Stellungnahme

zum Referentenentwurf vom 7. Mai 2020 für ein

Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)

Bundesverband der Deutschen Industrie e.V.

Stand: 3. Juli 2020

Inhaltsverzeichnis

Zusammenfassung

Die deutsche Industrie begrüßt das Vorhaben der Bundesregierung, die Cyberresilienz Deutschlands signifikant ganzheitlich zu stärken. Cyber- und IT-Sicherheit sind Grundlage für eine langfristige sichere digitale Transformation von Staat, Wirtschaft und Gesellschaft. Alle Beteiligten – vom Hard- und Software-Hersteller bis zu gewerblichen Betreibern, Privatanwendern und staatlichen Stellen – müssen aktiv und ganzheitlich in die Stärkung der Cyberresilienz einbezogen werden. Die deutsche Industrie wird hierzu auch weiterhin ihren Beitrag leisten, denn für das störungsfreie Funktionieren von in hohem Maße digitalisierten Prozessen in Unternehmen ist ein hoher Grad an Cyberresilienz eine Grundvoraussetzung.

Der Staat ist wiederum gefordert den regulatorischen Rahmen so auszugestalten, dass das Cybersicherheitsniveau Deutschlands ganzheitlich gestärkt wird, ohne den Unternehmen ungerechtfertigt hohe, respektive unklare Vorgaben aufzuerlegen. Das IT-Sicherheitsgesetz 2.0 könnte hierfür den geeigneten Rahmen bieten, lässt jedoch in der Version des Referentenentwurfs (RefE) vom 7. Mai 2020 die notwendige Rechtsklarheit vermissen und ist vielfach zu weitreichend und unbestimmt.

Die Wahrung von Cyber- und IT-Sicherheit ist eine globale Aufgabe, die angesichts des Ziels eines Europäischen Binnenmarktes mindestens eine eng abgestimmte Zusammenarbeit aller EU-Mitgliedstaaten verlangt. Nationale Insellösungen sind weder effizient noch effektiv. Sie erhöhen Aufwand und Kosten bei den Verpflichteten und verzerren den Wettbewerb. Rechtliche Flickenteppiche schaffen rechtliche Unsicherheiten, zulasten der verpflichteten Unternehmen sowie zulasten der Verbraucher und Geschäftskunden. Die Bundesregierung sollte im Rahmen der Deutschen EU-Ratspräsidentschaft und der anstehenden Review der NIS-Richtlinie auf einen einheitlichen europäischen Regulierungsrahmen hinwirken.

Aus Sicht des BDI sind mit Blick auf den vorliegenden Referentenentwurf insbesondere folgende weitere Punkte kritisch zu beurteilen:

- **Fehlende Evaluierung des IT-Sicherheitsgesetzes**: Bevor ein zweites IT-Sicherheitsgesetz initiiert wird, wäre es angezeigt gewesen, das erste IT-Sicherheitsgesetz eingehend zu analysieren – dies ist jedoch bis dato nicht erfolgt. Hierzu sollte in strukturierter Form auch die bisher betroffenen Wirtschaftsteile und Unternehmen konsultiert werden. In diesem Zusammenhang kritisiert die deutsche Industrie, dass im vorliegenden RefE keine Evaluierung des IT-SiG 2.0 vorgesehen ist.

Bundesverband der Deutschen Industrie e.V.
Mitgliedsverband BUSINESSEUROPE

Hausanschrift
Breite Straße 29
10178 Berlin
Postanschrift
11053 Berlin
Ansprechpartner
Steven Heckler

T: +493020281523
F: +493020282523
Internet
www.bdi.eu
E-Mail
S.Heckler@bdi.eu

- **IT-SiG 2.0 sollte kooperativem, nicht bestrafendem Ansatz folgen**: Statt wie bisher auf einen kooperativen/unterstützenden Ansatz zu setzen, folgt der derzeitige RefE einem bestrafenden Regulierungsansatz – vgl. starke Betonung der Rolle des BSI als Aufsichtsbehörde von Produktherstellern mit unzähligen Eingriffsmaßnahmen. Die deutsche Industrie würde einen kooperativen Ansatz, der eine stärkere Gewichtung auf die proaktive Unterstützung als auf eine reaktive Bestrafung von Unternehmen setzt, begrüßen.

- **Fehlende Einbettung in das europäische Rechtssystem:** Das langfristige Ziel einer europäischen Harmonisierung im Bereich IT-Sicherheit wird durch das IT-SiG 2.0 erschwert. Hierfür stehen beispielhaft das IT-Sicherheitskennzeichen, der neue KRITIS-Sektor „Entsorgung“ sowie der neue Begriff „Unternehmen im besonderen öffentlichen Interesse“. Bei der Definition Kritischer Komponenten im Bereich 5G, sollte sich der Gesetzgeber an dem gemeinsamen Instrumentarium (EU 5G-Toolbox) von Risikominderungsmaßnahmen, auf das sich die EU-Mitgliedstaaten geeinigt haben, orientieren. Nicht abgestimmte, nationalstaatliche Einzelmaßnahmen können für weltweit tätige Unternehmen enorme zusätzliche Kosten und damit Wettbewerbsnachteile bedeuten. Dies würde den Wirtschaftsstandort Deutschland nachhaltig schaden.

- **Mangelnde Rechtsklarheit, da Gesetzesdetails erst später geregelt werden sollen oder da Begriffe sehr weit gefasst sind**: Das IT-SiG 2.0 lässt in seiner aktuell vorliegenden Fassung an Rechtsklarheit für die deutsche Industrie zu wünschen übrig. So sind die neu einzuführenden Begriffe „IT-Produkte“ und „Kritische Komponente“ nicht hinreichend rechtlich präzise definiert. Anstatt weitere Details in einer RVO zu regeln, sollten diese direkt im IT-SiG 2.0 verbindlich bestimmt werden. Vielmehr sollte jedwede Ausweitung des Anwendungsbereichs von KRITIS-Regulierungen – auch mit Blick auf wettbewerbsrechtliche Implikationen – erst über die Review der NIS-Richtlinie erfolgen.

- **Unternehmen im besonderen öffentlichen Interesse**: Der BDI empfiehlt von einer einzelstaatlichen Einführung der Kategorie „Unternehmen im besonderen öffentlichen Interesse“ abzusehen. Im aktuellen RefE bleibt völlig unklar, welche Unternehmen hierunter fallen. Insbesondere die Unter-Kategorie „von besonderer volkswirtschaftlicher Bedeutung“ lässt völlig im Unklaren, welche Unternehmen hierunter fallen. Zudem lässt der nun vorgeschlagene Ansatz völlig außer Acht, dass deutsche Unternehmen vielfach in internationale Wertschöpfungsketten integriert sind. Ausländische Zulieferer

werden jedoch von §2 Abs. 14 Satz 2 nicht erfasst, d.h. diese bestehen als potenzielle Schwachstelle weiter. Zudem würde nahezu jedes Unternehmen in Deutschland – Industrie-KMU, Handwerksbetrieb und Restaurants eingeschlossen – über die dritte Kategorie (Unternehmen, die der GefahrstoffVO), in den Geltungsbereich des IT-SiG 2.0 fallen, da all diese Unternehmen Produkte verwenden, die der GefahrstoffVO unterliegen.

- **Meldepflichten haben Lagebild bisher nicht verbessert**: Die mit dem ersten IT-Sicherheitsgesetz eingeführte Meldepflicht von Cybersicherheitsvorfällen bei Kritischen Infrastrukturen hat bisher keine wahrnehmbare Verbesserung im Lagebild gebracht. Das BSI hat bisher keine unterjährigen branchenspezifischen Lagebilder veröffentlicht. Auch fehlt ein effizienter, harmonisierter Meldeweg an eine zentrale Meldestelle nach dem one-stop-shop-Prinzip. Zwar können Meldepflichten ein erster Schritt zu einer sinnvollen Verantwortungszuweisung von Herstellern sein, aber letztlich greifen sie zu kurz. Nur wenn Meldepflichten in ein verbessertes tagesaktuelles, ganzheitliches Lagebild sowie tagesaktuelle, branchenspezifische Warnungen münden, kann die deutsche Industrie aus dem beim BSI aggregierten Datenschatz auch einen Nutzen ziehen und ihre Anlagen und Systeme besser schützen. Neben einer Meldung sollten Hersteller auch angehalten werden, erkannte Sicherheitslücken entsprechend schließen zu müssen.

- **BSI stärken, aber nicht inhaltlich überfrachten**: Der BDI begrüßt die personelle Aufstockung des BSI. Allerdings sieht das IT-SiG 2.0 in Bezug auf das BSI eine Überfrachtung mit Aufgaben und Kompetenzen vor. So sieht der RefE vor, dass das BSI zukünftig den Stand der Technik bei sicherheitstechnischen Anforderungen entwickelt, IT-Produkte- und -Systeme untersucht, als Konformitätsbewertungsstelle fungiert, als nationale Cybersicherheitszertifizierungsstelle agiert und das IT-Sicherheitskennzeichen vergibt. Das BSI bekäme damit sehr weitreichende Kompetenzen, sowohl als Aufsichtsbehörde als auch als Normen- und Regulierungssetzer entlang des gesamten Produktlebenszyklusses. Hier gilt es, eine stärkere Trennung von Kompetenzen sicherzustellen und zukünftig weiter auf die Prozesse der europäischen Normung zu setzen.

- **Untersagung des Einsatzes Kritischer Komponenten nicht vertrauenswürdiger Hersteller**: § 9b hat in seiner jetzigen Ausgestaltung unkalkulierbare Risiken für Investitionen von KRITIS-Betreibern. Die angedachte Pflicht zur Anzeige Kritischer Komponenten und die Art ihres Einsatzes würde einen beträchtlichen Aufwand auf

Seiten des BSI und der KRITIS-Unternehmen ohne erkennbaren Mehrwert nach sich ziehen. Die Speicherung dieser sensiblen Informationen an einem Ort würde zudem ein unkalkulierbares Sicherheitsrisiko für den Bestand und das Funktionieren Kritischer Infrastrukturen sowie die damit verbunden Risiken für Staat, Gesellschaft und Unternehmen bedingen. Daher sollten sowohl die Anzeigepflicht als auch die Speicherung von sicherheitsrelevanten Informationen aus dem Entwurf genommen werden.

Es ist richtig, ausschließlich Kritische Komponenten vertrauenswürdiger Hersteller für den Einsatz zuzulassen. Der ausschließliche Einsatz von Komponenten vertrauenswürdiger Hersteller soll durch die Abgabe einer Garantieerklärung gegenüber dem Betreiber abgesichert werden. Mit dieser Vorgabe wird jedoch nur scheinbar die Sicherheit der KRITIS gewährleistet. Im Zweifel muss davon ausgegangen werden, dass Hersteller, die – ggf. sogar aufgrund rechtlicher Verpflichtungen in ihrem Land – mit Sicherheitslücken behaftete Komponenten in den deutschen Markt einführen wollen, die geforderte Garantieerklärung abgeben werden, ungeachtet der im RefE genannten Konsequenzen. Hinzu kommt, dass Verstöße gegen Garantieerklärungen von den KRITIS-Betreibern kaum nachzuweisen sein werden. Für eine solche Beweisführung dürfte in der Regel geheimdienstlich sichergestelltes Beweismaterial erforderlich sein – z.B. Erkenntnisse über die Verflochtenheit von Unternehmen und staatlichen Stellen, die vielfach nur durch nachrichtendienstliche Recherchen aufgedeckt werden können. KRITIS-Unternehmen werden sich diese Beweismittel weder selbst beschaffen können, noch werden diese Beweismittel von deutschen Behörden in einer Art und Weise zur Verfügung gestellt werden, mit der den Betreibern der Nachweis eines Verstoßes gegen die Garantieerklärung rechtlich sauber möglich sein wird. Zudem dürfte die rechtliche Überprüfung der Feststellung nach § 9b Abs. 4 BSIG, dass der Hersteller nicht vertrauenswürdig ist, regelmäßig aufgrund unzureichender Beweise zu Schwierigkeiten führen.

Erschwerend kommt hinzu, dass sich die Garantieerklärung des Herstellers ggü. KRITIS-Betreibern auf die gesamte Lieferkette bezieht. Problematisch ist insbesondere, dass Art und Umfang der „Garantieerklärung“ und deren Wirkung über die gesamte Lieferkette im aktuell vorliegenden RefE noch nicht konkretisiert ist. Es wird KRITIS-Betreibern vielfach nicht möglich sein, bei komplexen Hard-, Software- und Elektronik-Produkten globale Produktionsketten komplett nachzuvollziehen.

Die Möglichkeit, die Nutzung von im Einsatz befindlichen Komponenten zu untersagen, stellt ein hohes unternehmerisches Risiko für die Betreiber dar, welches zu einer stark eingeschränkten

Verfügbarkeit von kritischen Services und Produkten für Staat und Gesellschaft oder zu einer Existenzbedrohung für die betroffenen KRITIS-Betreiber führen kann. Der Gesetzentwurf lässt offen, wer die Kosten eines Rückbaus und den Ersatz von Komponenten zu tragen hat. Die deutsche Industrie fordert von der BReg, die Cyberresilienz Kritischer Infrastrukturen zu stärken, ohne die Rechts- und Investitionssicherheit für KRITIS-Betreiber zu mindern. Es braucht klare, herstellerunabhängige Sicherheitsanforderungen an die Hersteller, die gleichzeitig KRITIS-Betreiber mit der notwendigen Investitionssicherheit ausstatten.

- **Verbot von spezifischer Hardware und Technik:** Das Festschreiben eines Stands der Technik durch das BSI ist abzulehnen Der Stand der Technik entwickelt sich stetig weiter, basierend auf Standards und Innovationen sowie am Markt verfügbarer Technologien. Zudem ist zu befürchten, dass durch die Definition „Stand der Technik“ bereits eingesetzte Hardware und Technik verboten werden. Hier müssen Ausnahmen unter bestimmten Rahmenbedingungen möglich sein. Insbesondere ist ein Bestandsschutz für die bereits in Unternehmen von besonderem öffentlichen Interesse, in Kritischen Infrastrukturen sowie weiteren Unternehmen verbaute Technik sicherzustellen, sofern nicht ein berechtigtes Interesse durch einen bestätigten Sicherheitsmangel oder Vertrauensverlust besteht. Weiter ist sicherzustellen, dass die betroffenen Hersteller und Betreiber vorab vor anstehenden Verboten informiert werden.

- **Krisenreaktionspläne (§ 5c):** Um im Notfall gut vorbereitet zu sein, sind abgestimmte Krisenreaktionspläne von zentraler Bedeutung. Allerdings sollte es ureigene Aufgabe der Unternehmen sein, diese entsprechend einer unternehmensinternen Gefahrenprüfung zu erstellen und lediglich zur Prüfung an BSI und BBK zu geben. Ein weitergehendes Involvieren staatlicher Stellen wird als nicht notwendig erachtet und als nichtgerechtfertigten Eingriff in die unternehmerische Freiheit zu bewerten sein.

- **Unverhältnismäßige Bußgeldvorschriften:** Die vorgeschlagene Höhe für Bußgelder, die sich an der DSGVO orientiert, erachtet die deutsche Industrie mit Blick auf den Geltungsbereich des IT-SiG 2.0 (nur Deutschland und nicht ganz Europa) als völlig unverhältnismäßig. Schon im Bereich der DSGVO zeigt sich, dass der Bußgeldrahmen existenzvernichtend sein kann. Der Gesetzgeber sollte den Ausgleich zwischen maßvoll angemessener und wirksamer Sanktionierung anstreben. Daher sollte der Gesetzgeber deutlich geringere Geldbußen, als dies der aktuelle RefE vorsieht, ansetzen.

- **Erfüllungsaufwand für die Wirtschaft viel zu gering angesetzt**: Da zukünftig Zulieferer Maßnahmen umsetzen müssen und zahlreiche neue Branchen unter den Geltungsbereich des IT-SiG 2.0 fallen werden, scheint der Erfüllungsaufwand für die Wirtschaft mit 45,09 Millionen Euro zu gering angesetzt. Aus dem aktuell vorliegenden Referentenentwurf ist nicht nachvollziehbar, wie die Bundesregierung diesen Wert ermittelt hat. Hier gilt es, die weitreichenden unternehmensinternen Kosten für Personal und Anpassungen an Unternehmensprozesse besser zu berücksichtigen.

- **Mittelbare Lieferkettenverantwortung:** Durch die Ausweitung der durch das IT-SiG regulierten Sektoren rechnen wir damit, dass auch nicht regulierte Unternehmen und Sektoren mittelbar von den Vorschriften des IT-SiG 2.0 erfasst werden. Denn die betroffenen Unternehmen und Sektoren werden sich über die Verpflichtung ihrer Lieferanten bezüglich der Einhaltung der im IT-SiG 2.0 vorgeschriebenen Maßnahmen absichern. Das wird zu einem Mehr an Bürokratie in den Lieferprozessen führen und zu zusätzlichen Kosten in der gesamten Wirtschaft. Der Gesetzgeber sollte diesem mittelbaren Effekt Rechnung tragen, indem die Anforderungen des Gesetzes realistisch und umsetzbar, auch für nicht unmittelbar betroffene Unternehmen, gestaltet werden.

Ausgehend von dieser grundlegenden Analyse des Referentenentwurfs unterbreitet die deutsche Industrie folgende Handlungsempfehlungen:

- Das **IT-Sicherheitsgesetz 1.0** muss zügig, gemeinsam mit den bisher betroffenen Unternehmen u.a. auf Grundlage fachlich wissenschaftlicher Expertise eingehend analysiert und evaluiert werden. Die Ergebnisse müssen mit der Industrie geteilt werden.

