Stellungnahme

zum Diskussionsentwurf vom 2. Dezember 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: 7. Dezember 2020

Inhaltsverzeichnis

Zusammenfassung

Die deutsche Industrie begrüßt das Vorhaben der Bundesregierung, die Cyberresilienz Deutschlands ganzheitlich signifikant 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.

Die deutsche Industrie erwartet, dass der Staat den regulatorischen Rahmen so ausgestaltet, dass das Cybersicherheitsniveau Deutschlands ganzheitlich gestärkt wird, ohne den Unternehmen ungerechtfertigt hohe, respektive unklare Vorgaben aufzuerlegen. Das IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) könnte hierfür den geeigneten Rahmen bieten. Die deutsche Industrie sieht den vorliegenden **Diskussionsentwurf vom 2. Dezember 2020** jedoch **sehr kritisch und in weiten Teilen dringend überarbeitungsbedürftig**. **Das Gesetz greift vielfach zu weit in unternehmerische Prozesse ein, enthält unberechtigt umfangreiche Auskunftspflichten und zahlreiche vorgesehene Änderungen lassen zudem die notwendige Normklarheit vermissen.** Gemeinsam mit den Betroffenen hätte die Bundesregierung vor der Erarbeitung des IT-SiG 2.0 klare Schutzziele definieren und daran den Entwurf ausrichten sollen. Nur mit einer eindeutig definierten Zielrichtung kann ein Gesetz erfolgreich sein.

Die deutsche Industrie erachtet die **sehr kurze Frist von einer Woche** zur Stellungnahme zu einem nicht-ressortabgestimmten Diskussionsentwurf als **völlig inakzeptabel**. Das IT-Sicherheitsgesetz 2.0 ist das zentrale Legislativvorhaben in dieser Legislatur zur Weiterentwicklung des nationalen Regulierungsrahmens im Bereich Cybersicherheit. Eine vernünftige, tiefgreifende und der Bedeutung des Themas angemessene Befassung durch die Wirtschaft ist in solch einer kurzen Frist überhaupt nicht möglich. Es hätte vielmehr zuerst einer Einigung der Ressorts und anschließend einer mindestens vierwöchigen Verbändeanhörung bedurft. Im Idealfall hätte die Einbindung der Wirtschaft zu solch substanziellen Fragen bereits in der langen Vorbereitungszeit des Entwurfes in strukturierter Form stattgefunden. **Die Bundesregierung sollte sich bei zukünftigen Gesetzgebungsverfahren an den Verfahrensweisen des Konsultationsprozesses der Europäischen Kommission orientieren, die eine strukturierte, transparente und mehrstufige Beteiligung aller Interessierter ermöglicht.**

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

Aus Sicht der deutschen Industrie sind folgende Punkte kritisch zu beurteilen und sollten (teils umfangreich) nachjustiert werden:

- **Fehlende Evaluierung des IT-Sicherheitsgesetzes**: Bevor ein zweites IT-Sicherheitsgesetz initiiert wird, wäre es angezeigt gewesen, das erste IT-Sicherheitsgesetz eingehend transparent und unter Beteiligung der betroffenen Branchen zu analysieren – dies ist jedoch bis dato nicht erfolgt. Hierzu sollten in strukturierter Form auch die bisher betroffenen Wirtschaftsteile und Unternehmen konsultiert werden. Die deutsche Industrie begrüßt daher, dass nunmehr eine Evaluierung des IT-SiG 2.0 vorgesehen ist. Eine vollumfängliche verpflichtende **Evaluierung des IT-SiG 2.0** nach spätestens vier Jahren, jedoch zwingend vor einem IT-SiG 3.0, sollte in Artikel 7 des IT-SiG 2.0 festgeschrieben werden.

- **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:** 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 und rechtliche Flickenteppiche sind weder effizient noch effektiv. Sie erhöhen Aufwand und Kosten und schaffen zudem rechtliche Unsicherheiten zulasten der verpflichteten Unternehmen sowie zulasten der Verbraucher und Geschäftskunden.
  Beispielsweise durch die Einführung eines nationalen IT-Sicherheitskennzeichens sowie der neuen Kategorie „Unternehmen im besonderen öffentlichen Interesse“ erschwert das IT-SiG 2.0 das Ziel einer europäischen Harmonisierung im Bereich IT-Sicherheit. Das IT-SiG 2.0 muss eine inhaltliche Anschlussfähigkeit an den *EU Cybersecurity Act* sowie die potenzielle Einführung von Cybersicherheitsanforderungen in die vertikalen Richtlinien für Produktgruppen gewährleisten. Unrechtmäßige Marktzugangsbeschränkungen für Produkte müssen vermieden werden.
  Zudem sollte jedwede Ausweitung des Anwendungsbereichs von KRITIS-Regulierungen – auch mit Blick auf wettbewerbsrechtliche

Implikationen – erst über die Implementierung der Vorgaben der Überarbeitung der NIS-Richtlinie erfolgen. Bei der Definition Kritischer Komponenten im Bereich 5G, sollte sich der Gesetzgeber an dem gemeinsamen Instrumentarium von Risikominderungsmaßnahmen (EU 5G-Toolbox), 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 dem 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. Es bedarf rechtlich präziser Definitionen der neu einzuführenden Begriffe „IT-Produkte“ (§ 2 Abs. 9a) und „Kritische Komponente“ (§ 2 Abs. 13). Anstatt weitere Details in einer RVO zu regeln, sollten diese direkt im IT-SiG 2.0 verbindlich bestimmt werden.

- **Nationale Gesetzgebungsverfahren besser koordinieren:** Es bedarf einer stärkeren Abstimmung des hiesigen Gesetzgebungsverfahrens zum Parallelverfahren der Novellierung des TKG, das zum Teil vergleichbare Sachverhalte regelt und Definitionen beinhaltet.

- **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. Die deutsche Industrie fordert:
    1. Die Schaffung eines effizienten, harmonisierten Meldewegs an eine zentrale Meldestelle (one-stop-shop-Prinzip),
    2. ein verbessertes tagesaktuelles, ganzheitliches Lagebild sowie tagesaktuelle, branchenspezifische Warnungen, damit die deutsche Industrie aus dem beim BSI aggregierten Datenschatz auch einen Nutzen ziehen und ihre Anlagen und Systeme besser schützen kann,
    3. eine Verpflichtung des BSI, eingegangene Informationen zu verarbeiten und betroffene Unternehmen über erfolgte oder versuchte Angriffe auf ihre IT zu informieren,
    4. Unternehmen, die Cybersicherheitsvorfälle melden, sollte eine personalisierte Unterstützung angeboten werden und
    5. gesetzliche Rahmenbedingungen müssen geschaffen werden, um Wirtschaftsunternehmen über vorliegende Informationen

zu (Cyber)-Gefährdern zu informieren, auch über geheimschutzbetreute Unternehmen hinaus.

- **BSI stärken, aber nicht inhaltlich überfrachten (§ 3)**: Es gilt, das BSI personell und finanziell zu stärken und zugleich eine klare Kompetenzunterscheidung zwischen Normensetzung und deren Überprüfung sicherzustellen. Allerdings erachtet die deutsche Industrie eine Aufstockung der deutschen Cybersicherheitsbehörde um 799 Stellen als überzogen. Vielmehr sollte sich die Bundesregierung für eine Stärkung der ENISA einsetzen, da eine europaweite Bündelung von Kompetenzen und Zuständigkeiten, z.B. die Einführung eines IT-Sicherheitskennzeichens, im Bereich Cybersicherheit deutlich effizienter und kostengünstiger wäre.
  Zudem 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 nationale Behörde für die Cybersicherheitszertifizierung agiert und das IT-Sicherheitskennzeichen vergibt. Im Sinne der Stärkung der Digitalen Souveränität Deutschlands, sollten Beratungsleistungen zur IT-Sicherheit im behördlichen Umfeld sowie andere nunmehr für das BSI vorgesehene Aufgaben durch qualifizierte Unternehmen, so wie es bereits jetzt in einigen Bereichen erfolgt, im Sinne eines kooperativen Ansatzes übernommen werden. Nur so kann die deutsche IT-(Sicherheits-)Wirtschaft langfristig gestärkt werden. Es gilt insgesamt eine stärkere Trennung von Kompetenzen sicherzustellen und zukünftig weiter auf die Prozesse der europäischen Normung zu setzen.

- **Stand der Technik (§ 3 Abs. 1 Satz 2 Nr. 20):** Der BDI lehnt das Festschreiben eines Stands der Technik durch das BSI ab. Der Stand der Technik entwickelt sich stetig weiter, basierend auf Standards und Innovationen sowie am Markt verfügbarer Technologien. Der national definierte Stand der Technik würde daher bereits bei Veröffentlichung veraltet sein. Zudem widerspricht dieses nationale Ansinnen dem Gedanken des Europäischen Binnenmarkts. Die deutsche Industrie befürchtet zudem, dass durch die Definition „Stand der Technik“ bereits eingesetzte Hardware und Technik verboten werden. Hier müssen Ausnahmen unter bestimmten Rahmenbedingungen möglich sein, sofern nicht ein berechtigtes Interesse durch einen bestätigten Sicherheitsmangel oder Vertrauensverlust besteht. Weiter ist sicherzustellen, dass die betroffenen Hersteller und Betreiber vorab über anstehende Verbote informiert werden.

- **Speicherfrist von 4 Jahren für die Angriffserkennung (§ 8a Abs. 1b):** Betreiber Kritischer Infrastrukturen sollen zukünftig für die Angriffserkennung und -nachverfolgung relevante nichtpersonenbezogene Daten mindestens vier Jahre speichern (§ 8a). Der BDI lehnt diese Vorgabe als völlig realitätsfern ab. Selbst eine Verpflichtung zur Speicherung aller notwendigen Daten für ein Jahr würde massive Kosten verursachen, insbesondere, da entsprechende Unternehmen regelmäßig angegriffen werden. Pro Tag würden hier bei jedem Betreiber einer Kritischen Infrastruktur TByte an Daten anfallen, die gespeichert werden müssen. Diese müssten in Rechenzentren gespeichert werden, was eine signifikante Umweltbelastung zur Folge hätte, ohne einen erkennbaren Mehrwert zu liefern, da die betroffenen Unternehmen bereits Systeme implementiert haben, um schnell Angriffe zu erkennen.

- **Registrierungspflicht von KRITIS beim BSI (§ 8a Abs. 3 und 3a):** Es ist unklar, welchen Mehrwert die neuen Regelungen zur Registrierung von Kritischen Infrastrukturen beim BSI gegenüber dem bisherigen Registrierungsprozess haben sollen. 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. Die Weitergabe unternehmensinterner und mitunter hochsensibler Informationen widerstrebt dem Eigeninteresse eines jeden Wirtschaftsunternehmens, seine internen betriebssensiblen Informationen zu sichern und nicht nach außen zu geben.

