BDI

KURZ-STELLUNGNAHME | DIGITALISIERUNG | CYBERISCHERHEIT

IT-Sicherheitsgesetz 2.0

Kurz-Kommentierung des Gesetzentwurfs vom 16. Dezember 2020: Deutsche Industrie sieht umfassenden Änderungsbedarf

Stand: 26. Januar 2021

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. 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 Weiterentwicklung des IT-Sicherheitsgesetzes ist daher ein richtiger Schritt, der jedoch besser innerhalb der EU sowie mit Interessengruppen hätte abgestimmt werden müssen. Der Gesetzentwurf für ein IT-Sicherheitsgesetz 2.0, den das Bundekabinett am 16. Dezember 2020 beschlossen hat, ist in weiten Teilen dringend überarbeitungsbedürftig:

Mehr Europa, weniger nationales Klein-Klein:

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. Die deutsche Industrie sieht die Notwendigkeit, das IT-SiG 2.0 eng mit dem am 16. Dezember 2020 durch die EU-Kommission vorgelegten Entwurf einer NIS 2.0-Richtlinie zu harmonisieren.

Mangelnde Rechtsklarheit wegen nachgelagerter RVO & weitgefasster Begriffe:

Das IT-SiG 2.0 lässt an Rechtsklarheit zu wünschen übrig. Es bedarf rechtlich präziser Definitionen der Begriffe „IT-Produkte“ (§ 2 Abs. 9a) und „Kritische Komponente“ (§ 2 Abs. 13). Auch muss der Anwendungsbereich von § 2 Abs. 14 Nr. 2 direkt im Gesetz und nicht in einer RVO definiert werden.

Protokollierungsdaten (§ 2 Abs. 8a)

Die Definition des Terminus „Protokollierungsdaten“ ist nach Ansicht der deutschen Industrie nicht hinreichend genau. Die nunmehr gekürzte Definition ist viel zu unkonkret und verlangt eine deutliche Präzisierung und Eingrenzung. Protokollierungsdaten und deren Verarbeitung sollten dem Anwendungsbereich des § 87 Abs. 1 Nr. 6 BetrVG ausdrücklich entzogen werden, damit IT-Sicherheitsverantwortliche notwendige Daten erheben können, die schlussendlich die Cyberresilienz und damit auch den Schutz von Arbeitsplätzen sichern können.

BSI stärken, aber nicht inhaltlich überfrachten (§ 3):

Zur ganzheitlichen Stärkung der Cyberresilienz Deutschlands braucht es auch ein personell und finanziell gut ausgestattetes BSI. Eine Stellenzuwachs beim BSI um 799 FTE erachten wird jedoch 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 der Cybersicherheit deutlich effizienter und kostengünstiger wäre.

Ihr Ansprechpartner im BDI:

Steven Heckler | Referent | Cybersicherheit und Plattformökonomie | T: +49 30 2028-1523 | S.Heckler@bdi.eu | www.bdi.eu

Zudem muss eine Überfrachtung des BSI mit Aufgaben und Kompetenzen vermieden werden. So sieht der Gesetzentwurf vor, dass das BSI zukünftig den Stand der Technik bei sicherheitstechnischen Anforderungen entwickelt, IT-Produkte- und -Systeme untersucht, das IT-Sicherheitskennzeichen vergibt und als nationale Behörde für die Cybersicherheitszertifizierung agiert. 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 im Sinne eines kooperativen Ansatzes übernommen werden. Nur so kann die deutsche IT-(Sicherheits)-Wirtschaft langfristig gestärkt werden. Es gilt eine stärkere Trennung von Kompetenzen sicherzustellen und 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.

Meldepflichten haben Lagebild bisher nicht verbessert (§ 4b):

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. Der BDI fordert:

- Die Schaffung eines effizienten, harmonisierten Meldewegs an eine zentrale Meldestelle (one-stop-shop-Prinzip),
- 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,
- Eine Verpflichtung des BSI, eingegangene Informationen zu verarbeiten und betroffene Unternehmen über erfolgte oder versuchte Angriffe auf ihre IT zu informieren,
- Unternehmen, die Cybersicherheitsvorfälle melden, sollte eine personalisierte Unterstützung angeboten werden und
- Gesetzliche Rahmenbedingungen müssen geschaffen werden, um alle Wirtschaftsunternehmen über vorliegende Informationen zu (Cyber)-Gefährdern zu informieren.