- Bei Cybersicherheit ist ein **europaweit harmonisierter Regulierungsansatz** nationalen Alleingängen vorzuziehen. Da auf europäischer Ebene gerade erst der *EU Cybersecurity Act* beschlossen wurde und eine Einführung von Cybersicherheitsanforderungen in die vertikalen Richtlinien für Produktgruppen geprüft wird (siehe Funkanlagen- und Maschinenrichtlinie), muss das IT-SiG 2.0 unbedingt eine inhaltliche Anschlussfähigkeit an diese Vorhaben sicherstellen. Das IT-SiG 2.0 darf keine inkonsistenten Vorgaben, keine nationalen Sonderanforderungen und damit unrechtmäßige Marktzugangsbeschränkungen für Produkte im europäischen Gefüge verursachen.

- **Meldepflichten zu Cybervorfällen** müssen effizienter ausgestaltet (one-stop-shop-Prinzip) und personalisierte Unterstützungsleistungen des BSI für betroffene Unternehmen etabliert werden:
  - Unternehmen, die Cybersicherheitsvorfälle melden, sollte eine personalisierte Unterstützung angeboten werden,
  - Aus den Meldungen aus der Wirtschaft sollte ein Lagebild für die Industrie erarbeitet und unterjährig mit den relevanten Bundes- und Landessicherheitsbehörden sowie der Industrie in anonymisierter Form geteilt werden,
  - Meldungen aus der Wirtschaft sollten zu zeitnahen branchenspezifischen Warnungen führen,
  - Meldungen aus der Wirtschaft müssen zum Schließen von Sicherheitslücken führen – hierfür sollten, aufbauend auf ISO 29147, effektive Prozesse aufgesetzt werden,
  - Gesetzliche Rahmenbedingungen müssen geschaffen werden, um Wirtschaftsunternehmen über vorliegende Informationen zu (Cyber)-Gefährdern zu informieren, auch über geheimschutzbetreute Unternehmen hinaus.

- Es gilt, das **BSI personell und finanziell zu stärken** und zugleich eine **klare Kompetenzunterscheidung zwischen Normensetzung und deren Überprüfung** sicherzustellen. Vielfach sollte überprüft werden, ob nicht Unternehmen – im Sinne eines kooperativen Ansatzes – nunmehr für das BSI vorgesehene Aufgaben übernehmen können. Mit dem IT-SiG 2.0 sollte das Ziel verfolgt werden, Cybersicherheitsexpertise in den Unternehmen aufzubauen.

- Der vorgeschlagene **Bußgeldrahmen** muss **signifikant reduziert werden**. Der BDI empfiehlt deutlich geringere Geldbußen anzusetzen. So wird ermöglicht, dass statt eines reinen Compliance-Ansatzes eine vertrauensvolle, kooperative Beziehung aufgebaut wird.

- Es ist ein richtiger Schritt, dass KRITIS-Betreiber sowie Unternehmen im besonderen öffentlichen Interesse geeignete Prozesse vorsehen können, um die **Vertrauenswürdigkeit der Beschäftigten** zu überprüfen (§ 8a Abs. 1 und § 8b Abs. 3d BSIG). Staatliche Stellen müssen diese Möglichkeit unterstützen, z.B. indem Anträge auf Führungszeugnisse rasch bearbeitet werden. Hierfür müssen die notwendigen personellen Ressourcen vorgehalten werden. Auch die gegenseitige Anerkennung ausländischer Sicherheitsüberprüfungen muss dringend verbessert werden. Der Entwurf will erkennbar nicht die Mitwirkung ausländischer Spezialisten an allen Prozessen ausschließen oder beschränken, was zu begrüßen ist. Es müssen zukünftig auch Verfahren geschaffen werden, mit denen

ausländische Mitarbeiter in die Prüfung einbezogen werden können. Auch sind die Prozesslängen zu verkürzen. Mehrmonatige Wartezeiten, wie sie aktuell in der Sicherheitsüberprüfung vorkommen, hemmen die Wirtschaft und tragen nicht zur Sicherheit bei.

- Sinnvoll scheint, dem BSI die Möglichkeit zu geben, **Schadprogramme, Sicherheitslücken und andere Sicherheitsrisiken in öffentlich erreichbaren IT-Systemen unter Berücksichtigung eines sicheren Vorgehens zu detektieren** (§ 7b, § 7c BSIG). Allerdings muss das BSI dazu verpflichtet werden, die so gewonnen Erkenntnisse mit der Wirtschaft zu teilen, damit diese etwaige Sicherheitslücken und Schwachstellen beseitigen kann.

- Der BDI fordert die Aufnahme eines Artikels 6 in den RefE, der eine verpflichtende **Evaluierung des IT-SiG 2.0** nach spätestens vier Jahren, jedoch zwingend vor einem IT-SiG 3.0, vorschreibt.

Diese Handlungsempfehlungen werden im Nachfolgenden durch eine Bewertung der einzelnen Normen vertieft und ergänzt.

Anmerkungen zum Referentenentwurf

Die deutsche Industrie begrüßt das Vorhaben der Bundesregierung, die Cyberresilienz Deutschlands signifikant und ganzheitlich zu stärken. Cyber- und IT-Sicherheit müssen als gesamtgesellschaftliche Aufgabe von Staat, Wirtschaft und Zivilgesellschaft verstanden werden. Die deutsche Industrie wird hierzu ihren Beitrag auch weiterhin leisten, denn für das störungsfreie Funktionieren von hochgradig digitalisierten Prozessen in Unternehmen ist ein hoher Grad an Cybersicherheit Grundvoraussetzung. Damit dieses Ziel mit einem IT-Sicherheitsgesetz 2.0 erreicht werden kann, empfiehlt die Industrie einige grundlegende Anpassungen des derzeitigen Entwurfs.

Im Einzelnen

Zu Artikel 1 – Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)

Kernbestandteil des Zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0) sind weitreichende Anpassungen des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG). Hervorzuheben sind insbesondere die Einführung des KRITIS-Sektors „Entsorgung“, der neuen Kategorie „Unternehmen im besonderen öffentlichen Interesse“ und einer „Garantieerklärung für Kritische Komponenten“. Zudem soll der Kompetenzbereich des BSI massiv erweitert und ein nationales IT-Sicherheitskennzeichen eingeführt werden. Im Folgenden bewertet die deutsche Industrie die einzelnen Vorhaben:

Zu § 2 Abs. 8a „Protokollierungsdaten“

Die Definition des Terminus „Protokollierungsdaten“ ist nach Ansicht der deutschen Industrie nicht hinreichend genau. Wir empfehlen daher die folgende Konkretisierung der Definition:

„(8a) Protokollierungsdaten sind Aufzeichnungen über die Art und Weise, wie die Informationstechnik genutzt wurde, über technische Ereignisse oder Zustände innerhalb eines informationstechnischen Systems und wie dieses mit anderen kommuniziert hat. *Protokolldaten nach Absatz 8 sind eine Teilmenge der Protokollierungsdaten.* Protokollierungsdaten dienen der Erkennung, Eingrenzung oder Beseitigung von Störungen oder Fehlern bei der Kommunikationstechnik oder von Angriffen.“

Zudem weist die deutsche Industrie darauf hin, dass Protokollierungsdaten und Aufzeichnungsmechanismen vielfach in branchenspezifischen Standards

definiert werden. Schließlich bietet es sich an, die Protokollierungsdaten und deren Verarbeitung dem Anwendungsbereich des § 87 Abs. 1 Nr. 6 BetrVG ausdrücklich zu entziehen. Die unverhältnismäßig breite Auslegung dieser Vorschrift durch die Arbeitsgerichte führt dazu, dass kein Verantwortlicher und kein Auftragsverarbeiter, bei dem solche Protokollierungsdaten anfallen, sie ohne Zustimmung eines Betriebsrats verarbeiten kann, auch wenn er – z.B. aufgrund Art. 32 DSGVO – hierzu verpflichtet ist und die Daten nur für die gesetzlichen Zwecke verarbeitet. Dieser Zustand ist nicht hinnehmbar, und es ist nicht erkennbar, dass die höchstrichterliche Rechtsprechung die Normanwendung in Übereinstimmung mit dem Normzweck konkretisiert.

Zu § 2 Abs. 9a – „IT-Produkte“

Die im Referentenentwurf eingeführte Definition für „IT-Produkte“ ist nicht hinreichend genau. Der BDI fordert daher eine Positivbestimmung (konkrete Nennung der betroffenen Produkte und Anlagen) in der Definition „IT-Produkte“ (§ 2 Abs. 9a). Dies ist umso bedeutsamer, da fast alle denkbaren Produkte der Elektroindustrie und anderer Branchen in ein System von Hardware, Software und *embedded* Software integriert werden. Entsprechend können sehr viele Hersteller als Hersteller von IT-Produkten gelten.

Der BDI empfiehlt folgende Anpassung der Definition:

„(9a) IT-Produkte sind Software sowie alle einzelnen oder *bestimmungsgemäß oder durch die Hersteller freigegeben* miteinander verbundenen Hardwareprodukte *und Hardwarekomponenten, inklusive der zur einwandfreien Funktion bestimmungsgemäß eingesetzten Software, die vom Hersteller dafür vorgesehen sind, mit öffentlichen Kommunikations-Netzwerken (Internet) verbunden zu werden oder die der Vernetzung dienen (Netzwerkkomponenten)*.“

Zu § 2 Abs. 9b – „Systeme zur Angriffserkennung“

Die im Referentenentwurf eingeführte Definition „Systeme zur Angriffserkennung“ ist nicht hinreichend genau. Eine Definition, in welcher Form die Angriffserkennung erfolgt, ist unnötig.

Der BDI empfiehlt folgende Anpassung der Definition:

„(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.*~~“

Zu § 2 Abs. 10 Satz 1 Nr. 1 – Einführung des KRITIS-Sektors „Entsorgung“

Die Einführung des neuen KRITIS-Sektors „Entsorgung“ ist, auch angesichts der jüngsten Entwicklungen im Zuge der Corona-Pandemie, nachvollziehbar. Der betroffene Industriesektor sollte jedoch frühzeitig eng in eine praktikable und realitätsnahe Ausgestaltung, insbesondere mit Blick auf die Schwellwerte, ab denen ein Entsorgungsdienstleister unter die KRITIS-Verordnung fällt, einbezogen werden. Dabei gilt es, insbesondere zwischen den unterschiedlichen Stoffströmen zu unterscheiden.

Zu § 2 Abs. 13 – „Kritische Komponenten“

Positiv zu bewerten ist die grundsätzliche Erfassung der Kritischen Komponenten und deren Hersteller, da die Gewährleistung von Integrität und Verfügbarkeit Kritischer Infrastrukturen nur im Zusammenspiel von Herstellern und Betreibern möglich ist.

Allerdings fehlt der aktuell vorliegenden Definition für Kritische Komponenten die notwendige Bestimmtheit und Rechtsklarheit. Basierend auf der aktuellen Definition wäre jede IT-Komponente, die in Kritischen Infrastrukturen zum Einsatz kommt und dort von hoher Kritikalität ist, eine Kritische Komponente im Sinne des BSIG, ganz gleich, wo sie zum Einsatz kommt. Mit Blick auf Absatz 13 muss sichergestellt werden, dass IT-Produkte nur dann unter den Wirkbereich des §2 Abs, 13 BSIG fallen, wenn sie in Kritischen Infrastrukturen eingesetzt werden und dort für das ordnungsgemäße Funktionieren der KRITIS entscheidend sind. Zudem sollte klargestellt werden, dass nur dafür ausgewiesene speziell für den Einsatz in Kritischen Infrastrukturen hergestellte Kritische Komponenten in diese Kategorie fallen können. Weitere IT-Produkte müssen explizit ausgeklammert sein.

Aus Sicht der deutschen Industrie ist es von herausgehobener Bedeutung, den Schutz der öffentlichen TK-Infrastruktur vor Ausfall, Spionage und Sabotage zu schützen. Mit Blick auf den KRITIS-Sektor „Telekommunikationsinfrastrukturen“ erscheint in Abs. 13 Satz 2 erforderlich, die Definition von Kritischen Komponenten derart zu schärfen, als dass nur solche Komponenten zu Kritischen Komponenten mit Verweis auf 109 TKG gezählt werden, die im Falle ihres Ausfalls zu erheblichen Beeinträchtigungen oder Störungen von Telekommunikationsnetzen und -diensten führen können. Des Weiteren sollten Komponenten, die zur Wahrung der Systemsicherheit oder die zum Schutz vor Spionageaktivitäten durch drittgesteuerte Lieferanten als „Kritische Komponenten“ definiert werden. Der Gesetzgeber sollte bei der Definition „Kritischer Komponenten“ für 5G die entsprechenden Vorgaben der EU 5G Toolbox berücksichtigen und umsetzen. Erforderlich ist in diesem

Zusammenhang eine klare Beschreibung von kritischen Funktionen und Komponenten im TKG, die sich faktisch auf Kernnetzkomponenten beziehen. Zudem wäre eine spezifischere Verpflichtung wünschenswert, sodass Hersteller von Kritischen Komponenten in ihrem Verantwortungsbereich gleichermaßen Vorkehrungen für die IT-Sicherheit zu treffen haben, wie die Betreiber von KRITIS.

Zur Nennung / Bewertung von Komponenten sollte direkt auf internationale oder mindestens europäische Standards rekurriert werden. Sollte allein der BSI-Grundschutz Anwendung finden, würden für privatwirtschaftlich organisierte Leistungserbringer erhebliche, zusätzliche Dokumentations- und Kostenaufwände entstehen. Zudem sollte der Einsatz und die Auswahl von IT-Produkten generell gemäß einer risikobasierten Gesamtbetrachtung auf Systemebene erfolgen. Ein Komponentenkatalog allein ist nicht ausreichend und kann daher ausschließlich empfehlenden Charakter haben.

Mit Blick auf den KRITIS-Sektor „Energie“ ist wichtig, dass es zu keiner Doppelregulierung in Bezug auf die existierenden IT-Sicherheitskataloge nach EnWG sowie B3S nach BSIG kommt.

Die deutsche Industrie fordert den Gesetzgeber zudem auf, folgende Punkte rasch zu klären:

- Welche Auswirkung haben die Einführung der Definition „Kritische Komponenten“ und deren Hersteller sowie die Aufnahme in den genannten Katalog für all jene IT-Produkte, die bereits vor In-Kraft-Treten des IT-SiG 2.0 und des Katalogs eingebaut sind? Hier sollte Bestandsschutz gelten.
- Welche Auswirkungen hat die Definition für private 5G-Campusnetze?
- Wie ist die angemessene Beteiligung der Betreiber Kritischer Infrastrukturen vorgesehen, um einen frühen Interessenabgleich aller Beteiligen zu gewährleisten?
- Wie wird ein angemessenes Abstraktionsniveau für die angestrebten Kataloge erreicht?

Der BDI empfiehlt folgende Anpassung der Definition:

„(13) Kritische Komponenten im Sinne dieses Gesetzes sind IT-Produkte, die in Kritischen Infrastrukturen eingesetzt werden und die von hoher Bedeutung für das *ordnungsgemäße* Funktionieren *der Kritischen Infrastruktur* ~~*des Gemeinwesens*~~ sind, weil Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit dieser IT-Produkte zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen

oder zu Gefährdungen für die öffentliche Sicherheit führen können. Die Kritischen Komponenten im Sinne dieses Gesetzes werden für Betreiber nach § 8d Abs. 2 Nr. 1 ~~*durch den Katalog von Sicherheitsanforderungen nach*~~ *in* § 109 Abs. 6 TKG näher bestimmt. Alle übrigen Kritischen Komponenten werden in einem Katalog des Bundesamtes näher bestimmt. Das Bundesamt gibt den *Herstellern und* Betreibern *aller* Kritischer Infrastrukturen Gelegenheit *zur Mitwirkung bei der Erstellung des Katalogs nach Satz 3* ~~*Stellungnahme*~~. *Der so erstellte Katalog wird zum Zweck der europaweiten Harmonisierung mit der Europäischen Agentur für Cybersicherheit harmonisiert.* Der Katalog wird vom Bundesamt veröffentlicht.

Zu § 2 Abs. 14 – „Unternehmen im besonderen öffentlichen Interesse“

Zu Nummer 1: Es ist bedenklich, dass eine Liste der Unternehmen vom BMWi verwendet wird, die voraussichtlich in nächster Zeit unabhängig von diesem Gesetzvorhaben erweitert wird. Hier sollte der Gesetzgeber im Gesetzgebungsprozess zum IT-SiG 2.0 direkt die betroffenen Normadressaten klären und klare Kriterien für diese Kategorie von Unternehmen treffen.

Zu Nummer 2: Prinzipiell haben Unternehmen ein sehr großes Eigeninteresse ihre Infrastruktur und unternehmensinternen Prozesse zu sichern. Hierfür braucht es keine Regulierung. Die Einführung der Kategorie von Unternehmen, die aufgrund ihrer „volkswirtschaftlichen Bedeutung und insbesondere ihrer erbrachten Wertschöpfung von besonderem öffentlichem Interesse“ sind, lehnt die deutsche Industrie in ihrer jetzigen Ausgestaltung als viel zu weitreichend ab. Folgende Gründe sind hier anzuführen:

- Der aktuell vorliegende Gesetzentwurf beinhaltet keine objektiven Kriterien, durch die ersichtlich wäre, welche Unternehmen unter §2 Abs. 14 Nr. 2 fallen. Hier ist der Gesetzgeber gefordert, objektive Kriterien einzuführen. Die bereits diskutierten Ansätze „TOP-100 Liste der Monopolkommission“ oder „Börsennotierung“ sind jeweils wahllos, da die Corona-Krise verdeutlicht hat, dass Unternehmen aller Größenordnung sowie aller Wertschöpfungstiefen von besonderer Relevanz sein können. Um eine Handlungs- und Planungssicherheit für die Unternehmen zu gewährleisten, müssen die Kriterien nachvollziehbar und mittelfristig gleichbleibend sein.