- **Unternehmen im besonderen öffentlichen Interesse (§ 8f)**: 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 ist zu hinterfragen, warum gerade jene Unternehmen, die aufgrund ihrer Wertschöpfung zu „den größten Unternehmen“ zählen, besonderen Verpflichtungen unterliegen sollen. Insbesondere global tätige Unternehmen mit einer hohen volkswirtschaftlichen Bedeutung unterliegen bereits vielerlei Auflagen und Berichtspflichten, weshalb die angestrebte Kompetenzerweiterung des BSI als eine zusätzliche Aufsichts- und Regulierungsbehörde mit weitergehenden Berichtspflichten für große Teile der deutschen Wirtschaft eine erhebliche Mehrbelastung bedeuten würde, ohne dabei risikobasiert bereits existierende Sicherheitsmechanismen der Unternehmen zu berücksichtigen oder einen Beitrag zur Erhöhung des Sicherheitsniveaus zu leisten. Vielmehr wäre eine intensivere Unterstützung der

Cybersicherheitsbemühungen von KMU durch das BSI wünschenswert. Der in der Begründung enthaltene Verweis auf die Liste der Monopolkommission lässt zudem völlig offen, ob jeweils nur die in der Liste genannte Unternehmensform oder – im Falle einer Holding – auch alle dazugehörenden Unternehmen in den Anwendungsbereich dieses Gesetzes 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. Sollte eine einzelstaatliche Einführung der Kategorie „Unternehmen im besonderen öffentlichen Interesse“ als unabdingbar für die Cyberresilienz Deutschlands erachtet werden, so ist der im Vergleich zum Entwurf vom 7. Mai 2020 angepasste Verweis auf die StörfallVO, anstelle der GefahrstoffVO, zu begrüßen.

- **Untersagung des Einsatzes Kritischer Komponenten nicht vertrauenswürdiger Hersteller (§ 9b)**: § 9b bringt in seiner jetzigen Ausgestaltung unkalkulierbare Risiken für Investitionen von KRITIS-Betreibern. 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 führen kann. Die deutsche Industrie lehnt eine so breit gefasste Möglichkeit zur Untersagung ab. Der Gesetzentwurf muss dringend klarstellen, wer die Kosten eines Rückbaus und den Ersatz von Komponenten zu tragen hat. Die Situation ist vergleichbar zum Atom- bzw. Kohleausstieg, bei dem die Betreiber großzügig vom Staat entschädigt wurden. Es ist kein Grund ersichtlich, weshalb das für KRITIS nach dem IT-SiG 2.0 nicht vorgesehen werden sollte. Im Übrigen hat die britische Regierung solche Entschädigungen für KRITIS-Betreiber bei Ausbau von 5G-Komponenten gerade beschlossen.
  Auch birgt die Speicherung der in der Anzeige zum Einsatz Kritischer Komponenten enthaltenen sensiblen Informationen an einem Ort ein unkalkulierbares Sicherheitsrisiko für den Bestand und das Funktionieren Kritischer Infrastrukturen. Damit einher gehen Risiken für Staat, Gesellschaft und Unternehmen. Daher sollten die Anzeigepflicht und die Speicherung von sicherheitsrelevanten Informationen gestrichen 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. Aus Sicht der deutschen Industrie wird durch die Einführung einer Garantieerklärung jedoch das Schutzziel – Wahrung der Sicherheit der KRITIS – nur scheinbar 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. Die deutsche Industrie lehnt die Einführung der Garantieerklärung in ihrer aktuell vorgesehenen Ausgestaltung daher ab.
Verstöße gegen Garantieerklärungen werden von KRITIS-Betreibern weder überprüfbar und schon gar nicht nachzuweisen sein. Für eine solche Beweisführung dürfte in der Regel geheimdienstlich sichergestelltes Beweismaterial erforderlich sein – z.B. Erkenntnisse über die Verflochtenheit von Unternehmen und staatlichen Stellen. 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. 5 BSIG, dass der Hersteller nicht vertrauenswürdig ist, regelmäßig aufgrund unzureichender Beweise zu Schwierigkeiten führen. Daher können die Betreiber allenfalls dafür haften, dass eine formell ordnungsgemäße Herstellererklärung vorliegt.
Erschwerend kommt hinzu, dass sich die Garantieerklärung des Herstellers ggü. KRITIS-Betreibern auf die gesamte Lieferkette bezieht. Dies ist sowohl für die Hersteller als auch für jene Unternehmen entlang der Lieferkette, die die Erklärung selbst nicht direkt unterzeichnen, nicht realistisch und praktikabel. Die BReg muss definieren, wo die Lieferkette i.S.d. IT-SiG 2.0 endet – auf Ebene der Komponenten oder der Rohstoffe. Es wird KRITIS-Betreibern vielfach nicht möglich sein, bei komplexen Hardware-, Software- und Elektronik-Produkten globale Produktionsketten komplett nachzuvollziehen.
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.

- **Bußgeldvorschriften (§ 14):** Die nunmehr angepasste Höhe für Bußgelder erachtet die deutsche Industrie mit Blick auf den

Geltungsbereich des IT-SiG 2.0 als verhältnismäßig. Lediglich der Verweis auf § 30 Abs.2 Satz 3 OWiG ist abzulehnen, da er eine Verzehnfachung der potenziellen Bußgelder ermöglichen würde. Bei allen anderen Vorgaben des neuen Bußgeldrahmens schafft der Gesetzgeber einen Ausgleich zwischen maßvoll angemessener und wirksamer Sanktionierung.

- **Möglichkeit zur Prüfung der Vertrauenswürdigkeit der Beschäftigten schaffen:** Der im Entwurf vom 7. Mai 2020 enthaltene Ansatz, 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-E), war ein richtiger und sinnvoller Ansatz. Die deutsche Industrie fordert die Bundesregierung auf, diese Möglichkeit erneut im IT-SiG 2.0 als KANN-Option vorzusehen. Eine ausschließliche Fokussierung auf technische Sicherheit im IT-SiG 2.0 ist nicht zielführend, um die Cyberresilienz Deutschlands zu erhöhen. Unternehmen sollten auch die Möglichkeit erhalten, die Vertrauenswürdigkeit von Beschäftigten in als besonders sicherheitskritisch eingestuften Bereichen untersuchen zu können.

- **Cybersicherheit braucht ganzheitlichen Ansatz:** Die Erhöhung des Cybersicherheitsniveaus Deutschlands kann nur gemeinschaftlich erfolgen.
    1. ***Hersteller und Betreiber entlang der kompletten Wertschöpfungskette*** müssen in die Stärkung der Cyberresilienz einbezogen werden, denn viele Pflichten können nur von den Herstellern sinnvoll erfüllt werden, ihre Kunden müssen sie in den Anforderungen begleiten und ausschließlich Produkte einsetzen, die die Anforderungen erfüllen.
    2. ***Privatanwendern*** sollten zudem in der schulischen und hochschulischen Bildung, in Ausbildungen sowie in Angeboten des Lebenslangen Lernens Digitalkompetenzen vermittelt werden. Denn auch private Endnutzer können durch die Installation bereitgestellter Updates und Patches sowie die Berücksichtigung der Prinzipien der Cyberhygiene die Cyberresilienz der von ihnen eingesetzten Produkte und Dienstleistungen unterstützen.
    3. ***Staatliche Stellen*** – insbesondere BSI, BNetzA und die Nachrichtendienste – müssen betroffene Unternehmen – unter Beachtung der Responsible-Disclosure-Prinzipien – umgehend über ihnen bekannt gewordene sicherheitsrelevante Schwachstellen informieren, denn das Zurückhalten dieser Informationen kann weitreichende negative Folgen haben.

- **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 deutlich zu gering angesetzt. So werden die Aufwände, die Unternehmen durch Umsetzung von § 8 Abs. 7 und 8 entstehen, auf lediglich 19.552 Euro für die gesamte Wirtschaft geschätzt. Zur Umsetzung der Meldepflichten müssen Unternehmen im besonderen öffentlichen Interesse nicht nur ein Meldewesen, sondern zudem eine vorgelagerte Beobachtung des Netzwerkverkehrs (Monitoring) durchführen, da bereits Störungen, die „zu einer erheblichen Beeinträchtigung der Erbringung der Wertschöpfung“ bzw. „zu einem Störfall nach der Störfall-Verordnung in der jeweils geltenden Fassung“ führen können, gemeldet werden müssen. Allein das Vorhalten eines Mitarbeitenden, der sofortige Meldungen an das BSI veranlassen kann, dürfte regelmäßig zu jährlichen Kosten von mind. 25.000 Euro pro Betrieb führen. Zusätzlich sind Kosten für die Etablierung eines Meldewesens sowie für die technische Ausstattung einzuplanen. Damit werden für einen Betrieb bereits deutlich höhere Kosten anfallen, als die Bundesregierung für die gesamte Wirtschaft einplant. Es gilt, die weitreichenden unternehmensinternen Kosten für Personal und Anpassungen an Unternehmensprozesse ebenso wie die steigenden Kosten durch voraussichtlich kostenintensivere Produkte besser zu berücksichtigen.

- **Mittelbare Lieferkettenverantwortung:** Durch die Ausweitung der durch das IT-SiG regulierten Sektoren werden 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. Zwar erhöht dies auch auf breiterer Fläche die Cyberresilienz, doch 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 für alle Unternehmen realistisch und umsetzbar gestaltet werden.

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 „Siedlungsabfallentsorgung“, 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 im Sinne dieses Gesetzes sind Aufzeichnungen über technische Ereignisse oder Zustände innerhalb informationstechnischer Systeme. Protokollierungsdaten dienen der Erkennung, Eingrenzung oder Beseitigung von Störungen oder Fehlern bei der Kommunikationstechnik des Bundes oder der Erkennung, Eingrenzung oder Beseitigung von Angriffen auf die Kommunikations-technik des Bundes. *Protokolldaten nach Absatz 8 sind eine Teilmenge der Protokollierungsdaten.*“

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*, Hardware* sowie alle einzelnen oder miteinander verbundene ~~*Hardwareprodukte*~~ *Hardwarekomponenten, soweit deren Hersteller sie für den bestimmungsgemäßen Einsatz in einer Kritischen Infrastruktur nach § 2 Absatz 10 vorgesehen hat*.“

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 „Siedlungsabfallentsorgung“

Die Einführung des neuen KRITIS-Sektors „Siedlungsabfallentsorgung“ 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 Dienstleister der Siedlungsabfallentsorgung unter die KRITIS-Verordnung fällt, einbezogen werden. Dabei gilt es, insbesondere zwischen den unterschiedlichen Stoffströmen und der Herkunft der Abfälle zu unterscheiden.

Zu § 2 Abs. 11 – „Digitale Dienste“

In der Erstellung des IT-SiG 1.0 war strittig, ob sonstige digitale Dienste über Marktplätze, Suchmaschinen und Cloud hinaus ebenfalls in den Anwendungsbereich aufgenommen werden sollen, um eine systematische Erhöhung des IT-Sicherheitsniveaus über kritische IT-Infrastrukturen hinaus zu gewährleisten. Zu dieser Frage verhält sich der aktuelle Gesetzentwurf in keiner Weise. Hier zeigt sich deutlich, dass die oben bereits geforderte Evaluierung der bisherigen Regelungen nicht durchgeführt wurde und unbedingt erforderlich ist.

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. Der nunmehr vorliegende Entwurf sieht in einem ersten Schritt ausschließlich die Einführung Kritische Komponenten für Betreiber öffentlicher Telekommunikationsnetze vor. Diese Einschränkung ist aus Sicht der deutschen Industrie zweckdienlich, da eine direkte Ausweitung des Anwendungsbereichs über den TK-Sektor hinaus, ohnehin nicht umsetzbar gewesen wäre. Die Definition weiterer Kritischer Komponenten erfolgt gesetzlich.

Der aktuell vorliegenden Definition fehlt jedweder definitorische Charakter, da aus § 2 Abs. 13 nicht hervorgeht, was „Kritische Komponenten“ im Sinne dieses Gesetzes auszeichnet. Es mangelt dem Entwurf somit an der notwendigen Bestimmtheit und Rechtsklarheit. Basierend auf der aktuellen Definition ist völlig unklar, welche Komponenten zukünftig als „Kritische Komponenten“ definiert werden können. Mit Blick auf Abs. 13 muss sichergestellt werden, dass IT-Produkte nur dann unter den Wirkbereich des § 2 Abs. 13 BSIG fallen, wenn sie für das ordnungsgemäße Funktionieren der Kritischer Infrastrukturen entscheidend sind. Zudem sollte klargestellt werden, dass nur dafür ausgewiesene speziell für den Einsatz in Kritischen

Infrastrukturen hergestellte 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 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 bisher bei 3G und 4G-Netzen faktisch auf Kernnetzkomponenten beziehen. Zudem wäre eine spezifischere Verpflichtung wünschenswert, sodass Hersteller von Kritischen Komponenten in ihrem Verantwortungsbereich entsprechend angemessene 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. 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.

