Stellungnahme

zum Referentenentwurf (Stand 27.03.2019)

Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme

IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0)

Bundesverband der Deutschen Industrie e.V.

Stand: 28. Juni 2019

Inhaltsverzeichnis

Zusammenfassung

Die deutsche Industrie begrüßt das Vorhaben der Bundesregierung, die Cyberresilienz Deutschlands signifikant 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 in hohem Maße digitalisierten Prozessen in Unternehmen ist ein hoher Grad an Cybersicherheit eine Grundvoraussetzung. Damit dieses Ziel mit einem IT-Sicherheitsgesetz 2.0 erreicht werden kann, empfiehlt die Industrie einige grundlegende Anpassungen des derzeitigen Entwurfs.

Die deutsche Industrie hat naturgemäß ein sehr hohes Eigeninteresse, die Funktionsfähigkeit und Verfügbarkeit ihrer IT-Anwendungen und IT-Systeme abzusichern, nicht zuletzt um die eigene wirtschaftliche Leistungs- und Wettbewerbsfähigkeit sicherzustellen. Daher spricht sich die deutsche Industrie für einen kooperativen Ansatz bei der Stärkung der Cyberresilienz des Wirtschaftsstandortes Deutschland aus.

IT-Sicherheit ist nur dann zu erlangen, wenn alle Beteiligten im Rahmen ihrer Möglichkeiten mitwirken. Dabei ist zu berücksichtigen, dass das schwächste Glied in der Kette das Gesamtniveau der IT-Sicherheit bestimmt. In Bezug auf die Verteilung der Risikosphären erscheint der erste Gesetzesentwurf noch nicht hinreichend ausgewogen und verbesserungswürdig. Viele Risiken resultieren eben nicht aus der Sphäre von Betreibern Kritischer Infrastrukturen, sondern aus der Sphäre von Produkten und Services, die in Kritischen Infrastrukturen zum Einsatz kommen. Es ist daher erforderlich, dass alle Beteiligten entsprechend der Kritikalität der von ihnen gelieferten Produkte und Services sowie ihrer Möglichkeiten, Sicherheitslücken abzustellen, zur Verantwortung gezogen werden.

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

- **Fehlende Evaluierung des IT-Sicherheitsgesetzes**: Bevor ein zweites IT-Sicherheitsgesetz initiiert wird, wäre es angezeigt gewesen, das erste IT-Sicherheitsgesetz u.a. auf Grundlage fachlich wissenschaftlicher Expertise eingehend zu analysieren – dies ist jedoch bis dato nicht erfolgt. Hierzu sollte in strukturierter Form auch das Feedback der bisher betroffenen Wirtschaftsteile und Unternehmen eingeholt werden. Eine solche Evaluierung würde den zuvor angesprochenen kooperativen Ansatz deutlich unterstreichen.
- **Meldepflichten haben Lagebild bisher nicht verbessert**: Die mit dem Ersten IT-Sicherheitsgesetz eingeführte Meldepflicht von Cybersicherheitsvorfällen bei Kritischen Infrastrukturen hat bisher keine wahrnehmbare Verbesserung im Lagebild gebracht. Das BSI hat bisher keine unterjährigen branchenspezifischen Lagebilder veröffentlicht. Auch fehlt es an effizienten Meldestrukturen nach dem one-stop-shop-Prinzip. Es sollte also einen harmonisierten Meldeweg an eine zentrale Meldestelle geben und nicht wie zurzeit

Bundesverband der Deutschen Industrie e.V.
Mitgliedsverband
BUSINESSEUROPE

Hausanschrift
Breite Straße 29
10178 Berlin

Postanschrift
11053 Berlin

Ansprechpartner
Steven Heckler
Oliver Klein

T: +493020281523
T: +493020281502

Internet
www.bdi.eu

E-Mail
S.Heckler@bdi.eu
O.Klein@bdi.eu

im Entwurf des IT SiG 2.0. vorgesehen, je nach Sachverhalt eine Meldung an drei verschiedene Behörden erforderlich werden. Zwar können Meldepflichten ein erster Schritt zu einer sinnvollen Verantwortungszuweisung von Herstellern sein, aber letztlich greifen sie zu kurz. Nur wenn Meldepflichten in ein verbessertes ganzheitliches Lagebild sowie branchenspezifische Warnungen münden, kann die deutsche Industrie aus dem beim BSI aggregierten Datenschatz auch einen Nutzen ziehen und ihre Anlagen und Systeme besser schützen. Neben einer Meldung sollten Hersteller auch angehalten werden, erkannte Sicherheitslücken entsprechend zu schließen.

- **Fehlende Einbettung in das europäische Rechtssystem**: Das langfristige Ziel einer europäischen Harmonisierung im Bereich IT-Sicherheit wird durch das IT-SiG 2.0 erschwert. Hierfür stehen beispielhaft das IT-Sicherheitskennzeichen sowie die neuen deutschen Definitionen für Kritische Infrastrukturen, Cyberkritikalität und „Unternehmen im besonderen öffentlichen Interesse“. Nicht abgestimmte, nationalstaatliche Einzelmaßnahmen können gerade für weltweit tätige Unternehmen enorme zusätzliche Kosten und damit Wettbewerbsnachteile für in Deutschland tätige Unternehmen bedeuten. Dadurch würde dem Wirtschaftsstandort Deutschland nachhaltig geschadet.
- **BSI stärken aber nicht inhaltlich überfrachten**: Der BDI begrüßt die personelle Aufstockung des BSI. Allerdings sieht das IT-SiG 2.0 in Bezug auf das BSI eine Überfrachtung mit Aufgaben und Kompetenzen, die dessen Handlungsfähigkeit gefährden könnten. Darüber hinaus sieht das IT-SiG 2.0 zu viele Kontrollbefugnisse in der Hand einer einzelnen Behörde vor.
- **IT-Sicherheitsgesetz 2.0 schafft überbordende Bürokratie**: Im vorliegenden Entwurf werden Kontrollbefugnisse des BSI gegenüber einem sehr breiten Anwenderfeld der deutschen Wirtschaft ausgebaut, die mit einem enormen Bürokratieaufbau einhergehen. Gleichzeitig werden weder etablierte Sicherheitsmechanismen der Wirtschaft berücksichtigt, noch ein nachvollziehbarer wirksamer Sicherheitsnutzen geschaffen noch ist bis heute ein signifikanter Sicherheitszugewinn erkennbar. Der im Koalitionsvertrag angestrebte Bürokratieabbau wird durch derartige Maßnahmen ohne Verbesserung des Sicherheitsniveaus konterkariert.
- **Unspezifische und sehr weitreichende Ausweitung des Anwenderkreises**: Unklare Rechtsdefinitionen und Gesetzesformulierungen zu den Anwenderkreisen für „Infrastrukturen im besonderen Interesse“ und Unternehmen mit „Cyberkritikalität“ erschweren die Einsicht darüber, an wen sich die Vorschriften richten sollen und erzeugen Rechtsunsicherheit bei den möglicherweise betroffenen Unternehmen. So ist mit Blick auf den aktuellen Entwurf unklar, warum manche Domänen oder Branchen keine eigenen Sektoren i.S.d. § 2 Abs. 10 BSIG darstellen, jedoch als Betreiber von Infrastrukturen im besonderen öffentlichen Interesse i.S.d. § 2 Abs. 14

BSIG n.F. anzusehen sein werden. Der Ansatz, den Geltungsbereich ausschließlich auf die wirtschaftliche Ertragskraft bzw. eine Börsennotierung auszurichten und nicht auf den risikobasierten Ansatz, der auf die Aufrechterhaltung von Leistungen, die für das staatliche und soziale Gemeinwohl notwendig sind, abzielt, ist in nur geringem Maße nachvollziehbar.