- Zudem lässt der nun vorgeschlagene Ansatz völlig außer Acht, dass deutsche Unternehmen vielfach in weitreichende internationale Wertschöpfungsketten integriert sind. Ausländische Zulieferer werden jedoch von §2 Abs. 14 Satz 2 nicht erfasst, d.h. diese bestehen als potenzielle Schwachstelle weiter. Es ist daher fragwürdig, ob der

Aufwand der hier betrieben wird, wirklich zur Absicherung der Unternehmen führt. Selbst bei Ausweitung auf EU-Ebene bleibt bei Unternehmen mit internationaler Supply Chain für Angreifer immer die Möglichkeit gezielt ausländische Schlüsselzulieferer, welche nicht über diese Regelung erfasst sind, lahmzulegen.

- Der Verweis auf die „erheblichen volkswirtschaftlichen Schäden", die die Unternehmen als besonders im öffentlichen Interesse qualifizieren soll, ist zu allgemein gehalten und nicht mit vergleichbaren qualitativen und quantitativen Kriterien erschließbar.

- Global tätige Unternehmen mit einer hohen volkswirtschaftlichen Bedeutung unterliegen bereits zahlreichen Auflagen und Berichtspflichten. Daher bedeutet die angestrebte Kompetenzerweiterung des BSI als eine zusätzliche Aufsichts- und Regulierungsbehörde mit weitergehenden Berichtspflichten für die entsprechenden Unternehmen eine erhebliche Mehrbelastung, ohne dabei risikobasiert bereits existierende Sicherheitsmechanismen der Unternehmen zu berücksichtigen. Langfristig ist zu befürchten, dass dem Wirtschaftsstandort Deutschland geschadet wird und ein Nachteil deutscher Unternehmen gegenüber europäischen und internationalen Wettbewerbern eintritt.

Die deutsche Industrie fordert das BMWi und BMI auf, bereits direkt im Gesetzgebungsprozess zum IT-SiG 2.0 konkrete und präzise Kriterien für ein besonderes öffentliches Interesse von Unternehmen und den von ihnen erbrachten Wertschöpfungen zu definieren. Dies sollte nicht erst über eine zukünftige Rechtsverordnung (§ 10 Abs. 5) erfolgen.

Zu Nummer 3: In §2 Abs. 14 Nr. 3 muss der Bezug auf Gefahrstoffe geändert und durch den Bezug auf Störfälle ersetzt werden. Der generelle Bezug zur Gefahrstoffverordnung ist viel zu weitreichend, da alle Unternehmen von der Gefahrstoffverordnung betroffen sind, wenn schon ein gekennzeichnetes Produkt (z.B. „Reizung der Haut" für ein Reinigungsmittel) für eine Tätigkeit am Arbeitsplatz eingesetzt wird. Demnach würden zukünftig nahezu alle Unternehmen in Deutschland in den Geltungsbereich des IT-SiG 2.0 fallen – auch z.B. Restaurants. Kurzum: Über die GefahrstoffVO wird sowohl auf die Produktion als auch den Einsatz bestimmter Produkte, jedoch nicht direkt auf Unternehmen, verwiesen. Vielmehr ist die StörfallVO, deren Zweck es ist, die Allgemeinheit vor anlagenbezogenen gefährlichen Ereignissen zu schützen, einschlägig. Dadurch wäre eine Eingrenzung auf Unternehmen mit besonderer Relevanz für die öffentliche Sicherheit und Ordnung gewährleistet. Zudem würde dies den Adressatenkreis von §2 Abs. 14 Nr. 3 deutlich präzisieren und damit für mehr Rechtsklarheit sorgen.

Des Weiteren würde mit der Ausweitung des BSIG auf „Unternehmen im besonderen öffentlichen Interesse“ Deutschland einen Sonderweg in der EU gehen. Für international tätige Unternehmen ist eine Harmonisierung der nationalen Gesetze zwingend notwendig. Ansonsten stoßen Unternehmen bei der Etablierung effektiver interner Strukturen an ihre Grenzen. Es ist daher wünschenswert den Begriff zu streichen oder an die anderen nationalen Gesetze anzugleichen, um eine einheitliche EU-weite Lösung zu erreichen. Unklar bleibt weiterhin, ob dies nur für Unternehmen mit Sitz in Deutschland gilt oder auch für solche, die zwar einen ausländischen Sitz haben, aber große Repräsentanzen in Deutschland haben.

Zu § 3 „Aufgaben des BSI“

Die deutsche Industrie begrüßt das grundsätzliche Bestreben, das BSI als oberste deutsche Cybersicherheitsbehörde zu stärken. Dies muss jedoch mit Augenmaß erfolgen und signifikante Vorteile für Unternehmen und Einzelpersonen nach sich ziehen.

Das BSI soll zukünftig den Stand der Technik bei sicherheitstechnischen Anforderungen entwickeln, IT-Produkte- und -Systeme untersuchen, als Konformitätsbewertungsstelle fungieren, als nationale Cybersicherheitszertifizierungsstelle agieren, das IT-Sicherheitskennzeichen vergeben und den Einsatz von Kritischen Komponenten untersagen (§3 Abs. 1 Satz 2 Nr. 5a und 5b zusammen mit §3 Abs. 1 Satz 2 Nr. 20, § 7a und § 9a). Das BSI bekommt damit sehr weitreichende Kompetenzen sowohl als Aufsichtsbehörde, als auch als Normen- und Regulierungssetzer entlang des gesamten Produktlebenszyklusses. Hier gilt es, eine stärkere Trennung von Kompetenzen sicherzustellen und zukünftig weiter auf die Prozesse der europäischen Normung zu setzen.

Die deutsche Industrie lehnt es ab, dass das BSI bei Produkten, die entsprechend des EU Cybersecurity Acts unter die Assurance Level „low“ und „substantial“ fallen, als Stelle für Konformitätsbewertungen i.S.d. § 3 Abs. 1 Satz 5a eingerichtet wird. Eine entsprechende Kompetenzausweitung würde das bisherige Modell einer strikten Trennung solcher Tätigkeiten untergraben. Diese Funktion ist klar abgedeckt durch die Privatwirtschaft und sollte, außer entsprechend den Vorgaben aus dem EU Cybersecurity Act für das Assurance Level „high“ und damit die besonders sicherheitsrelevanten Bereiche – wie beispielsweise der Konformitätsbewertung von 5G-Netzwerkinfrastrukturkomponenten – nicht dem BSI übertragen werden. Zugleich ist aber zu beachten, dass auch die Kombination mehrerer Produkte der Assurance Levels „low“ und „substantial“ zu dem Assurance Level „high“ für das Gesamtsystem führen können. Durch Zergliederung des Gesamtsystems darf nicht der Schutzzweck insgesamt unterlaufen oder umgangen werden. Es ist

daher erforderlich, klarzustellen, dass neben der Betrachtung der Komponenten auch der Zusammenhang oder das Gesamtsystem, in dem sie eingesetzt werden, betrachtet werden müssen.

Mit Blick auf § 3 Abs. 1 Satz 2 Nr. 14 erscheint es zweifelhaft, inwieweit das BSI den ihm übertragenen Auftrag zur Beratung, Information und Warnung, insbesondere von Herstellern, Vertreibern und Anwendern unter Berücksichtigung der hierfür notwendigen Fachkenntnisse im Kontext der relevanten Branchen, zu erfüllen vermag. Sollte das BSI hierfür die notwendigen personellen Ressourcen vorhalten können, sollte aus Sicht der deutschen Industrie das BSI nicht lediglich eine risikodarstellende Beratung vornehmen, sondern ebenfalls eine Beratung im Hinblick auf die aus Sicht des BSI angemessenen Sicherheitsvorkehrungen anbieten. Dies könnte die tatsächliche Anhebung des Sicherheitsniveaus in der Breite bewirken. Angesichts des bekannten Fachkräftemangels, besonders im Bereich der IT, stellt sich der Industrie zudem die Frage, wie das BSI den im § 3 Abs. 1 Satz 2 Nr. 14 BSIG statuierten gesetzlichen Auftrag der Beratung von Herstellern und Anwendern tatsächlich erfüllen kann. Zudem sind die Pflichten des BSI zu konkretisieren, beispielsweise wie schnell das BSI zu warnen hat.

Der BDI spricht sich daher für folgende Änderungen des Gesetzestextes aus:

„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 ~~*besonderer*~~ Berücksichtigung der möglichen Folgen fehlender oder unzureichender Sicherheitsvorkehrungen *sowie zur Erreichung eines ausreichenden Sicherheitsniveaus*;“

Mit Blick auf die Entwicklung von Anforderungen an Identifizierungs- und Authentisierungsverfahren (§ 3 Abs. 1 Satz 2 Nr. 19) empfiehlt sich eine Abstimmung der Verfahren mit der Anwender- und Herstellerindustrie, um nicht an den tatsächlichen Bedarfen vorbei zu entwickeln. Es ist unklar, ob und in welchem Maße, die vom BSI veröffentlichten Anforderungen an Identifizierungs- und Authentifizierungsverfahren Anspruch auf Verbindlichkeit besitzen und inwieweit die Durchsetzung dieser Anforderungen unter Zugrundelegung der EU-Binnenmarktharmonisierung europarechtskonform umgesetzt werden kann.

Der BDI spricht sich daher für folgende Änderungen des Gesetzestextes aus:

„19. Empfehlungen für Identifizierungs- und Authentisierungsverfahren und Bewertung dieser Verfahren unter dem Gesichtspunkt der Informationssicherheit *und unter Berücksichtigung etablierter Markt- und Branchenstandards und dem Stand der Technik sowie dem Ziel, die Ergebnisse in die*

internationale Standardisierung nach Maßgabe der jeweiligen anwendbaren Bestimmungen einzubringen“

Die Entwicklung eines Stands der Technik durch das BSI ist abzulehnen (§ 3 Abs. 1 Satz 2 Nr. 20). Wichtig ist festzuhalten, dass ein Stand der Technik über das Handeln der Beteiligten (Entwickler und Hersteller) entsteht. Das BSI könnte sich lediglich bemühen, mit größtmöglicher Wahrscheinlichkeit den Stand der Technik zu beschreiben. Selbst wenn das gelungen ist, kann dieser aber schon am Tage nach der Veröffentlichung wieder überholt sein. Ob etwas Stand der Technik ist, kann immer nur aktuell und im Nachhinein im Einzelfall festgestellt werden. Folglich ist festzuhalten: „Stand der Technik“ ist keine deklaratorische Eigenschaft, sondern ein sich ergebender Zustand. Er ist laufenden Änderungen unterworfen, die der Regelsetzer nicht beeinflussen kann. Zudem bestünde die Gefahr, dass, wenn Deutschland national einen „Stand der Technik“ definieren würde, andere Länder ebenfalls einzelstaatlich den Stand der Technik definieren würden. Für weltweit agierende Konzerne würde dies bedeuten, dass sie ihre Produkte für jeden einzelnen Markt entwickeln und produzieren müssten, um den jeweiligen nationalen Anforderungen Rechnung zu tragen. Daher ist der Wortlaut von §3 Abs. 1 Satz 2 Nr. 20 abzulehnen. Es wäre vielmehr wünschenswert, wenn sich das BSI vermehrt in internationalen Standardisierungsgremien einbringen würde.

Der BDI spricht sich daher für folgende Änderungen des Gesetzestextes aus:

„20. Entwicklung und Veröffentlichung *sicherheitstechnischer Anforderungen an IT-Produkte unter Berücksichtigung etablierter Markt- und Branchenstandards und dem Stand der Technik mit dem Ziel, diese in die internationale Standardisierung nach Maßgabe der jeweiligen anwendbaren Bestimmungen einzubringen* ~~*eines Stands der Technik bei sicherheitstechnischen Anforderungen an IT-Produkte*~~.“

Zu § 4a „Kontrolle der Kommunikationstechnik des Bundes“

Mit Blick auf § 4a sieht der BDI die Notwendigkeit zur Klarstellung folgender Rechtsbegriffe:

- Zu Satz 1: Es empfiehlt sich, eine Präzisierung des Begriffs „mit Betriebsleistungen beauftragten Dritten“ vorzunehmen.

- Zu Satz 3: Hier sollte ebenfalls eine Präzisierung der „Dritten, die Schnittstellen zur Kommunikationstechnik des Bundes haben“, erfolgen. Es stellt sich die Frage, inwiefern Hersteller, die Schnittstellen zur Informationstechnik des Bundes haben (organisatorisch und/oder technisch), betroffen sind. Zudem bedarf es einer konkreteren

Definition, welche Schnittstellen unter den Anwendungsbereich des § 4a Satz 3 BSIG n.F. fallen.

Weiterhin ist den zu definierenden Dritten die Vertraulichkeit zuzusichern, da das Bundesamt Einblick in sehr weitgehende Informationen erhalten kann, die durchaus geschäftskritisch sein können, wenn sie z.B. Wettbewerbern bekannt würden.

Zu § 4b „Meldestelle für die IT-Sicherheit“

Der BDI begrüßt das grundsätzliche Vorhaben, das BSI zukünftig als zentrale Meldestelle mit einem umfassenden Überblick über die Cybersicherheitslage in Deutschland auszustatten. Damit hieraus ein Mehrwert für die deutsche Wirtschaft sowie weitere betroffene Stellen einhergeht, müssen jedoch folgende Punkte in den Gesetzesentwurf aufgenommen werden:

- Es gilt, die damit verbundenen Obliegenheiten des BSI detailliert im Gesetzestext zu definieren.

- Auf der Grundlage der schon gewonnenen Erfahrungen im Zusammenhang mit gesetzlichen Meldepflichten zu Informationssicherheitsvorfällen gehen Teile der deutschen Industrie davon aus, dass die Aktivitäten des BSI in Hinsicht auf die Entgegennahme, Analyse und Aufbereitung der so zugeleiteten Information über Sicherheitslücken oder Angriffsvektoren für die angeschlossenen Unternehmen zu kaum verwertbaren Erkenntnissen (sog. *actionable intelligence* i.S. des *Cyber Threat Management*) führen werden. Die deutsche Industrie sieht daher die dringende Notwendigkeit:
  - zukünftig die erhaltenen Informationen einzelfallbezogen zu beantworten,
  - zielgruppengerecht aufzubereiten und
  - in anonymisierter Form pro Quartal ein detailliertes Lagebild zu publizieren. Dieses gesamtdeutsche Lagebild muss mit der deutschen Wirtschaft sowie weiteren relevanten Stellen geteilt werden, um einen wichtigen Beitrag zur Stärkung der Cyberresilienz Deutschlands leisten zu können.

- Das BSI sollte in § 4b Nr. 1 verpflichtet werden, die erhaltenen Informationen binnen drei Tagen auszuwerten und in geeigneter Form, ohne Betriebs- und Firmengeheimnisse zu verletzen, mit anderen Wirtschaftsakteuren zu teilen, um dadurch die Weiterverbreitung von Schadsoftware sowie das Abstellen von potenziellen Angriffsvektoren zu fördern.

- Sollte das BSI durch Meldungen Erkenntnisse über Schwachstellen gewinnen, muss es diese Erkenntnisse unbedingt den betroffenen Unternehmen zukommen lassen und darf diese Schwachstellen nicht mit weiteren staatlichen Bedarfsträgern – auch nicht mit dem BMI oder über das BMI mit anderen staatlichen Stellen– für deren Tätigkeiten teilen. Nur zügig geschlossene Schwachstellen stärken die Cyberresilienz Deutschlands. Bis zu einer Schließung der Schwachstellen dürfen diese aber auch nicht öffentlich publik werden; dies würde dem Gedanken der Responsible Disclosure widersprechen. Nur dann, wenn ein Hersteller es ablehnt, die Schwachstellen in angemessener Frist zu schließen, wobei ihm Ermessensspielraum zukommt, sollte eine öffentliche Bekanntgabe möglich werden. Dies kann dadurch befördert und sichergestellt werden, dass das BSI seine Aufgaben auf der Grundlage wissenschaftlich-technischer Erkenntnisse nach den Anforderungen der jeweils fachlich zuständigen Ministerien durchführt.

- Der Meldeweg (direkt ans BSI oder über die jeweiligen Landesämter) muss im Gesetzestext spezifiziert werden. Der BDI spricht sich für eine direkte Meldung an das BSI aus.

- In § 4b Nr. 2 und 3 ist zudem das Wort „kann“ durch „muss“ zu ersetzen. Das BSI sollte die Pflicht haben, alle entsprechenden Informationen entgegenzunehmen. Im Doxxing-Skandal wurde deutlich, dass erst nach Bekanntwerden zahlreicher ähnlich gelagerter Fälle der Gesamtzusammenhang offensichtlich wurde. Schon daher darf dem BSI keine Selektion bei der Entgegennahme von Informationen zugestanden werden.

- Eine Weitergabe von Informationen nach § 4b Nr. 4 sollte speziell bei Produkten nur in Absprache mit dem Hersteller unter Beachtung von coordinated vulnerability disclosure (cvd) Prozessen erfolgen. Hierzu empfiehlt die deutsche Industrie die Berücksichtigung von ISO/IEC 29147:2018 Information technology – Security techniques — Vulnerability disclosure.

Darüber hinaus muss aus der Meldung auch seitens der meldenden Stelle eine Handlung erfolgen, welche dazu geeignet ist, die von der jeweiligen Sicherheitslücke ausgehende Gefahr entsprechend einzudämmen, etwa durch die Bereitstellung entsprechender Softwareupdates.