§ 13 Abs. 2 stellt zudem nicht klar, für welche weiteren KRITIS-Sektoren die Einführung Kritischer Komponenten durch den Gesetzgeber angestrebt wird. Mangels Planungssicherheit fordert die deutsche Industrie daher, bei der Einführung Kritischer Komponenten in weiteren KRITIS-Sektoren hinreichend lange Übergangsfristen zu gewährleisten. Viele Komponenten lassen sich nicht 1:1 austauschen, sondern erfordern weitere Änderungen in der Architektur der IT-Infrastruktur. Ebenso gilt es die notwendigen Anpassungen und Zertifizierungsprozesse bei den Herstellern zu berücksichtigen. Erfahrungsgemäß kann der Zeitraum zur Durchführung einer neuen Produktzertifizierung einen Zeitraum von bis zu zwei Jahren umfassen.

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

- Auswirkungen der Einführung der Definition „Kritische Komponenten“ sowie die Erweiterung des Sicherheitskatalogs und die Einführung der Liste Kritischer Funktionen auf bereits vor In-Kraft-Treten des IT-SiG 2.0 und des Katalogs eingebaut Komponenten: Hier sollte Bestandsschutz gelten,
- Auswirkungen auf private 5G-Campusnetze,
- Angemessene Beteiligung der Betreiber Kritischer Infrastrukturen, insbesondere der Telekommunikationsbranche und den Herstellern Kritischer Komponenten, um einen frühen Interessenabgleich aller Beteiligen zu gewährleisten
- Angemessenes Abstraktionsniveau für die angestrebten Kataloge.

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 „die nach ihrer inländischen Wertschöpfung zu den größten Unternehmen in Deutschland gehören und daher von erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland sind“ 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.

- 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. Nur so kann eine gezielte Einbeziehung weiterer relevanter Branchen außerhalb der KRITIS-Betreiber gewährleistet werden.

Zu Nummer 3: Die Anpassungen des Bezugs in §2 Abs. 14 Nr. 3 zur Störfallverordnung ist begrüßenswert. Die StörfallVO hat zum Ziel, die Allgemeinheit vor anlagenbezogenen gefährlichen Ereignissen zu schützen, dadurch wird eine Eingrenzung auf Unternehmen mit besonderer Relevanz für die öffentliche Sicherheit und Ordnung gewährleistet.

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 sowie Empfehlungen für Identifizierungs- und Authentisierungsverfahren entwickeln, als zentrale Ansprechstelle für KRITIS, Verwaltung und Unternehmen im besonderen öffentlichen Interesse fungieren, IT-Produkte- und -Systeme untersuchen, als nationale Behörde für die Cybersicherheitszertifizierung agieren und das IT-Sicherheitskennzeichen vergeben (§3 Abs. 1 Satz 2 Nr. 5a 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.

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. Grundsätzlich ist hier eine Stärkung des BSI in seiner Funktion zu begrüßen, es ist jedoch derzeit noch 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, Hersteller und Nutzer) 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, Betretensrechte"

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 und auf bereits etablierte Meldewege zurückzugreifen oder andere Meldepflichten abzulösen, statt einfach einen weiteren zusätzlichen verpflichtenden zu eröffnen.

- 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 § 5b „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. Weiterhin bleibt ungeklärt, welcher Rechtsweg im Falle von Fehlentscheidungen durch das BSI beschritten werden kann und welche Form der Haftung für Anordnungen mit weitreichenden negativen Folgen das BSI übernehmen muss.

Zu § 5c „Bestandsdatenauskunft“

§ 5c 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 ist, gemessen am intendierten Zweck der Norm, unverhältnismäßig zu sein. Hier bedarf es einer engeren Eingrenzung des Geltungsbereichs des § 5c. Darüber hinaus ist eine strikte Zweckbindung vorzusehen und ausdrücklich zu regeln, dass die abgefragten Bestandsdaten nur zur Information, unter keinen Umständen aber zu anderen Zwecken verwendet werden dürfen.

Nach Ansicht des BDI sollte § 5c wie folgt ergänzt werde:
„*(3) … Für die Entschädigung der Diensteanbieter ist § 23 des Justizvergütungs-und -entschädigungsgesetzes entsprechend anzuwenden.*“

(8) 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.“

Aus datenschutzrechtlichen Erwägungen ist die in § 5c Abs. 5 vorgesehene Befugnis des Bundesamts zur Weiterleitung von Daten an andere Behörden zu streichen.

Die Beachtung der unionsrechtlichen Rechtsprechung zur sog. Vorratsdatenspeicherung durch den deutschen Gesetzgeber wird diesseits als selbstverständlich angenommen.

Zu § 7 „Warnungen“

Die deutsche Industrie begrüßt, dass Hersteller von betroffenen Produkten vor der Veröffentlichung einer Warnung durch das BSI informiert werden sollen. Der BDI spricht sich dafür aus, dass Warnungen durch das BSI über Sicherheitslücken in Produkten (§ 7 Abs. 1a) grundsätzlich mit dem Produkthersteller kooperativ durchgeführt werden sollten (siehe *Coordinated Vulnerability Disclosure* z.B. ISO/IEC 29147:2018 Information technology – Security techniques – Vulnerability disclosure). Der BDI empfiehlt daher, dass § 7 Abs. 1 wie folgt geändert wird:

„Zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 14 kann das Bundesamt *gemeinsam mit dem Produkthersteller entsprechend dem Coordinated Vulnerability Disclosure-Prinzip* …“

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. 1a Nr. 2 wie folgt geändert wird:

„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 dem betroffenen Hersteller nach Veröffentlichung der Warnung zur Kenntnis zu geben ist*.“

Im Gesetzestext muss direkt geregelt sein, welchen Rechtsweg im Falle von Fehlentscheidungen durch das BSI Unternehmen beschreiten können und welche Form der Haftung für Anordnungen mit weitreichenden negativen Folgen das BSI übernehmen muss.

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.

Der deutliche Ausbau im BSI auch für Beratungsleistungen zu IT-Sicherheit im behördlichen Umfeld könnte das Marktangebot reduzieren und so die deutschen IT-Sicherheitsunternehmen wirtschaftlich treffen. Um ein gesundes Öko-System und eine leistungsstarke nationale IT-Sicherheitsindustrie zu erhalten, sollte von der neuen Formulierung im IT-SiG2.0 zur Beauftragung durch Drittunternehmen deutlich Gebrauch gemacht werden (Vgl. § 7a Abs. 1).

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. Die deutsche Industrie fordert daher eine Streichung von § 7a Abs. 2 und 4, da es durch das Übermitteln hochsensibler Geschäftsdaten an das BSI sowie das Sammeln dieser Daten beim BSI im Falle eines Cybersicherheitsvorfalls beim BSI zu einer massiven Schwächung der Digitalen Souveränität des Wirtschaftsstandorts Deutschland kommen kann. Dies kann nicht im Sinne des Gesetzgebers sein.

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. In dem Auskunftsverlangen gibt das Bundesamt die Rechtsgrundlage, den Zweck des Auskunftsverlangens und die benötigten Auskünfte an und

legt eine angemessene Frist für die Übermittlung der Auskünfte fest. Das Auskunftsverlangen enthält ferner einen Hinweis auf die in § 14 vorgesehenen Sanktionen. *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 Erkenntnissen über die Sicherheit in der Informationstechnik. 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“

Das BSI kann zukünftig zur Detektion von Sicherheitslücken und anderen Sicherheitsrisiken an den Schnittstellen öffentlich erreichbarer informationstechnischer Systeme zu öffentlichen Telekommunikationsnetzen Portscans durchführen. Diese Maßnahmen müssen sich auf das zur Detektion von Sicherheitslücken oder anderen Sicherheitsrisiken in der Informationstechnik von Kritischen Infrastrukturen, digitaler Dienste, Unternehmen im besonderen öffentlichen Interesse und dem Bund beschränken. Die deutsche Industrie

fordert, dass sämtliche bei Maßnahmen nach § 7b Abs. 1 erzielten Erkenntnisse unverzüglich mit dem betroffenen Wirtschaftsunternehmen zu teilen und anschließend alle übermittelten Daten inkl. Protokolldateien zu vernichten sind.

Im Fall der Detektion eines Schadprogramms, einer Sicherheitslücke oder eines anderen Sicherheitsrisikos an Schnittstellen von öffentlich erreichbaren informationstechnischen Systemen zu öffentlichen Telekommunikationsnetzen sollten KRITIS-Betreiber, Betreiber digitaler Dienste sowie Unternehmen im besonderen öffentlichen Interesse stets unverzüglich informiert werden (§ 7b Abs. 3), um diese abzustellen. Demnach wäre Abs. 3 wie folgt anzupassen:

„(3) Wird durch Maßnahmen gemäß Absatz 1 eine Sicherheitslücke oder ein anderes Sicherheitsrisiko eines informationstechnischen Systems erkannt ~~*und stehen überwiegende Sicherheitsinteressen nicht entgegen,*~~ sind die für das informationstechnische System Verantwortlichen darüber *unverzüglich* zu informieren. Das Bundesamt soll dabei auf bestehende Abhilfemöglichkeiten hinweisen. Sind dem Bundesamt die Verantwortlichen nicht bekannt oder ist ihre Identifikation nur mit unverhältnismäßigen Aufwand möglich und stehen überwiegende Sicherheitsinteressen nicht entgegen, ist hilfsweise der betreibende Dienstleister des jeweiligen Netzes oder Systems unverzüglich zu benachrichtigen. Das Bundesamt unterrichtet die Bundesbeauftragte oder den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit jeweils bis zum 30. Juni des Folgejahres über die Anzahl der gemäß Absatz 1 ergriffenen Maßnahmen.“

Sollten Betreiber einer Kritischen Infrastruktur, Betreibern digitaler Dienste oder Unternehmen im besonderen öffentlichen Interesse durch die Maßnahmen des BSI Schäden entstehen so muss die Haftung bei der Bundesrepublik Deutschland liegen. Dieser Positionierung Rechnung tragend, sollte § 7b wie folgt ergänzt werden:

„(5) Sollte durch Maßnahmen nach Absatz 1 dem Betreiber einer Kritischen Infrastruktur, Betreibern digitaler Dienste oder Unternehmen im besonderen öffentlichen Interesse Schäden entstehen, so haftet der Bund den Betreibern für diese Schäden sowie für Folgeschäden.“

Es wäre zudem zu begrüßen, wenn 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.

Zu § 7c „Anordnungen des Bundesamtes gegenüber Diensteanbietern“

Das BSI kann zur Abwehr konkreter erheblicher Gefahren für Schutzziele gegenüber Diensteanbietern mit mehr als 100.000 Kunden anordnen, dass sie die in § 109a Abs. 5 und 6 TKG genannten Maßnahmen treffen oder technische Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene IT-Systeme verteilen. Zu den Schutzzielen gehören: (1) Verfügbarkeit, Unversehrtheit, Vertraulichkeit der Kommunikationstechnik des Bundes, eines KRITIS-Betreibers, eines Unternehmens im besonderen öffentlichen Interesse, eines Anbieters Digitaler Dienste, (2) Verfügbarkeit, Unversehrtheit oder Vertraulichkeit von IT- oder TK-Diensten, oder (3) Informationen, deren Verfügbarkeit oder Vertraulichkeit eingeschränkt wird durch unerlaubte Zugriffe auf eine erhebliche Anzahl von TK- oder IT-Systemen von Nutzern. Das Bundesamt kann nach § 7c Abs. 3 verlangen, dass der Diensteanbieter den Datenverkehr an eine vom Bundesamt benannte Anschlusskennung umleitet.