Schwachstellen immer nach dem Responsible Disclosure-Prinzip melden (§§ 4b, 7a)

Sollte das BSI – oder irgendeine andere staatliche Stelle – durch Meldungen (nach § 4b) oder durch eigene Untersuchung (nach § 7a) Erkenntnisse über Schwachstellen gewinnen, muss es diese unbedingt den betroffenen Unternehmen unter Einhaltung der Responsible-Disclosure-Prinzipien zukommen lassen und darf diese Schwachstellen nicht mit weiteren staatlichen Bedarfsträgern für deren Tätigkeiten teilen. Nur zügig geschlossene Schwachstellen stärken die Cyberresilienz Deutschlands. Bis zu einer Schließung der Schwachstellen dürfen diese nicht öffentlich publik werden. Nur dann, wenn ein Hersteller es ablehnt, die Schwachstellen in angemessener Frist zu schließen, sollte eine öffentliche Bekanntgabe möglich werden.

Registrierungspflicht von KRITIS beim BSI (§ 8b Abs. 3 und 3a):

Der BDI lehnt es ab, dass das BSI zukünftig Unternehmen selbst als KRITIS registrieren kann. Dies muss auch weiterhin durch die Unternehmen erfolgen. Die relativ geringen rechtlichen Anforderungen

an die Annahme, dass ein Betreiber seine Pflicht zur Registrierung nicht erfüllt, scheinen gegenüber dem sehr weitgehenden Eingriff in die unternehmerische Selbstbestimmtheit als unverhältnismäßig. Es bedarf einer Streichung dieser Vorgabe.

Unternehmen im besonderen öffentlichen Interesse (§§ 2 Abs. 14 Nr. 2, 8f und 10 Abs. 5):

Der BDI empfiehlt von einer einzelstaatlichen Einführung der Kategorie „Unternehmen im besonderen öffentlichen Interesse“ abzusehen. Der Gesetzentwurf lässt völlig unklar, welche Unternehmen hierunter fallen. Insbesondere fehlen klare Kriterien, nach denen Unternehmen von besonderer volkswirtschaftlicher Bedeutung nach § 2 Abs. 14 Nr. 2 dieser Kategorie per RVO nach § 10 Abs. 5 zugeordnet werden. 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. Auch ist zu hinterfragen, warum gerade jene Unternehmen, die aufgrund ihrer Wertschöpfung zu „den größten Unternehmen“ zählen, besonderen Verpflichtungen unterliegen sollen. Gerade global tätige Unternehmen unterliegen bereits vielerlei Auflagen und Berichtspflichten, weshalb die angestrebte Kompetenzerweiterung des BSI als eine zusätzliche Aufsichts- und Regulierungsbehörde mit weitergehenden Berichtspflichten eine erhebliche Mehrbelastung bedeuten würde. Vielmehr wäre eine intensivere Unterstützung der Cybersicherheitsbemühungen von KMU durch das BSI wünschenswert. Ferner lässt der nun vorgeschlagene Ansatz völlig außer Acht, dass deutsche Unternehmen in internationale Wertschöpfungsketten integriert sind, denn er erfasst ausländische Zulieferer nicht.

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. Der Gesetzentwurf muss dringend klarstellen, wer die Kosten eines Rückbaus und den Ersatz von Komponenten zu tragen hat – eine Regelung vergleichbar dem Atom- bzw. Kohleausstieg wäre angezeigt.