Zu § 5 Abs. 11 „Maßnahmen zur Abwehr von Gefahren für die Kommunikationstechnologie der Länder“

§ 5 Abs. 11 sieht vor, dass das BSI Maßnahmen zur Abwehr von Gefahren für die Kommunikationstechnologie der Länder bei IT-Dienstleistern und -anbietern, die entsprechende Leistungen für die Länder erbringen, durchführen darf. Hier sollte präzisiert werden, wie tiefgreifend diese Maßnahmen sein können. Die aktuelle Formulierung ließe beispielsweise die Möglichkeit zu, dass das BSI in das Unternehmen kommen und die Kontrolle über Entwicklung und Fertigung von Produkten übernehmen könnte. Zudem gilt es zu klären, wie die Haftung des BSI in solchen Fällen ausgestaltet wäre, wenn im Zuge dessen Maßnahmen angewiesen worden sind, die in anderen Bereichen geschäftsschädigend sind. Auch die Folgenbeseitigung bei im Ergebnis rechtswidrigen Maßnahmen ist ausdrücklich zu regeln; ein bloßer Verweis auf das hauptsächlich richterrechtlich entwickelte Instrument des allgemeinen öffentlich-rechtlichen Folgenbeseitigungsanspruchs reicht nicht aus. Dies ist besonders im Hinblick auf die zu Art. 74 Abs. 1 Nr. 25 GG ergangene Rechtsprechung wichtig.

Zu § 5a „Wiederherstellung der Sicherheit oder Funktionsfähigkeit informationstechnischer Systeme in herausgehobenen Fällen“

Die Rechte Dritter, die ggf. durch die vom BSI ergriffenen Maßnahmen zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems gleichfalls beeinträchtigt werden, finden in der Normfassung keine Beachtung. Es gilt zu klären, inwieweit das BSI auf der Grundlage der intensiv verwendeten unbestimmten Rechtsbegriffe („herausgehobener Fall“, „Maßnahmen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit … erforderlich sind …“) tatsächlich zu Eingriffen in die Rechtssphäre Dritter ermächtigt werden soll und wie die Folgenbeseitigung gestaltet ist.

§ 5b Abs. 1 sollte daher wie folgt lauten:
„(1) Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Stelle des Bundes oder eines Betreibers einer Kritischen Infrastruktur oder eines Unternehmens im besonderen öffentlichen Interesse nach § 2 Abs. 14 Nr. 1, 2 oder 3 um einen herausgehobenen Fall, so kann das Bundesamt auf Ersuchen der betroffenen Stelle oder des betroffenen Betreibers die Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind. *Soweit das Bundesamt erste Maßnahmen zur Schadensbegrenzung und Sicherstellung des Notbetriebes vor Ort ergreift, werden hierfür keine Gebühren oder Auslagen für*

die Tätigkeit des Bundesamtes erhoben. Hiervon unberührt bleiben etwaige Kosten für die Hinzuziehung qualifizierter Dritter.“

Nach dem aktuellen Entwurf entfallen im § 5b Abs. 1 die Sätze 2 und 3, wonach heute für Maßnahmen des Bundesamtes keine Gebühren und Auslagen verlangt werden sollen. Nach Ansicht des BDI sollten auch zukünftig „Maßnahmen zur Schadensbegrenzung und Sicherstellung des Notbetriebes vor Ort“ kostenfrei durch das BSI erfolgen.

Zu § 5c „Sicherheit und Funktionsfähigkeit informationstechnischer Systeme im Falle erheblicher Störungen“

Der Referentenentwurf vernachlässigt bei der Erarbeitung von Krisenreaktionsplänen durch das BSI gemeinsam mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und der jeweils zuständigen Aufsichtsbehörde des Bundes die Beteiligung einer wichtigen Akteursgruppe – die betroffenen Betreiber Kritischer Infrastrukturen, Unternehmen von besonderem öffentlichen Interesse sowie den Betreibern und den Lieferanten der Kritischen Komponenten. Die Sicherheit von Mitarbeitern, Stakeholdern, Maschinen, Anlagen und Prozessen sind den Unternehmen ein zentrales Anliegen. Viele Unternehmen verfügen schon heute über intern ausgearbeitete qualitativ hochwertige Krisenreaktionspläne. Es liegt im ureigenen Interesse dieser Unternehmen, dass die implementierten Krisenreaktionspläne und -prozesse dafür Sorge tragen, dass im Notfall die angemessenen Maßnahmen rechtzeitig durchgeführt werden.

Es gilt, die zu erarbeitenden Krisenreaktionspläne mit dem Fokus auf die relevanten Kommunikations- und Koordinierungsschnittstellen gemeinsam mit der Wirtschaft auszuarbeiten. Nur so kann eine reibungslose Reaktion auf Krisen gewährleistet werden, denn nur die betroffenen Unternehmen haben umfangreiche Kenntnisse ihrer Geschäftsprozesse und/oder kaufmännische, respektive unternehmerische Verantwortung. Die deutsche Industrie empfiehlt zudem, statt Krisenreaktionspläne zu erarbeiten, für die Schnittstelle zu Betreibern Kritischer Infrastrukturen und Betreibern weiterer Anlagen im besonderen öffentlichen Interesse Krisenkommunikationspläne zu erarbeiten. Solche Pläne könnten zusammen mit weiteren die IT-Sicherheit eines Unternehmens betreffenden Informationen in einer IT-Sicherheitsbilanz zusammengefasst und bei Bedarf für Aufsichtsbehörden bereitgehalten werden.

Die Einführung des § 5c Abs. 4 stellt einen wesentlichen Eingriff in unternehmerische Prozesse und die unternehmerische Entscheidungsfreiheit dar. Es ist ein wesentliches Eigeninteresse von Wirtschaftsunternehmen seine Systeme bestmöglich vor erheblichen Störungen zu schützen. Die Übertragung von Verantwortlichkeit im Sinne einer Pflicht zum

Informationsaustausch bis hin zu einer Weisungsbefugnis erhöht daher nicht das IT-Sicherheitslevel in den betroffenen Unternehmen: Die regelmäßige Überprüfung der implementierten Sicherheitsmaßnahmen durch Auditoren oder durch Zertifizierung sind dazu probate und bereits vielschichtig eingesetzte Instrumente.

Soweit § 5c Abs. 4 Nr. 2 BSIG-E. die Verpflichtung des Betroffenen zur Herausgabe von Informationen an das BSI anordnet, bietet die Norm hierfür keine hinreichende Ermächtigungsgrundlage, da zum einen die Art der abverlangten Informationen aufgrund der verwendeten unbestimmten Rechtsbegriffe auf Tatbestandsseite schon zu unspezifisch formuliert wurde und zum anderen die hierdurch beeinträchtigten Rechtsgüter, die durch das Gesetz zu schützenden Rechtsinteressen regelmäßig überwiegen. Auch ist aus der Gesetzbegründung nicht erkennbar, inwieweit Rechtsgüter Dritter und deren rechtliche Verankerung in einschlägigen Normen (bspw. Geschäftsgeheimnisgesetz) vom BSI zum Gegenstand einer vorrangigen Abwägung gemacht werden müssen, bevor eine Informationsanforderung gegenüber einem Betroffenen ausgesprochen wird.

Der Begriff der „Reaktionsmaßnahmen des Bundes“ sollte definiert werden. Eingriffsbefugnisse des Bundes gegenüber KRITIS-Betreibern dürfen hieraus nicht resultieren. Zumindest muss es bei der Zuständigkeit des BSI bleiben, um eine Spaltung der Verantwortlichkeiten auf mehrere Behörden sowie widerstreitende Pflichten zu unterbinden.

Detaillierte Informationen zu festgestellten Störfällen müssen aus Sicherheitsgründen beim Wirtschaftsunternehmen verbleiben. Unternehmen sollten grundsätzlich die Möglichkeit haben, IT-Beeinträchtigungen zunächst intern zu analysieren, Fehlerquellen aufzudecken und Gegenmaßnahmen einzuleiten, bevor sie freiwillig qualitativ aufbereitete Informationen über relevante Beeinträchtigungen mit Marktteilnehmern und Behörden teilen. Der Entwurf stellt aus Sicht der betroffenen Unternehmen auch nicht sicher, dass etwaige Daten nicht anderweitig vom BSI oder anderen Behörden genutzt oder weitergegeben werden.

Die Regelung in § 5c Abs. 4 Nr. 3 muss im Einklang stehen mit BImschG und den Erlaubnisauflagen nach §18 BetrSichV.

Der BDI spricht sich daher für folgende Änderung des Gesetzestexts aus:

„(1) Das Bundesamt stellt im Einvernehmen mit
1. dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, ~~und~~
2. der jeweils zuständigen Aufsichtsbehörde des Bundes und

3. *den Betreibern Kritischer Infrastrukturen nach § 2 Abs. 10 sowie den Unternehmen im besonderen öffentlichen Interesse nach §2 Abs. 14 Nummer 1 bis 3* einen Gesamtplan für die Reaktionsmaßnahmen des Bundes auf, um *die notwendigen Vorbereitungen und Koordinationsarbeiten für* die Aufrechterhaltung oder Wiederherstellung der informationstechnischen Systeme, Komponenten oder Prozesse bei Betreibern Kritischer Infrastrukturen oder Unternehmen im besonderen öffentlichen Interesse für den Fall einer erheblichen Störung im Sinne des § 8b Absatz 4 Nummer 2, die zu erheblichen Versorgungsengpässen oder Gefährdungen für die öffentliche Sicherheit führen können, sicherzustellen. Sofern nach Satz 1 keine zuständige Aufsichtsbehörde des Bundes benannt ist, ist das zuständige Ressort zu beteiligen.

(2) Der Gesamtplan soll die an der Krisenreaktion beteiligten Behörden, Betreiber Kritischer Infrastrukturen und Unternehmen im besonderen öffentlichen Interesse in die Lage versetzen, im Notfall unverzüglich Entscheidungen *innerhalb ihrer Verantwortungsbereiche* zu treffen und die erforderlichen Maßnahmen rechtzeitig durchzuführen. *Notfall-Entscheidungen der Betreiber Kritischer Infrastrukturen können je nach notwendiger Krisenreaktion von dem Gesamtplan abweichen.*“

Zu § 5d „Bestandsdatenauskunft“

§ 5d sieht vor, dass das BSI Bestandsdaten von TK-Dienstleistern anfordern darf, wenn es Kenntnis von Beeinträchtigungen der Sicherheit oder Funktionsfähigkeit von IT-Systemen Dritter erlangt hat und die direkte Kontaktaufnahme mit Dritten notwendig erscheint. Schon heute können zahlreiche Behörden solche Anfragen stellen, sodass diese weitere Möglichkeit nicht erschwerend wirkt. Wünschenswert wäre, dass sich das BSI entsprechend seines Vorbildcharakters zur Nutzung der Schnittstelle nach § 113 Abs. 5 Satz 2 TKG verpflichtet (ETSI-Schnittstelle), um die sichere und vertrauliche Datenübermittlung von und zu den Providern sicherzustellen. Die im ursprünglichen Entwurf vorgesehene Entschädigung nach § 23 JVEG ist wieder in den Gesetzestext aufzunehmen. Es ist kein Grund ersichtlich, warum in diesem Beauskunftungsfall, anders als in anderen Fällen, eine Entschädigung nicht vorgesehen sein soll. Eine nicht gerechtfertigte Ungleichbehandlung erscheint rechtlich problematisch.

Die Intensität des Eingriffs in die informationelle Selbstbestimmung der Betroffenen scheint, gemessen am intendierten Zweck der Norm, unverhältnismäßig zu sein. Hier bedarf es einer engeren Eingrenzung des Geltungsbereichs des § 5d.

Nach Ansicht des BDI sollte § 5d wie folgt ergänzt werde:

„*(3) … Für die Entschädigung der Diensteanbieter ist § 23 des Justizvergütungs-und -entschädigungsgesetzes entsprechend anzuwenden.*

(6) Die nach Absatz 1 bis 5 erhobenen und verarbeiteten Daten müssen nach Behebung der Beeinträchtigung der Sicherheit unverzüglich, jedenfalls innerhalb einer Woche, gelöscht oder mindestens unumkehrbar anonymisiert werden.“

Zu § 7 „Warnungen“

Die Warnung durch das BSI über Sicherheitslücken in Produkten (§7 Abs.1 Nr. 1 Satz 1 Zif a) sollte mit dem Produkthersteller kooperativ durchgeführt werden, siehe *Coordinated Vulnerability Disclosure* (z.B. ISO/IEC 29147:2018 Information technology –Security techniques – Vulnerability disclosure).

Der BDI empfiehlt, dass in §7 Abs.1 Nr. 1 Satz 1 Zif. a wie folgt geändert wird:

„a) *gemeinsam mit dem Produkthersteller entsprechend dem Coordinated Vulnerability Disclosure-Prinzip* Warnungen vor Sicherheitslücken in informationstechnischen Produkten und Diensten,“

Hersteller müssen grundsätzlich in einem angemessenen Zeitraum vor Veröffentlichung einer Warnung durch das BSI informiert werden, um entsprechende Lösungen zur Behebung der Sicherheitslücken in Produkten für Kunden anbieten zu können. Der BDI empfiehlt, dass in §7 Abs.1 Nr. 1 Satz 2 wie folgt geändert wird:

„Sicherheitsmaßnahmen sowie den Einsatz bestimmter Sicherheitsprodukte, informationstechnischer Produkte und Dienste empfehlen. Das Bundesamt kann zur Wahrnehmung der Aufgaben nach Satz 1 Dritte einbeziehen, wenn dies für eine wirksame und rechtzeitige Warnung erforderlich ist. Die Hersteller betroffener Produkte sowie Betreiber Kritischer Infrastrukturen nach § 2 Absatz 10 sind rechtzeitig vor Veröffentlichung der Warnungen zu informieren. Diese Informationspflicht besteht nicht, wenn hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks gefährdet wird-~~*oder wenn berechtigterweise davon ausgegangen werden kann, dass der Hersteller an einer vorherigen Benachrichtigung kein Interesse hat*~~. *Die Entscheidung, betroffene Hersteller nicht zu informieren, bedarf der schriftlichen Begründung, die den Herstellern nach Veröffentlichung der Warnung zur Kenntnis zu geben ist.* 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 hierfür sind insbesondere die besondere Gefährdung bestimmter Einrichtungen oder die besondere Zuverlässigkeit des Empfängers.“

Zu § 7a „Untersuchung der Sicherheit in der Informationstechnik“

Der Gesetzentwurf sieht vor, dass das BSI informationstechnische Produkte und Systeme untersuchen kann und ein Auskunftsrecht ggü. Herstellern, auch zu technischen Details, erhält. Die so gewonnenen Erkenntnisse darf das BSI weitergeben, veröffentlichen und die Öffentlichkeit darüber informieren, wenn ein Hersteller den Aufforderungen des BSI nur unzureichend nachkommt.

Aus dem Gesetzesentwurf sowie aus dessen Begründung geht nicht hervor, inwieweit der Gesetzgeber im Kontext des Auskunftsverlangens des BSI gegenüber Herstellern informationstechnischer Produkte eine sachgerechte Abwägung der Interessen der Allgemeinheit an der Sachverhaltsaufklärung sowie dem Interesse des in Anspruch genommenen Betroffenen an der Geheimhaltung von produkt- bzw. servicebezogenen Informationen vorgenommen hat. Insbesondere ist das Verhältnis der entsprechenden Auskunftsrechte zum GeschGehG gänzlich unklar. Mit Blick auf „Auskünfte, insbesondere auch zu technischen Details“ (§ 7a Abs. 2) muss der Gesetzgeber sicherstellen, dass das BSI ein Verfahren etabliert, welches, soweit technisch und prozedural möglich, den Schutz von Betriebs- und Geschäftsgeheimnissen gewährleistet und die Gefahr von Industriespionage minimiert.

Der BDI empfiehlt folgende Anpassung an § 7a Abs. 2:

„(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. Bei der Versendung des Auskunftsverlangens an einen Hersteller gibt das Bundesamt die Rechtsgrundlage, den Zweck des Auskunftsverlangens und die benötigten Auskünfte an und legt eine angemessene Frist für die Übermittlung der Auskünfte fest. Das Auskunftsverlangen enthält ferner einen Hinweis auf die in § 14 vorgesehenen Sanktionen. *Um den Schutz von Geschäfts- und Betriebsgeheimnissen des Herstellers nach Satz 1 zu wahren, nutzt das Bundesamt ein sicheres Verfahren zu Übermittlung von Daten. Ist dem Hersteller nach Satz 1 eine sichere Übermittlung auf elektronischem Wege nicht möglich, so gewährt dieser Einsicht an einem Ort, der sich unter der Kontrolle des Herstellers befindet und an dem der Hersteller die Sicherheitsbestimmungen festlegt.*“

Wenn Schwachstellen gemeldet werden, für die ein Patch zeitnah nicht verfügbar ist, darf eine externe Kommunikation nur in Absprache mit den Herstellern erfolgen, um Schäden für Kunden und Betreiber durch die Veröffentlichung von Angriffsmöglichkeiten zu vermeiden. Das BSI muss verpflichtet sein, dem Hersteller unverzüglich den Eingang der Meldung über die Beschreibung der Angriffsmöglichkeit sowie den Inhalt der vom BSI geplanten externen Kommunikation rechtzeitig vor deren Veröffentlichung mitzuteilen. Dem Hersteller muss angemessene Zeit eingeräumt werden, den Punkt zu beheben, bevor eine Veröffentlichung erfolgt.