Aufgrund der weit gefassten Schutzziele entsteht hier ein unverhältnismäßiges Eingriffsrecht für das BSI. Der Entwurf lässt zudem definitorische Klarheit vermissen, z.B. mit Blick auf das Wort „Kunden“. Hier gilt es zu klären, ob private oder juristische Person gemeint sind sowie ob ausschließlich deutsche Kunden für die Bemessungsgrundlage erheblich sind.

Die in Absatz 1 textierte Anordnungsbefugnis ist sehr kritisch, da nicht ersichtlich ist, auf welcher Basis das BSI sinnhafte konkrete Maßnahmen anordnen kann, da letztlich die Anbieter selbst ihre Systeme am besten kennen. Insofern sind konkrete und eindeutige Hinweise auf Schwachstellen wünschenswert. Die Beseitigung der Schwachstellen muss hingegen durch den Anbieter von Telemediendienste erfolgen. Den im Entwurf vorgesehenen Eingriff in das Recht am eingerichteten und ausgeübten Gewerbebetrieb sowie in das Eigentumsrecht halten wir in der vorliegenden Form für nicht gerechtfertigt.

Schließlich lehnt die deutsche Industrie § 7c Abs. 3 kategorisch ab, da die Pflicht zur Umleitung des Datenverkehrs an eine vom Bundesamt benannte Anschlusskennung im Konflikt zum Fernmeldegeheimnis steht. Denn wird diesem Dritten „Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation“ im Sinne des § 88 Abs. 3 TKG verschafft, stellt eine solche Maßnahme einen Eingriff in das Fernmeldegeheimnis dar, wie er etwa bei der Telekommunikationsüberwachung in den Bereichen polizeilicher Gefahrenabwehr oder der Strafverfolgung stattfindet. Diese Maßnahmen sind nur

unter strengen Voraussetzungen und in der Regel auf Basis einer richterlichen Anordnung zulässig. Aufgrund der vergleichbaren Schwere des Eingriffs ist ein Richtervorbehalt auch hier zwingend erforderlich. Gleichzeitig sollte darauf geachtet werden, dass die Tätigkeiten des BSI nicht mit Aufgaben der Strafverfolgung vermengt werden bzw. sie in ihrer Auswirkung mit ihnen gleichkommen. Die deutsche Industrie empfiehlt, § 7c Abs. 3 gänzlich zu streichen.

Zu § 7d „Anordnungen des Bundesamtes gegenüber Anbietern von Telemediendiensten“

Die in Absatz 1 textierte Anordnungsbefugnis ist analog zu § 7c BSIG-E sehr kritisch, da nicht ersichtlich ist, auf welcher Basis das BSI sinnhafte konkrete Maßnahmen anordnen kann, da letztlich die Anbieter selbst ihre Systeme am besten kennen. Insofern sind konkrete und eindeutige Hinweis auf Schwachstellen wünschenswert. Die Beseitigung der Schwachstellen muss hingegen durch den Anbieter von Telemediendienste erfolgen.

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 BSI gegenüber privaten Unternehmen, die IT-Dienstleistungen für die Bundesverwaltung erbringen. Weiterhin können Unternehmen des Bundes, die dieser Regulierung unterliegen, gleichzeitig auch Unternehmen in besonderem öffentlichen Interesse sein. Hier ist eine Doppelregulierung mit unklaren und ungerechtfertigt hohen Anforderungen zu vermeiden. Unabhängig davon ist für die deutsche Industrie nicht nachzuvollziehen, warum gerade der Bereich der IT mit einer der höchsten Anforderungen an IT-Sicherheit, nämlich der Bundeswehr, hier auf Basis einer intransparenten Verwaltungsvereinbarung ausgenommen werden soll.

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

Spätestens ein Jahr nach In-Kraft-Treten des IT-SiG 2.0 müssen Bereiter Kritischer Systeme im Rahmen angemessener organisatorischer und technischer Vorkehrungen auch Systeme zur Angriffserkennung implementiert haben. Das Vorhalten von Systemen zur Angriffserkennung ist aus Sicht des BDI eine sinnvolle Maßnahme, um die Cyberresilienz Kritischer Infrastrukturen

zu stärken. Es ist jedoch zu prüfen, ob es Branchen gibt, in denen die Nutzung solcher Systeme zum Verlust von Gewährleistungs- und Wartungsansprüchen führen können.

Des Weiteren sieht § 8a Abs. 1b vor, dass Betreiber Kritischer Infrastrukturen für die Angriffserkennung und -nachverfolgung relevante nicht-personenbezogene Daten, die beim Betrieb einer Kritischen Infrastruktur anfallen, mindestens vier Jahre speichern müssen. Die deutsche Industrie lehnt diese Anforderung als völlig realitätsfern ab. Betreiber Kritischer Infrastrukturen werden in § 8a Abs. 1a verpflichtet, Systeme zur Angriffserkennung zu installieren, um „fortwährend Bedrohungen zu identifizieren und zu vermeiden“. Es ist nicht ersichtlich, warum diese Daten für vier gespeichert werden müssen. Bei Unternehmen fallen vielfach 1TByte an Daten pro Tag an. Diese verpflichtend für vier Jahre speichern zu müssen, ist aus unternehmerischer Sicht nicht darstellbar. Zudem hätte die Umsetzung dieser Forderung auch massive ökologische Implikationen, ohne eine signifikante Stärkung der Cyberresilienz zu gewährleisten.

Die deutsche Industrie empfiehlt folgende Anpassung an § 8a Abs. 1b:
„(1b) Betreiber Kritischer Infrastrukturen ~~*müssen*~~ *können* für die Angriffserkennung und -nachverfolgung relevante nicht personenbezogene Daten, die beim Betrieb einer Kritischen Infrastruktur anfallen, *maximal* ~~*mindestens*~~ vier Jahre speichern.“

Die deutsche Industrie fordert die Wiederaufnahme des im Referentenentwurf vom 7. Mai 2020 enthaltenen Paragrafen § 8a Abs. 1 und § 8b Abs. 3d „Überprüfung der Vertrauenswürdigkeit der Beschäftigten“. Die Möglichkeit, dass Betreiber Kritischer Infrastrukturen sowie Unternehmen im besonderen öffentlichen Interesse geeignete Prozesse vorsehen können, um die Vertrauenswürdigkeit der Beschäftigten zu überprüfen, ist von herausgehobener Bedeutung. Neben technischen Maßnahmen ist es sinnvoll, MitarbeiterInnen, die in sicherheitskritischen Stellen im Unternehmen, z.B. in für die IT-Sicherheit zuständigen Abteilungen, tätig sind, auf ihre Vertrauenswürdigkeit zu untersuchen. Die würde die Bestrebungen der Unternehmen, ihre Cyberresilienz ganzheitlich zu stärken, unterstützen. 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.

Wiederaufnahme von Abs. 1 Satz 3 in § 8a:

„*Zur Umsetzung von Maßnahmen nach Satz 1 können Betreiber Kritischer Infrastrukturen auch geeignete Prozesse vorsehen, um die Vertrauenswürdigkeit der Beschäftigten zu überprüfen, die in Bereichen tätig sind, in denen in besonderem Maße auf die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit informationstechnischer Systeme, Komponenten oder Prozesse, die für die Funktionsfähigkeit der Kritischen Infrastruktur maßgeblich sind, eingewirkt werden kann.*“

Zu § 8b „Zentrale Stelle für die Sicherheit in der Informationstechnik Kritischer Infrastrukturen“

Die deutsche Industrie fordert das Bundesamt für Sicherheit in der Informationstechnik dazu auf, die im Rahmen des IT-Sicherheitsgesetz (1.0) eingeführten Pflichten zur kontinuierlichen Aktualisierung eines Lagebilds bezüglich der Sicherheit in der Informationstechnik der Kritischen Infrastrukturen sowie die unverzügliche Unterrichtung der Betreiber Kritischer Infrastrukturen sowie zukünftig auch der Unternehmen im besonderen öffentlichen Interesse umzusetzen (§ 8b Abs. 2 Nr. 3 und 4). Der bisher einmal pro Jahr veröffentlichte Lagebericht zur Cybersicherheit des BSI erfüllt nach Ansicht der deutschen Industrie die Vorgaben des IT-SiG hinsichtlich „kontinuierlich“ und „unverzüglich“ nicht. Grundsätzlich gilt: Die Berichtspflichten müssen verhältnismäßig bleiben. Nur Daten zu meldepflichtigen Vorfällen sollten geteilt werden müssen. Aus den Meldungen an das BSI müssen sich spürbare Vorteile für die betroffenen Unternehmen ergeben.

§ 8b Abs. 3 IT-SiG 2.0 verpflichtet Betreiber Kritischer Infrastrukturen zur Registrierung beim BSI und der Benennung einer jederzeit erreichbaren Kontaktstelle. Es ermöglicht darüber dem BSI, Betreiber Kritischer Infrastrukturen selbst zu registrieren, sofern ein Betreiber die Registrierungspflicht nicht selbst erfüllt. Die deutsche Industrie lehnt die Möglichkeit zur Registrierung eines Unternehmens als Betreiber einer Kritischen Infrastruktur ab. Das BSI sollte vielmehr diese Unternehmen schriftlich zur Registrierung auffordern. Nur so kann zudem sichergestellt werden, dass Unternehmen die Pflicht zur Einrichtung einer jederzeit erreichbaren Kontaktstelle nach § 8b Abs. 3 Satz 3 gewährleistet ist.

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 deutsche Industrie regt daher an, dass § 8b Abs. 3 wie folgt gefasst wird: „(3) Betreiber Kritischer Infrastrukturen sind verpflichtet, die von ihnen betriebenen Kritischen Infrastrukturen beim Bundesamt zu registrieren und eine Kontaktstelle zu benennen. ~~*Die Registrierung eines Betreibers einer Kritischen Infra-struktur kann das Bundesamt auch selbst vornehmen, wenn der Betreiber seine Pflicht zur Registrierung nicht erfüllt.*~~ *Kommt ein Betreiber seiner Pflicht zur Registrierung nicht nach, so weist das Bundesamt den Betreiber auf seine Pflicht zur Registrierung hin und setzt ihm eine Pflicht zur Registrierung.* Die Betreiber haben sicherzustellen, dass sie über die benannte oder durch das Bundesamt festgelegte Kontaktstelle jederzeit erreichbar sind. Die Übermittlung von Informationen durch das Bundesamt nach Absatz 2 Nummer 4 erfolgt an diese Kontaktstelle.“

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 Schutz der relevanten Informationen gewährleistet werden soll. Der BDI fordert daher die Streichung von § 8b Abs. 3a.