Es ist richtig, ausschließlich vertrauenswürdige Hersteller für den Einsatz kritischer Komponenten zuzulassen. Die vorgesehene Kombination aus technischer Überprüfung und politischer Vertrauenswürdigkeitsüberprüfung ist zielführend. Der 5G-Netzausbau muss praxisnah ausgestaltet werden, der vorliegende Entwurf gewährleistet dies nicht. Durch die Einführung einer Garantieerklärung wird dieses Schutzziel – Wahrung der Sicherheit der KRITIS – nur scheinbar gewährleistet. Die deutsche Industrie lehnt ihre Einführung in der vorgesehenen Ausgestaltung ab. 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 potenziellen Konsequenzen. Zudem werden Verstöße gegen Garantieerklärungen von KRITIS-Betreibern weder überprüfbar noch nachzuweisen sein. Die Garantieerklärung des Herstellers ggü. KRITIS-Betreibern soll sich auf die gesamte Lieferkette beziehen. Die BReg muss definieren, wo die Lieferkette i.S.d. IT-SiG 2.0 endet. 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.

Freiwilliges IT-Sicherheitskennzeichen (§ 9c):

Die deutsche Industrie begrüßt das Ansinnen der Bundesregierung, das Cybersicherheitsniveau eines Produktes für VerbraucherInnen kenntlich zu machen. Eine Einführung eines freiwilligen, rein

nationalen IT-Sicherheitskennzeichen lehnen wir jedoch ab. Es braucht ein europaweit einheitliches, europaweit gültiges IT-Sicherheitskennzeichen. Der EU Cybersecurity Act liefert hierfür auch bereits die rechtliche Grundlage, an deren Umsetzung sich Deutschland aktiv beteiligen sollte, statt einen nationalen Einzelweg zu beschreiten. Hersteller, die ihre Produkte auf dem europäischen Binnenmarkt in Verkehr bringen, sollten mit einheitlichen Informationspflichten die Cyberresilienz ihres Produktes kennzeichnen können, das spart Kosten und erhöht die Vergleichbarkeit.

RVO zur Def. von Komponenten oder Prozesse deren Interoperabilität, die Offenlegung von Schnittstellen und die Einhaltung etablierter technischer Standards bestimmen (§ 10 Abs. 6)

Interoperabilität erstmalig explizit als eine Maßnahme zur Steigerung der IT-Sicherheit zu nennen, ist positiv. Die deutsche Industrie erachtet die vorgesehenen Möglichkeiten für BMI und BMWi jedoch als viel zu weitreichend. Die staatliche Definition technischer Standards, die Offenlegung von Schnittstellen und die Interoperabilität in jedwedem informations- und kommunikationstechnischen System, Komponente oder Prozess ist ein zu weitreichender Eingriff in die Privatautonomie der Unternehmen. Es braucht eine deutliche Begrenzung des Anwendungsbereichs und eine Definition des Schutzziels.

Bußgeldvorschriften (§ 14):

Die nunmehr angepasste Höhe für Bußgelder von 100.000 bis 2 Mio. Euro 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 akzeptablen Ausgleich zwischen maßvoll angemessener und wirksamer Sanktionierung.

Möglichkeit zur Überprüfung 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. Diese Möglichkeit muss im IT-SiG 2.0 als KANN-Option eingeführt werden. Eine ausschließliche Fokussierung auf technische Sicherheit ist nicht zielführend. Unternehmen sollten auch die Möglichkeit erhalten, die Vertrauenswürdigkeit von Beschäftigten und Bewerbern in als besonders sicherheitskritisch eingestuften Bereichen untersuchen zu können.

Speicherung von Daten für die Angriffserkennung:

Es muss dringend von jedwedem Verpflichtungstatbestand – wie in früheren Versionen des Gesetzentwurfs vorgesehen – zur Speicherung von für die Angriffserkennung und Angriffsnachverfolgung relevanten nicht-personenbezogenen Daten, die beim Betrieb einer Kritischen Infrastruktur anfallen, abgesehen werden. Bei Unternehmen fallen vielfach 1TByte an Daten pro Tag an. Diese verpflichtend für mehrere 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.

Beteiligung von Interessensgruppen gewährleisten:

Die deutsche Industrie erachtet die sehr kurze Frist von 27 Stunden zur Stellungnahme zu einem nicht final ressortabgestimmten Referentenentwurf als völlig inakzeptabel. 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.

Die **detaillierte BDI-Stellungnahme** finden Sie auf der BDI-Homepage: https://bdi.eu/media/publikationen/#/publikation/news/referentenentwurf-fuer-ein-it-sicherheitsgesetz-2-0/