In § 7a Abs. 4 erhält das Bundesamt weitreichende Befugnisse zur Weitergabe und Veröffentlichung von Kenntnissen. Das Bundesamt darf seine Erkenntnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung der Aufgaben nach § 3 Abs. 1 Satz 2 erforderlich ist. Es bedarf einer Konkretisierung der Zweckbindung hinsichtlich der weiterzugebenden und zu veröffentlichenden Informationen, damit sichergestellt ist, dass die Informationen – insbesondere zu Sicherheitslücken und Schadprogrammen – ausschließlich zur Erhöhung der IT-Sicherheit als auch der Cyberresilienz und für keinen anderen Zwecke genutzt werden. Weiter muss sichergestellt werden, dass Erkenntnisse des Bundesamtes vor einer Veröffentlichung den Betreibern von Kritischen Infrastrukturen nach Sektoren-Relevanz zur Verfügung gestellt werden, um eine Behebung von bis dahin unbekannten Sicherheitslücken vor Veröffentlichung zu gewährleisten.

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

Die deutsche Industrie lehnt es ab, dass das BSI zukünftig unkoordinierte Penetrationstests und RedTeaming-Aktivitäten auch auf IT-Infrastrukturen von KRITIS-Betreibern durchführen darf (§ 7b Satz 1). Dies birgt potenziell große Gefahren und könnte im schlimmsten Fall die Sicherheit und Verfügbarkeit der Kritischen Infrastrukturen gefährden. Zudem müsste ex ante geklärt werden, wer für Betriebsausfälle und weitere Schäden, die durch Maßnahmen des BSI zur Detektion von Schadprogrammen, Sicherheitslücken und anderen Sicherheitsrisiken in öffentlich erreichbaren informationstechnischen Systemen ausgelöst werden, haftet. Hier muss die Haftung bei der Bundesrepublik Deutschland liegen.

Dieser Positionierung Rechnung tragend, sollte § 7b wie folgt ergänzt werden:

„(3a) Sollte durch Maßnahmen nach Absatz 1 dem Betreiber einer Kritischen Infrastruktur oder einem anderen Unternehmen Schäden entstehen, so haftet der Bund den Betreibern für diese Schäden sowie für Folgeschäden.“

Es wäre vielmehr zu begrüßen, dass das BSI zukünftig verstärkt die Zuverlässigkeit und Unabhängigkeit von IT-Dienstleistern zertifiziert. Entsprechend bereits laufende Ansätze, wie die Zertifizierung von Penetrationstestern, sollten ausgebaut werden. Sodann könnten Betreiber Kritischer Infrastrukturen angehalten werden, regelmäßige Penetrationsteste durch unabhängige Dritte durchzuführen zu lassen. Die Ergebnisse könnten – auf freiwilliger Basis – dem BSI vorgelegt werden.

Im Fall der Detektion eines Schadprogramms, einer Sicherheitslücke oder eines anderen Sicherheitsrisikos in einem informationstechnischen System sollten KRITIS-Betreiber sowie Unternehmen im besonderen öffentlichen Interesse stets informiert werden (§ 7b Abs. 3).

Sollte der Gesetzgeber an seinem Vorhaben festhalten, so sollte das Ausnutzen von Schwachstellen und der Versuch dessen bei dem betreffenden Betreiber bzw. wirtschaftlichem Eigner vorab angemeldet und offengelegt werden, um im Gefahrenfall schnell reagieren zu können. Sämtliche bei Maßnahmen nach § 7b Abs. 1 erzielten Erkenntnisse sind unverzüglich mit dem betroffenen Wirtschaftsunternehmen zu teilen und anschließend alle übermittelten Daten inkl. Protokolldateien zu vernichten. Zugriffe sind wieder zu löschen.

Zu § 7c „Detektion zum Schutz der Mitglieder der Verfassungsorgane“

Die deutsche Industrie sieht es sehr kritisch, dass jene Bundesbehörde, die als Ansprechpartner der deutschen Industrie in Cybersicherheitsfragen dienen soll, dem Bundeskriminalamt Erkenntnisse über Schwachstellen übermitteln soll. Für die deutsche Industrie ist das BSI ein wichtiger und vertrauenswürdiger Partner und sollte dies auch zukünftig sein. Schon aus diesem Grund sieht es die deutsche Industrie kritisch, wenn das BSI als Bundesbehörde den Zielkonflikt zwischen IT-Sicherheit und innerer Sicherheit lösen soll.

Zu § 8 „Vorgaben des Bundesamtes“

§ 8 ermöglicht dem BSI, Mindeststandards für die Sicherheit der Informationstechnik des Bundes zu erarbeiten, die auch von öffentlichen Unternehmen, die mehrheitlich im vollen Eigentum des Bundes stehen und die IT-Dienstleistungen für die Bundesverwaltung erbringen, zu befolgen sind. Im Sinne einer klaren Kompetenzaufteilung begrüßt der BDI dieses Vorhaben. Allerdings muss im Sinne eines Level Playing Fields gewährleistet sein, dass vergleichbare Mindeststandards auch für private Unternehmen, die IT-Dienstleistungen für die Bundesverwaltung erbringen, gelten. Gleiches gilt

bzgl. der Weisungsbefugnis des BSIs gegenüber privaten Unternehmen, die IT-Dienstleistungen für die Bundesverwaltung erbringen.

Zu § 8a Abs. 1 und § 8b Abs. 3d Überprüfung der Vertrauenswürdigkeit der Beschäftigten“

Die Möglichkeit, dass KRITIS-Betreiber sowie Unternehmen im besonderen öffentlichen Interesse geeignete Prozesse vorsehen können, um die Vertrauenswürdigkeit der Beschäftigten zu überprüfen, ist ein richtiger Schritt. Staatliche Stellen müssen diese Möglichkeit unterstützen, z.B. indem Anträge auf Führungszeugnisse rasch bearbeitet werden. Hierfür müssen die notwendigen personellen Ressourcen vorgehalten werden. Eine entsprechende personelle Aufstockung der zuständigen Stellen ist unbedingt angezeigt. Darüber hinaus sind die Prozesse auch für ausländische Arbeitnehmer praxisgerecht zu gestalten; wir verweisen auf unsere Ausführungen in der Einleitung.

Zu § 8a „Sicherheit in der Informationstechnik von KRITIS“

Bei der Festlegung von Systemen zur Angriffserkennung durch das BSI gilt es, die entsprechenden sektorspezifischen Verfügbarkeiten von Technologien sowie Branchenstandards zu berücksichtigen. Es ist unklar, inwieweit die Technische Richtlinie zur Ausgestaltung des Einsatzes von Systemen zur Angriffserkennung durch das BSI so gestaltet werden soll, dass sie den individuellen Ansprüchen der betroffenen Unternehmen entspricht. Es gilt insbesondere, den jeweiligen Stand der Technik zu berücksichtigen. Andernfalls besteht die Gefahr, dass die Anforderungen an Systeme zur Angriffserkennung das Gebot der Verhältnismäßigkeit missachten. Somit bedarf es Ausnahmeregelungen für jene Branchen und Unternehmen, wo der Einsatz von Systemen zur Angriffserkennungen negative unternehmerische Implikationen nach sich zieht: In einigen Branchen, wie beispielsweise dem Energiesektor, würde der Einsatz einer entsprechenden Technologie sogar zum Verlust von Gewährleistungs- und Wartungsansprüchen führen. Daher gilt es, bei der Definition der entsprechenden Technologien, die Betreiber Kritischer Infrastrukturen sowie die Betreiber von Anlagen im öffentlichen Interesse einzubeziehen.

Die Anforderung, Daten „unverzüglich zu löschen, wenn sie nicht für die Vermeidung von Störungen nach Abs. 1 Satz 1 erforderlich sind“ ist praxisfern, daher sind angemessene Speicherfristen vorzusehen, die auch nachträglich eine Erkennung von Angriffen ermöglichen.

Bevor weiterführende Berichtspflichten an das BSI für Unternehmen eingeführt werden, sollte der Mehrwert, der sich aus einer Berichtspflicht gegenüber dem BSI für die IT-Sicherheit in den betroffenen Unternehmen ergibt,

belegt werden. Darüber hinaus ist auszuschließen, dass Doppelberichtspflichten (Meldung von Datenpannen einerseits, Meldungen an das BSI andererseits) entstehen, die nicht nur die Unternehmen unverhältnismäßig belasten, sondern im Ergebnis auch die Selbstbelastungsfreiheit, die ohnehin stark eingeschränkt ist, völlig entwerten würden.

Die Berichtspflichten müssen verhältnismäßig bleiben. Nur Daten zu meldepflichtigen Vorfällen sollten geteilt werden müssen.

Aus Sicht des BDI sollte Abs. 1a mindestens wie folgt angepasst werden, um die Einhaltung des Stands der Technik sicherzustellen:

„(1a) Die Verpflichtung der Betreiber Kritischer Infrastrukturen, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen nach Abs. 1 Satz 1 zu treffen, umfasst auch den Einsatz von Systemen zur Angriffserkennung. Die eingesetzten Systeme zur Angriffserkennung haben dem jeweiligen Stand der Technik zu entsprechen. Die Einhaltung des Standes der Technik wird vermutet, wenn die Systeme der Technischen Richtlinie des Bundesamtes in der jeweils geltenden Fassung *mindestens* entsprechen.“

Zudem sollte der oben genannte Begriff „Systeme zur Angriffserkennung“ hinreichend präzise im IT-Sicherheitsgesetz 2.0 definiert werden.

Aus Sicht des BDI sollte Abs. 1c wie folgt angepasst werden:

„(1c) Im Rahmen des Einsatzes von Systemen zur Angriffserkennung erhobene Daten, die für ~~*den Schutz vor Angriffen auf Informationstechnik oder*~~ die Aufklärung und Strafverfolgung eines Angriffs erforderlich sind, haben *bei Anzeige oder nach Aufforderung* die Betreiber den dafür zuständigen Behörden zu übermitteln.“

Zudem sollte der vorgeschlagene Abs. 3 Satz 4 gestrichen werden, da die dort genannte Liste vielfach hochsensible Informationen enthält, die nicht grundlos nach extern gegeben und an zentraler Stelle gesammelt werden sollten, da sonst potenziell Kritische Infrastrukturen deutlich vulnerabler würden. Aus dem RefE wird nicht klar, warum das BSI diese Informationen benötigt.

~~„Die Betreiber übermitteln dem Bundesamt dabei zusätzlich eine Liste aller IT-Produkte, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen von Bedeutung sind, weil Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit dieser IT-Produkte zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit~~

~~einer Kritischen Infrastruktur oder zu einer Gefährdung der öffentlichen Sicherheit und Ordnung führen können.“~~

Zu § 8b Abs. 2 „Krisenkommunikationssystem“

Betreiber Kritischer Infrastrukturen erhalten nach § 8 Abs. 2 zukünftig Anspruch auf Zugang zu einem einheitlichen Krisenkommunikationssystem. Ein einheitliches Krisenkommunikationssystem im Sinne des § 8b Abs. 2 BSIG-E existiert derzeit nicht, wird jedoch, sofern es gemeinsam mit den Betreibern Kritischer Infrastrukturen entwickelt und an deren Bedarfen ausgerichtet wird, grundsätzlich begrüßt. Um eine effektive, technologieneutrale Einbindung eines einheitlichen Krisenkommunikationssystems in die Abläufe der Unternehmen zu gewährleisten, sollten klare Anforderungen an die Daten- und Kommunikationsstrukturen gestellt werden. Diese sollten zeitnah mit den Betreibern Kritischer Infrastrukturen entwickelt werden. Weiter bleibt unklar, ob Betreibern Kritischer Infrastrukturen der Zugang und die Nutzung des einheitlichen Krisenkommunikationssystems unentgeltlich möglich sein wird. Dies gilt besonders, da davon auszugehen ist, dass im Zuge der fortschreitenden Implementierung aus der Anspruchsberechtigung ein Verwendungszwang für KRITIS-Betreiber erwachsen wird.

Aus Sicht des BDI ist folgender Satz in Abs. 2 zu ergänzen:

„ … Abfrage der technischen Anforderungen an das Krisenkommunikationssystem sowie Zugang und Nutzung des einheitlichen Krisenkommunikationssystems ist für Betreiber Kritischer Infrastrukturen unentgeltlich möglich.“

Zu § 8b Abs. 3 und 3a „Registrierung von Kritischen Infrastrukturen beim BSI“

§ 8b Abs. 3 und 3a IT-SiG 2.0 definiert die Aufgaben des BSI und die sich daraus ergebende Kooperation mit Betreibern Kritischer Infrastrukturen. Außerdem regelt es den Registrierungsprozess durch Betreiber Kritischer Infrastrukturen beim BSI.

Es ist unklar, welchen Mehrwert die Regelungen nach Abs. 3 und 3a gegenüber dem bisherigen Registrierungsprozess haben soll. Zudem erscheinen die relativ geringen rechtlichen Anforderungen an die Annahme, dass ein Betreiber seine Pflicht zur Registrierung nicht erfüllt, gegenüber dem sehr weitgehenden Eingriff in die unternehmerische Selbstbestimmtheit als unverhältnismäßig. Grundsätzlich könnte hiervon jedes Unternehmen betroffen sein – auch ohne dem Anwendungsbereich des IT-SiG 2.0 zu unterliegen. Daher muss hier der Mechanismus mindestens über Ansprache und Stellungnahmen der potenziell betroffenen Unternehmen die Wahrung der Eigeninteressen gewährleisten.

Die Weitergabe unternehmensinterner Informationen und die daran geknüpfte Möglichkeit des BSI, sich von nahezu allen Unternehmen für eine KRITIS Bewertung erforderliche Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vorlegen zu lassen, widerstrebt dem Eigeninteresse eines jeden Wirtschaftsunternehmen, seine internen betriebssensiblen Informationen zu sichern und nicht nach außen zu geben. Es ist unklar, wie der Geheimschutz der relevanten Informationen gewährleistet werden soll.

Zu § 8b Abs. 3b und 3c „Registrierung von Unternehmen im besonderen öffentlichen Interesse beim BSI“

Durch § 8b Abs. 3b werden Unternehmen im besonderen öffentlichen Interesse nach § 2 Abs. 14 Nr. 1 und 2 verpflichtet, sich beim BSI zu registrieren und eine zu den üblichen Geschäftszeiten erreichbare Stelle zu benennen. Unternehmen im besonderen öffentlichen Interesse nach § 2 Abs. 14 Nr. 3 hingegen bleibt es freigestellt, ob sie sich beim BSI registrieren oder nicht.

Ein Vorteil aus der Registrierung beim Bundesamt könnte für Unternehmen im besonderen öffentlichen Interesse daraus erwachsen, dass sie regelmäßig Lagebilder zu IT-Sicherheit erhalten. Die Erfahrungen aus dem IT-Sicherheitsgesetz zeigen jedoch, dass das Bundesamt vielfach keine unterjährigen, branchenspezifischen Lagebilder veröffentlicht. Erst wenn das Bundesamt die regelmäßige Veröffentlichung von branchenspezifischen Lagebildern erfüllen kann, wäre eine Ausweitung von Registrier- und Meldepflichten zielführend. Aus dem aktuellen Gesetzentwurf geht in keinster Weise hervor, welche Vorteile sich für Unternehmen im besonderen öffentlichen Interesse nach § 2 Abs. 14 Nr. 1, 2 und 3 aus der Registrierung beim BSI ergeben. Zudem sind sie *per definitionem* keine Kritische Infrastruktur und sollten somit auch nicht ähnlich umfangreiche Pflichten erfüllen müssen.

Dem Rechnung tragend, schlägt der BDI folgende Anpassung an § 8b vor:
„3b) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 ~~*Nummer 1 und 2 sind verpflichtet, sich beim Bundesamt zu registrieren und eine zu den üblichen Geschäftszeiten erreichbare Stelle zu benennen. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Stelle.*~~
~~*(3c) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 3*~~ können eine freiwillige Registrierung beim Bundesamt und Benennung einer zu den üblichen Geschäftszeiten erreichbaren Stelle vornehmen. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese benannte Stelle.“

Zu § 8b Abs. 4a und 4b Meldung von Störungen durch Unternehmen im besonderen öffentlichen Interesse nach § 2 Abs. 14 Nr. 1 & 2

Durch § 8b Abs. 4a werden Unternehmen im besonderen öffentlichen Interesse nach § 2 Abs. 14 Nr. 1 und 2 zur sofortigen Meldung von Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer IT-Systeme, Komponenten oder Prozesse verpflichtet, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Wertschöpfung geführt haben und führen können. Unternehmen im besonderen öffentlichen Interesse nach § 2 Abs. 14 Nr. 3 sind zu einer unverzüglichen Meldung von (§ 8b Abs. 4b) Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse verpflichtet, die zu einer erheblichen Gefahr für die öffentliche Sicherheit und Ordnung geführt haben oder führen können. Dieses Vorhaben weist die deutsche Industrie als völlig unverhältnismäßig zurück, insbesondere da dies sowohl Unternehmen nach § 2 Abs. 14 Nr. 1 und 2 betrifft, obwohl nur Unternehmen nach Nr. 2 wegen ihrer Wertschöpfung behördenseitig ausgewählt wurden.

Zudem sind die Begriffe „Störung“ und „erhebliche Störung“ “, insbesondere im Kontext einer Beeinträchtigung der Erbringung der Wertschöpfung, nicht definiert, wodurch es an Rechtsklarheit für die betroffenen Unternehmen fehlt. Um Unternehmen Rechtssicherheit hinsichtlich Meldepflichten einzuräumen, müssten in § 2 beide Begriffe hinreichend genau bestimmt werden.