- **Unverhältnismäßige Auskunftspflichten gegenüber dem BSI**: Es ist unklar, warum der bisherige Prozess der Eigenregistrierung betroffener Unternehmen als KRITIS als nicht mehr ausreichend betrachtet wird. Zudem stellt sich die Frage, warum Unternehmen zur Weitergabe aller aus Sicht des BSI relevanten interner Aufzeichnungen, Schriftstücke und sonstiger Unterlagen verpflichtet werden sollen. Diese Auskunftspflicht bei minimalem Anfangsverdacht stellt einen unverhältnismäßigen Eingriff in die unternehmerische Selbstbestimmtheit dar und wirkt wie ein Generalverdacht gegenüber allen in Deutschland tätigen Unternehmen.
- **Mangelnde Rechtsklarheit, da Gesetzesdetails erst später geregelt werden sollen**: Das Zweite IT-Sicherheitsgesetz lässt in seiner aktuell vorliegenden Fassung an Rechtsklarheit für die deutsche Industrie zu wünschen übrig. Anstatt weitere Details in Rechtsverordnungen zu regeln, sollte der Gesetzgeber diese direkt im Rahmen des IT-SiG 2.0 verbindlich bestimmen.
- **Vertrauenswürdigkeitserklärung für Hersteller von KRITIS-Kernkomponenten nicht einführen:** Die deutsche Industrie spricht sich mehrheitlich gegen die Einführung einer Vertrauenswürdigkeitserklärung in der jetzigen Ausgestaltung aus. Aus Sicht der deutschen Industrie würde die von der Bundesregierung vorgeschlagene Vertrauenswürdigkeitserklärung (1) unkalkulierbare Folgen für Unternehmen haben und gleichzeitig (2) folgenlos für internationale Zulieferer bleiben: (1) Im schlimmsten Fall könnte eine Vertrauenswürdigkeitserklärung, ohne zur Stärkung der Cyberresilienz beizutragen, die Wettbewerbsfähigkeit der deutschen Industrie schwächen. Die Vertrauenswürdigkeitserklärung wird zu hohen Erfüllungsaufwendungen bei deutschen Unternehmen führen, da Unternehmen verpflichtet werden, entlang der gesamten, häufig hochkomplexen Wertschöpfungskette von allen Zulieferern eine Vertrauenswürdigkeitserklärung einzufordern. Es muss geklärt werden, wie die Produktion notwendiger KRITIS-Kernkomponenten sichergestellt werden kann, auch wenn die von Zuliefern unterzeichnete Vertrauenswürdigkeitserklärung vom BSI als gegenstandslos erklärt wird. (2) Zum anderen werden sich internationale Zulieferer in einer Abwägung zwischen der Einhaltung gesetzlicher Vorgaben in ihrem Heimatmarkt oder der Vertrauenswürdigkeitserklärung gegenüber ihrem deutschen Handelspartner, stets für eine Rechtstreue gegenüber ihrer nationalen Regierung entscheiden. Es stellt sich die Frage, ob solch eine Vertrauenswürdigkeitserklärung im Endeffekt lediglich zu einer „Scheinsicherheit“ beiträgt. Zu klären ist zudem, wie die Versorgung mit bestimmten KRITIS-

Kernkomponenten sichergestellt werden wird, sofern die potenziellen Anbieter aus Drittstaaten eine deutsche Vertrauenswürdigkeitserklärung mit Blick auf die Gesetzeslage auf ihrem Heimatmarkt nicht unterzeichnen wollen/können.

- **Unverhältnismäßige Bußgeldvorschriften:** Die vom BMI vorgeschlagene Höhe für Bußgelder, die sich an der DSGVO orientiert, erachtet die deutsche Industrie mit Blick auf das Thema Cybersicherheit als völlig unverhältnismäßig. Eine Begründung für die Höhe der DSGVO-Bußgelder war, dass entsprechende Datenschutzverletzungen Auswirkungen auf einen Markt von 500 Millionen Nutzerinnen und Nutzern haben würden – der deutsche Markt (Geltungsbereich IT-SiG 2.0) hat jedoch nur 80 Millionen. Hier gilt es, deutlich geringere Geldbußen von max. 100.000 Euro anzusetzen.
- **Erfüllungsaufwand für die Wirtschaft viel zu gering angesetzt**: Da zukünftig Zulieferer Maßnahmen umsetzen müssen und zahlreiche neue Branchen unter den Geltungsbereich des IT-SiG 2.0 fallen werden, scheint der Erfüllungsaufwand für die Wirtschaft mit 45,09 Millionen Euro zu gering angesetzt. Aus dem aktuell vorliegendem Referentenentwurf ist nicht nachvollziehbar, wie die Bundesregierung diesen Wert ermittelt hat.
- **Fehlende Verpflichtung des Bundes zur Unterstützung des Föderalismus:** Insbesondere vor dem Hintergrund eines bisher fehlenden regelmäßig veröffentlichten Lagebildes, ist das BSI zum verpflichtenden Austausch von weitreichenden Lagebildinformationen mit anderen Bundes- aber insbesondere auch Landessicherheitsbehörden explizit und geregelt zu verpflichten. Diese Verpflichtung ist dringend notwendig, um Informationslücken, die in der Vergangenheit oft zu Ermittlungsmissständen führten, zu schließen.

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

- Das **IT-Sicherheitsgesetz 1.0 muss** zügig, gemeinsam mit den bisher betroffenen Unternehmen u.a. auf Grundlage fachlich wissenschaftlicher Expertise eingehend analysiert und **evaluiert werden** und Ergebnisse müssen mit der Industrie geteilt werden.
- Es sollte **keine** unverhältnismäßige und nicht an objektiven Kriterien gebundene **Ausweitung der Pflichten Kritischer Infrastrukturen auf weite Teile der Wirtschaft** erfolgen.
- Die **Vertrauenswürdigkeitserklärung für KRITIS-Kernkomponenten** muss einem **Praxischeck** unterzogen werden. In ihrer jetzigen Ausgestaltung scheint sie nicht zweckdienlich.
- Bei Cybersicherheit ist ein **europaweit harmonisierter Regulierungsansatz** nationalen Alleingängen vorzuziehen. Da auf europäischer Ebene gerade erst der EU Cybersecurity Act beschlossen wurde und eine Einführung von Cybersicherheitsanforderungen in die vertikalen Richtlinien für Produktgruppen geprüft wird (siehe

Funkanlagen- und Maschinenrichtlinie), muss das zweite deutsche IT-SiG unbedingt eine inhaltliche Anschlussfähigkeit an diese Vorhaben sicherstellen. Das IT-SiG 2.0 darf keine verteilten inkonsistenten Vorgaben, keine nationalen Sonderanforderungen und damit unrechtmäßigen Marktzugangsbeschränkungen für Produkte im europäischen Gefüge verursachen.

