bitkom

Auf einen Blick

IT-Sicherheitsgesetz 2.0

Bitkom-Bewertung

Bitkom unterstützt die Zielsetzung der Bundesregierung, IT-Sicherheit zum Schutz der a) Kritischen Infrastrukturen, b) Bundesverwaltung und c) Verbraucher zu gewährleisten. Allerdings erachtet Bitkom die angedachte Umsetzung in wesentlichen Punkten als **kritisch und überarbeitungsbedürftig**.

Das Wichtigste

- **Unzureichende Festlegung auf Schutzziele**
  Bitkom fordert ein klares, dem IT-SiG 2.0 vorangestelltes Konzept zu den Schutzzielen Vertraulichkeit, Integrität und Verfügbarkeit sowie die konsistent darauf ausgerichtete, gesetzgeberische Umsetzung. Nur auf Basis eines klaren Zielverständnisses und einer nachvollziehbaren Evaluierung des IT-SiG 2015 lassen sich geeignete Schutzmaßnahmen definieren. Diese sind dabei im Hinblick auf Innovationsfreundlichkeit, Investitionsschutz und Rechtssicherheit auf ihre Tauglichkeit zu bewerten. Sicherheit und Schutz sind Zustände, die erreicht und gehalten werden müssen. Dies kann nicht statisch geschehen, sondern die Maßnahmen, die Sicherheit und Schutz bewirken, bedürfen einer permanenten Wirksamkeitsprüfung, Anpassung und Weiterentwicklung.

- **Wenig zielgerichtete Regulierung**
  Als unmittelbare Folge der fehlenden Konkretisierung von Schutzzielen wirkt das Gesetz inhaltlich überdehnt. Dies gilt sowohl für den sich zwischen BSI und den Sicherheitsbehörden abzeichnenden Interessenskonflikt, als auch für den nach wie vor zu unbestimmten Begriff der Vertrauenswürdigkeit. Der Schutzbedarf ist in erster Linie etwas technisch-agnostisches und bedarf einer regel- und kritikalitätsbasierten Prüfung (und Zertifizierung). Anders als überprüfbare technische Kriterien sind Garantieerklärungen ein politisch motiviertes Instrument, ohne in der Umsetzung ausreichend Rechtssicherheit zu gewährleisten. Dies mag zwar sicherheitspolitisch gewollt sein, Bitkom lehnt die jetzige Ausgestaltung jedoch ab.

- **Fokussierung der Kompetenzen von BSI und BMI erforderlich**
  Betreiber kritischer Infrastrukturen und auch Unternehmen im besonderen öffentlichen Interesse haben die Hoheit über ihre Prozesse, Ausstattungen und Geschäftstätigkeit. Bitkom lehnt technische Zugriffs- und Weisungsbefugnisse des BSI ebenso ab, wie pauschale Anordnungsbefugnisse des BMI. Dabei wird mit der erstmaligen Nennung von Interoperabilität eine eigentlich gestalterische Maßnahme mit Visionspotenzial zur langfristigen Steigerung der IT-Sicherheit im Gesetzestext in Betracht gezogen. Weshalb der Gesetzgeber diesen Punkt starr und bestrafend anstatt stimulierend ausgestaltet, erschließt sich Bitkom nicht.

- **Mangelnde Einbindung der Wirtschaft**
  Eine rechtzeitige Beteiligung der Wirtschaft im Gesetzgebungsverfahren ist unabdingbar. Bitkom stellt fest, dass bereits zum wiederholten Male Fristen zur Stellungnahme gesetzt werden, die eine der volkswirtschaftlichen Bedeutung des Themas angemessene Befassung nicht zulassen und der Betroffenheit der Wirtschaft nicht gerecht werden. Während einer laufenden Frist zur Stellungnahme einen wesentlich abgeänderten, nicht final abgestimmten Entwurf herauszugeben und eine 27-stündige Frist zur Kommentierung anzusetzen, ist absolut inakzeptabel.

Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
19(4)741 A

bitkom

Stellungnahme

zum Entwurf für ein zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)

10.12.2020

Bitkom
Bundesverband
Informationswirtschaft,
Telekommunikation
und Neue Medien e.V.

Sebastian Artz
Referent IT-Sicherheit
s.artz@bitkom.org

Albrechtstraße 10
10117 Berlin

Präsident
Achim Berg

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Vorwort

Das Bundesministerium des Innern, für Bau und Heimat (BMI) hat am 02.12.2020 einen nicht abgestimmten Diskussionsentwurf eines zweiten Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0) vorgelegt und bis zum 09.12.2020 um Stellungnahme gebeten. Kurz vor Ablauf der eigens durch das BMI gesetzten laufenden Frist wurde am 09.12.2020 ein signifikant abgeänderter, nach wie vor nicht ressortübergreifend abgestimmter Referentenentwurf zirkuliert, zu dem innerhalb von 27 Stunden, bis zum 10.12.2010 um 14 Uhr, Stellung bezogen werden soll. **Ein derartiges Vorgehen ist absolut inakzeptabel.**

Angesichts der wachsenden Bedeutung des Cyberraums und informationstechnischer Systeme in der gesamten wirtschaftlichen und gesellschaftlichen Breite, und der damit einhergehenden hybriden und sich ausweitenden Bedrohungslage, ist es grundsätzlich zu begrüßen, dass die Bundesregierung Cyber- und IT-Sicherheit verstärkt in den Blick nimmt. Es stellen sich jedoch unmittelbar daran anknüpfend richtungsweisende Folgefragen, die der Gesetzgeber unbeantwortet lässt. Aktuell fehlt dem Gesetzesentwurf ein klares Bekenntnis dazu, welche konkreten Schutzziele mit dem IT-SiG 2.0 verfolgt werden sollen. Nur auf Basis eines klaren Zielverständnisses lassen sich geeignete Maßnahmen auswählen. Dabei müssen alle Maßnahmen auf Innovationsfreundlichkeit, Investitionsschutz und Rechtssicherheit überprüft und bewertet werden.

Grundprämisse für die Gewährleistung eines hohen Cybersicherheitsniveau ist, dass alle relevanten Stakeholder, von Betreibern über Hersteller bis hin zu staatlichen Stellen, auf vertrauensvoller und kooperativer Basis an einem Strang ziehen und ihre jeweilige Verantwortung innerhalb des Gesamtökosystems übernehmen. Eins muss ins andere greifen, denn im Cyberraum beginnen die Gefahren am schwächsten Glied in der Kette. Hierzu bedarf es des fairen und innovationsstimulierenden Wettbewerbs, basierend auf gleichen Regeln für gleiche Dienste und Angebote sowie der Vielfalt von Technologien und Anbietern. Die Relevanz eines technologieneutralen Ansatzes ist dabei von fundamentaler Bedeutung. Für alle Hersteller – ganz gleich welcher Produkte und Angebote sowie unabhängig ihrer Herkunft – sollten die gleichen produkt- und angebotsspezifi-

schen Prüfkriterien, Regeln und Verfahren gelten. Dabei darf sich das Zusammenwirken mitnichten nur auf die nationale Ebene beschränken. In einem starken, vereinten und zukunftsgerichteten Europa muss Cyber- und IT-Sicherheit global, mindestens aber gesamteuropäisch, gedacht werden. Andernfalls würden selbst gut gemeinte Maßnahmen als Sammelsurium nationaler Alleingänge ohne signifikante Steigerung des Sicherheitsniveaus ins Leere laufen. Die Kohärenz der deutsch-europäischen Cybersicherheitsausrichtung ist für Bitkom von zentraler Bedeutung.