~~*„(3a) Rechtfertigen Tatsachen die Annahme, dass ein Betreiber seine Pflicht zur Registrierung nach Absatz 3 nicht erfüllt, so hat der Betreiber dem Bundesamt auf Verlangen die für die Bewertung aus Sicht des Bundesamtes erforderlichen Aufzeichnungen, Schriftstücke und sonstigen Unterlagen in geeigneter Weise vor-zulegen und Auskunft zu erteilen.“*~~

Darüber hinaus sieht der BDI die Anforderung, das Betreiber von Kritischen Infrastrukturen sowie Unternehmen im besonderen öffentlichen Interesse dem Bundesamt alle zur Bewältigung der Störung notwendigen Informationen einschließlich personenbezogener Daten zukommen lassen muss kritisch. Damit Betreiber Kritischer Infrastrukturen sowie Unternehmen im besonderen öffentlichen Interesse dieser Anforderungen nachkommen könnten, braucht es zu mindestens einen hochgradig gesicherten Kommunikationskanal zwischen BSI und dem entsprechenden Betreiber der Kritischen Infrastruktur, respektive des Unternehmens im besonderen öffentlichen Interesse. Bevor solch eine Anforderung umgesetzt werden könnte, müsste dieser Kommunikationskanal etabliert werden. Aus daten- und geheimschutzrechtlichen Erwägungen empfiehlt der BDI jedoch die komplette Streichung von § 8b Abs. 4a.

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. 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, eine Selbsterklärung zur IT-Sicherheit beim Bundesamt vorzulegen. Diese soll Informationen zu folgenden Themen enthalten:

- Zertifizierungen im Bereich der IT-Sicherheit, die in den letzten zwei Jahren durchgeführt wurden und deren Prüfgrundlage sowie Geltungsbereich,
- in den letzten zwei Jahren durchgeführte Sicherheitsaudits oder Prüfungen im Bereich der IT-Sicherheit, deren Prüfgrundlage und Geltungsbereich oder
- wie sichergestellt wird, dass die für das Unternehmen besonders schützenswerten IT-Systeme, Komponenten und Prozesse angemessen geschützt werden und ob dabei der Stand der Technik eingehalten wird.

Die Absicht des Gesetzgebers, weitere Unternehmen in die Erhöhung der IT-Sicherheit einzubeziehen und das IT-Sicherheitsniveau in einer gesamtgesellschaftlichen Perspektive so zu erhöhen ist grundsätzlich begrüßenswert. Aus Sicht der deutschen Industrie ist jedoch unklar, warum gerade die Unternehmen im besonderen öffentlichen Interesse, also zumeist größere Unternehmen, die eine eigene IT-Abteilung mit Cybersicherheitsspezialisten haben, eine Selbsterklärung zur IT-Sicherheit erarbeiten und beim BSI vorlegen müssen. Die Auswirkungen der Corona-Pandemie haben in den vergangenen Monaten verdeutlicht, dass gerade der Ausfall von kleineren Zulieferern weitreichende Auswirkungen auf Wertschöpfungsprozesse in größeren Unternehmen haben kann. Daher sollten zukünftig 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.

Damit Unternehmen dem BSI exakt jene Informationen bereitstellen, die es für eine effiziente Prüfung benötigt, sollte das Bundesamt verpflichtend spätestens sechs Monate nach In-Kraft-Treten des IT-SiG 2.0 ein Formular zur Verfügung stellen, über das die Sicherheitserklärung erfolgen kann. Abs. 2 sollte daher wie folgt angepasst werden:

„(2) Das Bundesamt führt *spätestens sechs Monate nach In-Kraft-Treten dieses Gesetzes* ~~verbindliche~~ Formulare für die Selbsterklärung nach Absatz 1 ein~~*führen*~~. *Die Nutzung dieser Formulare steht Unternehmen im besonderen öffentlichen Interesse frei, sofern sie die darin geforderten Inhalte in geeigneter Weise dem Bundesamt übermitteln.*“

Durch § 8f Abs. 5 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 (vgl. § 8f Abs. 6).

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:
„(5) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 ~~*Nummer 1 und 2 sind verpflichtet, sich binnen ab sechs Monate nach Inkrafttreten dieses Gesetzes beim Bundesamt zu registrieren und eine zu den*~~

~~*üblichen Geschäftszeiten erreichbare Stelle zu benennen. Die Übermittlung von Informationen durch das Bundesamt nach § 8b Absatz 2 Nummer 4 erfolgt an diese Stelle.*~~

~~*(6) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 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 § 8b Absatz 2 Nummer 4 erfolgt an diese Stelle."

Durch § 8f Abs. 7 werden Unternehmen im besonderen öffentlichen Interesse nach § 2 Abs. 14 Nr. 1 und 2 zur unverzüglichen 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. 8) 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 oder vorliegen könnte, 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 zudem hieraus Vorteile ziehen können.

Der BDI empfiehlt folgende Anpassung an den Absätzen7 und 8:

„(7) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1 und 2 ~~haben~~ *sind angehalten* spätestens ab sechs Monate nach Inkrafttreten dieses Gesetzes die folgenden Störungen ~~*unverzüglich*~~ über die nach Absatz 5 benannte Stelle an das Bundesamt zu melden …“

„(8) Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 3 ~~*haben*~~ *sind angehalten* spätestens ab sechs Monate nach Inkrafttreten dieses Gesetzes die folgenden Störungen ~~unverzüglich~~ an das Bundesamt zu melden…“

Der BDI spricht sich zudem ausdrücklich für die Wiederaufnahme der im Referentenentwurf vom 7. Mai 2020 enthaltenen Möglichkeit zur Überprüfung der Vertrauenswürdigkeit von beschäftigten bei Unternehmen im besonderen öffentlichen Interesse aus. Technische und organisatorische IT-Sicherheitsmaßnahmen laufen ins Leere, wenn sie von Personen ausgeführt werden, die dem Unternehmen schaden wollen. Sogenannte Innentäter sind eine der größten Herausforderungen für die Wahrung der Cyberresilienz für Unternehmen. Analog zum vorbeugenden personellen Sabotageschutz im nicht-öffentlichen Bereich sollte Unternehmen im besonderen öffentlichen Interesse die Möglichkeit eingeräumt werden, eine Sicherheitsüberprüfung (Ü1) für Mitarbeitende sowie Bewerberinnen und Bewerber, die in als besonders sicherheitskritischen Bereichen eines Unternehmens tätig sind / sein werden, zu beantragen. Der Staat sollte Unternehmen im besonderen öffentlichen Interesse kostenlos unterstützen, in dem er Sicherheitsüberprüfungen durchführt. Hierfür muss der Staat ausreichende personelle Kapazitäten vorhalten, damit Bewerbungsverfahren zügig abgeschlossen werden können. Nur durch einen ganzheitlichen Ansatz kann die Cyberresilienz Deutschlands nachhaltig und vollumfänglich gestärkt.

Es bedarf der Wiederaufnahme folgender Rechtsvorschrift:

„*(10) § 8a Absatz 1 Satz 3 gilt auch für Unternehmen im besonderen öffentlichen Interesse nach § 2 Absatz 14 Nummer 1, 2 und 3.*“

Zu § 9 Abs. 4 und 4a „Zertifizierung“

In § 9 Abs. 4 wird ergänzt, dass ein Sicherheitszertifikat nur dann erteilt werden darf, wenn informationstechnische Systeme, Komponenten, Produkte oder Schutzprofile die festgelegten Kriterien erfüllen und das BMI die Erteilung nicht untersagt hat. Das BMI kann die Erteilung eines Sicherheitszertifikats untersagen, wenn überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung entgegenstehen (§ 9 Abs. 4a). Die deutsche Industrie sieht zudem sehr kritische die Vermengung von technischer Überprüfung und politischer Bewertung, die in Abs. 4a vorgenommen wird, insbesondere, da § 9b bereits die Möglichkeit zur Untersagung des Einsatzes Kritischer Komponenten durch das BMI eröffnet. Zudem ist zu klären, inwiefern die Untersagung durch das BMI bei jenen IT-Produkten, die nicht Kritische Komponenten und nicht unter die Assurance Levels substantial und high des EU Cybersecurity Acts fallen, europarechtskonform wäre. Der BDI empfiehlt die Streichung dieser Maßnahme. Darüber hinaus wird durch die unmittelbare Beteiligung des BMI eine weitere Behörde in den Kommunikationsreigen mit Herstellern und Betreibern eingezogen. Die deutsche Industrie weist hier erneut auf das Erfordernis einer one-stop-shop Lösung hin.

Die deutsche Industrie empfiehlt zudem die Aufnahme einer Vorrangregelung für die Zertifizierung Kritischer Komponenten nach § 2 Abs. 13 in der Vorrangregelung des § 9 Abs. 2, da das Vorhandensein eines Zertifikats zukünftig Voraussetzung für den weiteren Ausbau Kritischer Infrastrukturen sein wird und eine unnötige Verzögerung aufgrund mangelnder Ressourcen im BSI nicht hinnehmbar wäre. Daher fordert die deutsche Industrie folgende Anpassung:

„(2) Für bestimmte Produkte oder Leistungen kann beim Bundesamt eine Sicherheits- oder Personenzertifizierung oder eine Zertifizierung als IT-Sicherheitsdienstleister beantragt werden. Die Anträge werden in der zeitlichen Reihenfolge ihres Eingangs bearbeitet; hiervon kann abgewichen werden, wenn das Bundesamt wegen der Zahl und des Umfangs anhängiger Prüfungsverfahren eine Prüfung in angemessener Zeit nicht durchführen kann und an der Erteilung eines Zertifikats ein öffentliches Interesse besteht. *Abweichend von Satz 2 werden Anträge auf Zertifizierung von Kritischen Komponenten nach Paragraf 2 Absatz 13 stets innerhalb einer Frist von drei Monaten bearbeitet.* Der Antragsteller hat dem Bundesamt die Unterlagen vorzulegen und die Auskünfte zu erteilen, deren Kenntnis für die Prüfung und Bewertung

des Systems oder der Komponente oder der Eignung der Person sowie für die Erteilung des Zertifikats erforderlich ist."

Die deutsche Industrie empfiehlt zudem die Aufnahme einer Verpflichtung zur schriftlichen Begründung bei Versagung des Zertifikats in Abs.4. Diese wäre aus Gründen eines effektiven Rechtsschutzes zwingend erforderlich. Ebenfalls ist in Abs. 4 zu berücksichtigen, dass der EU Cybersecurity Act vorsieht, dass bereits vorhandene Zertifizierungsschemata innerhalb der EU wechselseitig anerkannt werden. Weitere Prüfungen bzw. ergänzende lokale Verpflichtungen sind im EU Cybersecurity Act nicht vorgesehen. Insofern ist zu kritisieren, dass die Bemühungen der ENISA zur begrüßenswerten harmonisierten Durchsetzung des Cybersecurity Acts durch das IT-SiG 2.0 konterkariert werden. Es widerspricht fundamental dem Ansatz eines harmonisierten EU-Binnenmarktes, wenn auf dem CSA basierende Zertifizierungen in Deutschland nicht anerkannt werden würden. Der BDI sieht daher folgende Ergänzung an § 9 als zwingend erforderlich:

„(4b) *Erteilt das Bundesamt das Sicherheitszertifikat nicht, so erhält der Antragsteller eine schriftliche Begründung über die Gründe für die Nicht-Erteilung innerhalb von einem Monat.*"

„(4c) *Zertifikate, die von anerkannten Konformitätsbewertungsstellen und Nationale Behörden für die Cybersicherheitszertifizierung auf Basis eines Cybersicherheitszertifizierungsschemata nach Verordnung (EU) 2019/881 tragen, sind den Sicherheitszertifikaten dieses Paragraphs gleichgesetzt. Eine erneute Zertifizierung in Deutschland ist nicht notwendig.*"

Zu § 9a „Nationale Behörde für die Cybersicherheitszertifizierung"

Bundesamt für Sicherheit in der Informationstechnik fungiert nach § 9a als nationale Behörde für die Cybersicherheitszertifizierung und übernimmt damit, die in der Verordnung (EU) 2019/881 genannten Aufgaben. Das BSI wird zukünftig Konformitätsbewertungsstellen eine Befugnis im Anwendungsbereich der Verordnung (EU) 2019/881 tätig zu werden. Sowohl das BSI als auch die ernannten Konformitätsbewertungsstellen können ausgestellte Cybersicherheitszertifikate widerrufen oder EU-Konformitätserklärungen im Sinne der Verordnung (EU) 2019/881 für ungültig erklären.

