannten Zertifizierungsstelle überprüft und zertifiziert wurden.“

cc) In dem neuen Satz 7 wird die Angabe „§ 11“ durch die Angabe „§ 62“ ersetzt.

c) Absatz 4 Satz 1 Nummer 3 wird wie folgt gefasst:

„3. Welche technischen Vorkehrungen oder sonstigen Schutzmaßnahmen zur Erfüllung der durch die Vorgaben des Katalogs von Sicherheitsanforderungen nach Absatz 6 konkretisierten Verpflichtungen aus den Absätzen 1 und 2 getroffen oder geplant sind; sofern der Katalog lediglich Sicherheitsziele vorgibt, ist darzulegen, dass mit den ergriffenen Maßnahmen das jeweilige Sicherheitsziel vollumfänglich erreicht wird.“

d) Absatz 5 wird wie folgt geändert:

aa) In Satz 5 werden die Wörter „Europäische Agentur für Netz- und Informationssicherheit“ durch die Wörter „Agentur der Europäischen Union für Cybersicherheit“ ersetzt.

bb) In Satz 8 werden die Wörter „Europäische Agentur für Netz- und Informationssicherheit“ durch die Wörter „Agentur der Europäischen Union für Cybersicherheit“ ersetzt.

e) Absatz 6 wird wie folgt geändert:

aa) Satz 1 wird wie folgt gefasst:

„Die Bundesnetzagentur legt im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit durch Verfügung in einem Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten fest:

1. Einzelheiten der nach den Absätzen 1 und 2 zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen unter Beachtung der verschiedenen Gefährdungspotenziale der öffentlichen Telekommunikationsnetze und öffentlich zugänglichen Telekommunikationsdienste,

2. welche Funktionen kritische Funktionen im Sinne von § 2 Absatz 13 Satz 1 Nummer 3 Buchstabe b des BSI-Gesetzes sind, die von kritischen Komponenten im Sinne von § 2 Absatz 13 des BSI-Gesetzes realisiert werden, und

3. wer als Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial einzustufen ist.“

bb) Nach Satz 2 wird folgender Satz eingefügt:

„Die nach den Absätzen 1, 2 und 4 Verpflichteten haben die Vorgaben des Katalogs spätestens ein Jahr nach dessen Inkrafttreten zu erfüllen, es sei denn, in dem Katalog ist eine davon abweichende Umsetzungsfrist festgelegt worden.“

f) Absatz 7 wird wie folgt geändert:

aa) Nach Satz 1 werden die folgenden Sätze eingefügt:

„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 den Absätzen 1 bis 3 erfüllt sind. Die Bundesnetzagentur legt den Zeitpunkt der erstmaligen Überprüfung nach Satz 2 fest."

bb) In dem neuen Satz 4 wird die Angabe „Satz 1" durch die Wörter „den Sätzen 1 und 2" ersetzt und werden nach dem Wort „Bundesnetzagentur" die Wörter „und an das Bundesamt für Sicherheit in der Informationstechnik, sofern dieses die Überprüfung nicht vorgenommen hat," eingefügt.

cc) Folgender Satz wird angefügt:

„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."

3. § 113 Absatz 3 wird wie folgt geändert:

a) In Nummer 7 wird der Punkt am Ende durch ein Komma ersetzt.

b) Folgende Nummer 8 wird angefügt:

„8. An das Bundesamt für Sicherheit in der Informationstechnik zum Schutz der Versorgung der Bevölkerung in den Bereichen des § 2 Absatz 10 Satz 1 Nummer 1 des BSI-Gesetzes oder der öffentlichen Sicherheit, um damit eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme einer Kritischen Infrastruktur oder eines Unternehmens im besonderen öffentlichen Interesse abzuwenden, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, das auf die informationstechnischen Systeme bestimmbarer Infrastrukturen oder Unternehmen abzielen wird, und die in die Auskunft aufzunehmenden Daten im Einzelfall erforderlich sind, um den Betreiber der betroffenen Kritischen Infrastruktur oder das betroffene Unternehmen im besonderen öffentlichen Interesse vor dieser Beeinträchtigung zu warnen, über diese zu informieren oder bei deren Beseitigung zu beraten oder zu unterstützen."