- **Meldepflichten zu Cybervorfällen müssen effizienter ausgestaltet (one-stop-shop-Prinzip) und entsprechende personalisierte Unterstützungsleistungen des BSI für betroffene Unternehmen etabliert werden**:
  - Unternehmen, die Cybersicherheitsvorfälle melden, sollte eine personalisierte Unterstützung angeboten werden,
  - Aus den Meldungen aus der Wirtschaft sollte ein Lagebild für die Industrie erarbeitet und unterjährig mit den relevanten Bundes- und Landessicherheitsbehörden sowie der Industrie geteilt werden,
  - Meldungen aus der Wirtschaft sollten zu zeitnahen branchenspezifischen Warnungen führen
  - Meldungen aus der Wirtschaft müssen zum Schließen von Sicherheitslücken führen,
  - Gesetzliche Rahmenbedingungen müssen geschaffen werden, um Wirtschaftsunternehmen über vorliegende Informationen zu (Cyber)-Gefährdern zu informieren, auch über Geheimschutzbetreute Unternehmen hinaus.
- Mit dem IT-SiG 2.0 sollte gezielt **Bürokratieabbau** und nicht Bürokratieaufbau betrieben werden.
- Es gilt, das **BSI personell und finanziell zu stärken** ohne es inhaltlich zu überfrachten.
- **Verpflichtung des BSI zum Austausch von Lageinformationen innerhalb der staatlichen Strukturen** (Bundes und Landesebene) **und mit Wirtschaftsunternehmen** sollte verbindlich eingeführt werden. Dies sollte unabhängig einer etwaigen Geheimschutzbetreuung eines Unternehmens möglich sein.
- Der BDI fordert die **Einbeziehung der KRITIS-Zulieferer in die UP-KRITIS-Dialoge und die sonstigen KRITIS-Dialogplattformen**. Wenn IT-Sicherheit über den Produktlebenszyklus sowie die gesamte Lieferkette hinweg betrachtet werden soll, müssen die KRITIS-Zulieferer gleichberechtigt in die Abstimmungsprozesse für Rechtsverordnungen, Branchen- und BSI-Standards einbezogen werden. Selbstverständlich gilt dies auch für das Teilen von sicherheitsrelevanten Informationen durch das BSI.
- Der vorgeschlagene **Bußgeldrahmen** muss signifikant reduziert werden.
- Die vorgeschlagenen **Anpassungen am StGB** müssen signifikant überarbeitet 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 einer hoher Grad an Cybersicherheit eine 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). Neben einer weitreichenden Ausweitung der KRITIS-Definition, sollen zukünftig auch sogenannte „Infrastrukturen im besonderen öffentlichen Interesse“ sowie Unternehmen, die sich durch eine „Cyberkritikalität“ auszeichnen, die gleichen Registrierungs-, Melde- und Lieferkettenüberwachungspflichten wie KRITIS-Betreiber haben. Zudem soll der Kompetenzbereich des BSI um den Verbraucherschutz erweitert und ein nationales IT-Sicherheitskennzeichen eingeführt werden. Im Folgenden bewertet die deutsche Industrie die einzelnen Vorhaben:

Zu § 2 Absatz 9 – „Protokollierungsdaten“

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

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

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

Zu § 2 Absatz 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 mit den einhergehenden Pflichten aus § 8h gelten.

Zudem stellt sich die Frage, ob Software sowie alle jene miteinander verbundenen Hardwareprodukte und -komponenten, die Fehler enthalten und deshalb nicht einwandfrei funktionieren, ausgeschlossen sein sollen. Es ist zu bedenken, dass durchschnittlich in 1.000 Zeilen Quellcode eines technischen Produktes im mittleren einstelligen Bereich Fehler enthalten sind. Jeder dieser Fehler kann potenziell zu minimalen Funktionsabweichungen führen. Damit würden aktuell alle von Menschen programmierte vernetzbare Produkte nicht in den Geltungsbereich dieser Definition fallen.

Sollte sich der Gesetzgeber nicht auf eine konkrete Nennung der betroffenen Produkte und Anlagen verständigen können, so sollte die Definition mindestens wie folgt präzisiert werden:

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

Zu § 2 Absatz 10 – Nennung von KRITIS-Sektoren

Durch die mit dem Referentenentwurf vorgeschlagene Gesetzessystematik bleibt unklar, wie sich die Sektoren i.S.d. § 2 Abs. 10 BSIG inhaltlich von den Infrastrukturen im besonderen öffentlichen Interesse i.S.d. § 2 Abs. 14 n.F. BSIG sowie den Betreibern von Anlagen, die als „cyberkritisch“ i.S.d. § 8g BSIG n.F. gelten, unterscheiden.

Ohne Konkretisierung der entsprechenden Rechtsverordnung nach § 10 Abs. 5 BSIG ist eine eindeutige Zuordnung einzelner nicht genannter Branchen unter die einschlägigen gesetzlichen Regelungen nur schwerlich möglich.

Unter dem Blickwinkel der Normklarheit und Wesentlichkeit sollte der Gesetzgeber die maßgeblichen Unterscheidungskriterien für die oben benannten Normadressaten schon in der gesetzlichen Regelung des BSIG aufnehmen,

anstatt diesbezüglich auf die weitere Konkretisierung durch die ausführende Rechtsverordnung nach § 10 Abs. 5 BSIG zu verweisen. So ist mit Blick auf den aktuellen Entwurf unklar, warum manche Domänen oder Branchen keine eigenen Sektoren i.S.d. § 2 Abs. 10 BSIG darstellen, jedoch als Betreiber von Infrastrukturen im besonderen öffentlichen Interesse i.S.d. § 2 Abs. 14 BSIG n.F. anzusehen sein werden.

Zu § 2 Absatz 13 – „Kernkomponenten für Kritische Infrastrukturen“

Positiv zu bewerten ist die grundsätzliche Erfassung der Kernkomponenten für Kritische Infrastrukturen (KRITIS-Kernkomponenten) und deren Hersteller. Allerdings geht die aktuell vorliegende Definition für KRITIS-Kernkomponenten aufgrund ihrer Unbestimmtheit zu weit. Basierend auf der aktuellen Definition wäre nahezu jede IT-Komponente eine KRITIS-Kernkomponente (dies gilt insbesondere für den KRITIS-Sektor TK/Rechenzentren). Mit Blick auf Absatz 13 muss sichergestellt werden, dass IT-Produkte, die als KRITIS-Kernkomponenten definiert sind, nicht ausschließlich in Kritischen Infrastrukturen eingesetzt, sondern auch in weiteren Anlagen verwendet werden dürfen.

Im Abs. 13 Satz 1 wird mit Blick auf den Sektor Energie auch die Netzleittechnik als kritische Kernkomponente aufgeführt. Für Betreiber von Raffinerien die auch eine Netzleittechnik haben ist damit unklar, ob sie ebenfalls unter den Anwendungsbereich von Absatz 13 Satz 1 fallen. Hier ist der Gesetzgeber gefordert, schnell die notwendige Klarheit herbeizuführen.