Unternehmen sollten grundsätzlich die Möglichkeit haben, IT-Beeinträchtigungen zunächst intern zu analysieren, Fehlerquellen aufzudecken und Gegenmaßnahmen einzuleiten, bevor sie anschließend freiwillig qualitativ aufbereitete Informationen über relevante Beeinträchtigungen mit Behörden teilen. Die Verpflichtung eines Unternehmens zur unverzüglichen Meldung einer Störung schränkt den für die Analyse der Störung notwendigen Zeitrahmen enorm ein, sodass eine Evaluation, ob überhaupt eine Beeinträchtigung für die Wertschöpfung vorliegt, nur erschwert erfolgen kann. Der Entwurf stellt aus Sicht der betroffenen Unternehmen nicht sicher, dass etwaige hochsensible Daten nicht anderweitig vom BSI oder anderen Behörden genutzt oder weitergegeben werden.

Da Unternehmen im besonderen öffentlichen Interesse nach § 2 Abs. 14 Nr. 1, 2 und 3 keine Kritischen Infrastrukturen sind, sollten diese keine Verpflichtung zur Meldung von Störungen haben, sondern vielmehr dazu angehalten werden. Unternehmen im besonderen öffentlichen Interesse nach § 2 Abs. 14 Nr. 1, 2 und 3, die die Möglichkeit zur Meldung von Störungen der Verfügbarkeit, der Integrität, der Authentizität und der Vertraulichkeit ihrer

informationstechnischen Systeme, Komponenten oder Prozesse Gebrauch machen, sollten hieraus Vorteile ziehen können.

Der BDI empfiehlt folgende Anpassung an den Absätzen 4a und 4b:

„(4a) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1 und 2 ~~*haben*~~ *sind angehalten* die folgenden Störungen ~~*unverzüglich*~~ an das Bundesamt zu melden …“

„(4b) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 3 ~~*haben*~~ *sind angehalten* die folgenden Störungen ~~*unverzüglich*~~ an das Bundesamt zu melden …“

Zu § 8e „Auskunft des BSI an Dritte“

Nach dem Entwurf bezieht sich das Auskunftsrecht auf jeden Dritten. Für eine sachgerechte Entscheidung über die Auskunftserteilung ist eine Abwägung der Interessen der Betreiber und der Dritten erforderlich. Dritte müssen daher ein berechtigtes Interesse an der Auskunftserteilung haben und dieses schriftlich darlegen müssen. Ohne berechtigtes Interesse sollte keine Auskunft erteilt werden müssen. Das Interesse des Dritten muss das Interesse des KRITIS-Betreibers deutlich überwiegen. Zudem sind die Betreiber vor einer Entscheidung über die Auskunft über die Person des Dritten sowie den Antragsgrund und die Interessendarlegung zu informieren und anzuhören. Der Schutz von Geschäftsgeheimnissen ist zu wahren.

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

Unternehmen im besonderen öffentlichen Interesse nach § 2 Abs. 14 Nr. 1 und 2 sind verpflichtet, ein umfassendes IT-Sicherheitskonzept beim Bundesamt vorzulegen. Die Forderung zur Einreichung eines IT-Sicherheitskonzeptes in deutscher Sprache, das die Informationstechnischen Systeme, Komponenten und Prozesse vor dem Hintergrund der Wertschöpfung des Unternehmens abbildet, lässt sich aufgrund der immer weiter wachsenden Komplexität moderner Wertschöpfungsketten nicht anwenderorientiert umsetzen. Dies zeigt sich zum Beispiel in der wachsenden Zahl eingebundener Partner oder externer Dienstleister in den Wertschöpfungsketten. Ein sich derart orientierendes IT-Sicherheitskonzept hätte wenig Mehrwert für das Sicherheitsniveau der betroffenen Unternehmen und auch nur bedingt Aussagekraft über die organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen. Zudem lässt § 8f Abs. 1 völlig offen, in welchem Detailgrad und welcher Detailtiefe „Systeme, Komponenten und Prozesse“ im Rahmen eines IT-Sicherheitskonzepts aufgelistet werden sollen.

Aus Sicht der deutschen Industrie ist zudem unklar, warum gerade die Unternehmen im besonderen öffentlichen Interesse, also zumeist größeren Unternehmen, die eine eigene IT-Abteilung mit Cybersicherheitsspezialisten haben, ein IT-Sicherheitskonzept erarbeiten und beim BSI vorlegen müssen. Die Auswirkungen der Corona-Pandemie haben in den vergangenen Wochen verdeutlicht, dass gerade der Ausfall von kleineren Zulieferern weitreichende Auswirkungen auf Wertschöpfungsprozesse in größeren Unternehmen haben kann. Vielmehr sollten kleine Unternehmen, die nur sehr begrenzte Mittel für den Schutz der eigenen IT und OT aufwenden können, jedoch für die Wertschöpfungsketten von Unternehmen im besonderen öffentlichen Interesse von herausgehobener Bedeutung sind, durch das Bundesamt in ihren Bestrebungen, die eigene IT- und OT-Resilienz zu stärken, unterstützt werden. In diesem Zusammenhang sollte die Bundesregierung ihre vielfältig bereits existierenden Angebote (Transferstelle IT-Sicherheit in der Wirtschaft, Allianz für Cybersicherheit, etc.) stärker als bisher bündeln und zielgerichtet Unternehmen über deren Leistungsspektrum informieren. Dies würde die Cyberresilienz der deutschen Industrie signifikant verbessern.

§ 8f lässt zudem offen, welche Anforderungen an das IT-Sicherheitskonzept gestellt werden. Der BDI empfiehlt, ein IT-Sicherheitskonzept in dem aktuell vorgesehenen Umfang nicht einzuführen. Jedwedes Sicherheitskonzept sollte auf internationalen Standards, hier ISO 27001 nativ oder eine englischsprachige internationalisierte Form des BSI IT-Grundschutzes im Rahmen der EU, aufbauen. Des Weiteren muss der Gesetzgeber präzisieren, wann ein System „maßgeblich“ ist und wie das Gesetz den Begriff der „Wertschöpfung“ versteht.

Zu § 9a „Freiwilliges IT-Sicherheitskennzeichen“

Nach aktuellen Schätzungen wird es im Jahr 2022 797,6 Millionen vernetzte Geräte in Deutschland geben – zum Vergleich, 2017 waren es 464,5 Millionen. Jeder Verbraucher / jede Verbraucherin in Deutschland wird folglich circa 9,7 vernetzte Geräte besitzen – verglichen mit 5,7 im Jahr 2017.[1] Der Bundesverband der Deutschen Industrie begrüßt das grundsätzliche Ansinnen der Bundesregierung das Cybersicherheitsniveau eines Produktes für Verbraucherinnen und Verbraucher kenntlich zu machen. Eine harmonisierte Regelung für den EU-Binnenmarkt (inkl. Norwegen und Schweiz) vereinfacht die Umsetzung für international agierende Unternehmen und bietet einen besseren Ansatz zur Anhebung des Sicherheitsniveaus. Hersteller, die ihre Produkte auf dem Europäischen Binnenmarkt in Verkehr bringen, sollten mit einheitlichen Informationspflichten die Cyberresilienz ihres Produktes

[1] CISCO. 2019. Visual Networking Index: Forecast Highlights Tool. URL: https://www.cisco.com/c/m/en_us/solutions/service-provider/vni-forecast-highlights.html# (Zugriff: 5. März 2019)

kennzeichnen können. Nur so entsteht eine brauchbare Vergleichbarkeit der Informationen. Daher spricht sich der BDI *gegen die Einführung eines rein nationalen IT-Sicherheitskennzeichens* aus.

Der BDI spricht sich für die Einführung eines Kennzeichens zur Cyber- und IT-Sicherheit eines Produktes aus, welches sich an folgenden sieben Handlungsempfehlungen orientiert:

1. Einen europaweit harmonisierten Ansatz statt 27 einzelstaatliche Lösungen wählen
2. Transparente und international anerkannte Normen als Basis einer Konformitätsbewertung etablieren
3. Nur einen Standard pro Produktgruppe für Konformitätsbewertung verwenden
4. Konformitätsbewertung risikobasiert auswählen
5. Effiziente Marktaufsicht gewährleisten
6. IT-Sicherheitskennzeichen transparent und verbraucherverständlich ausgestalten
7. Verbrauchern das IT-Sicherheitskennzeichen umfassend erklären

Eine eindeutige, leicht verständliche und tagesaktuelle Information über die Cyberresilienz eines Produktes kann aus Sicht der Industrie ein geeigneter Weg sein, um die cybersicherheitsbezogene Qualität der im Einsatz befindlichen Produkte, verstanden sowohl als Hard- wie Software, nachhaltig zu verbessern. Der BDI empfiehlt, dass sich die Bundesregierung für ein mindestens europaweit gültiges, mindestens europaweit einheitliches, flächendeckend eingeführtes, leicht verständliches und mit einer effizienten Marktaufsicht umgesetztes IT-Sicherheitskennzeichen im Rahmen der deutschen Ratspräsidentschaft und darüber hinaus auf europäischer Ebene starkmacht.

Der BDI verweist mit Blick auf den Vorschlag, ein IT-Sicherheitskennzeichen einzuführen, auf das BDI-Positionspapier „IT-Sicherheitskennzeichen: Europaweit einheitliches Label produktgruppenübergreifend einführen“. Dieses steht auf der BDI-Homepage zum Download bereit: https://bdi.eu/publikation/news/it-sicherheitskennzeichen/

Zu § 9b „Untersagung des Einsatzes Kritischer Komponenten nicht vertrauenswürdiger Hersteller“

Betreiber Kritischer Infrastrukturen werden durch § 9b verpflichtet, den Einsatz Kritischer Komponenten dem BMI anzuzeigen (Abs. 1) und nur Kritische Komponenten von jenen Herstellern einzusetzen, die eine Garantieerklärung über ihre Vertrauenswürdigkeit ausstellen (Abs. 2). Die Garantieerklärung erstreckt sich dabei über die gesamte Lieferkette. Das BMI wird insbesondere unter Berücksichtigung überwiegend öffentlicher Interessen und

sicherheitspolitischer Erwägungen die Kriterien für die Garantieerklärung ausgestalten. Das BMI kann den Einsatz einer Kritischen Komponente untersagen (Abs. 3), wenn ein Hersteller entsprechend der Kriterien nach Abs. 4 nicht vertrauenswürdig ist. Eine Untersagung des Einsatzes weiterer bereits angezeigter (Abs. 5 Nr. 1) und eingebauter Komponenten (Abs. 5 Nr. 2) sowie aller Komponenten des entsprechenden Herstellers (Abs. 6) kann durch das BMI erfolgen.

§ 9b hat in seiner jetzigen Ausgestaltung unkalkulierbare Risiken für Investitionen von Betreibern Kritischer Infrastrukturen. Dies betrifft insbesondere die Möglichkeit, die Nutzung im Einsatz befindlicher Kritischer Komponenten nachträglich zu untersagen. Erschwerend kommt hinzu, dass sich die Garantieerklärung des Herstellers ggü. KRITIS-Betreibern auf die gesamte Lieferkette bezieht. Hier besteht Unklarheit wieweit der im IT-SiG 2.0 eingeführte Begriff Lieferkette gefasst ist. Es wird nicht genau spezifiziert, ob die gesamte Lieferkette bis zum Rohstoff oder nur in Bezug auf verbaute Komponenten als Lieferkette gemeint ist. Das Einholen einer Garantieerklärung über die gesamte Lieferkette hinweg gestaltet sich nochmals schwerer, wenn quelloffene Bestandteile eingesetzt werden. Bei „Open Source“ gibt es keinen Hersteller im Sinne des Gesetzes, der eine Garantieerklärung zur Vertrauenswürdigkeit abgeben kann, gleichwohl werden sie durchaus in nennenswertem Umfang eingesetzt. Es wird für KRITIS-Betreiber nahezu unmöglich sein, bei komplexen Hard-, Software- und Elektronik-Produkten globale Produktionsketten komplett nachzuvollziehen und für jede Komponente eine Garantieerklärung einzuholen. Die hierfür notwendigen Aktivitäten seitens der KRITIS-Betreiber in Beschaffung, Vertragsverhandlungen und Überprüfung würden zu signifikanten zusätzlichen Aufwänden führen. Daher sollten Art und Umfang der „Garantieerklärung“ und deren Wirkung über die gesamte Lieferkette im IT-SiG 2.0 deutlich konkretisiert und auch der Umgang mit quelloffenen Bestandteilen beschrieben werden.

Die Anzeige des Einsatzes einer Kritischen Komponente bringt unüberschaubaren bürokratischen Aufwand mit sich und wird in der Praxis nicht zu leisten sein. Die zentrale Speicherung derartiger sicherheitsrelevanter Informationen birgt zudem ein enormes Sicherheitsrisiko. Der BDI empfiehlt, auf Anzeige und Speicherung der Informationen zu verzichten.

Die Einholung der Garantieerklärung in der im Entwurf gewählten Ausgestaltung enthält keinen Mehrwert. Es ist davon auszugehen, dass alle Hersteller diese Erklärung abgeben werden, auch solche, die von Beginn an in Schädigungsabsicht handeln oder liefern. Die Kontrolle der Einhaltung der Garantieerklärung ist kaum möglich. Insbesondere Informationen zu einer etwaigen Zusammenarbeit mit ausländischen Geheimdiensten oder zu Industriespionage werden vielfach nur auf Basis nachrichtendienstlicher

Ermittlungen beschaffen werden können. Dies darf nicht von den KRITIS-Betreibern verlangt werden.

Zudem wäre zu klären, ob Betreiber Kritischer Infrastrukturen, in denen Kritische Komponenten von nicht-vertrauenswürdigen Herstellern verbaut sind, die betroffenen Bereiche ihrer Kritischen Infrastruktur abschalten müssten – und wenn ja, in welcher Frist. Eine entsprechende Pflicht zum Abschalten einer Kritischen Infrastruktur könnte weitreichende Auswirkungen auf die Versorgung der Bevölkerung mit der Dienstleistung dieser Kritischen Infrastruktur – einschließlich Strom, Wasser und Telekommunikationsdienstleistungen – haben. Solch eine Regelung wäre insbesondere in jenen Fällen problematisch, in denen es nur sehr wenige Hersteller gibt, die vergleichbare Kritische Komponenten produzieren. Die Aberkennung der Vertrauenswürdigkeit eines Herstellers dieser Kritischen Komponente könnte zu einem Engpass bei Ersatzteilen führen und zudem die Wartung und den Bau dieser Kritischen Infrastruktur massiv verteuern.

Der Gesetzgeber verschiebt mit dem vorgeschlagenen § 9b lediglich die Entscheidung über den Einsatz von Komponenten bestimmter Anbieter beim Ausbau des 5G-Netzes. Aus Sicht der deutschen Industrie ist dies der falsche Ansatz. Im Rahmen des Gesetzgebungsprozesses zum IT-SiG 2.0 sollte direkt geklärt werden, welche Kritischen Komponenten von welchen Herstellern eingesetzt werden dürften. Nur so wird die dringend benötigte Rechts- und Investitionssicherheit geschaffen, um den Ausbau von öffentlichen 5G-Netzen zügig voranzutreiben. Zudem sollte geklärt werden, dass die Garantieerklärung sowie jedwede Untersagung des Einsatzes von Komponenten sich ausschließlich auf Kritische Infrastrukturen nach § 2 Abs. 10 erstreckt. Unternehmen, die z.B. 5G-Campusnetze betreiben, sollten nicht unter den Anwendungsbereich von § 9b fallen, da es sich bei Campusnetzen um nicht-öffentliche Netze handelt.

Da vielfach nicht nur ein Ressort, sondern auch eine Aufsichtsbehörde für Betreiber Kritischer Infrastrukturen maßgeblich ist, sollte das BMI nur im Einvernehmen mit der jeweiligen Aufsichtsbehörde und unter Konsultation des Betreibers einer Kritischen Infrastruktur den Einsatz einer Kritischen Komponente untersagen dürfen.

Zudem werden bereits bei verschiedenen Zulassungsprozessen – beispielsweise bei Produkten für die Telematikinfrastruktur und damit für den KRITIS-Bereich eHealth – im Zulassungsprozess genau die Herkunft von Komponenten ausführlich gefordert. Es ist nicht auszuschließen, dass Hersteller gleiche Anforderungen doppelt erfüllen müssen, zum einen in der Garantieerklärung und parallel noch einmal bei bereits bestehenden Zertifizierungs- und Zulassungsanforderungen ihrer Produkte.

Der BDI empfiehlt daher folgende Anpassung an Abs. 3:

„(3) Ist der Anwendungsbereich des § 9b eröffnet, ist eine Feststellung nach § 9 Absatz 4 Nr. 2 entbehrlich. Zum Zwecke der Gewährleistung der nationalen Sicherheitsinteressen der Bundesrepublik Deutschland prüft das Bundesministerium des Innern, für Bau und Heimat stattdessen den Einsatz der Kritischen Komponente nach Absatz 1 in Hinblick auf die Vertrauenswürdigkeit des Herstellers und kann gegenüber dem Betreiber der Kritischen Infrastruktur im Einvernehmen mit den jeweils betroffenen Ressorts, *dem Einvernehmen mit der zuständigen Aufsichtsbehörde auf Bundesebene sowie unter Konsultation mit dem betroffenen Betreiber der Kritischen Infrastruktur und dem Hersteller der Kritischen Komponente* den Einsatz untersagen, wenn der Hersteller der kritischen Komponente nicht vertrauenswürdig ist."