Die deutsche Industrie begrüßt grundsätzlich die Umsetzung der Anforderungen nach Verordnung (EU) 2019/881 in nationales Recht und die Stärkung des BSI als nationale Behörde für die Cybersicherheitszertifizierung. Es ist von herausgehobener Bedeutung, dass das BSI rasch die personellen Ressourcen zur Verfügung hat, um die sich darauf ergebenen neuen Aufgaben zu implementieren. Die deutsche Industrie lehnt es jedoch ab, dass das BSI sowie die nationalen Konformitätsbewertungsstellen EU-weit gültige

Konformitätserklärungen nach Verordnung (EU) 2019/881 für ungültig erklären können. Eine Aberkennung eines Zertifikats sollte im Sinne einer größtmöglichen Binnenmarktsharmonisierung ausschließlich durch die ENISA als europäische Cybersicherheitsagentur erfolgen.

Die deutsche Industrie begrüßt ausdrücklich die nunmehr vorgesehene Trennung zwischen BSI als nationaler Behörde für die Cybersicherheitszertifizierung und privatwirtschaftlichen Konformitätsbewertungsstellen, die durch das BSI auf Antrag ernannt werden. Das BSI sollte selbst nicht als Konformitätsbewertungsstelle fungieren, sondern vielmehr ausschließlich als unabhängige Aufsichtsbehörde agieren.

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 im Einvernehmen mit dem jeweils betroffenen Ressort innerhalb von einem Monat nach Eingang der Anzeige des Einsatzes untersagen (Abs. 3). Unternehmen dürfen während dieser Sperrfrist die angezeigte Komponente nicht einsetzen. Das BMI kann den weiteren Betrieb einer im Einsatz befindlichen Kritischen Komponente untersagen (Abs. 4). Eine Untersagung des Einsatzes weiterer bereits angezeigter (Abs. 6 Nr. 1) und eingebauter Komponenten (Abs. 6 Nr. 2) sowie aller Komponenten des entsprechenden Herstellers (Abs. 7) kann durch das BMI erfolgen.

Es ist richtig, ausschließlich Kritische Komponenten vertrauenswürdiger Hersteller für den Einsatz zuzulassen. § 9b hat jedoch in seiner jetzigen Ausgestaltung unkalkulierbare Risiken für Investitionen von Betreibern Kritischer Infrastrukturen. Die Möglichkeit, die Nutzung von im Einsatz befindlichen Komponenten zu untersagen, kann und wird zu einer stark eingeschränkten Verfügbarkeit von kritischen Services und Produkten für Staat und Gesellschaft führen. Die deutsche Industrie lehnt zudem die Anzeigepflicht des Einsatzes einer Kritischen Komponente ab, da die Anzeigen hochgradig sensible und für das störungsfrei Funktionieren der Kritischen Infrastrukturen enthalten werden. Der BDI empfiehlt, auf die Anzeige zu verzichten.

Die in Abs. 1 vorgesehene Verortung der Zuständigkeit für die Anzeige des Einsatzes Kritischer Komponenten beim Bundesministerium des Innern, für Bau und Heimat wird den Prozess unnötig aufblähen, da das BSI für die Cybersicherheitszertifizierung zuständig ist und im Telekommunikationssektor die Bundesnetzagentur die Federführung innehat. Daraus resultierende Verzögerungen dürften dazu führen, dass sich politische Ziele eines raschen Infrastrukturausbaus in eine fernere Zukunft verschieben. Dies betrifft insbesondere die Möglichkeit, die Nutzung im Einsatz befindlicher Kritischer Komponenten nachträglich zu untersagen.

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. De facto könnten die Betreiber ohnehin nur die formelle Ordnungsmäßigkeit der Herstellererklärung prüfen und dafür haften. Inhaltliche Prüfungen sind den Betreibern ebenso wenig möglich wie eine Haftung dafür zumutbar. An dieser Stelle wird der grundlegende Konstruktionsfehler des IT-Sicherheitsgesetzes als solches deutlich: Die nahezu ausschließliche Betreiberfokussierung führt dazu, dass über Umwege versucht wird, Hersteller regulatorisch zu erfassen.

Erschwerend kommt hinzu, dass sich die in Abs. 2 genannte 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 einzelnen Hersteller im Sinne des Gesetzes, der eine Garantieerklärung zur Vertrauenswürdigkeit abgeben kann, gleichwohl werden quelloffene Bestandteile in nennenswertem Umfang eingesetzt. Daher wäre klarzustellen, wie in solchen Fällen mit der Verpflichtung zur Abgabe einer Garantieerklärung umzugehen ist. 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 Reduktion der Sperrfrist, innerhalb der das BMI den Einsatz angezeigter Kritischer Komponenten untersagen, auf einen Monat ist ein begrüßenswerter Schritt, auch wenn dies weiterhin den Aufbau von TK-Netzen verzögert – wenn auch weniger lang als in früheren Entwürfen angedacht.

Die deutsche Industrie sieht zwingenden Anpassungsbedarf an § 9b Abs. 4. Die Möglichkeit zur Untersagung des weiteren Einsatzes verbauter und im Einsatz befindlicher Kritischer Komponenten durch das BMI kann in Konsequenz dazu führen, dass bestimmte Kritische Infrastrukturen ihre Dienste nicht weiter anbieten können. 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 anhand objektiver Kriterien festgestellt werden kann, dass eine sofortige und unmittelbare Bedrohung ausgeschlossen ist. 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.

Es ist nach dem Gesetzentwurf zudem davon auszugehen, dass die Betreiber das Kostenrisiko eines Rückbaus allein tragen müssen. Unter solchen Rahmenbedingungen besteht eine erhebliche Schwächung der erforderlichen Investitionssicherheit. Hier ist dringend eine Klarstellung erforderlich. Zudem bedarf es Kostenkompensationen, die erforderliche Rück- und Umbaumaßnahmen in einem adäquaten, die realen Kosten abbildenden Rahmen ausgleichen. Dieser staatliche Ersatz wirtschaftlicher Schäden wäre wegen Inanspruchnahme der Betreiber im öffentlichen Interesse, analog beispielsweise dem Vorgehen beim Atom- und/oder Kohleausstieg, zwingend. Auch im KRITIS-Bereich müssen solche Regelungen Anwendung finden. So setzt zum Beispiel die britische Regierung derzeit rechtsstaatliche Anforderung um und hat entschieden, allein für den Verzicht eines Herstellers in britischen Mobilfunknetzen insgesamt rund 280 Mio. Euro an die Netzbetreiber zu zahlen. Die deutsche Industrie fordert daher (1) die Einführung praxisnahen Übergangsfristen, während derer eine Kritische Komponente eines nicht länger als vertrauenswürdig eingestuften Herstellers noch verwendet werden darf; und (2) eine Kostenkompensation bei Rück- und Umbaumaßnahmen:

Der BDI würde eine Streichung von § 9b Abs. 4 präferieren. Sollte an der Einführung von § 9b Abs. 4 festgehalten werden, so ist zwingend folgende Anpassung notwendig:
„(4) Das Bundesministerium des Innern, für Bau und Heimat kann den weiteren Betrieb einer kritischen Komponente gegenüber dem Betreiber der Kritischen Infrastruktur im Einvernehmen mit dem jeweils betroffenen Ressort untersagen oder Anordnungen erlassen, wenn der Hersteller der kritischen Komponente sich als nicht vertrauenswürdig erwiesen hat. *Um die Versorgung mit der Dienstleistung der Kritischen Infrastruktur gewährleistet werden kann, erhält der Betreiber der von Satz 1 betroffenen Kritischen Infrastruktur eine Übergangsfrist, während der der Betreiber die Kritische Komponente uneingeschränkt weiterbetreiben darf.*“

Zudem sollte geklärt werden, dass die Garantieerklärung sowie jedwede Untersagung des Einsatzes von Komponenten sich ausschließlich auf Kritische Infrastrukturen nach § 2 Abs. 10 erstreckt.

Während Hersteller Kritischer Komponenten für einen bestimmten Zeitraum nach Inverkehrbringung ihrer Kritischen Komponenten Updates zur Verfügung stellen, weist die deutsche Industrie mit Blick auf §9b 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 vor Vertragsabschluss gegenüber dem KRITIS-Betreiber transparent darlegen und garantieren, wie lange Updates angeboten werden.

Mit Blick auf §9b 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 oder waren, missbräuchlich auf die Sicherheit, Integrität, Verfügbarkeit oder Funktionsfähigkeit der Kritischen Infrastruktur einwirken zu können. Ein Verstoß nach Nummer 5 liegt nicht vor, wenn der Hersteller nachweisen kann, dass er die technische Eigenschaft im Sinne von Nummer 5 *ordnungsgemäß und nach Stand der Technik 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 von mind. 5-8 Jahren Rechnung getragen werden, um die Netzabdeckung sowie Ausbauverpflichtungen nicht zu gefährden. Die Kostenerstattung bleibt davon unberührt.

Der BDI empfiehlt daher die Ergänzung von § 9b um einen Abs. 8:

„*(8) 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.

Hinsichtlich der bei einer Beurteilung der Vertrauenswürdigkeit zu beteiligenden Institutionen ist es begrüßenswert, dass der Gesetzgeber das Einvernehmen des BMI mit den anderen Ressorts, so insbesondere dem BMWi, als Handlungsvoraussetzung definiert. Zu kritisieren ist hingegen, weshalb er von diesem Grundsatz in Abs. 7 abweicht und bei der wiederholten Feststellung der nicht vorliegenden Vertrauenswürdigkeit eines Herstellers ausschließlich das BMI zur Entscheidung berechtigt, den Einsatz aller Kritischer Komponenten dieses Herstellers zu untersagen, die anderen Ressorts jedoch nicht beteiligt werden. Der BDI fordert daher folgende Anpassung an Abs. 7:

„(7) Bei wiederholter Feststellung nicht vorliegender Vertrauenswürdigkeit nach Absatz 5 Nummer 1 bis 3 kann das Bundesministerium des Innern, für Bau und Heimat *im Einvernehmen mit dem jeweils betroffenen Ressort* den Einsatz aller kritischen Komponenten des Herstellers untersagen.“

Die deutsche Industrie fordert von der BReg, die Cyberresilienz Kritischer Infrastrukturen zu stärken, ohne die Rechts- und Investitionssicherheit für KRITIS-Betreiber zu mindern.

Zu § 9c „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 kennzeichnen können. Nur so entsteht eine brauchbare Vergleichbarkeit der

[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)

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 und
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 auf europäischer Ebene starkmacht. Von jedwedem nationalen Vorhaben zur Einführung eines IT-Sicherheitskennzeichens sollte die Bundesregierung Abstand nehmen. Die deutsche Industrie empfiehlt daher die Streichung von § 9c sowie von § 10 Abs. 3. Stattdessen spricht sich die deutsche Industrie für eine Umsetzung des im EU Cybersecurity Acts enthaltenen „elektronischen Beipackzettels“ aus. Gleichzeitig sollte das BSI jedoch bereits erstellte Technischen Richtlinien der ENISA als Blaupause zur Verfügung stellen bzw. deren europaweite Anerkennung beantragen.

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 § 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 Kriterien zur Identifizierung der in den Anwendungsbereich von § 2 Abs. 14 Nr. 2 fallenden Unternehmen.