4. § 113 Absatz 5 wird wie folgt geändert:

a) In Nummer 8 wird der Punkt am Ende durch ein Komma ersetzt.

b) Folgende Nummer 9 wird angefügt:

„9. Das Bundesamt für Sicherheit in der Informationstechnik zum Schutz der Versorgung der Bevölkerung in den Bereichen des § 2 Absatz 10 Satz 1 Nummer 1 des BSI-Gesetzes oder der öffentlichen Sicherheit, um damit eine Beeinträchtigung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme einer Kritischen Infrastruktur oder eines Unternehmens im besonderen öffentlichen Interesse abzuwenden, wenn Tatsachen den Schluss auf ein wenigstens seiner Art nach konkretisiertes und zeitlich absehbares Geschehen zulassen, das auf die informationstechnischen Systeme bestimmbarer Infrastrukturen oder Unternehmen abzielen wird, und die in die Auskunft aufzunehmenden Daten im Einzelfall erforderlich sind, um den Betreiber der betroffenen Kritischen Infrastruktur oder das betroffene Unternehmen im besonderen öffentlichen Interesse vor dieser Beeinträchtigung zu warnen, über diese zu informieren oder bei deren Beseitigung zu beraten oder zu unterstützen."

Artikel 3 Änderung des Energiewirtschaftsgesetzes

Artikel 3 ändert mWv. 28. Mai 2021 EnWG § 11

In § 11 des Energiewirtschaftsgesetzes vom 7. Juli 2005 (BGBl. I S. 1970, 3621), das zuletzt durch Artikel 2 des Gesetzes vom 25. Februar 2021 (BGBl. I S. 298) geändert worden ist, werden nach Absatz 1c die folgenden Absätze 1d und 1e eingefügt:

„(1d) Betreiber von Energieversorgungsnetzen und von solchen Energieanlagen, die durch Inkrafttreten der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur bestimmt wurden, haben spätestens ab dem 1. Mai 2023 in ihren informationstechnischen Systemen, Komponenten oder Prozessen, die für die Funktionsfähigkeit der von ihnen betriebenen Energieversorgungsnetze oder Energieanlagen maßgeblich sind, in angemessener Weise Systeme zur Angriffserkennung einzusetzen. Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorsehen. Dabei soll der Stand der Technik eingehalten werden. Der Einsatz von Systemen zur Angriffserkennung ist angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den möglichen Folgen eines Ausfalls oder einer Beeinträchtigung des betroffenen Energieversorgungsnetzes oder der betroffenen Energieanlage steht.

(1e) Betreiber von Energieversorgungsnetzen und Energieanlagen, die nach der Rechtsverordnung gemäß § 10 Absatz 1 des BSI-Gesetzes als Kritische Infrastruktur gelten, haben dem Bundesamt für Sicherheit in der Informationstechnik erstmalig am 1. Mai 2023 und danach alle zwei Jahre die Erfüllung der Anforderungen nach Absatz 1d nachzuweisen. Das Bundesamt für Sicherheit in der Informationstechnik hat die hierfür eingereichten Nachweisdokumente unverzüglich an die Bundesnetzagentur weiterzuleiten. Das Bundesamt für Sicherheit in der Informationstechnik und die Bundesnetzagentur haben sicherzustellen, dass die unbefugte Offenbarung der ihnen nach Satz 1 zur Kenntnis gelangten Angaben ausgeschlossen wird. Das Bundesamt für Sicherheit in der Informationstechnik kann bei Mängeln in der Umsetzung der Anforderungen nach Absatz 1d oder in den Nachweisdokumenten nach Satz 1 im Einvernehmen mit der Bundesnetzagentur die Beseitigung der Mängel verlangen.“

Artikel 4 Änderung der Außenwirtschaftsverordnung

Artikel 4 ändert mWv. 28. Mai 2021 AWV § 55

§ 55 Absatz 1 Satz 2 Nummer 2 der Außenwirtschaftsverordnung vom 2. August 2013 (BGBl. I S. 2865), die zuletzt durch Artikel 7 Absatz 19 des Gesetzes vom 12. Mai 2021 (BGBl. I S. 990) geändert worden ist, wird wie folgt gefasst:

„2. Kritische Komponenten im Sinne des § 2 Absatz 13 des BSI-Gesetzes entwickelt oder herstellt oder Software, die branchenspezifisch zum Betrieb von Kritischen Infrastrukturen im Sinne des BSI-Gesetzes dient, besonders entwickelt oder herstellt,“.