Vor diesem Hintergrund muss Bitkom die folgenden erfolgskritischen Punkte im aktuellen Entwurf des IT-SiG 2.0 zur Sprache bringen:

Legislative Interdependenzen im Gesamtkontext und generelle Verfahrenskritik

Komplexität ist der größte Feind von Sicherheit. Mit dem wechselseitigen Zusammenspiel aus

- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG (2.0)),
- Europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-Richtlinie (2.0)),
- Verordnung zur Bestimmung Kritischer Infrastrukturen nach BSIG (KRITIS-V),
- Telekommunikationsgesetz (TKG),
- Telekommunikationsmodernisierungsgesetz (TKG-E),
- Katalog von Sicherheitsanforderungen für das Betreiben von Telekommunikations- und Datenverarbeitungssystemen sowie für die Verarbeitung personenbezogener Daten nach § 109 TKG (insb. Anhang II),
- Liste der kritischen Funktionen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial als Ergänzung zur Anlage 2 des Katalogs von Sicherheitsanforderungen nach § 109 Abs. 4 TKG,
- EU Cybersecurity Act (CSA, Verordnung EU 2019/881),
- verschiedener (CSA-)Zertifizierungsschemata,
- einzelner Technischer Richtlinien des BSI und
- weiterer noch zu spezifizierender Rechtsverordnungen

existiert eine multidimensionale Gemengelage, bei der es essenziell ist, dass sich alle Elemente nahtlos zusammenfügen. Mit der parallelen Überarbeitung sowie der erstmaligen Anfertigung einiger der genannten Gesetzestexte besteht grundsätzlich das inhärente Risiko, ein dysfunktionales Gesamtkonstrukt zu schaffen. Es ist dringend geboten, die Konsolidierung der Regelungsgegenstände eng und widerspruchsfrei zu fassen und Redundanzen auszuschließen. Die verzögerte Veröffentlichung der

verschiedenen Gesetzestexte hat Zweifel an einem konsistenten Gesamtvorgehen genährt, mit negativen Konsequenzen für die Erwartungs-, Investitions-, und Rechtssicherheit in der Wirtschaft. Das wiederholte Vorlegen eines inoffiziellen und an zentralen Stellen unvollständigen »Diskussionsentwurfs« eines TKG-E hat dies ebenso sehr verdeutlicht wie der am 2. Dezember vorliegende, nicht abgestimmte Gesetzestext eines IT-SiG 2.0. Trotz der enormen Relevanz der Gesetzesinhalte und ungeachtet einzelner im Vorfeld publik gewordener Referentenentwürfe wurde lediglich eine Kommentierungsfrist von einer Woche gewährt, nachdem ursprünglich sogar nur eine 2,5 arbeitstägige Frist angesetzt wurde. Unmittelbar vor Ablauf der vom BMI eigens nach außen getragenen Kommentierungsfrist wurde dann ein wesentlich abgeänderter, nicht im Änderungsmodus nachvollziehbarer Referentenentwurf, mit einer Kommentierungsfrist von 27 Stunden, an die unmittelbar betroffene Wirtschaft übermittelt.

Der Bundesregierung und den Bundesministerien ist es in einer zweijährigen Debatte nicht gelungen, einen aus ihrer Sicht konsistenten Referentenentwurf zu entwickeln. Das federführende BMI hat es zudem versäumt, eine frühzeitige, sachgerechte Beteiligung der Betroffenen zu ermöglichen. Dies wird der Betroffenheit der gesamten Wirtschaft in keiner Weise gerecht.

Vernachlässigung der kooperativen und dialogbasierten Erfolgskomponente zur Steigerung der IT-Sicherheit

Transparenz ist eine wesentliche Grundlage für Vertrauen. Dies setzt einen kooperativen Ansatz mit klar definierten Regeln für alle Seiten voraus. Der Gesetzgeber hat mit dem IT-SiG 2015 einen aus Sicht des Bitkom passenden regulatorischen Rahmen gesetzt und ca. 2.000 Betreiber kritischer Infrastrukturen sowie deren Zulieferer verpflichtet, ein ISMS (Informationssicherheitsmanagementsystem) einzuführen bzw. das bestehende zu ergänzen. Die dort für Unternehmen bzw. Behörden geltenden Regelungen sind regelmäßig zu evaluieren und auf Basis von Erfahrungen und Risiken zu überarbeiten. Bitkom erwartet eben diese Best Practice auch von Gesetzgeber, d. h. die Evaluation und risikogemäße Weiterentwicklung des IT-SiG. Mit dem IT-SiG 2.0 wird nun allerdings der regulative Rahmen ausgeweitet, ohne dass den betroffenen Branchen der gesetzgeberische Handlungsbedarf aufgezeigt wurde. Damit wird die erfolgskritische kooperative, gemeinschaftliche Herangehensweise zugunsten eines verstärkt bestimmenden Ansatzes vernachlässigt. Zweckdienlicher wäre es, die vertrauensvolle Zusammenarbeit im Rahmen der bereits etablierten und geschätzten Initiativen des UP KRITIS sowie der Allianz für Cyber-Sicherheit zu stärken und die dortigen Erkenntnisse über entsprechende Feedback-Schleifen verstärkt im Gesetzgebungsprozess zu berücksichtigen. Aus unserer Sicht muss die nachvollziehbare Evaluierung des IT-SiG 2.0 im Vorfeld der Ausarbeitung eines

IT-SiG 3.0 verpflichtend gemacht werden. Gleiches gilt für die Ausgestaltung künftiger Rechtsverordnungen. Bereits bestehende Gesprächskanäle können hier problemlos und ressourcenschonend genutzt werden. Ein Mangel an Koordination manifestiert sich dabei auch auf europäischer Ebene.