Während Hersteller Kritischer Komponenten für einen bestimmten Zeitraum nach Inverkehrbringung ihrer Kritischen Komponenten Updates zur Verfügung stellen, weist die deutsche Industrie mit Blick auf Abs. 4 Nr. 4 darauf hin, dass solche Software-Updates nicht für einen unbegrenzten Zeitraum zur Verfügung gestellt werden. Somit kann es Schwachstellen geben, die Hersteller nicht beseitigen, da für die entsprechenden Kritischen Komponenten der zeitliche Rahmen, in dem Updates angeboten werden, überschritten ist. Wenn KRITIS-Betreiber diese Kritischen Komponenten weiter einsetzen, darf dies keine Auswirkungen auf die Bewertung der Vertrauenswürdigkeit des Herstellers Kritischer Komponenten haben. Hersteller Kritischer Komponenten müssen jedoch bei Vertragsabschluss gegenüber dem KRITIS-Betreiber darlegen, wie lange Updates angeboten werden. Bekannte bzw. bekannt gewordene Schwachstellen oder Manipulationen sind unverzüglich dem Betreiber der Kritischen Infrastruktur zu melden, auch nach Ablauf des Updatezeitraums. Dies sollte in Abs. 4 Nr. 4 berücksichtigt werden.

Mit Blick auf Abs. 4 Nr. 5 stellt die deutsche Industrie fest, dass Remote Service, Fernwartung, Condition-Monitoring oder ähnliche Funktionen, die schaltenden Zugriff beinhalten, jeweils theoretisch auch geeignet sind, missbräuchlich auf die Infrastruktur einzuwirken. Werden diese Funktionen entweder durch eigentlich berechtigte oder aber durch nichtberechtigte Personen missbräuchlich genutzt oder weisen sie schlichte technische Fehlfunktionen auf, dann kann dadurch ein Schaden verursacht werden. Damit wären nach dem Wortlaut alle Hersteller, die solche Funktionen in ihren Geräten anbieten, automatisch nicht vertrauenswürdig. Dies kann nicht gewollt sein. Viele dieser Dienste stellen den eigentlichen Mehrwert deutscher Industriekomponenten dar, und sie ermöglichen gerade den möglichst ununterbrochenen Betrieb und die rasche Störungsbeseitigung, die eben nicht mehr von der physikalischen Anwesenheit von Technikern vor Ort abhängen muss. Die darüber abgebildeten digitalen Dienstleistungen bilden den Mehrwert von

Industrie 4.0. Sollte dies beibehalten werden, ist die Forschung und Entwicklung sowie der weitere Einsatz von Komponenten für Industrie 4.0 in Gefahr.

Der BDI spricht sich daher für die Änderung von § 9b Abs. 4 Nr. 5 aus:

„5 die kritische Komponente über technische Eigenschaften verfügt, die *ohne ausreichende Sicherheitsmaßnahmen bei bestimmungswidrigem Gebrauch* geeignet sind, missbräuchlich auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können. Dies gilt nicht, wenn der Hersteller nachweisen kann, dass er die technische Eigenschaft *ordnungsgemäß abgesichert oder* nicht implementiert hat und er diese jeweils ordnungsgemäß beseitigt hat."

Da Betreiber Kritischer Infrastrukturen in den vergangenen Jahren in ihre Infrastrukturen investiert haben, bevor die entsprechenden Regelungen in Kraft getreten sein werden, müssen sie vor einer unzulässigen Überdehnung faktischer Rückwirkung geschützt werden. Schließlich greifen die Verpflichtung zur Einholung von Garantieerklärungen, Zertifizierungen und Anzeige des Komponenteneinsatzes erst nach In-Kraft-Treten des IT-SiG 2.0. Diesen Bedenken kann durch angemessene Übergangsfristen mind. 5-8 Jahren Rechnung getragen werden, um die Netzabdeckung sowie Ausbauverpflichtungen nicht zu gefährden.

Der BDI empfiehlt daher die Ergänzung von § 9b um einen Abs. 7:

„*(7) Die Verpflichtung zur Ausstellung einer Garantieerklärung sowie die Möglichkeit zur Untersagung des Einsatzes Kritischer Komponenten entsprechend der Absätze 1 bis 6 erstreckt sich nur auf Komponenten deren Einsatz nach In-Krafttreten des Zweiten Gesetzes zur Stärkung der Sicherheit in der Informationstechnik begonnen hat.*"

Die Untersagung der Nutzung bestimmter Herstellerkomponenten wird nach dem Entwurf auf in der Person des Herstellers liegenden Umständen gestützt, entfaltet aber die Wirkung im Ergebnis gegenüber dem KRITIS-Betreiber. Dieser hat keine Möglichkeit, Vorkehrungen zur Vermeidung einer solchen Anordnung zu treffen. Er ist jedoch derjenige, den die Folgen der Anordnung treffen, wenn er nicht zur Vorbereitung einer solchen Anordnung gehört oder beigeladen wird. Diese Betroffenheit verlangt einen dem Art. 19 Abs. 4 GG genügenden Rechtsschutz. Im Hinblick auf die Sicherstellung der Versorgung mit kritischen Services erscheint der Entwurf nicht zu Ende gedacht. Im Falle eines angeordneten Rückbaus von Komponenten muss die Funktionsfähigkeit der Kritischen Infrastruktur sichergestellt sein. Das bedingt ausreichende Fristen für den Rückbau sowie eine Sicherstellung der Finanzierung des Ersatzes der Komponenten. Andernfalls droht die Insolvenz der Betreiber sowie die Betriebsunterbrechung bei den Kritischen Infrastrukturbetreibern.

Es muss zudem sichergestellt werden, dass sich weder KRITIS-Betreiber noch Hersteller von Kritischen Komponenten langwierigen Rechtsstreitigkeiten ausgesetzt sehen.

Die deutsche Industrie fordert von der BReg, die Cyberresilienz Kritischer Infrastrukturen zu stärken, ohne die Rechts- und Investitionssicherheit für KRITIS-Betreiber zu mindern. Insgesamt hinterfragen zudem Teile der deutschen Industrie, inwiefern die Einführung von § 9b für alle Kritischen Infrastrukturen sinnvoll ist. Der § 9b wird schließlich vordergründig eingeführt, um den Einsatz von vertrauenswürdigen Netzwerkkomponenten in öffentlichen TK-Netzen zu befördern.

Zu § 10 Abs. 5 – „RVO zur Definition der Unternehmen im besonderem öffentlichen Interesse“

§ 10 Abs. 5 sieht vor, dass das BMI per Rechtsverordnung die unter § 2 Abs. 14 Nr. 2 fallenden Unternehmen definiert. Der BDI spricht sich für eine Definition von objektiven Kriterien zur Bestimmung von Unternehmen im besonderen öffentlichen Interesse direkt im Rahmen des Gesetzgebungsprozesses zum IT-Sicherheitsgesetz 2.0 aus. Das IT-SiG 2.0 sollte hinsichtlich seines Geltungs- und Anwendungsbereichs umgehend Klarheit schaffen.

Der BDI empfiehlt daher die Streichung von § 10 Abs. 5 und eine konkrete Benennung der einbezogenen Kriterien zur Identifizierung der betroffenen Unternehmen in § 2 Abs. 14 Nr. 2.

Zu § 14 „Bußgelder“

Paragraf 14 Abs. 1 IT-SiG 2.0 enthält einen Katalog von Ordnungswidrigkeiten. Bei Verstößen gegen die entsprechenden Bestimmungen können Bußgelder bis zu 20 Millionen Euro oder von zwei respektive vier Prozent des weltweiten Jahresumsatzes, je nachdem welcher Betrag höher ist, festgesetzt werden. Im Fall einer Ordnungswidrigkeit oder eines Cybersicherheitsvorfalls könnten die Bußgelder das betroffene Unternehmen massiv zusätzlich finanziell schädigen. Dies ist insbesondere von Bedeutung, da sich die Folgen von erfolgreichen Cyberangriffen für die deutsche Wirtschaft laut einer Bitkom-Studie aus dem Jahr 2019 ohnehin bereits auf Kosten von mehr als 100 Milliarden Euro im Jahr belaufen. Der Gesetzgeber übersieht mit der Einführung dieser Regelung, dass die Erhöhung der IT-Sicherheit ein wesentliches unternehmerisches Interesse der Verpflichteten darstellt. Dies gilt insbesondere hinsichtlich der bestehenden vertraglichen Pflichten gegenüber den Kunden der Verpflichteten, der Wettbewerbssituation im Markt sowie der Verantwortung gegenüber den Aktionären und Investoren. Die Bußgeldrahmen in der geplanten Ausgestaltung stellen zudem ein nahezu nicht zu kalkulierendes Kostenrisiko für die Verpflichteten dar.

Zudem sind viele Cybersicherheitsvorfälle DSGVO-relevant sind, wodurch es zu einer Kumulierung von Bußgeldern kommen könnte. Eine deutlich geringere Grenze für Geldbußen sollte angesetzt werden. Ein nationaler Alleingang würde zudem im Europäischen Binnenmarkt wettbewerbsverzerrend wirken. Grundsätzlich ist bei Cybersicherheit eine harmonisierte Betrachtung der Schutzziele für den europäischen Binnenmarkt und eine durch alle Partner und Beteiligte europäisch erarbeitete Umsetzung im Rahmen von EU-Normen der vorzugswürdige Weg.

2019 gab es zahlreiche Ransomware-Vorfälle in der deutschen Industrie. Der Schaden belief sich teilweise auf mehr als eine Million Euro pro Tag. Nicht selten standen die Produktionsanlagen vier bis sechs Wochen still. Die Überarbeitung des IT-Sicherheitsgesetzes bietet eine gute Gelegenheit, die Frage nach der Unterstützung der mittelständischen deutschen Industrie erneut zu diskutieren. Insbesondere das BSI muss in dieser Rolle gestärkt werden und sollte noch intensiver die konkreten Bedarfe der Unternehmen im Auge haben. Die Umsetzung von geeigneten Maßnahmen zum Schutz des Mittelstandes kann auch regional in enger Kooperation mit oder auch koordiniert durch die Bundesländer erfolgen.

Die im Entwurf in § 14 BSIG abgebildeten Bußgeldvorschriften sind zudem unverhältnismäßig und stehen in keinem angemessenen Verhältnis zum möglichen ordnungswidrigen Verhalten, wie beispielsweise einer versäumten Meldepflicht. So wird eine versäumte Meldepflicht eines KRITIS-Betreibers mit bis zu 10 Millionen Euro bestraft, während Verstöße gegen Regelungen nach § 9b nicht bußgeldbewehrt sind. Die Bußgeldvorschriften dürfen – hier ist ein Vergleich zu jenen in anderen EU-Mitgliedsstaaten heranzuziehen – nicht zu einer Bestrafung im Übermaß für hiesige Unternehmen führen (siehe zum auszugsweisen Vergleich die Tabelle unten). Sollte die Bundesregierung die Notwendigkeit zu einem Bußgeldrahmen sehen, so fordert die deutsche Industrie die Bundesregierung auf, einen Bußgeldrahmen zu entwickeln, der den jeweiligen Tatbeständen und dem sich durch sie verwirklichten Unrecht sowie der Prävention angemessene, gerechte Bußgelder einführt, die zugleich einen Fortbestand des jeweiligen Unternehmens ermöglichen.

Frankreich	loi n°2018-133	Opérateurs de Services Essentiels können mit Bußgeldern von 75.000 bis 125.000 Euro bestraft werden
Italien	Decreto Legislativo 18 maggio 2018, n.65 („NIS“)	*Operatori di servizio essenziale* sowie *fornitori di servizio digitale* können mit Bußgeldern von 12.000 bis 150.000 Euro bestraft werden, soweit der Anwendungsbereich der Verwaltungsstrafen (*sanzioni*

		amministrative) eröffnet und kein Straftatbestand erfüllt ist (Art. 21 Abs. 1 S. 1 1. HS NIS)
Niederlande	The Network and Information Systems Security Act	Abhängig vom Straftatbestand werden Bußgelder von ein bis fünf Millionen Euro fällig
Spanien	Royal Decree No.12/2018 on Network and Information System Security	Strafen bis zu 1 Millionen Euro

Vor diesem Hintergrund schlägt der BDI vor:

1. den angestrebten Maximalbußgeldrahmen von 20.000.000 signifikant zu senken, insbesondere da sonst die Gefahr besteht, dass eine ungewollte Bereinigung des Marktes um Marktteilnehmer nur deswegen eintreten würde, weil sich diese existenzbedrohenden Sanktionen ausgesetzt sehen könnten, nicht etwa aber, weil sie durch die Sanktion von unrechtmäßigem Handeln abgehalten werden würden Dies kann nicht im Sinne einer gerade auch mittelstandsgeprägten Wirtschaft gewünscht sein.
2. dass eine relative Höhe (von 2, respektive 4 % vom weltweiten Jahresumsatz) gänzlich gestrichen wird, da durch die Anknüpfung an den Umsatz Unternehmen mit geringeren Margen härter bestraft werden als Unternehmen mit hohen Margen. Es ist zu befürchten, dass die Bußgelder schnell eine existenzielle Bedrohung darstellen können.

Der BDI schlägt daher die Anpassung von § 14 Abs. 6 wie folgt vor:

„Verstöße gegen die Bestimmungen des Absatzes 1 ~~*Nummer 2, 6, 13 und 16*~~ können mit Geldbußen von bis zu ~~*20 000 000*~~ *XXX.XXX* EURO ~~*oder von bis zu 4 % des gesamten weltweit erzielten jährlichen Unternehmensumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist,*~~ geahndet werden. ~~*Verstöße gegen die übrigen Bestimmungen des Absatzes 1 können mit Geldbußen von bis zu 10 000 000 EURO oder von bis zu 2 % des gesamten weltweit erzielten jährlichen Unternehmensumsatzes des vorangegangenen Geschäftsjahrs, je nachdem, welcher der Beträge höher ist, geahndet werden.*~~“

§ 14 Abs. 7 BSIG sieht eine Privilegierung in Bezug auf die Ahndung von Ordnungswidrigkeiten für solche Anbieter vor, die ihre Hauptniederlassung nicht in einem EU-Mitgliedstaat haben, nicht in einem anderen EU-Mitgliedstaat niedergelassen sind, dort aber einen Vertreter benannt haben und in diesem Mitgliedstaat dieselben digitalen Dienste anbieten. Gründe für diese Privilegierung lassen sich dem Entwurf nicht entnehmen.

Zu Artikel 2 – Änderung des Telekommunikationsgesetzes

Angesichts der steigenden Zahl von personenbezogenen Daten, die unrechtmäßig verarbeitet und weitergegeben werden, sieht der Gesetzgeber die Notwendigkeit zur Verschärfung der Anforderungen im Telekommunikationsgesetz (TKG) vor. Aus Sicht der deutschen Industrie vergisst der Gesetzgeber jedoch den grundgesetzlich verbrieften Schutz des Fernmeldegeheimnisses. Im weiteren Gesetzgebungsprozess müssen die folgenden Punkte unbedingt berücksichtigt werden:

Zu § 109 „Technische und organisatorische Schutzmaßnahmen“

Nach der neuen Vorschrift sollen die Einzelheiten der nach den Abs. 2 Satz 1 bis 4 zu treffenden Maßnahmen sowie Einzelheiten der Festlegung kritischer Funktionen und der Bestimmung der Kritischen Komponenten nach Satz 5 von der BNetzA im Einvernehmen mit BSI und BfDI im Katalog von Sicherheitsanforderungen nach Abs. 6 festgelegt werden. Aus Sicht der Industrie besteht keine Veranlassung Maßnahmen detaillierter zu regeln, als in der aktuellen Fassung des TKG. Es ist nicht bekannt, dass die Praxis die Notwendigkeit detaillierterer Regelungen aufgezeigt hätte. Die Funktionsfähigkeit der Infrastruktur und der Services steht im ureigensten Interesse der Provider. Die Provider treffen alle notwendigen Vorkehrungen nach dem Stand der Technik, um Ausfall- und Angriffsrisiken zu minimieren. Ein Eingriff in die unternehmerische Freiheit bzgl. der Ausgestaltung solcher Maßnahmen ist daher weder erforderlich noch angemessen. Im Übrigen bestehen zudem rechtliche Bedenken, derlei grundrechtsintensive Regelungen in einer untergesetzlichen Regelung und nicht direkt im Gesetz zu regeln. Der BDI empfiehlt, den Passus aus dem RefE zu streichen.

Sollte der Gesetzgeber an der Weiterentwicklung des Sicherheitskatalogs als untergesetzliche Regelung festhalten, so sollte zu mindestens die Bestimmung der Kritischen Komponenten unter Anhörung und Beteiligung der KRITIS-Betreiber sowie der betroffenen Hersteller Kritischer Komponenten erfolgen, da nur sie über ausreichende Kenntnis bzgl. der Architektur und Funktionsweise der KRITIS-Technik und über die zu minimierenden Risiken verfügen. Der BDI schlägt daher folgende Formulierung vor:

„Nach Abs. 2 Satz 3 werden folgende Sätze eingefügt:
Der Umfang der Maßnahmen nach Satz 1 und 2 richtet sich nach dem jeweiligen Gefährdungspotenzial des öffentlichen Telekommunikationsnetzes oder öffentlich zugänglichen Telekommunikationsdienstes. Sicherheitsrelevante Netz- und Systemkomponenten, die kritische Funktionen erfüllen, (Kritische Komponenten) dürfen nur eingesetzt werden, wenn sie von einer anerkannten Prüfstelle überprüft und von einer anerkannten

Zertifizierungsstelle zertifiziert wurden. Die *Einzelheiten der nach den Satz 1 bis 4 zu treffenden Maßnahmen sowie Einzelheiten der* Festlegung kritischer Funktionen und der Bestimmung der Kritischen Komponenten nach Satz 5 legt die Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik und der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit *und im Einvernehmen mit den KRITIS-Betreibern sowie den betroffenen Herstellern Kritischer Komponenten* im Katalog von Sicherheitsanforderungen nach Absatz 6 fest."