Es erscheint in Abs. 13 Satz 3 erforderlich, die Definition von Kernkomponenten derart zu schärfen, als dass nur solche Komponenten zu KRITIS-Kernkomponenten gezählt werden können, die im Falle ihres Ausfalls mit Verweis auf 109 TKG zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen und -diensten führen können. Zudem wäre eine spezifischere Verpflichtung wünschenswert, so dass die Hersteller von KRITIS-Kernkomponenten in ihrem Verantwortungsbereich gleichermaßen Vorkehrungen für die IT-Sicherheit zu treffen haben, wie die Betreiber von KRITIS. So dann wären in Bezug auf § 2 Abs. 13 Satz 3 KRITIS-Kernkomponenten auch im TKG unmittelbar zu verankern und nachgelagert durch den in § 109 Abs. 6 TKG adressierten Sicherheitskatalog zu definieren und auszugestalten.

Nach §2 Abs. 13 Satz 7 sind all jene IT-Produkte im Sektor Transport & Verkehr, die zum Betrieb von Anlagen oder Systemen zur Beförderung von Personen oder Güter im Luft-, Straßen- und Schienenverkehr, im ÖPNV sowie der Schifffahrt eingesetzt werden, KRITIS-Kernkomponenten. Dies bedeutet, dass alle IT-Produkte, die bei der Beförderung von Personen und Cargo zum Einsatz kommen, KRITIS-Kernkomponenten wären. Dies Definition ist viel zu weit und sollte auf die in § 8 der BSI-KritisV bereits spezifizierten Anlagen und Systeme reduziert werden. Folglich bedarf es einer genaueren Abgrenzung in den einzelnen Sektoren. So sollten einzelne

Fahrzeuge, die ebenfalls IT-Produkte zur Steuerung des Fahrzeuges (Fahrzeug = System?) enthalten, nicht als Kritische Infrastruktur eingestuft werden. Zudem muss hier geklärt werden, ob und wenn ja welche Zulieferer der (Automobil)-Industrie unter die Vorschriften i.S.d. § 2 Abs. 13 Satz 7 fallen.

Zu § 2 Absatz 14 – „Infrastrukturen im besonderem öffentlichen Interesse“

Die Einführung des Terminus „Infrastrukturen im besonderen öffentlichen Interesse“ ist zu unbestimmt. Mit der Einführung des Terminus „Infrastrukturen im besonderen öffentlichen Interesse“ beschreitet Deutschland einen nationalen Sonderweg, der vom durch die NIS-Richtlinie eingeschlagenen EU-weit teilharmonisierten Ansatz abweicht. Bei ausbleibender EU-weiter Harmonisierung könnte dies zu einem wirtschaftlichen Standortnachteil werden. Die deutsche Industrie fordert die Bundesregierung auf, eine schnellstmögliche Harmonisierung zu erreichen (beste Lösung) oder im Nicht-Erfolgsfall auch eine deutsche Rücknahme auf das EU-Niveau zur Diskussion zu stellen. Ein einheitlicher Europäischer Binnenmarkt bedarf gleicher oder zumindest gleichwertiger Anforderungen für gleiche Unternehmenstypen.

Insbesondere fehlt eine Benennung konkreter Kriterien, warum eine Infrastruktur und deren Anlagen als „im besonderen öffentlichen Interesse“ eingestuft werden. Der Gesetzgeber sollte direkt im Gesetzgebungsprozess des IT-Sicherheitsgesetzes die Wesensmerkmale derartiger Infrastrukturen genauer spezifizieren sowie inhaltlich von den Kritischen Intrastrukturen i.S.d. § 2 Abs. 10 BSIG sowie von „Cyberkritikalität“ i.S.d. § 8g BSIG n.F. abgrenzen. Die im Entwurf aufgezählten Infrastrukturen (Kultur und Medien, Rüstung sowie Unternehmen mit Zulassung zum Teilbereich des regulierten Marktes) werden in diese Kategorie gefasst, obwohl die spezifischen Gründe, weshalb ihre Funktionsfähigkeiten ein erhebliches Interesse für die Gesellschaft darstellen, sich stark voneinander unterscheiden.

Der Einbezug von Unternehmen über Zulassungsfolgepflichten (Prime Standard) nach § 48 Börsenordnung der Frankfurter Wertpapierbörse erscheint willkürlich und scheint nur darauf ausgerichtet, möglichst viele Unternehmen des DAX und MDAX zu erreichen. Eine Risikoorientierung ist hier nur bedingt zu erkennen. Zudem widerspricht der § 2 Abs. 14 Satz 2 damit dem Gleichbehandlungsgrundsatz.

Im Umkehrschluss wäre es ebenfalls wünschenswert, dass auch die Unternehmen, die unter die Kategorie der „Infrastrukturen im besonderen öffentlichen Interesse“ fallen, nicht nur Verpflichtungen auferlegt bekämen, sondern auch bevorzugt mit Informationen versorgt werden würden, die für ihre Sicherheit von Bedeutung sind. Folglich müssten diese Unternehmen auch am UP-KRITIS partizipieren dürfen. Diese Forderung begründet sich in der Einstufung dieser Unternehmen als Teil der Sicherheitsarchitektur der Bundesrepublik Deutschland.

Zudem ist zu klären, was als „erhebliche volkswirtschaftliche Schäden“ definiert wird. Diese bewusst offen formulierte Definition des Anwendungsbereichs ist zu allgemein gehalten und nicht direkt mit qualitativen und quantitativen Kriterien erschließbar.

Unternehmen mit „Zulassung zum Teilbereich des regulierten Marktes“ unterliegen bereits jetzt vielerlei Folge- und Berichtspflichten; die angestrebte Kompetenzerweiterung des BSI als eine zusätzliche Aufsichts- und Regulierungsbehörde mit weitergehenden Berichtspflichten für die entsprechenden Unternehmen stellt eine erhebliche Mehrbelastung dar, ohne dabei risikobasiert bereits existierende Sicherheitsmechanismen der Unternehmen zu berücksichtigen. Der damit verbundene Aufwand konterkariert jede Bemühung zum Bürokratieabbau.

Mit Blick auf die Einbeziehung von Unternehmen der Rüstungsindustrie wäre es zudem wünschenswert, wenn der Verweis auf die entsprechend geltenden Absätze des § 60 Außenwirtschaftsverordnung eingefügt werden würde.

Zu § 3 Aufgaben des Bundesamtes für Sicherheit in der Informationstechnik

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.

Die deutsche Industrie lehnt es ab, dass das BSI bei Produkten, die entsprechend des EU Cybersecurity Acts unter die Assurance Level „low“ und „substantial“ fallen, als Stelle für Konformitätsbewertungen i.S.d. § 3 Abs. 1 Satz 5a eingerichtet wird. Eine entsprechende Kompetenzausweitung würde das bisherige Modell einer strikten Trennung solcher Tätigkeiten untergraben. Diese Funktion ist klar abgedeckt durch die Privatwirtschaft und sollte, außer entsprechend den Vorgaben aus dem EU Cybersecurity Act für das Assurance Level „high“ und damit die besonders sicherheitsrelevanten Bereiche – wie beispielsweise der Konformitätsbewertung von 5G-Netzwerkinfrastrukturkomponenten – nicht dem BSI übertragen werden.

Mit Blick auf § 3 Abs. 1 Satz 14 wäre es aus Sicht der deutschen Industrie hilfreich, wenn das BSI nicht lediglich eine risikodarstellende Beratung vornimmt, sondern ebenfalls eine Beratung im Hinblick auf die aus Sicht des BSI angemessenen Sicherheitsvorkehrungen anbieten würde. Dies könnte die tatsächliche Anhebung des Sicherheitsniveaus in der Fläche bewirken. Angesichts des bekannten Fachkräftemangels besonders im Bereich der IT stellt sich der Industrie zudem die Frage, wie das BSI den im § 3 Abs. 1 Nummer 14 BSIG statuierte gesetzliche Auftrag der Beratung von Herstellern und

Anwendern tatsächlich erfüllen kann. Zudem sind die Pflichten des BSI zu konkretisieren, beispielsweise wie schnell das BSI zu warnen hat.