Die sicherheitsfördernde Hebelwirkung legislativer Harmonisierung auf europäischer Ebene wird unzureichend berücksichtigt

Durch die Verzögerung auf deutscher Seite kommt es aktuell zur parallelen Überarbeitung des IT-SiG und dessen europäischen Pendant, der NIS-Richtlinie. Während das IT-SiG 2015 im Vorfeld der Verabschiedung der NIS-Richtlinie im Jahr 2016 als Musterbeispiel herangezogen werden konnte, besteht aktuell keine Abstimmung beider Verfahren, so dass – obwohl beide Vorhaben auf die Steigerung des Schutzes kritischer Infrastrukturen abzielen – die parallel stattfindenden Überarbeitungen in Silos stattfinden und der übereinstimmenden Zielsetzung zuwiderlaufen. Unsere Sorgen beruhen konkret auf drei Vorhaben des deutschen Gesetzgebers:

1. Einführung einer neuen nationalen Sonderkategorie: »Unternehmen von besonderem öffentlichen Interesse« (§ 2 Abs. 14 in Verbindung mit § 8f BSIG-E)
2. Ausweitung der nationalen KRITIS-Sektoren auf den Bereich der »Siedlungsabfallentsorgung« (§ 2 Abs. 10 BSIG-E)
3. Einführung eines freiwilligen nationalen IT-Sicherheitskennzeichens (§ 9c BSIG-E)

Entgegen der aktuellen Ausgestaltung müssen die genannten Vorhaben auf das elementar wichtige Ziel europäischer Harmonisierung im Bereich Cyber- und IT-Sicherheit einzahlen. Andernfalls sind negative wettbewerbsrechtliche Implikationen für den Wirtschaftsstandort Deutschland absehbar, im schlechtesten Fall auch durch nicht abgestimmte Doppelregulierungen. Dies gilt insbesondere für die neugeschaffene Sonderkategorie »Unternehmen von besonderem öffentlichen Interesse«, die europa-weit ihresgleichen sucht. Aus dem Grund ist von dieser einzelstaatlichen Quasi-KRITIS-Kategorie abzuraten.

Mit Blick auf das Ziel, die Sicherheit informationstechnischer Systeme zu steigern, kann es nicht im Interesse der Politik sein, das IT-SiG 2.0 im kommenden Jahr erneut aufzuschnüren und – im schlechtesten Fall erneut ohne nachvollziehbare Evaluierung – mit einem IT-SiG 3.0 fortzufahren, nur um die sich bereits abzeichnende Fehlabstimmung mit der NIS-Review wieder zu beheben. Dies hätte zweifelsohne negative Auswirkungen auf den Wirtschaftsstandort Deutschland und auf die mit dem IT-SiG 2.0 ohnehin schon induzierte Rechtsunsicherheit für die Unternehmen, wie der nachfolgende Punkt aufzeigt.

Definitorische Ungenauigkeit von verwendeten Begrifflichkeiten und induzierte Rechtsunsicherheit

Die definitorische Ungenauigkeit manifestiert sich insbesondere in drei Begrifflichkeiten:

1. Unternehmen im besonderen öffentlichen Interesse (§§ 2 Abs. 14 und 8f BSIG-E)
2. IT-Produkte (§ 2 Abs. 9a BSIG-E)
3. Kritische Komponenten (§ 2 Abs. 13 BSIG-E)

Während IT-Produkte als »*Softwareprodukte sowie alle einzelnen oder miteinander verbundenen Hardwareprodukte*« definiert werden, sind Kritische Komponenten »*[…] IT-Produkte, die in Kritischen Infrastrukturen eingesetzt werden, die von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit dieser IT-Produkte zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit Kritischer Infrastrukturen oder zu Gefährdungen für die öffentliche Sicherheit führen können, wenn diese*

1. *auf Grund eines Gesetzes als solche bestimmt werden oder*
2. *auf Grund eines Gesetzes als kritisch bestimmte Funktionen realisieren, aus denen nach dem Gesetz kritische Komponenten abgeleitet werden können*«.

Während die Definition von IT-Produkten weiterhin zu viel Interpretationsspielraum lässt, ist der unternommene Versuch, Kritische Komponenten regulatorisch besser zu fassen, grundsätzlich zu begrüßen. Aus Gründen der Rechts-, Investitions- und Planungssicherheit muss die Definition Kritischen Komponenten aber aus dem Gesetz selbst heraus und hinreichend genau erfolgen. Der Entwurf wird dieser Anforderung aktuell nicht gerecht. Dabei begrüßt Bitkom grundsätzlich den in § 2 Abs. 13 Nr. 2 enthaltenen Ansatz, Kritische Komponenten über kritische Funktionen zu definieren. Allerdings enthält die aktuelle Formulierung in § 2 Abs. 13 Nr. 2 zu viele Unwägbarkeiten. Was genau ist mit der Formulierung »auf Grund eines Gesetzes« gemeint? Welche(s) Gesetz(e)? Wird es eine Anhörung und Beteiligung der Wirtschaft geben? Die Gesetzesbegründung gibt Aufschluss: »*Für den Bereich der Kritischen Infrastrukturen, die ein öffentliches Telekommunikationsnetz betreiben oder öffentlich zugängliche Telekommunikationsdienste erbringen, legt beispielsweise § 109 Absatz 6 des Telekommunikationsgesetz fest […]. Komponenten, welche die in dem Katalog von Sicherheitsanforderungen aufgeführten Funktionen realisieren, sind damit kritische Komponenten im Sinne des § 2 Absatz 13 BSIG.*« Bitkom fordert eine entsprechende Konkretisierung unmittelbar in § 2 Abs. 13 Nr. 2 vorzunehmen. Die hinreichend genaue, rechtssichere Definition Kritischer Komponenten ist zwingend erforderlich. Dies gilt umso mehr für § 2 Abs. 13 Nr. 1, wo aktuell eine direkte, gesetzliche Be-

stimmung (siehe Gesetzesbegründung) kritischer Komponenten vorgesehen ist. Bitkom lehnt die in § 2 Abs. 13 Nr. 1 vorgesehene, gesetzliche Bestimmung kritischer Komponenten ab. Es bedarf zwingend an Transparenz und unmittelbaren Beteiligungsmöglichkeiten für die durch die Entscheidung Betroffenen. Es sollte zusätzlich klargestellt werden, dass nur speziell für den Einsatz in Kritischen Infrastrukturen hergestellte Kritische Komponenten – identifiziert vor allem durch die Betreiber selbst – als eben solche gelten können. Agnostische IT-Produkte, deren Verwendung sich nicht ausschließlich auf KRITIS-Bereiche beschränkt, müssen zunächst ausgeklammert sein. Vor diesem Hinter-grund ist es zu begrüßen, dass gemäß § 2 Abs. 13 Satz 2 Einschränkungen der vorgesehenen Regelung möglich erscheinen.

Die Einordnung und Bewertung Kritischer Komponenten im legislativen Gesamtkontext des IT-SiG 2.0 wird ab Seite 11 fortgeführt.