Artikel 5 Änderung des Zehnten Buches Sozialgesetzbuch

Artikel 5 wird in 1 Vorschrift zitiert und ändert mWv. 28. Mai 2021 SGB X § 67c

In § 67c Absatz 3 Satz 1 des Zehnten Buches Sozialgesetzbuch – Sozialverwaltungsverfahren und Sozialdatenschutz – in der Fassung der Bekanntmachung vom 18. Januar 2001 (BGBl. I S. 130), das zuletzt durch Artikel 14 des Gesetzes vom 4. Mai 2021 (BGBl. I S. 882) geändert worden ist, werden nach dem Wort „Verantwortlichen“ die Wörter „oder für die Wahrung oder Wiederherstellung der Sicherheit und Funktionsfähigkeit eines informationstechnischen Systems durch das Bundesamt für Sicherheit in der Informationstechnik“ eingefügt.

Artikel 6 Evaluierung

Artikel 6 ändert mWv. 28. Mai 2021 ITSiG Artikel 10

(1) Das Bundesministerium des Innern, für Bau und Heimat berichtet dem Deutschen Bundestag unter Einbeziehung von wissenschaftlichem Sachverstand über die Wirksamkeit der in diesem Gesetz enthaltenen Maßnahmen für die Erreichung der mit diesem Gesetz verfolgten Ziele

1. bis zum 1. Mai 2023 hinsichtlich des § 2 Absatz 10, der §§ 8a, 8b, 8d und 8e sowie § 10 Absatz 1 des BSI-Gesetzes (Artikel 1) und

2. bis zum 1. Mai 2025 hinsichtlich des Gesetzes im Übrigen.

(2) Artikel 10 des IT-Sicherheitsgesetzes vom 17. Juli 2015 (BGBl. I S. 1324), das durch Artikel 5 Absatz 8 des Gesetzes vom 18. Juli 2016 (BGBl. I S. 1666) geändert worden ist, wird aufgehoben.

Artikel 7 Inkrafttreten

(1) Dieses Gesetz tritt vorbehaltlich des Absatzes 2 am Tag nach der Verkündung*) in Kraft.

(2) Artikel 1 Nummer 4, 6 und 12 tritt am 1. Dezember 2021 in Kraft.

Der Bundespräsident

Frank-Walter Steinmeier

Die Bundeskanzlerin

Dr. Angela Merkel

Der Bundesminister des Innern, für Bau und Heimat

Horst Seehofer

*) Die Verkündung erfolgte am 27. Mai 2021.

6. Zentrale Ansprechstellen Cybercrime der Polizeien für Wirtschaftsunternehmen in Deutschland (ZAC)

Land / Bund		Rufnummer	E-Mail
	Baden-Württemberg	+49 711 5401-2444	cybercrime@polizei.bwl.de
	Bayern	+49 89 1212-3300	zac@polizei.bayern.de
	Berlin	+49 30 4664-972972	zac@polizei.berlin.de
	Brandenburg	+49 3334 388-8686	zac@polizei.brandenburg.de
	Bremen	+49 421 362-19820	cybercrime@polizei.bremen.de
	Hamburg	+49 40 4286-75455	zac@polizei.hamburg.de
	Hessen	+49 611 83-8377	zac.hlka@polizei.hessen.de
	Mecklenburg-Vorpommern	+49 3866 64-4545	cybercrime.lka@polmv.de
	Niedersachsen	+49 511 26262-3804	zac@lka.polizei.niedersachsen.de https://www.zac-niedersachsen.de/
	Nordrhein-Westfalen	+49 211 939-4040	cybercrime.lka@polizei.nrw.de
	Rheinland-Pfalz	+49 6131 65-2565	lka.cybercrime@polizei.rlp.de
	Saarland	+49 681 962-2448	cybercrime@polizei.slpol.de
	Sachsen	+49 351 855-3226	zac.lka@polizei.sachsen.de
	Sachsen-Anhalt	+49 391 250-2244	zac.lka@polizei.sachsen-anhalt.de
	Schleswig-Holstein	+49 431 160-42727	cybercrime@polizei.landsh.de
	Thüringen	+49 361 57431-4545	cybercrime.lka@polizei.thueringen.de
	Bundeskriminalamt	+49 611 55-15037	CC12-ZAC@bka.bund.de

Herausgeber Verband der Automobilindustrie e.V.
Behrenstraße 35, 10117 Berlin
www.vda.de

Version Version 1.0, Oktober 2021