Mit Blick auf die Entwicklung von Anforderungen an Identifizierungs- und Authentisierungsverfahren (§ 3 Abs. 1 Satz 19) sowie die Entwicklung und Veröffentlichung sicherheitstechnischer Anforderungen an IT-Produkte (§ 3 Abs. 1 Satz 20) empfiehlt sich eine Abstimmung der Verfahren mit der Anwender- und Herstellerindustrie, um nicht an den tatsächlichen Bedarfen vorbeizuentwickeln. Es ist unklar, ob und in welchem Maße die vom BSI veröffentlichten Anforderungen an Identifizierungs- und Authentifizierungsverfahren Anspruch auf Verbindlichkeit besitzen und inwieweit die Durchsetzung dieser Anforderungen unter Zugrundelegung der EU-Binnenmarktharmonisierung europarechtskonform umgesetzt werden kann.

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

„19. Entwicklung von Anforderungen an 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 einzubringen“

„20. Entwicklung sicherheitstechnischer Anforderungen an IT-Produkte unter Berücksichtigung etablierter Markt- und Branchenstandards und dem Stand der Technik mit dem Ziel, diese in die internationale Standardisierung einzubringen.“

Zu § 4a Kontrolle der Kommunikationstechnik des Bundes

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

- Zu Satz 1: Es empfiehlt sich, eine Präzisierung des Begriffs „mit Betriebsleistungen beauftragten Dritten“ vorzunehmen.
- Zu Satz 3: Hier sollte ebenfalls eine Präzisierung der „Dritten, die Schnittstellen zur Kommunikationstechnik des Bundes haben“ erfolgen. Es stellt sich die Frage, inwiefern Hersteller, die Schnittstellen zur Informationstechnik des Bundes haben (organisatorisch und/oder technisch), betroffen sind. Zudem bedarf es einer konkreteren Definition, welche Schnittstellen unter den Anwendungsbereich des § 4a Satz 3 BSIG n.F. fallen.

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

Zu § 4b Meldestelle für die Sicherheit in der Informationstechnik

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

- Es gilt, die damit verbundenen Obliegenheiten des BSI detailliert im Gesetzestext zu definieren.
- Auf der Grundlage der schon gewonnenen Erfahrungen im Zusammenhang mit gesetzlichen Meldepflichten zu Informationssicherheitsvorfällen gehen Teile der deutschen Industrie davon aus, dass die Aktivitäten des BSI in Hinsicht auf die Entgegennahme, Analyse und Aufbereitung der so zugeleiteten Information über Sicherheitslücken oder Angriffsvektoren für die angeschlossenen Unternehmen zu kaum verwertbaren Erkenntnissen (sog. *actionable intelligence* i.S. des Cyber Threat Management) führen werden. Die deutsche Industrie sieht daher die dringende Notwendigkeit, (a) zukünftig die erhaltenen Informationen einzelfallbezogen zu beantworten, (b) zielgruppengerecht aufzubereiten und (c) 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.
- Sollte das BSI durch Meldungen Erkenntnisse über Schwachstellen gewinnen, muss es diese Erkenntnisse unbedingt den betroffenen Unternehmen zukommen lassen und diese Schwachstellen nicht mit weiteren staatlichen Bedarfsträgern für deren Tätigkeiten teilen. Nur zügig geschlossene Schwachstellen stärken die Cyberresilienz Deutschlands. Dies kann dadurch 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 Nummer 2 und 3 ist zudem das Wort „kann“ durch „muss“ zu ersetzen. Das BSI sollte die Pflicht haben, alle entsprechenden Informationen entgegenzunehmen. Im jüngsten Doxing-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.
- Darüber hinaus muss aus der Meldung auch seitens der meldenden Stelle eine Handlung erfolgen, welche dazu geeignet ist, die von der jeweiligen Sicherheitslücke ausgehende Gefahr entsprechend

einzudämmen, etwa durch die Bereitstellung entsprechender Softwareupdates.

Zu § 5 Absatz 11

§ 5 Abs. 11 sieht vor, dass das BSI Maßnahmen zur Abwehr von Gefahren für die Kommunikationstechnologie des Bundes bei IT-Dienstleistern und -anbietern, die entsprechende Leistungen für den Bund erbringen, durchführen darf. Hier sollte präzisiert werden, wie tiefgreifend diese Maßnahmen sein können. Die aktuelle Formulierung ließe beispielsweise die Möglichkeit zu, dass das BSI in das Unternehmen kommen und die Kontrolle über Entwicklung und Fertigung von Produkten übernehmen könnte. Zudem gilt es zu klären, wie die Haftung des BSI in solchen Fällen ausgestaltet wäre, wenn im Zuge dessen Maßnahmen angewiesen worden sind, die in anderen Bereichen geschäftsschädigend sind.

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.

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

§ 5b Abs. 1 sollte daher wie folgt lauten:
„(1) Handelt es sich bei einer Beeinträchtigung der Sicherheit oder Funktionsfähigkeit eines informationstechnischen Systems einer Stelle des Bundes oder eines Betreibers einer Kritischen Infrastruktur oder eines Betreibers einer weiteren Anlage im besonderen öffentlichen Interesse um einen herausgehobenen Fall, so kann das Bundesamt auf Ersuchen der betroffenen Stelle oder des betroffenen Betreibers die Maßnahmen treffen, die zur Wiederherstellung der Sicherheit oder Funktionsfähigkeit des betroffenen informationstechnischen Systems erforderlich sind. *Soweit das Bundesamt erste Maßnahmen zur Schadensbegrenzung und Sicherstellung des Notbetriebes vor Ort ergreift, werden hierfür keine Gebühren oder Auslagen für die Tätigkeit des Bundesamtes erhoben. Hiervon unberührt bleiben etwaige Kosten für die Hinzuziehung qualifizierter Dritter."*

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

Der Referentenentwurf vernachlässigt bei der Erarbeitung von Krisenreaktionsplänen durch das BSI gemeinsam mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und der jeweils zuständigen Aufsichtsbehörde des Bundes die Beteiligung einer wichtigen Akteursgruppe – die betroffenen Betreiber Kritischer Infrastrukturen, Betreiber weiterer Anlagen im öffentlichen Interesse sowie den Betreibern und den Lieferanten der KRITIS-Kernkomponenten. Die Sicherheit von Mitarbeitern, Stakeholdern, Maschinen, Anlagen und Prozessen sind den Unternehmen ein zentrales Anliegen. Es gilt, die zu erarbeitenden Krisenreaktionspläne gemeinsam mit der Wirtschaft auszuarbeiten. Nur so kann eine reibungslose Reaktion auf Krisen gewährleistet werden, denn nur die betroffenen Unternehmen haben umfangreiche Kenntnisse ihrer Geschäftsprozesse und/oder kaufmännische, respektive unternehmerische Verantwortung. Die deutsche Industrie empfiehlt zudem, statt Krisenreaktionspläne zu erarbeiten, für die Schnittstelle zu Betreibern Kritischer Infrastrukturen und Betreibern weiterer Anlagen im besonderen öffentlichen Interesse Krisenkommunikationspläne zu erarbeiten. Solche Pläne könnten zusammen mit weiteren die IT-Sicherheit eines Unternehmens betreffenden Informationen in einer IT-Sicherheitsbilanz zusammengefasst und bei Bedarf für Aufsichtsbehörden bereitgehalten werden.