Kompetenzerweiterung für das Bundesamt für Sicherheit in der Informationstechnik (BSI)

Bitkom begrüßt die personelle Aufwertung und finanzielle Stärkung des BSI. In der Vergangenheit konnten wir unter dem Dach des Bitkom auf die vertrauensvolle Zusammenarbeit und den fachlichen Dialog mit den Spezialisten des BSI zählen, um die Cyber- und IT-Sicherheit in Deutschland gemeinsam voranzubringen. Wir freuen uns darauf, den kooperativen Austausch in Zukunft mit einem personell gestärkten BSI weiter zu intensivieren. Gleichzeitig gibt es im Zuge der Änderungen des BSIG wesentliche Aspekte, die es kritisch hervorzuheben gilt:

- Die Kompetenzausweitung und der damit einhergehende massive Personalaufbau aufseiten des BSI lassen befürchten, ja sogar erwarten, dass die Behörde über Jahre an Wachstumsschmerzen kranken wird und die hochgesteckten Ziele kurz- und mittelfristig nicht zu erreichen vermag. Zudem führt die Kombination von Aufgaben unterschiedlicher Zielrichtung (objektive Sachverhaltsaufklärung zu präventiven und repressiven Zwecken einerseits und einseitig zielgerichtete Durchsetzung von Interessen von Verbrauchern als einer bestimmten gesellschaftlichen Gruppe andererseits) zu nicht auflösbaren Interessenskonflikten und erscheint aus diesem Grund verfassungsrechtlich problematisch. Die Neupositionierung des BSI als starke Aufsichtsbehörde mit weitreichenden Eingriffsmöglichkeiten und zusätzlichen Weisungsbefugnissen lässt außer Acht, dass viele der vorgesehenen zusätzlichen Aufgaben des Bundesamts im Kompetenzbereich qualifizierter vertrauenswürdiger Unternehmen und Institutionen liegen. Daneben ist es zurückzuweisen, dass das BSI einzelnen Unternehmen technische Zugriffs- und Weisungsbefugnisse erteilen darf (bspw. gemäß

§ 7c BSIG-E). Im Sinne einer effizienten Aufgabenteilung sollte das BSI nicht in bewährte privatwirtschaftliche Prozesse eingreifen oder sich diese komplett zu eigen machen. Cybersicherheit ist eine Querschnittsaufgabe und muss horizontal wie vertikal gestärkt werden. Die Bündelung von möglichst vielen Kompetenzen auf staatlicher Seite trägt dieser Querschnittslogik nicht im ausreichenden Maße Rechnung und dämpft den so wichtigen Aufbau von IT-Expertise in der wirtschaftlichen Breite.

- Bitkom spricht sich gegen die nationale Entwicklung und Festschreibung eines Stands der Technik durch das BSI aus. Die aktuell gewählte gesetzliche Formulierung des §3 Abs. 1 Satz 2 Nr. 20 verkennt, dass sich der Stand der Technik an den Prozessen der Normung und Standardisierung orientiert, im Einvernehmen aller relevanten Stakeholder vielmehr ein Beobachtungswert der Marktanwendung darstellt und somit erst ex-post als solcher identifiziert werden kann. Somit wäre das BSI lediglich in der Lage einen zeitlich bereits überholten Näherungswert abzubilden, der dem internationalen Marktgeschehen hinterherhinkt. Die Entwicklung des Stands der Technik kann nur in enger Abstimmung und unter Einbeziehung der betroffenen Branchen sowie nach transparenten Beteiligungskriterien erfolgen. Gleiches gilt für die Ausarbeitung von Technischer Richtlinien, die internationale Normen und Standards als Ausgangsbasis verstehen müssen, nicht vice versa.

- Der Einführung eines durch das BSI verantworteten freiwilligen IT-Sicherheitskennzeichens steht Bitkom grundsätzlich positiv und offen gegenüber. Es ist jedoch zu betonen, dass ein IT-Sicherheitskennzeichen nur als ein Mosaikstein eines umfassenden Gesamtkonzepts für mehr IT-Sicherheit verstanden werden kann. Sicherheit ist ein Prozess und keine Momentaufnahme in Form eines Kennzeichens. Damit ein solches Kennzeichen seine volle Wirkkraft entfalten kann, sollte es sich auf grundlegende, produktübergreifende Schutzanforderungen beschränken und in einen Gesamtkontext eingebettet und von vornherein als europäische Lösung oder europäisch skalierbar konzipiert werden. Bei national unterschiedlichen Regelungen hingegen bestünde die Gefahr einer erheblichen Beeinträchtigung des nach dem AEUV gewährleisteten freien Waren- und Dienstleistungsverkehrs innerhalb Europas in Bezug auf IT-Produkte. Bitkom empfiehlt, innerhalb des § 9c BSIG-E auf anerkannte internationale, zumindest aber europäisch anerkannte, einheitliche Regelungen, Normen und Standards zu referenzieren. Erst wenn internationale und europäische Normen und Standards nicht existieren oder anwendbar sind, sollte auf nationale oder branchenspezifische Standards sowie Technische Richtlinien des BSI zurückgegriffen werden. Dies knüpft unmittelbar an die Ausführungen des vorherigen Absatzes an. Darüber hinaus muss es immer möglich sein, das IT-Sicherheitskennzeichen online zu veröffentlichen, nicht nur wenn die Beschaffenheit des Produktes das Anbringen nicht möglich macht. Aus

dem Grund muss § 9c Abs. 6 BSIG-E folgendem Wortlaut Rechnung tragen:
»*das IT-Sicherheitskennzeichen ist entweder auf dem jeweiligen Produkt oder dessen Umverpackung anzubringen, oder elektronisch zu veröffentlichen*.«

- Während die Untersuchung informationstechnischer Produkte und Systeme auf der Basis genereller Marktbeobachtungsbefugnisse durchaus zu begrüßen ist, überschreitet die aktuell intendierte Ausweitung der Befugnisse im Sinne der in § 7a Abs. 2 und 4 dargelegten Auskunftspflicht eine rote Linie. Derart uneingeschränkte und anlasslose Auskunftsrechte – »insbesondere auch zu technischen Details« – stehen im ungeklärten Rechtsverhältnis, wenn nicht sogar im klaren Widerspruch zum Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG).

- Im Zuge der Kompetenzausweitung des BSI ist eine klare Priorisierung der Aufgaben in Anlehnung an die noch zu definierenden Schutzziele dringlich geboten. Die im Zuge des IT-SiG 1.0 eingeführten Meldepflichten von Cybersicherheitsvorfällen haben bisher keine signifikante Verbesserung im Lagebild gebracht. Das BSI sollte der monatlichen und für die einzelnen Sektoren individuellen Erstellung von Lagebildern Priorität einräumen, bevor sich das Augenmerk auf die Erschließung neuer Kompetenzfelder richtet. Während die Festlegung auf das BSI als zentrale Meldestelle zu begrüßen ist, wird im aktuellen Gesetzesentwurf die Chance vertan, ein effizientes, harmonisiertes und dem one-stop-shop-Prinzip folgenden Meldewesens zu schaffen. Dies gilt es im Sinne des Bürokratieabbaus nachzuholen.