Zu § 14 „Bußgelder“

Paragraf 14 Abs. 1 BSIG-E enthält einen Katalog von Ordnungswidrigkeiten. Bei Verstößen gegen die entsprechenden Bestimmungen können Bußgelder bis zu zwei Millionen Euro festgesetzt werden, deren Höhe jedoch aufgrund des Verweises auf § 30 Abs. 2 Satz 3 OWiG für juristische Personen und Personenvereinigungen verzehnfacht werden kann. Die deutsche Industrie begrüßt die signifikante Reduktion der Bußgeldhöhen auf zwei Millionen Euro (im Vergleich zum Entwurf vom 7. Mai 2020). Die nunmehr gewählte Höhe schafft eine akzeptable Balance zwischen staatlicher Bestrafung bei Zuwiderhandlungen gegen die Vorgaben des IT-SiG 2.0 und den Anforderungen der deutschen Wirtschaft, Unternehmen nach einem Cybersicherheitsvorfall nicht mit überbordenden Strafen zu belegen. 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. Die deutsche Industrie lehnt daher entschieden den Verweis auf § 30 Abs. 2 Satz 3 OWiG für juristische Personen und Personenvereinigungen ab. Es braucht eine maßvolle Balance zwischen Ausgleich zwischen angemessener und wirksamer Sanktionierung, der durch den Verweis auf § 30 Abs. 2 Satz 3 OWiG nicht gewahrt wird.

Die deutsche Industrie fordert daher folgende Anpassung an § 14 Abs. 2:
„(2) Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 1 Buch-stabe a, Nummern 2, 9, 13, 14, 16, 17 und 18 mit einer Geldbuße bis zu 2 Millionen Euro geahndet werden~~, auf § 30 Absatz 2 Satz 3 des Gesetzes über Ordnungswidrigkeiten wird verwiesen~~. Die Ordnungswidrigkeit kann in den Fällen des Absatzes 1 Nummer 1 Buchstabe b und Nummern 3, 5, 8, 10, 11, 12 und 15 mit einer Geldbuße bis zu 1 Million Euro geahndet werden. In

den übrigen Fällen kann die Ordnungswidrigkeit mit einer Geldbuße bis zu 100.000 Euro geahndet werden.“

Allerdings können nationale Alleingang 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-Richtlinien und -Verordnungen der vorzugswürdige Weg.

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.

Die textlichen Änderungen entsprechen im Wesentlichen den Änderungen im TKG-E (Stand: 02.11.2020). Misslich ist jedoch, dass das IT-SiG-E an der Stelle die Struktur des TKG-E nicht angenommen hat, so dass ein Abgleich der beiden Gesetzesentwürfe unnötig kompliziert ist. Auch ist es schwierig, dass es an einigen Stellen, wie weiter ausgeführt werden wird, Textpassagen des TKG-E an dieser Stelle im IT-SiG 2.0 nicht entsprechend nachgezogen werden.

Im weiteren Gesetzgebungsprozess müssen die folgenden Punkte unbedingt berücksichtigt werden:

Zu § 109 Abs. 2 Einsatz Kritischer Komponenten

Entsprechend den Anpassungen an § 109 TKG, dürfen Betreiber öffentlicher Telekommunikationsdienste nur Kritische Komponenten einsetzen, die von einer anerkannten Prüfstelle überprüft und von einer anerkannten Zertifizierungsstelle zertifiziert wurden. Für die deutsche Industrie ist eine leistungsfähige, sichere, souveräne, vertrauenswürdige und verlässliche digitale Infrastruktur von zentraler Bedeutung, um die Wettbewerbsfähigkeit der Industrie am Standort Deutschland nachhaltig zu stärken. Sicherheit hat oberste Priorität und muss sowohl auf europäischer als auch auf nationaler Ebene gedacht werden.

So wird bspw. die in § 162 TKG-E verwendet Formulierung „daran mitwirkt“ hier nicht nachvollzogen. Das ist unglücklich, da mit der neuen Kategorie betroffener Unternehmen die Grundlagen für konkrete Mitwirkungspflichten definiert werden könnten. Sinnvollerweise sollten, wie bereits mehrfach erläutert, auch Hersteller von Komponenten mit kritischen Funktionen im Allgemeinen, aber auch im TKG im Speziellen, als Regelungsadressat erfasst sein. Entsprechend wäre es begrüßenswert, wenn in § 162 TKG-E Absätze 2 und 4 „Mitwirker“ analog zu Absatz 1 TKG-E ebenfalls als Regelungsadressaten benannt werden, so dass auch der Katalog der Sicherheitsanforderungen nach § 164 TKG-E (vormals § 109 Abs. 6) eine unmittelbare Wirkung entfalten und eine angemessene Verteilung der Verantwortung für Telekommunikationsinfrastrukturen bewirkt werden kann.

Die Ausgestaltung von Prüfkriterien, Regeln und Verfahrens sollte zwingend risikobasiert erfolgen. An als kritisch einzustufende Komponenten und Funktionen sind zur Risikoreduzierung unter Umständen höhere Anforderungen zu stellen. Bei der Ausgestaltung weiterführender Sicherheitsanforderungen darf jedoch nicht außer Acht gelassen werden, dass nach § 109 TKG und dem Katalog der Sicherheitsanforderungen 1.0 ohnehin angemessene, erforderliche technische Vorkehrungen und sonstige Maßnahmen zum Schutz der Telekommunikationsdienste und -netze für jede Komponente und Funktion zu treffen sind. Mit dieser über Jahrzehnte geltenden und für jeden Anwendungsfall modifizierbaren Anforderung, bestehen bereits – wie die Praxis gezeigt hat – gute und bewährte Regelungen. Diese Feststellung steht der Auffassung des BDI nicht entgegen, in der Praxis bessere Vorkehrungen zum Schutz der Telekommunikationsdienste und -netze zu treffen. Insbesondere, da sich die Arten der Bedrohung von Telekommunikationsinfrastrukturen gewandelt haben, gegen die sich verantwortungsvoll handelnde Betreiber, aber auch Staaten, schützen müssen. Offene Angriffe sind seltener geworden. Subtile Angriffe aber, die oft indirekt erfolgen und bisweilen über Jahre unbemerkt bleiben bevor sie aktiviert werden (sog. Advanced Persistant Threats, APT) – und die deswegen umso wirkungsvoller sind – haben an Bedeutung gewonnen.

Aus Abs. 2 ist nicht ersichtlich, dass eine Betriebserlaubnis für die Verwendung von Komponenten nur für einen in der Zukunft liegenden Zeitpunkt erteilt werden kann. Insofern ist hier, analog der grundsätzlichen Klarstellung im BSIG-E, eine Klarstellung erforderlich, dass diese Anforderung ausschließlich für in der Zukunft zum Einsatz kommende Technik greifen soll, so dass ein umfassender Bestandsschutz gewährleistet werden kann. Gleichzeitig muss jedoch sichergestellt werden, dass durch die Überprüfung und Zertifizierung keine langwierigen bürokratischen Verfahren entstehen, die den Einsatz innovativer Technologien verzögern.

Die deutsche Industrie empfiehlt daher folgende Anpassung an Abs. 2 Satz 3:

„Kritische Komponenten im Sinne des § 2 Absatz 13 des BSI-Gesetzes dürfen nur eingesetzt werden, wenn sie *vor dem erstmaligen Einsatz* ~~*von einer anerkannten Prüfstelle überprüft*~~ und von einer anerkannten Zertifizierungsstelle *überprüft und* zertifiziert wurden.“

Zu § 109 Abs. 6 Katalog von Sicherheitsanforderungen

Nach § 109 Abs. 6 TKG-E erstellt die BNetzA im Einvernehmen mit dem BSI und dem BfDI einen Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie

für die Verarbeitung personenbezogener Daten. Dieser definiert (1) die Einzelheiten der zu treffenden technischen Vorkehrungen und sonstigen Maßnahmen, (2) die Vorgaben zur Bestimmung der kritischen Komponenten sowie (3) die Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial.

Die Bundesnetzagentur hat bereits den Sicherheitskatalog nach § 109 Abs. 6 TKG in den vergangenen Monaten unter Beteiligung der Industrie überarbeitet. Auch wurde die Erarbeitung zur Liste kritischer Funktionen bereits initiiert. Die deutsche Industrie erachtet eine sehr enge Verzahnung sowie zeitgleiche Beratung aller relevanter Rechtsvorschriften, inkl. IT-SiG 2.0, Sicherheitskatalog, Liste Kritischer Komponenten, Liste Kritischer Funktionen und TKG-Novelle, als zwingend erforderlich, damit sich widersprechende Vorgaben vermieden werden. Das bisher sehr unabgestimmte und zeitlich verzögerte sowie versetzte Vorgehen ist nicht weiter hinnehmbar, insbesondere da die Betreiber von Telekommunikationsnetzen weitreichende Ausbauverpflichtungen im Rahmen der Frequenzauktion eingegangen sind. Ziel muss es daher sein, praxistaugliche Anforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen zu schaffen.

Der Anwendungsbereich des TKG und des Sicherheitskatalogs nach § 109 TKG richtet sich im Wesentlichen an die Betreiber von Telekommunikationsnetzen. Gleichzeitig gilt, dass Sicherheit einen kooperativen Ansatz mit Pflichten und Verantwortungszuweisungen für alle Akteure voraussetzt. Daher bedarf es einer zusätzlichen adäquaten Regelung an anderer Stelle.

Kritisch ist hier, dass nach Abs. 6 Satz 1 Nr. 3 die Erweiterung des TKG-E, in Form der Ermächtigung zum Erlass eines Katalogs von Sicherheitsanforderungen für das Betreiben von Telekommunikationssystemen um Anforderungen zur Offenlegung und Interoperabilität von Schnittstellen von Netzkomponenten einschließlich einzuhaltender technischer Standards, nicht nachvollzogen wurde. Damit fehlt hier die Schaffung der Grundlage, soweit erforderlich Open RAN auch regulatorisch zu unterstützen, um bestehende Abhängigkeiten herstellerunabhängig zu reduzieren.

Insofern ist die Aufnahme folgender konkreter Änderung aus dem TKG-E erforderlich:

„4. Der Katalog von Sicherheitsanforderungen nach Satz 1 kann auch Anforderungen zur Offenlegung und Interoperabilität von Schnittstellen von Netzkomponenten einschließlich einzuhaltender technischer Standards enthalten.“

Es muss zudem klargestellt werden, dass die Anforderungen nach § 109 TKG Abs. 6 nur für jene öffentliche Telekommunikations- und Datenverarbeitungsinfrastrukturen gilt, die nach In-Kraft-Treten des IT-SiG 2.0 und der sich anschließenden Veröffentlichung des überarbeiteten Sicherheitskatalogs nach § 109 Abs.6 TKG sowie der Liste Kritische Funktionen und der Liste Kritischer modernisiert oder gebaut werden. Bestehende Telekommunikations- und Datenverarbeitungssysteme müssen Bestandsschutz genießen. Die in Abs. 6 Satz 3 vorgesehene Umsetzung der Pflichten aus dem Sicherheitskatalog innerhalb von einem Jahr, sofern der Katalog keine anderen Fristen angibt, erscheint hinsichtlich der Komplexität der Prüfungen nicht sachgerecht. Eine Zertifizierung aller Komponenten dürfte in diesem Zeitraum kaum möglich sein.

Die deutsche Industrie fordert daher eine Präzisierung von § 109 Abs. 6 Satz 3:

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

Zu § 109 Abs. 7 Überprüfung durch qualifizierte unabhängige Stelle

Nach § 109 Abs. 7 TKG-E sind Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial verpflichtet, sich alle zwei Jahre einer Überprüfung durch eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde zu unterziehen. Darauf werden sich zusätzliche Mehraufwände für die betroffenen Unternehmen ergeben.