Die Einführung des § 5c Abs. 4 stellt einen wesentlichen Eingriff in unternehmerische Prozesse und die unternehmerische Entscheidungsfreiheit dar. Es ist ein wesentliches Eigeninteresse von Wirtschaftsunternehmen seine Systeme bestmöglich vor erheblichen Störungen zu schützen. Die Übertragung von Verantwortlichkeit im Sinne einer Pflicht zum Informationsaustausch bis hin zu einer Weisungsbefugnis erhöht daher nicht das IT Sicherheitslevel in den betroffenen Unternehmen: Die regelmäßige Überprüfung der implementierten Sicherheitsmaßnahmen durch Auditoren oder durch Zertifizierung sind dazu probate und bereits vielschichtig eingesetzte Instrumente.

Viele Unternehmen verfügen schon heute über intern ausgearbeitete qualitativ hochwertige Krisenreaktionspläne. Es liegt im ureigenen Interesse dieser Unternehmen, dass die implementierten Krisenreaktionspläne und -prozesse dafür Sorge tragen, dass im Notfall die angemessenen Maßnahmen rechtzeitig durchgeführt werden. Unternehmen nehmen die Sicherheit ihrer Mitarbeiter, Stakeholder, Maschinen, Anlagen und Prozesse sehr ernst.

Aus der Norm geht nicht hervor, welche Verbindlichkeit die besagten Krisenreaktionspläne für die betroffenen Betreiber weiterer Anlagen im besonderen öffentlichen Interesse für den Fall des Eintritts einer erheblichen Störung i.S.d. § 8b Abs. 4 Nummer 2 BSIG n.F. besitzen sollen. Folglich können die Krisenreaktionspläne nur einen unverbindlichen Charakter haben, der nicht mit einer Umsetzungspflicht belegt ist.

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

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

Zu § 5d Bestandsdatenauskunft

§ 5d sieht vor, dass das BSI Bestandsdaten von TK-Dienstleistern anfordern darf, wenn es Kenntnis von Beeinträchtigungen der Sicherheit oder Funktionsfähigkeit von IT-Systemen Dritter erlangt hat und die direkte Kontaktaufnahme mit Dritten notwendig erscheint. Schon heute können zahlreiche Behörden solche Anfragen stellen, so dass diese weitere Möglichkeit nicht erschwerend wirkt. Wünschenswert wäre, dass sich das BSI entsprechend seinem Vorbildcharakter 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. Schließlich ist positiv zu bewerten, dass eine Entschädigung nach § 23 JVEG vorgesehen wurde.

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

Zu § 7 – Warnungen

Bezugnehmend auf die Möglichkeit des BSI, Warnungen nach § 7 auszusprechen, sollte folgender Satz gestrichen werden:

„Diese Informationspflicht besteht nicht, wenn hierdurch die Erreichung des mit der Maßnahme verfolgten Zwecks gefährdet wird oder wenn berechtigter Weise davon ausgegangen werden kann, dass der Hersteller an einer vorherigen Benachrichtigung kein Interesse hat.“

Hersteller sollten grundsätzlich vor Veröffentlichung einer Warnung durch das BSI informiert werden, um entsprechende Lösungen zur Behebung der Sicherheitslücken in Produkten für Kunden anbieten zu können.

Zu § 7a Untersuchung der Sicherheit in der Informationstechnik

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

Aus dem Gesetzesentwurf sowie aus dessen Begründung geht nicht hervor, inwieweit der Gesetzgeber im Kontext des Auskunftsverlangens des BSI gegenüber Herstellern informationstechnischer Produkte eine sachgerechte Abwägung der Interessen der Allgemeinheit an der Sachverhaltsaufklärung sowie dem Interesse des in Anspruch genommenen Betroffenen an der Geheimhaltung von produkt- bzw. servicebezogenen Informationen vorgenommen hat. Insbesondere ist das Verhältnis der entsprechenden Auskunftsrechte zum GeschGehG gänzlich unklar.

Wenn Schwachstellen gemeldet werden, für die ein Patch zeitnah nicht verfügbar ist, darf eine externe Kommunikation nur in Absprache mit den Herstellern passieren, um Schäden für Kunden und Betreiber durch das Öffentlichmachen von Angriffsmöglichkeiten zu vermeiden. Sinnvoll wäre eine Pflicht des BSI, 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.

Zum Schutz des geistigen Eigentums muss als sinnvolle Einschränkung eingefügt werden, dass jedwede Untersuchung von Quellcode und anderen relevanten Materialien, welche unter dem Schutz des geistigen Eigentums stehen, an einem unter Kontrolle des Herstellers sich befindenden sicheren Ort durchgeführt wird.

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

Die deutsche Industrie lehnt es ab, dass das BSI zukünftig unkoordinierte Penetrationstests und RedTeaming-Aktivitäten auch auf IT-Infrastrukturen von KRITIS-Betreibern durchführen können soll (§ 7b Satz 1). Dies birgt potenziell große Gefahren und könnte im schlimmsten Fall die Sicherheit Kritischer Infrastrukturen gefährden.

Es wäre vielmehr 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.

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

Zu § 7c Detektion zum Schutz der Mitglieder der Verfassungsorgane

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

Zu § 8 Vorgaben des Bundesamtes

§ 8 ermöglicht dem BSI, Mindeststandards für die Sicherheit der Informationstechnik des Bundes zu erarbeiten, die auch von öffentlichen Unternehmen, die mehrheitlich im vollen Eigentum des Bundes stehen und die IT-Dienstleistungen für die Bundesverwaltung erbringen, zu befolgen sind. Im Sinne einer klaren Kompetenzaufteilung begrüßt der BDI dieses Vorhaben.

Zu § 8a Sicherheit in der Informationstechnik Kritischer Infrastrukturen

Bei der Festlegung von Systemen zur Angriffserkennung durch das BSI gilt es, die entsprechenden sektorspezifischen Verfügbarkeiten von Technologien sowie Branchenstandards zu berücksichtigen. Es ist unklar, inwieweit die Technische Richtlinie zur Ausgestaltung des Einsatzes von Systemen zur

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

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

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

Die Vorgabe, jedes Quartal an unterschiedliche Personen und Behörden einen detaillierten Bericht zu den Systemen zur Angriffserkennung zu geben ist ein Meldezwang, der den mit dem IT-SiG 2.0 verbundenen bürokratischen Aufwand unangemessen erhöhen würde. Unternehmen sollten ihre knappen personellen Ressourcen in die Gewährleistung eines hohen Cybersicherheitsschutzniveaus investieren können und nicht in das Verfassen von Berichten.