- Die Handhabung von Schwachstellen ist das Rückgrat zur nachhaltigen Steigerung von IT-Sicherheit in der wirtschaftlichen Breite und den Schutz informationstechnischer Systeme in Bereichen kritischer Infrastrukturen. Es braucht eine ausnahmslose Meldepflicht entdeckter Sicherheitslücken, die auch für staatliche Stellen gilt. Der aktuelle Gesetzesentwurf (§ 4b BSIG-E in Verbindung mit §§ 7, 7a, 7b, 7c und 7d BSIG-E) läuft dem allerdings zuwider. Die inhärente Intransparenz könnte zu einem Vertrauensverlust der Wirtschaft in das BSI führen. Dabei ist ein dysfunktionales Schwachstellenmanagement noch die kleinere Problemdimension. Schwerwiegender für das dem BSI entgegengebrachte Vertrauen ist der im nachfolgenden Punkt ausgeführte Interessenskonflikt mit den Sicherheitsbehörden.

Interessenskonflikt zwischen dem BSI und den Sicherheitsbehörden

Übergeordnete Zielsetzung des IT-SiG (2.0) muss die Steigerung der technischen Sicherheit von Kritischen Infrastrukturen, Unternehmen im besonderen öffentlichen Interesse und digitalen Diensten sein. Gleichzeitig wird der Versuch unternommen, das Mandat des BSI mit den Aufgaben der Sicherheitsbehörden in Einklang zu bringen. IT-Sicherheitsziele und Strafverfolgung sollten aber nicht miteinander vermengt werden, da dies weder zum Schutz unserer informationstechnischen Ziele beiträgt noch einer erfolgreichen Strafverfolgung gerecht wird. Bitkom empfiehlt, IT-Sicherheitsziele klar zu definieren und diese dem IT-Sicherheitsgesetz als Anker und Leitbild voranzustellen. Dabei empfiehlt sich die typische CIA-Security-Triangel, bestehend aus Confidentiality (Vertraulichkeit), Integrity (Integrität) und Availability (Verfügbarkeit), da diese dem Großteil der in Kritischen Infrastrukturen, in Unternehmen im öffentlichen Interesse und bei Digitalen Diensten verwendeten Risikomanagementsystemen zugrunde liegt.

Der Interessenskonflikt zwischen den Aufgaben des BSI und der Zuständigkeit der Sicherheitsbehörden manifestiert sich in den folgenden Punkten:

- Gemäß § 7b BSIG-E soll das BSI künftig zum Aufspüren von Sicherheitslücken gesetzlich legitimiert in die IT-Systeme und technischer Anlagen von kritischen Infrastrukturen eingreifen können. Die im Gesetz beschriebenen Portscans können auch als Schwachstellenscans interpretiert werden, welche als kritisch zu bewerten sind, da (zumindest) ein aktiver Schwachstellenscan das Potential hat, Dienste und Programme in Ihrer Verfügbarkeit zu stören bzw. deren Ausführung zu verhindern. Während es zwar zu begrüßen ist, dass mit Aufnahme einer »weißen Liste« eine gewisse Konkretisierung und Einschränkung der Kompetenzausweitung vorgenommen wird, können die Vorbehalte nicht vollständig ausgeräumt werden. Bitkom bewertet die aktuelle Ausgestaltung daher als problematisch; einerseits im Hinblick auf die nicht abschätzbaren und weitrechenden Konsequenzen für die Funktionstüchtigkeit der Systeme und damit für die Versorgungs- und physische Sicherheit der Bevölkerung, andererseits im Sinne eines argumentativ nicht auflösbaren Knotens der Unsicherheit. Auf welcher Basis sollen Betreiber und Unternehmen künftig Schwachstellen melden, wenn nicht gewährleistet ist, dass die Erkenntnisse und Informationen zur Beseitigung von Gefährdungslagen verwendet sondern potenziell an die Sicherheitsbehörden weitergegeben werden können? Hersteller müssen unverzüglich nach Bekanntwerden von Sicherheitslücken in ihren Produkten darüber informiert werden, um diese schnellstmöglich beheben zu können. Ein Bruch mit diesem Grundsatz würde einen Vertrauensverlust der Wirtschaft in das BSI nach sich ziehen.

- Gemäß § 7c Abs. 1 Nr. 1 kann das Bundesamt gegenüber einem Anbieter von Telekommunikationsdiensten zur Abwehr konkreter erheblicher Gefahren für die in Absatz 2 genannten Schutzziele anordnen, dass er die in § 109a Absätze 5 oder 6 des Telekommunikationsgesetzes bezeichneten Maßnahmen trifft. § 7 Abs. 3 gestattet in diesem Fall die Anordnung gegenüber dem Diensteanbieter, den Datenverkehr an eine vom Bundesamt benannte Anschlusskennung umzuleiten. Mit der ausdrücklichen Hervorhebung dieser in das Fernmeldegeheimnis eingreifenden Anordnungskompetenz erkennt der Gesetzgeber, dass ein solcher Eingriff einer ausdrücklichen Ermächtigung bedarf. Jedoch trifft diese Norm nicht die Anforderungen, die an eine Ermächtigung zum Eingriff in das Fernmeldegeheimnis zu stellen sind. Die Umleitung von Datenverkehren an eine andere Anschlusskennung ermöglicht die Kenntnisnahme der Inhalte der Kommunikation durch Dritte. Eine solche Kenntnisnahme durch Dritte steht jedoch unter einem richterlichen Vorbehalt. Zudem lässt die Vorschrift völlig offen, welchem Personenkreis die Nutzer der anderen Anschlusskennung zugeordnet sein müssen. Insoweit ist der Anwendungsbereich auf solche Nutzer zu beschränken, die den Inhalt des Datenverkehrs zur Abwehr einer konkreten Gefahr unbedingt benötigen. Im Übrigen dürfte ein Eingriff in das Fernmeldegeheimnis nur zum Schutz gleichwertiger oder höherwertiger Rechtsgüter möglich sein. Auch insoweit ist der Anwendungsbereich deutlich einzuschränken.

- Die Zweckmäßigkeit und Sinnhaftigkeit der neu eröffneten Möglichkeiten zur Kontrolle der KRITIS-Sektoren automatisierte Ermittlungen auf individueller Anwender- und Nutzerebene durchzuführen und Informationen im Sinne der in § 5c BSIG-E vorgesehenen Bestandsdatenauskunft zu sammeln und zu verarbeiten, ist unter Gesichtspunkten der Beseitigung von Störungen kritisch zu hinterfragen und abzulehnen. Die in § 5c Abs. 5 BSIG-E vorgesehene Befugnis zur Weiterleitung der in diesem Verfahren erlangten Daten an andere Behörden ist zu streichen. Dagegen ist zumindest die Aufnahme der in § 5c Abs.8 vorgesehenen Entschädigungsregelung zu begrüßen.