Zu § 109a Abs. 1a „Meldungen an das Bundeskriminalamt"

Ein Erbringer öffentlich zugänglicher Telekommunikationsdienste hat das BKA über Vorfälle zu unterrichten, bei denen er feststellt, dass bei ihm gespeicherte Daten unrechtmäßig übermittelt oder auf sonstige Weise Dritten unrechtmäßig zur Kenntnis gelangt sind (§ 109a Abs. 1a). Eine Pflicht des Anbieters, solche Feststellungen zu treffen, folgt nach Ansicht der deutschen Industrie nicht aus dieser Vorschrift. Daher sind von dem Anbieter keine Erkundigungen einzuholen oder Recherchen anzustellen. Dies trifft nach Ansicht der deutschen Industrie auch in dem Fall zu, in dem zwar Anhaltspunkte für eine unrechtmäßige Nutzung vorliegen, die Unrechtmäßigkeit anhand dieser Anhaltspunkte jedoch nicht offenbar ist. Aus Gründen der Rechtssicherheit sollte dies ausdrücklich jedenfalls in der Gesetzesbegründung klargestellt werden.

Nach § 109a Abs. 1 besteht bereits im Fall einer Verletzung des Schutzes personenbezogener Daten unverzüglich eine Pflicht zur Meldung an die BNetzA und den BfDI. Aus Sicht der deutschen Industrie stellt sich die Frage, warum nicht die beiden Behörden entsprechende Meldungen und hieraus resultierende Erkenntnisse an das Bundeskriminalamt weitergeben. Im Sinne eines one-stop-shop-Prinzips sollten Diensteerbringer eine Verletzung des Schutzes personenbezogener Daten sowie von Cybersicherheitsvorfällen nur an eine zentrale Stelle melden müssen. Die so gemeldeten Informationen können dann von unterschiedlichen staatlichen Stellen verarbeitet werden.

Zudem ist die Umsetzbarkeit und Vereinbarkeit dieser Vorschrift mit den Rechtsstaatsprinzipien der Bundesrepublik zu hinterfragen. Die rechtliche Bewertung, ob eine Nutzung von Daten rechtmäßig oder rechtswidrig ist, setzt die Kenntnis des vollständigen Sachverhalts voraus. Hierfür wäre ein weitreichender Eingriff in das Fernmeldegeheimnis notwendig. Die Feststellung der Unrechtmäßigkeit setzt aufgrund der Schwierigkeit der rechtlichen Fragestellungen juristische Fachexpertise voraus, die die Verpflichteten in dem für solche Prüfungen erforderlichen Umfang nicht vorhalten können, um unverzügliche Meldungen an das BKA absetzen zu können.

Zudem sollte nicht die Unverzüglichkeit der Meldung an das BKA im Zentrum der Norm stehen, sondern das Abstellen eines womöglich unberechtigten Zugriffs auf „Telekommunikations- oder Datenverarbeitungssysteme“, um einen potenziellen weiteren Schaden für die Nutzer des Telekommunikations- oder Datenverarbeitungssystems zu verhindern.

Unter rechtsstaatlichen Gesichtspunkten ist anzumerken, dass die Ermittlung von Ordnungswidrigkeiten und Straftaten eine staatliche Aufgabe ist, die nicht in die Hände der Privatwirtschaft gelegt werden darf. Unsere Rechtsordnung sieht bislang eine Anzeige von Sachverhalten nur bei schwerwiegenden Straftaten, nicht aber leichten Straftaten und Ordnungswidrigkeiten, vor. Dieser Grundsatz wird mit dem Entwurf gebrochen. Zum Schutz vor Denunziation muss an diesem Grundsatz aber festgehalten und auf die Einführung einer solchen Meldepflicht verzichtet werden. Die Unverhältnismäßigkeit dieser Verpflichtung wird noch dadurch verstärkt, dass der Verstoß hiergegen gemäß § 149 Abs. 1 Nr. 21g TKG-E bußgeldbewehrt sein soll, wobei unklar ist, wann „hinreichende Anhaltspunkte“ vorliegen. Damit dürfte der Ordnungswidrigkeitentatbestand auch gegen das Bestimmtheitsgebot verstoßen (s. auch unten zu § 149 TKG-E).

Die deutsche Industrie schlägt die Streichung des § 109 Abs. 1a TKG vor.

Zu § 109a Abs. 8 „Maßnahmen des BSI zur Abwehr erheblicher Gefahren für die Kommunikationstechnik des Bundes, von KRITIS sowie Unternehmen im besonderen öffentlichen Interesse“

Zur Abwehr erheblicher Gefahren von der Kommunikationstechnik des Bundes, von Kritischen Infrastrukturen sowie Unternehmen im besonderen öffentlichen Interesse erhält das BSI zukünftig weitgehende Anordnungsbefugnisse gegenüber dem Diensteanbieter – einschließlich der Möglichkeit zur Anordnung zur Bereinigung betroffener Datenverarbeitungssysteme von einem konkret benannten Schadprogramm.

Anbieter haben selbst ein hohes Interesse an einem möglichst störungsfreien Betrieb ihrer Anlagen, um Leistungen gegenüber ihren Kunden vertragsgerecht erbringen zu können. Zudem verfügen die Anbieter über technische und organisatorische Fachkenntnisse zu ihren Anlagen, Diensten und Betriebsabläufen, die sie in die Lage versetzen, unverzügliche und angemessene Maßnahmen zur Störungsbeseitigung vornehmen zu können und die Störungsauswirkungen für Kunden möglichst gering zu halten. Diese Fachkenntnisse liegen dem Bundesamt heute nicht vor und können aus Gründen der Machbarkeit und des Aufwandes nicht erhoben werden. Vor diesem Hintergrund erscheint diese Eingriffsmöglichkeit weder hinsichtlich der Abwehr erheblicher Gefahren noch hinsichtlich des Interesses der Anbieter und der Kunden

bzgl. einer möglichst störungsfreien Nutzung von Diensten als sachgerecht. Auf die Aufnahme eines solchen Anordnungsrechts sollte daher verzichtet werden.

Zu § 110 Abs. 1a „Einrichtung von Prozessen sowie einer Stelle zur Annahme Auskunfts-, Bereitstellungs- oder Löschungsverlangen nach § 112 TKG“

Nach § 110 Abs. 1a müssen Betreiber von Telekommunikationsanlagen, über die öffentlich zugängliche Telekommunikationsdienste erbracht werden sowie Anbieter von Telekommunikationsdiensten im räumlichen Zuständigkeitsbereich der BNetzA Auskunfts-, Bereitstellungs- oder Löschungsverlangen nach § 112 TKG ausführen und hierfür eine Stelle zur elektronischen und postalischen Entgegennahme entsprechender Ersuche einrichten.

Zu § 149 Abs.1 „Bußgeldvorschriften“

Nach Ansicht der deutschen Industrie ist die angestrebte Erweiterung von § 149 Abs. 1 TKG viel zu weitreichend und teilweise unvereinbar mit dem strafrechtlichen Bestimmtheitsgebot. Auch hier wird übersehen, dass die Erhöhung der IT-Sicherheit ein wesentliches unternehmerisches Interesse der Verpflichteten darstellt. Dies gilt insbesondere hinsichtlich der bestehenden vertraglichen Pflichten gegenüber den Kunden der Verpflichteten, der Wettbewerbssituation im TK-Markt sowie der Verantwortung gegenüber den Aktionären und Investoren. Mangels Erforderlichkeit sollte von einer Erweiterung dieses Katalogs Abstand genommen werden. Wenigstens gilt es, die im Referentenentwurf aufgeführten Nr. 21g und 21j zu löschen.

Zu Artikel 3 – Änderung des Telemediengesetzes

Neben den Anpassungen am BSIG und am TKG sieht das Zweite IT-Sicherheitsgesetz auch einige wenige Änderungen am Telemediengesetz vor. In diesem Zusammenhang sind die entsprechenden Ausführungen zum TKG jeweils mit zu berücksichtigen.

Zu § 13 „Pflichten des Diensteanbieters“

Die Ausführungen zu § 109a Abs. 8 TKG gelten entsprechend. Auf die Aufnahme eines solchen Anordnungsrecht sollte daher verzichtet werden.

Sollte der Gesetzgeber die Aufnahme des Anordnungsrechts nach § 13 Abs 7a dennoch für notwendig erachten, so gilt es detailliert zu klären, wie die Haftung des BSI im Falle von geschäftsschädigenden Auswirkungen dieser Anordnungen geregelt ist. In diesem Fall schlägt der BDI folgende Anpassung an §13 Abs. 7a vor:

„Das Bundesamt für Sicherheit in der Informationstechnik kann zur Abwehr von Gefahren für die Kommunikationstechnik des Bundes oder eines Betreibers einer Kritischen Infrastruktur oder für ein~~e *Infrastruktur*~~ *Unternehmen* im besonderen öffentlichen Interesse gegenüber Diensteanbietern in begründeten Ausnahmefällen die Umsetzung erforderlicher technischer und organisatorischer Vorkehrungen zur Sicherstellung der Schutzgüter nach Absatz 7 Satz 1 anordnen, wenn hierdurch eine konkrete Gefahr für Datenverarbeitungssysteme einer Vielzahl von Nutzern durch unzureichend gesicherte Telemedienangebote beseitigt werden kann. *Das Bundesamt haftet für etwaige durch Anordnungen nach Satz 1 dieses Absatzes hervorgerufene Schäden der Kommunikationstechnik des Bundes oder eines Betreibers einer Kritischen Infrastruktur oder eines Unternehmens im besonderen öffentlichen Interesse.*“

Zu § 15 „Nutzungsdaten“

Die Ausführungen zu § 109a Abs. 1a TKG gelten entsprechend. Auf die Aufnahme einer solchen Vorschrift sollte verzichtet werden.

Zu § 15b „Pflichten der Diensteerbringer“

Diensteerbringer müssen nach § 15b Abs 1. TMG das BKA informieren, wenn über ihre Dienste rechtswidrig erlangte personenbezogene Daten oder Geschäftsgeheimnisse über seinen Dienst Dritten unrechtmäßig zur Kenntnis gegeben oder veröffentlicht werden. Zudem muss der Diensteerbringer nach Abs. 2 den Zugang zu diesen Daten sperren. Die Ausführungen zu § 109a Abs. 1a TKG gelten entsprechend. Überdies ist die vorgesehene Meldepflicht

im TMG an das Vorliegen weiterer auslegungsbedürftiger Voraussetzungen geknüpft („große Zahl von Personen“, „Datenbestand von großem Ausmaß“), die dem Normadressat eine rechtssichere Pflichterfüllung unmöglich machen. Entsprechendes gilt für die Sperrpflicht nach § 15b Abs. 2 TMG-E, die an das Vorliegen „zureichend tatsächlicher Anhaltspunkte“ geknüpft ist. unbestimmte Begriffe aufgenommen. Verstärkt werden die Bedenken an der Angemessenheit dieser Pflichten wiederum durch die geplante Bußgeldbewehrung (vgl. § 16 Abs. 2 Nr. 7 und Nr. 8). Auf die Aufnahme von § 15 b TMG-E sollte daher verzichtet werden.

Zu § 16 „Bußgeldvorschriften“

Die Ausführungen zu § 149 Abs. 1 TKG gelten entsprechend.

Zu Artikel 4 – Änderung der Außenwirtschaftsverordnung

Zu § 55 Abs. 1 Satz 2 Nr. 2 und Abs. 1 Satz 3

Das Zweite IT-Sicherheitsgesetz wird Auswirkungen auf den Anwendungsbereich der sektorübergreifenden Prüfung haben. So soll der Begriff der Software durch eine Aufzählung spezifischer Technologien präzisiert werden. Dazu soll in Satz 2 Nr. 2 von § 55 AWV das Wort „Software“ durch die Wörter „KRITIS-Komponenten nach § 2 Abs. 13 des BSI-Gesetzes in der jeweils geltenden Fassung“ ersetzt werden. Folglich könnte das BMWi zukünftig all jene Unternehmenserwerbungen und Unternehmensanteilserwerbungen von Unternehmen, die KRITIS-Komponenten fertigen, prüfen.

Die deutsche Industrie spricht sich grundsätzlich für den Schutz der digitalen technologischen Souveränität der deutschen Wirtschaft aus. Vor diesem Hintergrund scheint eine Anpassung des § 55 Abs. 1 der Außenwirtschaftsverordnung verständlich. Allerdings ist die im ersten Referentenentwurf des IT-Sicherheitsgesetzes 2.0 gewählte Änderung abzulehnen.

Eine Präzisierung der Kriterien für Überprüfungen von Direktinvestitionen aus Drittländern durch die Bundesregierung könnte die Rechtssicherheit für Investoren und Unternehmen erhöhen und wäre grundsätzlich im Interesse der deutschen Industrie. Die nun geplante Änderung der Außenwirtschaftsverordnung sieht jedoch keine Präzisierung, sondern vielmehr eine Erweiterung der zu prüfenden Wirtschaftssektoren vor. So soll künftig nicht nur Software, sondern IT-Produkte und damit auch Hardwarekomponenten, im Fokus der staatlichen Investitionsprüfungen stehen. Außerdem kommt zu den bisher sieben Software-Zielbranchen (Software- und IT-Hardware-Zielbranchen: Energie, Wasser, Nahrungsmittelversorgung etc.) eine neue achte Branche hinzu, nämlich die der „Anlagen und Systeme zur Abfallentsorgung“.

Offene Grenzen und Auslandsinvestitionen sind von großer Wichtigkeit für die international ausgerichtete deutsche Industrie. In Deutschland arbeiten mehr als drei Millionen Menschen für Unternehmen, die ganz oder teilweise in der Hand ausländischer Investoren sind. Der BDI steht verschärften Investitionskontrollen seit Jahren kritisch gegenüber. Investitionsprüfungen und Investitionsverbote belasten Unternehmen mit Bürokratie, schrecken Investoren ab und beschleunigen die Spirale des weltweit zunehmenden Investitionsprotektionismus. Auch vor dem Hintergrund von zwei Verschärfungen der Investitionsprüfungen in den letzten beiden Jahren (AWV-Novellen 2017 und 2018) ist eine weitere Verschärfung im Zuge des 2. IT-Sicherheitsgesetzes abzulehnen.

Einführung Artikel 6 – Evaluierung

Bevor ein zweites IT-Sicherheitsgesetz initiiert wird, wäre es angezeigt gewesen, das erste IT-Sicherheitsgesetz u.a. auf Grundlage fachlich wissenschaftlicher Expertise eingehend zu analysieren. Hierzu sollte in strukturierter Form auch das Feedback der bisher betroffenen Wirtschaftsteile und Unternehmen eingeholt werden. Eine solche Evaluierung würde den zuvor angesprochenen kooperativen Ansatz deutlich unterstreichen. Weiterhin ist im vorliegenden Entwurf keine Evaluierung des Gesetzes vorgesehen. Dies wird damit begründet, dass bereits nach Artikel 10 des ersten IT-Sicherheitsgesetzes eine Evaluierung durchgeführt wird. Stattdessen möchte der Gesetzgeber die Ergebnisse des zweiten IT-Sicherheitsgesetzes, in die Evaluierung des vorhergegangenen einfließen lassen. Dies würde zu einer weiteren Verzögerung bei der Generierung von wissenschaftlich fundierten Informationen über die Wirksamkeit der IT-Sicherheitsgesetze führen.

Die deutsche Industrie fordert die Aufnahme eines Artikels 6, der eine verpflichtende Evaluierung des IT-SiG 2.0 nach spätestens vier Jahren, jedoch zwingend vor einem IT-SiG 3.0 vorschreibt.

§ 1 „Evaluierung“

Das Bundesministerium des Innern, für Bau und Heimat ist spätestens vier Jahre nach In-Kraft-Treten oder vor Beginn einer Ressortabstimmung zu einem dritten Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme aufgefordert, eine umfangreiche Evaluierung des Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) und des Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0) durchführen zu lassen.

§ 2 „Art und Umfang der Evaluierung“

Die Evaluierung nach § 1 dieses Gesetzes hat vollumfänglich und nach besten wissenschaftlichen Standards durch eine unabhängige Stelle zu erfolgen.

§ 3 „Veröffentlichung der Ergebnisse“

Die Ergebnisse der Evaluierung nach § 1 sind spätestens sechs Monate vor Beginn einer Ressortabstimmung zu einem Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme öffentlich auf der Homepage des Bundesministeriums des Innern, für Bau und Heimat zu veröffentlichen.

Über den BDI

Der BDI transportiert die Interessen der deutschen Industrie an die politisch Verantwortlichen. Damit unterstützt er die Unternehmen im globalen Wettbewerb. Er verfügt über ein weit verzweigtes Netzwerk in Deutschland und Europa, auf allen wichtigen Märkten und in internationalen Organisationen. Der BDI sorgt für die politische Flankierung internationaler Markterschließung. Und er bietet Informationen und wirtschaftspolitische Beratung für alle industrierelevanten Themen. Der BDI ist die Spitzenorganisation der deutschen Industrie und der industrienahen Dienstleister. Er spricht für 40 Branchenverbände und mehr als 100.000 Unternehmen mit rund acht Mio. Beschäftigten. Die Mitgliedschaft ist freiwillig. 15 Landesvertretungen vertreten die Interessen der Wirtschaft auf regionaler Ebene.

Impressum

Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

Ansprechpartner

Steven Heckler
Referent
Telefon: 030 2028-1523
s.heckler@bdi.eu

BDI Dokumentennummer: D 1187