Zu § 8a Absatz 6 – Vertrauenswürdigkeitserklärung für Hersteller von KRITIS-Kernkomponenten

Mit § 8a Abs. 6 BSIG n.F. sieht der deutsche Gesetzgeber die Einführung einer Vertrauenswürdigkeitserklärung für Hersteller von KRITIS-Kernkomponenten vor. Dadurch soll zukünftig gewährleistet werden, dass Kernkomponenten, die in Kritischen Infrastrukturen zum Einsatz kommen, nur von vertrauenswürdigen Herstellern bezogen werden. Diese Regelung soll Auswirkungen auf die gesamte Lieferkette entfalten.

Wie in der BDI-Stellungnahme vom April 2019 zum Vorschlag der Bundesnetzagentur für einen Aktualisierten Katalog von Sicherheitsanforderungen zu § 109 Telekommunikationsgesetz dargelegt, spricht sich der BDI dafür aus, dass technikbezogene Zertifizierungen und Sicherheitsüberprüfungen niemals die einzige Dimension zur Stärkung der Widerstandsfähigkeit von Kritischen Infrastrukturen sein dürfen. Vielmehr müssen sie Teil einer

ganzheitlichen Bedrohungsanalyse sein. In diese Prüfung müssen auch gesetzliche Rahmenbedingungen und gängige Praktiken einbezogen werden, denen die Anbieter auf ihrem Heimatmarkt oder mit Tochtergesellschaften in einem Drittstaat ausgesetzt sind, die aber für ihre Tätigkeit in der EU relevant sind (bspw. verpflichtende Weitergabe von Daten an staatliche Stellen).

Die deutsche Industrie erachtet eine Vertrauenswürdigkeitserklärung für Hersteller von KRITIS-Kernkomponenten in der jetzigen Form jedoch als den falschen Schritt, um potenzielle negative Auswirkungen von gesetzlichen Rahmenbedingungen und gängigen Praktiken auf Drittmärkten wirksam entgegenzuwirken. Diese müssen vielmehr direkt Teil des Katalogs von Sicherheitsanforderungen zu § 109 Telekommunikationsgesetz sein.

Im vorliegenden Entwurf umfassen die sogenannten KRITIS-Kernkomponenten sämtliche IT-Produkte, die für den Betrieb einer Kritischen Infrastruktur dienen oder dafür entwickelt wurden. Diese sehr umfassende Regelung würde einen erheblichen Mehraufwand für alle beteiligten Hersteller von KRITIS-Kernkomponenten sowie Teilen von KRITIS-Kernkomponenten erfordern. Für Betreiber wäre diese Verpflichtung zudem mit einer hohen Rechtsunsicherheit verbunden, da nur mit einem erheblichen Mehraufwand gewährleistet werden kann, dass alle, an der oftmals internationalen Lieferkette des Herstellers beteiligten Akteure, den rechtlichen Vorgaben entsprechen. Dies wirkt umso schwerwiegender, als dass mit dem neuen IT-SiG 2.0 der Anwendungskreis der Betroffenen erheblich auf einen Großteil der deutschen Wirtschaft ausgedehnt werden soll. Mit der Erklärung der Vertrauenswürdigkeit müsste in jedem Fall eine adäquate Verantwortungs- und Haftungsverlagerung einhergehen, da Betreiber Kritischer Infrastrukturen nicht für die Folgen eines etwaigen Bruchs der Vertrauenswürdigkeit anderer eintreten können bzw. selbige zu verantworten haben.

Die Vertrauenswürdigkeitserklärung läuft zudem Gefahr, ein zahnloser aber aufwendiger Papiertiger zu sein. Die Abgabe der geforderten Vertrauenswürdigkeitserklärung scheint aus Sicht der deutschen Industrie nur sinnvoll, wenn das BSI den sachlichen Gehalt dieser Erklärung mit geeigneten Mitteln verifizieren kann. Insbesondere ist zu bedenken, dass internationale Zulieferer deutscher Unternehmen auch nach Abgabe der Vertrauenswürdigkeitserklärung sich an die nationalen Gesetze und Vorgaben auf ihrem Heimatmarkt halten müssen.

Auch sollte spätestens im Zuge der Erlassung von Mindestanforderungen auch geregelt sein, welche operativen Maßnahmen ggf. vorher zu ergreifen sind, um im Falle eines Entzugs der Vertrauenswürdigkeit den Betrieb der betroffenen Kritischen Infrastruktur aufrechterhalten zu können. In diesem Kontext sind auch im Rahmen der Allgemeinverfügung neben den Mindestanforderungen Aussagen darüber zu treffen, welche Maßnahmen im Falle des Entzuges der Vertrauenswürdigkeitserklärung zu ergreifen sind und auch, wer ggf. für die Kosten, welche nicht im Verantwortungsbereich des Betreibers einer Kritischen Infrastruktur liegen können, aufkommen muss. Zudem

erscheint eine Klarstellung erforderlich, welche Rechtsanforderung (Erfüllung von Sicherheitsanforderungen versus Betriebskontinuität) aus Sicht des Gesetzgebers seitens des KRITIS-Betreibers prioritär zu betrachten ist.

Sollte die Bundesregierung auf der Einführung der Vertrauenswürdigkeitserklärung bestehen, so gilt es, den Begriff der kritischen IT-Komponenten zu präzisieren und eng zu fassen, damit rechtssicher nur die Komponenten gemeint sind, die zum Betreiben der Kritischen Infrastruktur notwendig sind.

Die Abgabe einer Vertrauenswürdigkeitserklärung durch Lieferanten von KRITIS-Kernkomponenten darf, sollte sie ungeachtet der hier aufgeführten kritischen Anmerkungen eingeführt werden, aus pragmatischer wie aus juristischer Perspektive nur ihre Wirkung auf zukünftige Lieferantenbeziehungen von Herstellern von KRITIS-Kernkomponenten entfalten. Die vom Gesetzesentwurf geforderte Abgabe einer Vertrauenswürdigkeitserklärung über eine globale Lieferkette hinweg ist insoweit bedenklich, da auf diese Weise in schon bestehende Lieferbeziehungen eingegriffen wird.
Es gilt zu prüfen, ob die Vertrauenswürdigkeitserklärung eine europarechtswidrige Beschränkung des Marktzugangs darstellt.

Zu § 8b Absatz 2 Krisenkommunikationssystem

Betreiber Kritischer Infrastrukturen erhalten nach § 8 Abs. 2 zukünftig Anspruch auf Zugang zu einem einheitlichen Krisenkommunikationssystem. Ein einheitliches Krisenkommunikationssystem im Sinne des § 8b Abs. 2 BSIG-E existiert derzeit nicht, wird jedoch, sofern es gemeinsam mit den Betreibern Kritischer Infrastrukturen entwickelt und an deren Bedarfen ausgerichtet wird, grundsätzlich begrüßt. Es bleibt offen, auf welcher Technologie dieses Krisenkommunikationssystem basieren soll. Weiter bleibt unklar, ob Betreibern Kritischer Infrastrukturen der Zugang und die Nutzung des einheitlichen Krisenkommunikationssystems unentgeltlich möglich sein wird. Es ist davon auszugehen ist, dass im Zuge der fortschreitenden Implementation aus der Anspruchsberechtigung ein Verwendungszwang für KRITIS-Betreiber erwachsen wird.

Aus Sicht der deutschen Industrie ist folgender Satz zu ergänzen:
Zugang und Nutzung des einheitlichen Krisenkommunikationssystems ist für Betreiber Kritischer Infrastrukturen unentgeltlich möglich.