- Die in § 8a Abs. 1b vorgesehene Speicherfrist von 4 Jahren für die Angriffserkennung und -nachverfolgung relevanter und nicht-personenbezogener Daten ist abzulehnen und der genannte Absatz zu streichen. Andernfalls müssten Betreiber Kritischer Infrastrukturen Datenhalden von mehreren TByte vorhalten, ohne erkennbaren Mehrwert zur Steigerung der IT-Sicherheit.

Einsatz Kritischer Komponenten (nicht) vertrauenswürdiger Hersteller

Oberste Maxime ist und muss sein, dass Kritische Infrastrukturen jederzeit ein Höchstmaß an Sicherheit gewährleisten und Risiken einer technischen Kompromittierung minimiert werden. An dieser Stelle sei ausdrücklich und wiederholt betont, dass sich alle Beteiligten – sowohl Hersteller Kritischer Komponenten als auch Betreiber Kritischer Infrastrukturen – ihrer Verantwortung bewusst sind und ihren Beitrag zur gemeinsamen Zielsetzung zu leisten bereit sind. In Anbetracht der hybriden und wachsenden Bedrohungslage erachten wir den Einsatz sicherer Produkte in Bereichen Kritischer Infrastruktur für nachvollziehbar und grundsätzlich richtig. Hierbei müssen im Sinne einer Gleichbehandlung die dafür angelegten Maßstäbe transparent gemacht werden und nachvollziehbar sein. Dies lässt sich am besten als harmonisierter Ansatz auf europäischer Ebene verfolgen. Bitkom fordert deshalb eine voll umfassende Umsetzung der EU 5G-Toolbox.

Anknüpfend an die bereits genannte Forderung, die Schutzziele klar zu definieren, ist an dieser Stelle einmal mehr deutlich zu machen, dass der Schutzbedarf etwas technisch-agnostisches ist und einer regel- und kritikalitätsbasierten Prüfung unterliegen muss und auf die rechtssichere Investitionsplanbarkeit einzahlt. Beides muss hinreichend gewährleistet werden für einen privatwirtschaftlichen Akteur. Bestehende Zertifizierungsprozesse und anerkannte Rahmenwerke gilt es zu nutzen. Dagegen sieht der Gesetzgeber ein zweistufiges Verfahren vor, bei dem eine technische Prüfung und Zertifizierung kritischer Komponenten mit einer politischen Bewertung der durch die Hersteller abgegebenen Garantieerklärung kombiniert wird. Kritische Komponenten müssen also auf Basis technischer Kriterien geprüft und zertifiziert werden. Zusätzlich dazu müssen die Hersteller von kritischen Komponenten noch eine politische Überprüfung der von ihnen abgegebenen und sich auf die gesamte Lieferkette erstreckenden Garantieerklärung durchlaufen. Letztendlich soll also die Entscheidung darüber, ob eine Kritische Komponente eines bestimmten Herstellers verbaut werden darf oder nicht, auf politischer Ebene getroffen werden.

Ausgehend von der politischen Diskussion, nicht nur eine technische Zertifizierung kritischer Komponenten festzuschreiben, sondern auch die Abgabe von Garantieerklärungen einzufordern, ist es für Bitkom von zentraler Bedeutung, die beiden Säulen auch als solche zu verstehen. § 9 Abs. 4a und die darin beschriebene Entzugsoption von bereits erteilten Zertifikaten durch das BMI ist somit zu streichen. Der Entzug eines erteilten, gültigen technischen Zertifikats ist ausschließlich auf Basis valider (neuer) Erkenntnisse technischer Natur denkbar, nicht aber durch politische Vertraulichkeitsbescheide.

Sofern, trotz erheblicher Bedenken, der Gesetzgeber dennoch an letztgenannten festhalten möchte, so können diese ausschließlich Gegenstand von § 9b sein und bedürfen einer Konkretisierung im Gesetz, um Planungssicherheit und Investitionsschutz sicherzustellen.

Dieser Logik folgend müssen beide Säulen, die technische Zertifizierung Kritischer Komponenten sowie die Abgabe von Garantieerklärungen, nachfolgend losgelöst voneinander adressiert werden:

- **Technische Zertifizierung Kritischer Komponenten**

  Wie bereits erläutert differenziert § 2 Abs. 13 zwischen Kritischen Komponenten, die als kritisch bestimmte Funktionen realisieren und solchen, die gesetzlich bestimmt werden.

  Hinsichtlich der für TK-Diensteanbieter näher spezifizierten Kritischen Komponenten, und wie bereits in der Bitkom Stellungnahmen zum Katalog von Sicherheitsanforderungen gemäß § 109 TKG (§ 162 im Zuge der TKG Novellierung)[1] und zur Liste kritischer Funktionen[2] argumentiert, begrüßen wir grundsätzlich den Ansatz und das Verfahren, Kritische Komponenten über die Umsetzung der kritischen Funktionen zu definieren. Bitkom unterstützt das Bestreben, die kritischen Funktionen eng an der EU-Risikoanalyse und den Implementierungsempfehlungen der EU-Toolbox zu orientieren und technologieneutrale Funktionen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial als Regelungsgegenstand zu beschreiben. Einerseits erscheint dieses Vorgehen zielführender, als eine Gesamtliste kritischer Komponenten zu erarbeiten und fortwährend zu pflegen. Anderseits garantiert eine solche Definition ein angemessenes und schwerlich zu unterlaufendes Verständnis kritischer Komponenten. Allerdings darf es nicht dazu kommen, dass alle der eingesetzten Komponenten als »kritisch« bewertet werden. Dies würde zu einer »Bottom-Up«-Regulierungskette führen, d. h. die über ihre Funktionen als kritisch eingestuften Komponenten würden alle § 9b BSIG-E unterliegen. In Summe können spezifische Komponenten also nur als Ableitung Kritischer Funktionen verstanden werden, wobei auch Funktionen klar zu definieren sind.

  Im Gegensatz dazu lehnt Bitkom die gesetzliche Festlegung Kritischer Komponenten ohne Beteiligung und frühzeitige Einbindung von Unternehmen ab (§ 2 Abs. 13

[1] ↗ Stellungnahme zum Katalog von Sicherheitsanforderungen nach § 109 TKG | Bitkom e.V. sowie Bitkom views concerning the catalogue of security requirements for the operation of telecommunications and data processing systems and for the processing of personal data – pursuant to § 109 of the Telecommunications Act (TKG) Version 2.0 | Bitkom e.V.

[2] ↗ Stellungnahme: zur „Liste der kritischen Funktionen für öffentliche Telekommunikationsnetze und -dienste mit erhöhtem Gefährdungspotenzial“ | Bitkom e.V.