Abs. 7 sieht zudem vor, dass die BNetzA zur Überprüfung einzelner Verpflichtungen Dritte beauftragen kann, insbesondere auch andere nationale Behörden. Doppelzuständigkeiten führen zu Intransparenz und zum Teil widersprüchlichen Ausführungen/Interpretationen zu/von Verpflichtungen, woraus sich Risiken zu Lasten der Sicherheit ergeben können. Zudem führen Doppelzuständigkeiten zu höheren Aufwänden auf Seiten aller Beteiligten und zu einer Verlangsamung notwendig umzusetzender Maßnahmen. Vor diesem Hintergrund schlagen wir vor, die in diesem Absatz definierten Kompetenzen ausschließlich der BNetzA zu übertragen.

Die deutsche Industrie empfiehlt daher folgende Änderungen:

„(7) Die Bundesnetzagentur kann anordnen, dass sich die Betreiber öffentlicher Telekommunikationsnetze oder die Anbieter öffentlich zugänglicher Telekommunikationsdienste einer Überprüfung ~~*durch eine qualifizierte*~~

~~*unabhängige Stelle oder eine zuständige nationale Behörde*~~ unterziehen, in der *durch die Bundesnetzagentur* festgestellt wird, ob die Anforderungen nach den Absätzen 1 bis 4 erfüllt sind. Unbeschadet von Satz 1 haben sich Betreiber öffentlicher Telekommunikationsnetze mit erhöhtem Gefährdungspotenzial alle zwei Jahre einer Überprüfung durch ~~*eine qualifizierte unabhängige Stelle oder eine zuständige nationale Behörde*~~ *die Bundesnetzagentur* zu unterziehen, in der festgestellt wird, ob die Anforderungen nach den Absätzen 1 bis 4 erfüllt sind. Die Bundesnetzagentur legt den Zeitpunkt der erstmaligen Überprüfung fest. ~~*Der nach den Sätzen 1 und 2 Verpflichtete hat eine Kopie des Überprüfungsberichts unverzüglich an die Bundesnetzagentur und an das Bundesamt für Sicherheit in der Informationstechnik, sofern dieses die Überprüfung nicht vorgenommen hat, zu übermitteln. Er trägt die Kosten dieser Überprüfung.*~~ Die Bewertung der Überprüfung sowie eine diesbezügliche Feststellung von Sicherheitsmängeln im Sicherheitskonzept nach § 163 erfolgt durch die Bundesnetzagentur im Einvernehmen mit dem Bundesamt für Sicherheit in der Informationstechnik.“

Zu § 113 „Manuelle Auskunftsverfahren“

Zukünftig dürfen Unternehmen, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken, auch auf schriftliches Verlangen durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) dem BSI Daten zukommen lassen. Diese Erweiterung ist aus Sicht der deutschen Industrie mit Blick auf die vorgenannten Anpassungen am BSIG und TKG zielführend. Die bloße Erwähnung des BSI als eine zum Datenabruf berechtigte Stelle ist dabei aber aus rechtlicher Sicht nicht ausreichend. Wie bei den übrigen zum Datenabruf berechtigen Behörden müssen auch hier die Tatbestandsvoraussetzungen für den Abruf von Daten und deren Verwendungszwecke detailliert aufgelistet werden, um den Vorgaben des Bundesverfassungsgerichts zu entsprechen. Der Entwurf ist entsprechend anzupassen.

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 § 15d „Meldepflicht bei unrechtmäßiger Übermittlung oder unrechtmäßiger Kenntniserlangung von Daten“

Grundsätzlich ist die Aufnahme der Meldeverpflichtung für sogenannte Over-the-Top-Anbieter bei Sicherheitsvorfällen sinnvoll und zielführend, um das Sicherheitsniveau insgesamt zu heben. Um nicht jeden einzelnen Datenabfluss meldepflichtig zu machen, wurden richtigerweise Kriterien zum drohenden Schadensausmaß aufgenommen. Diese erscheinen allerdings wenig klar und werden zu Rechtsunsicherheit führen.

Kritischer ist aber die Unterrichtungspflicht des Diensteanbieters an das BKA, da dies eine weitere Meldestelle bedeutet, die den Abstimmungsbedarf zur Erfüllung der Pflichten weiter komplexiert. Für Anbieter von TK- und Mediendiensten kann dabei im ungünstigsten Fall ein Schadensereignis unabhängige Meldungen an BSI, BNetzA und BKA bedeuten. Der hiermit verbundene Mehrfachaufwand wird erheblich sein und de facto die Ressource, die für die Behebung des Vorfalls benötigt wird, allein mit Reporting-Aufgaben binden. Der BDI spricht sich bei jedweder Meldepflicht die Umsetzung des one-stop-shop-Prinzips aus, um Meldungen für die betroffenen Unternehmen effizient durchzuführen.

Im Unterschied zu der als Vorbild dienenden – und noch nicht in Kraft getretenen – Regelung des § 3a NetzDG enthält § 15d TMG-E keine Vorschrift zur Information des Betroffenen. Es muss deshalb davon ausgegangen werden, dass die Information des Betroffenen durch das BKA erfolgt. Wann und unter welchen Voraussetzungen ein Betroffener durch das BKA informiert wird, erschließt sich bisher nicht.

Die Übermittlung an das BKA muss, sofern vorhanden, die für eine retrograde Identifizierung des jeweiligen Anschlussinhabers erforderlichen Daten, insbesondere die IP-Adresse einschließlich der Portnummer und des Zeitstempels enthalten. Die Pflicht zur Übermittlung der Portnummer erscheint allerdings fragwürdig, da sie keinen wesentlichen Mehrwert für die Identifizierung eines Internetnutzers bringt. So müssten die Internetzugangsprovider ihrerseits ebenfalls Portnummern speichern, um dem BKA einen Abgleich mit den vom Telemedienanbieter übermittelten Daten zu ermöglichen. Wie sich in der Diskussion um die Einführung der entsprechenden

Meldepflicht nach dem NetzDG gezeigt hat, ist dies zumindest bei den großen Internetzugangsdiensteanbietern nicht der Fall. Damit ist die Übermittlung eventuell vorhandener Portnummern weder sinnvoll noch verhältnismäßig.

Wer mehr als 100.000 Kunden hat, hat für die Übermittlung der Benachrichtigung an das BKA eine gesicherte, elektronische Schnittstelle bereitzuhalten und zu nutzen. Die Ausgestaltung der Schnittstelle soll sich nach den Anforderungen des BKA richten. Es wäre wünschenswert, wenn dabei bereits andere vorhandene elektronische Kommunikationswege berücksichtigt werden könnten. So dürften einige der nach § 15d TMG Verpflichteten bereits über eine Schnittstelle zur Übermittlung und zum Empfang elektronischer Dokumente im Bereich der Telekommunikationsüberwachung verfügen. Ebenso verfügt das BKA über eine solche ETSI-ESB. Zur Vermeidung unnötiger Investitionen auf Seiten der Provider sollte die Nutzung dieser alternativen sicheren Kommunikationskanäle in jedem Fall erlaubt werden. Zudem braucht es eine klarere Definition des Begriffs „Kunde“. Aktuell ist unklar, ob darunter sowohl private als auch juristische Personen fallen.

Zu Artikel 4 – Änderung des Gesetzes über die Elektrizitäts- und Gasversorgung (EnWG)

Zu § 11 Einführung der Abs. 1d, 1e und 1f

Unternehmen des KRITIS-Sektors „Energie“, die unter den Anwendungsbereich des IT-SiG 2.0 und der KRITIS-VO fallen, müssen (1d) in ihren informationstechnischen Systemen, Komponenten oder Prozessen, die für die Funktionsfähigkeit der von ihnen betriebenen Energieversorgungsnetze oder Energieanlagen maßgeblich sind, in angemessener Weise Systeme zur Angriffserkennung einsetzen; (1e) für die Angriffserkennung und Angriffsnachverfolgung relevante nicht personenbezogene Daten, die beim Betrieb eines Energieversorgungsnetzes oder einer Energieanlage anfallen, mindestens vier Jahre speichern; und (1f) die Erfüllung der Anforderung nach Abs. 1d dem BSI nachweisen.

Das Vorhalten von Systemen zur Angriffserkennung ist aus Sicht des BDI eine sinnvolle Maßnahme, um die Cyberresilienz Kritischer Infrastrukturen zu stärken. Es ist jedoch zu prüfen, inwiefern die Nutzung solcher Systeme zum Verlust von Gewährleistungs- und Wartungsansprüchen führen können.

Die deutsche Industrie lehnt die Anforderung nach Abs. 1e als völlig realitätsfern ab. Betreiber Kritischer Infrastrukturen werden in § 8a Abs. 1a BSIG-E und § 11 Abs. 1d verpflichtet, Systeme zur Angriffserkennung zu installieren, um „fortwährend Bedrohungen zu identifizieren und zu vermeiden“. Es ist nicht ersichtlich, warum diese Daten für vier Jahre gespeichert werden müssen. Bei Unternehmen fallen vielfach 1TByte an Daten pro Tag an. Diese verpflichtend für vier Jahre speichern zu müssen, ist aus unternehmerischer Sicht nicht darstellbar. Zudem hätte die Umsetzung dieser Forderung auch massive ökologische Implikationen, ohne eine signifikante Stärkung der Cyberresilienz zu gewährleisten.

Die deutsche Industrie empfiehlt folgende Anpassung an § 11 Abs. 1e:
„(1e) Nach Absatz 1d Verpflichtete ~~*müssen*~~ *können* für die Angriffserkennung und -nach-verfolgung relevante nicht personenbezogene Daten, die beim Betrieb eines Energie-versorgungsnetzes oder einer Energieanlage anfallen, *maximal* ~~*mindestens*~~ vier Jahre speichern.“

Zu Artikel 5 – Änderung der Außenwirtschaftsverordnung

Zu § 55 Abs. 1 Satz 2 Nr. 2 – Kritische Komponenten

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 § 55 Abs. 1 AWV eine Nummer 2 mit Wortlaut „kritische Komponenten im Sinne des § 2 Absatz 13 des BSI-Gesetzes entwickelt oder herstellt“ eingeführt werden. Folglich könnte das BMWi zukünftig all jene Unternehmenserwerbungen und Unternehmensanteilserwerbungen von Unternehmen, die kritische Komponenten nach § 2 Abs. 13 des BSI-Gesetzes fertigen, prüfen.

Die deutsche Industrie spricht sich grundsätzlich für den Schutz der digitalen technologischen Souveränität der deutschen Wirtschaft aus. Vor diesem Hintergrund scheint eine Einführung von Nr. 2 in § 55 Abs. 1 AWV verständlich. Allerdings ist die im 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 zusätzlich jedwede kritische Komponente, 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 Entsorgung von Siedlungsabfällen“.

Offene Grenzen und Auslandsinvestitionen sind von großer Relevanz 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 IT-SiG 2.0 abzulehnen.

Einführung Artikel 7 – Evaluierung

Die im Gesetz nunmehr vorgesehene Evaluierung begrüßt die deutsche Industrie ausdrücklich. Allerdings wird keine vollumfängliche Evaluierung des IT-SiG 2.0 angestrebt. Die deutsche Industrie fordert, dass Artikel 7 eine verpflichtende vollumfängliche Evaluierung des IT-SiG 2.0 nach spätestens vier Jahren, jedoch zwingend vor einem IT-SiG 3.0 vorschreibt. Wir schlagen daher folgende Formulierung vor und empfehlen die Streichung der bisherigen Formulierung:

§ 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 vollumfängliche 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 Artikel 7 § 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 dritten 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 1287