Nr. 1BSIG-E). Betreiber kritischer Infrastrukturen und Hersteller kritischer Komponenten sind vor Bekanntgabe etwaiger Allgemeinverfügungen intensiv zu beteiligen. Bitkom fordert einmal mehr die rechtssichere und hinreichend genaue Definition Kritische Funktionen, um Kritische Komponenten klar fassen/identifizieren zu können. Kritische Komponenten bzw. Komponenten mit kritischen Funktionen können i. S. dieses Gesetzes nur dann kritisch sein, wenn ihre Funktionalitäten in Bezug auf die Einsatzumgebung im Falle ihrer Beeinträchtigung den KRITIS-Schutzzielen zuwiderlaufen. Spezifikationen erfolgen Sektor spezifisch im Rahmen einer Rechtsverordnung unter Beteiligung der betroffenen KRITIS-Sektoren. Grundsätzlich müssen ausreichend lange Umsetzungsfristen gewährt werden. Dies ist insbesondere deshalb wichtig, weil viele Komponenten nicht 1:1 ausgetauscht werden können, sondern weitere Anpassungen erforderlich machen. Es bedarf der Einbindung und Anhörung von Unternehen, bevor eine Komponente gesetzlich als kritisch eingestuft wird. Andernfalls droht Überforderung in Branchen und Unternehmen. Erfahrungswerte aus dem TK-Sektor lassen sich nicht einfach flächendeckend übertragen. Dies verkennt die aktuelle Gesetzesbegründung. Die Zertifizierungspflicht Kritischer Komponenten und die Abgabe von Garantieerklärungen im Sinne des Bestandschutzes können frühestens mit Inkrafttreten des IT-SiG 2.0 erfolgen.

Zusammenfassend festzuhalten ist, dass Bitkom ein hohes Maß an technischer Sicherheit von in Kritischen Infrastrukturen verbauten Komponenten befürwortet und die vorgesehene Säule technischer Zertifizierung auf Basis kritischer Funktionen generell unterstützt. Hersteller wie Betreiber sind dazu bereit, ihre jeweiligen Beiträge zu leisten. Was es braucht, ist allerdings ein klarer, kritikalitätsbasierter Kriterien- und Funktionskatalog, sodass alle Akteure die Sicherheit und Integrität von Komponenten eigenständig verstehen und bewerten können. Bitkom steht bereit, um den weiteren technischen Prozess so praxistauglich und sicherheitssteigernd wie möglich zu gestalten. IT-Sicherheit muss aus technischer Sicht gedacht und adressiert werden. Hierfür ist das BSIG das geeignete Rahmenwerk. Anders sieht es bei der zusätzlichen zweiten Säule aus, der politischen Vertrauenswürdigkeit.

- **Garantieerklärungen und geopolitische Unwägbarkeiten**

Neben der technisch-agnostischen Zertifizierung Kritischer Komponenten wirkt der Begriff der Vertrauenswürdigkeit schwer greifbar. Garantieerklärungen sind ein politisch gewolltes Instrument und bieten keine ausreichende Rechtssicherheit. Objektiv stellt sich für Bitkom die Frage: hilft das gewählte Instrument der Garantieerklärung in seiner jetzigen Ausgestaltung bei der Gewährleistung der Schutzziele? Die Antwort des Bitkom lautet: nein. Die fehlende Benennung konkreter Para-

meter für die Garantieerklärung und der Verweis auf »sicherheitspolitische Belange« führen dazu, dass nach aktueller Lesart bspw. selbst harmlose Wartungsschnittstellen den Entzug der Vertrauenswürdigkeit eines Herstellers rechtfertigen könnten.

Dabei ist sich Bitkom natürlich der geopolitischen Dimensionen und vermeintlichen Beweggründe bewusst. Nicht zuletzt haben wir mit unserem Positionspaper zur Digitalen Souveränität[3] den Diskurs maßgeblich mitgestaltet und unterstützen die EU Toolbox, inkl. der strategischen Maßnahmen. Gleichwohl ist zu konstatieren, dass eindimensionale politische Versuche, die Deutungshoheit rund um Debatten wie 5G, GAIA-X und den Ausschluss von Einzelakteuren zu erlangen, auf den ersten Blick sinnvoll erscheinen mögen. Bei genauerer Betrachtung bringt uns die politische Einordnung der Welt in geopolitische Hemisphären nur bedingt weiter und garantiert uns keineswegs die Fähigkeit, künftig autonom und selbstbestimmt im Sinne unserer Digitalen Souveränität zu handeln.

Im Kern lautet die zentrale Frage: wo soll und wo wird Innovation künftig stattfinden? Innovationen im Digitalkontext werden auch in Zukunft nicht an nationalstaatlichen Grenzen halt machen. Deutsche wie europäischen Entscheidungsträger sollten daher alles daran setzten, unseren digitalen europäischen Binnenmarkt langfristig zu stärken und ein prosperierendes Ökosystem aus nationalen, europäischen und internationalen Playern zu schaffen, die die Innovationen von Morgen in Europa und in Deutschland hervorbringen. Dabei geht es schon längst nicht mehr nur um 5G. Die Wirtschaft ist bereits weiter und beschäftigt sich mit Interoperabilität, OpenRan, Netzwerkvirtualisierung, 6G und vielem mehr – nicht zuletzt, um aus privatwirtschaftlichen Gründen einseitige Abhängigkeiten zu reduzieren und neue Handlungsalternativen aus eigenen Stücken heraus zu schaffen. Bitkom wünscht sich einen grundsätzlichen Narrativwechsel, im Sinne einer proaktiven, bestmöglichen Unterstützung und Förderung des von der Wirtschaft bereits eingeschlagenen Wegs. Zur Stärkung der europäischen und deutschen Wirtschaft braucht es dazu eine ressortübergreifend kooperativ-ausgerichtete, zukunfts- und europäisch-fokussierte sowie sicherheits- und forschungsgetriebene Innovations- und Industriepolitik.

Als Digitalwirtschaft sind wir uns unserer Rolle im IT-Sicherheitskontext bewusst und alle Einzelakteure zur Mitwirkung im Rahmen der individuellen Möglichkeiten bereit, den Schutze nationaler und europäischer Kritischer Infrastrukturen mitzugestalten. Mit dem Vorhaben, politisch die Oberhand und das Letztentscheidungsrecht behalten zu wollen – entgegen aller Unwägbarkeiten und negativen Auswirkun-

[3] ↗ Digitale Souveränität: Anforderungen an Technologien- und Kompetenzfelder mit Schlüsselfunktion | Bitkom e.V.

gen auf wirtschaftliche Prozesse und Innovationen – liegt der Ball allerdings weit im Feld der nationalen Politik. Sie muss sich daran messen lassen.

- **Zentrale Aspekte, die es bei der Vertrauenswürdigkeitsprüfung hervorzuheben gilt**

  - Grundsätzlich gilt, dass der Entzug der Vertrauenswürdigkeit und etwaige damit verbundene Rückbauverpflichtungen ein enormes Investitionsrisiko darstellen und im Extremfall die Existenz eines Unternehmens gefährden. Es gibt weder eine Haftungsdeckelung noch eine Haftungszuweisung. Wenngleich Bitkom bereits die jetzige Ausgestaltung der Vertrauenswürdigkeitsprüfung nicht unterstützt, muss explizit auf nachgelagerte Unwägbarkeiten und Risiken hingewiesen werden. Was soll geschehen, wenn ein Lieferant seine Vertrauenswürdigkeit einbüßt, obgleich bereits seine Technik Bestandteil der Infrastruktur ist? Der Gesetzesentwurf nennt den Rückbau von verbauten Komponenten explizit als Option. Dies ist im Sinne des Bestandsschutzes nicht tragbar und daher abzulehnen. Klare Verantwortlichkeiten, Ausstiegsszenarien und Übergangsfristen müssen Rechtssicherheit garantieren. Nach aktuellem Stand des Gesetzestextes drohen bspw. der europäischen Mobilfunkbranche Mehrkosten von mehreren Milliarden Euro, wodurch Verzögerungen im (5G-)Netzausbau nicht ausgeschlossen werden können. Falls der Gesetzgeber tatsächlich am Vorhaben festhalten sollte, ist ein ausreichend ausgestatteter Kompensationsfonds zu schaffen. Andernfalls werden die mittelfristig anfallenden Kosten eines international nicht kompetitiven Telekommunikationsnetzes für Wirtschaft, Wissenschaft, Gesellschaft und Politik um ein vielfaches höher ausfallen und Deutschland als Zukunftsstandort von Schlüsselindustrien international zurückwerfen.

  - Um die Beschaffungspflichten und damit die Ausstattungsfähigkeiten der Betreiber kritischer Infrastrukturen realistisch abzubilden, bedarf es der Klarstellung/ Anerkennung, dass Betreiber Kritischer Infrastrukturen die Hoheit über und auch die Verantwortung für ihre Prozesse, Ausstattungen und Geschäftstätigkeit haben. Somit obliegt ihnen die Einschätzung der entsprechenden Kritikalität im Gesamtkontext. Diese Kompetenzen können weder vom BSI abgebildet werden, noch erscheint es als sinnvoll, die Verantwortung auf die Hersteller zu projizieren. Gleichwohl müssen natürlich auch die Hersteller in die Pflicht genommen werden und ihren Beitrag zur Erhöhung der Sicherheit informationstechnischer Systeme leisten. Eine Blankogarantie über die Vertrauenswürdigkeit der gesamten Lieferketten gemäß § 9b Abs. 2 Satz 2 BSIG-E gehört aber nicht dazu und ist nicht praktikabel. Es sollte explizit auf bestehende und international anerkannte Zertifizierungsrahmen verwiesen werden, um den zu erwartenden Bürokratieaufwand

so gering wie möglich zu halten. Es ist überlegenswert, ob nicht Akteure, die schon heute im Rahmen von KRITIS, der TKG oder anderen gesetzlichen Verpflichtungen, einer herausgehobenen Nachweispflicht nachkommen müssen, von einer weiteren (zweiten) Nachweisplicht ausgenommen werden sollten, sodass eine objektiv unnötige Doppelpflicht und -aufsicht ausgeschlossen ist.

- Ferner muss verhindert werden, dass durch vorsätzlich begangene und schuldhaft herbeigeführte unerlaubte Handlungen eines Herstellers den Betreibern gesetzlich nicht abgedeckte finanzielle Schäden entstehen. In gleicher Manier ist es zu vermeiden, dass sich Hersteller von Kritischen Komponenten in Rechtsstreitigkeiten wiederfinden, wo sie sich über Jahre hinweg gegen schwer nachweisbare Anschuldigungen und politisch gewollte Entscheidungen zur Wehr setzen mussten. Sollte es jedoch zum Entzug der Vertrauenswürdigkeit eines Herstellers kommen, darf dies nur Folgen für Kritische Komponenten des Herstellers haben, nicht aber für nicht-Kritische Komponenten. Die Formulierung in § 9b Abs. 6 ist daher zu begrüßen.

- Abschließend ist explizit zu betonen, dass die Zertifizierungspflicht Kritischer Komponenten und die Abgabe von Garantieerklärungen frühestens mit Inkrafttreten des IT-SiG 2.0 erfolgen kann. Erfahrungsgemäß ist davon auszugehen, dass eine mehrjährige Übergangfrist nach Inkrafttreten nötig sein wird, alleine um die Zertifizierungsprozesse durchlaufen zu können.

Ermächtigung zum Erlass von Rechtsverordnungen

Der in § 10 Abs. 6. enthaltene Ansatz, Interoperabilität erstmalig explizit als eine gestalterische Maßnahme mit Visionspotenzial zur langfristigen Steigerung der IT-Sicherheit im Gesetzestext zu nennen, ist positiv zu würdigen. In Ermangelung einer Gesetzesbegründung – inkl. europarechtlicher Einordnung – und der damit fehlenden Möglichkeit der abschließenden Bewertung, wird dieser Absatz in der Branche kontrovers diskutiert. Eine intensive Einbeziehung der betroffenen Sektoren ist nicht nur im Zuge der Veröffentlichung einer etwaigen Rechtsverordnung erforderlich, sondern auch schon bei der weiteren Ausgestaltung des Gesetzgebungsprozesses.

Bußgelder

Es bedarf einer Balance zwischen maßvoller und wirksamer Sanktionierung. Die aktuell festgeschriebenen Bußgeldhöhen für Ordnungswidrigkeiten erachtet Bitkom mit Blick auf den Geltungsbereich des IT-SiG 2.0 als nachvollziehbar. Allerdings darf es für

Bitkom keinen Verweis auf § 30 Abs.2 Satz 3 OWiG und die damit verbundene Möglichkeit hebelbarer Bußgelder geben. Andernfalls müssten Unternehmen die gesamte Fülle der nachfolgend gelisteten, hebelbaren Ordnungswidrigkeiten fürchten und enorme Summen an Rückstellungen bilden, die dann wiederum nicht in risikobasiert identifizierte Schutzmaßnahmen zur Absicherung der Infrastrukturen investiert werden könnten. Im EU-Durchschnitt ist die Höhe der Bußgelder zudem um ein vielfaches geringer und es erschließt sich nicht, weshalb Unternehmen in Deutschland wettbewerblich benachteiligt werden sollten.

Es darf nicht übersehen werden, dass die Erhöhung der IT-Sicherheit ein wesentliches unternehmerisches Interesse der Verpflichteten darstellt. Dies gilt insbesondere hinsichtlich der bestehenden vertraglichen und außervertraglichen Pflichten gegenüber Kunden, der Wettbewerbssituation im Markt sowie der Verantwortung von Unternehmen gegenüber Aktionären und Investoren.

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.