Zu § 8b Absatz 3 und 3a Registrierung beim BSI

§ 8b BSIG definiert die Aufgaben des BSI und die sich daraus ergebende Kooperation mit Betreibern Kritischer Infrastrukturen. Außerdem regelt es den Registrierungsprozess durch Betreiber Kritischer Infrastrukturen beim BSI.

Es ist unklar, welchen Mehrwert die Regelungen nach Absatz 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.

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

Die geheimschutzbetreute Industrie unterliegt bereits Vorgaben der Gesetzgebung (GHB, IT-GA). Mit Blick auf § 8 Abs. 3 muss eine Informationstechnische Geheimschutzanweisung (IT-GA) des BMWi nach Vorgaben des BSI einer Registrierung nach dem IT-SiG 2.0 gleichzusetzen sein, da sonst Mehrfacherfassung entstünde.

Zu § 8f Anforderungen für Betreiber von Infrastrukturen im besonderen öffentlichen Interesse

Durch § 8f BSIG n.F. würden Betreiber von Infrastrukturen im besonderen öffentlichen Interesse mit den gleichen Auflagen versehen wie KRITIS-Infrastrukturen. Im IT-Sicherheitsgesetz 2.0 bedarf es der Einführung einer Abstufung zwischen KRITIS-Infrastrukturen und Infrastrukturen im besonderen öffentlichen Interesse. Eine einfache Zuweisung der KRITIS-Anforderungen ist nicht verhältnismäßig.

Zu § 8g Cyberkritikalität

Die deutsche Industrie lehnt die über § 8g eingeführten weitgehenden Befugnisse des BSI auf nicht bereits unter die definierten KRITIS-Sektoren fallenden Unternehmen ab. § 8g ist in seinem Anwendungsbereich so offen formuliert, dass damit Rechtsunsicherheit für einen großen Teil der deutschen Wirtschaft geschaffen würde. Der sachliche Anwendungsbereich im Gesetz muss daher wesentlich konkreter ausgeführt werden.

Der vorliegende Entwurf enthält keine konkreten Kriterien, ab wann ein potenzieller Betreiber einen ausreichenden „hohen Grad an Vernetzung“ aufweist oder ab wann eine tatsächliche und hinreichend schwere Gefährdung für ein Grundinteresse der Gesellschaft vorliegt, um unter diese Regelung zu

fallen. Zunächst muss zwischen der Vernetzung nach außen mit anderen Geräten, Anwendungen und Plattformen und der Vernetzung nach innen zwischen Hardware, (*embedded*) Software in der Anlage unterschieden werden. Andernfalls ist jede Art von Vernetzung möglich, dies würde wiederum dazu führen, dass alles als potenziell cyberkritisch gelten muss.

Vor diesem Hintergrund schlägt die deutsche Industrie die vollständige Löschung von § 8g BSIG n.F. vor.

Zu § 8h Hersteller von IT-Produkten

Die Meldepflicht von Herstellern von IT-Produkten bei erheblichen Störungen der Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität ist grundsätzlich positiv zu werten. Allerdings konzentriert sich die neue Anforderung im Gegensatz zu den Berichtspflichten für KRITIS-Betreiber an ihre Lieferanten/Hersteller nicht auf bestimmte Vorfälle, die den Betrieb stören, sondern auf unbeabsichtigte Schwachstellen oder Schwachstellen in einem Produkt, die es einem Angreifer ermöglichen könnten, das Produkt zu gefährden. Offen erscheint die Definition des Begriffs einer erheblichen Störung von IT-Produkten mit entsprechenden Auswirkungen auf KRITIS-Betreiber (gem. § 2 Abs. 10) bzw. Infrastrukturen im besonderen öffentlichen Interesse (gem. § 2 Abs. 14). Hier ist eine verbindliche Ausgestaltung in Form einer Rechtsverordnung oder Allgemeinverfügung anzuregen.

Die im Entwurf enthaltene Anforderung könnte als Verpflichtung verstanden werden, alle schwerwiegenden Schwachstellen „unverzüglich“ dem BSI zu melden, noch bevor sie untersucht oder behoben werden (konnten). Eine solche Benachrichtigung könnte Bemühungen untergraben, die dringendsten Probleme zu priorisieren und entsprechende Ressourcen darauf zu lenken. Dies würde die Sicherheitslage insgesamt schwächen, da der Kreis der beteiligten Parteien vor der Behebung der Schwachstelle unnötig erweitert wird, während gleichzeitig die Beteiligten wahrscheinlich keine verwertbaren Informationen erhalten. Der Gesetzgeber sollte Hersteller vielmehr dazu verpflichten, die gleichen Informationen über Sicherheitsrisiken zeitnah und für alle gleichzeitig in einem Format zu veröffentlichen, das von öffentlichen Stellen und Betreibern Kritischer Infrastrukturen, die die Technologie des betroffenen Herstellers einsetzen, verwendet wird.

Ergänzend zu den Meldepflichten ergeben sich aus dem Gesetzesentwurf keine unmittelbaren Pflichten, die zur Behebung der etwaigen Störungen notwendigen Maßnahmen seitens der Hersteller zu treffen bzw. solche Maßnahmen zu ergreifen, die die Eintrittswahrscheinlichkeit von Störungen minimieren helfen. Hier ist es angezeigt, dass Hersteller von kritischen Komponenten entsprechend auch unmittelbar im TKG verpflichtet werden, erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT-Produkte zu vermeiden und zu beseitigen.

Zu § 9a Freiwilliges IT-Sicherheitskennzeichen

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 Absatz 2a Ausgestaltung IT-Sicherheitskennzeichen

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 § 14 Bußgeldvorschriften

§ 14 Abs. 1 BSIG enthält einen Katalog von Ordnungswidrigkeiten. Bei Verstößen gegen die entsprechenden Bestimmungen können Bußgelder in Höhe von bis zu 10 Millionen oder respektive 20 Millionen Euro oder 2 respektive 4 Prozent des weltweiten Jahresumsatzes fällig werden. Es wird dabei übersehen, dass die Erhöhung der IT-Sicherheit ein wesentliches unternehmerisches Interesse der Verpflichteten darstellt. Dies gilt insbesondere hinsichtlich der bestehenden vertraglichen Pflichten gegenüber den Kunden der Verpflichteten, der Wettbewerbssituation im Markt sowie der Verantwortung gegenüber den Aktionären und Investoren. Daher sollte mangels Erforderlichkeit von der Aufnahme einer solchen Regelung Abstand genommen werden.

Bei den Bußgeldvorschriften manifestiert sich ebenso die bereits zuvor kritisierte Ungleichbehandlung von Herstellern und Providern. Während Hersteller von IT-Produkten noch nicht einmal zu Präventions- und Störungsbeseitigungsmaßnahmen verpflichtet werden, sollen die Betreiber von IT- und TK-Anlagen mit hohen Bußgeldern überzogen werden.

Die im Entwurf in § 14 Abs. 2 BSIG abgebildeten Bußgeldvorschriften sind zudem unverhältnismäßig und stehen in keinem angemessenen Verhältnis zum möglichen ordnungswidrigen Verhalten, wie beispielsweise einer versäumten Meldepflicht. Die Bußgeldrahmen stellen zudem ein nahezu nicht zu kalkulierendes Kostenrisiko für die Verpflichteten dar. Vor diesem Hintergrund schlägt der BDI vor:

1. eine signifikante Senkung des angestrebten Maximalbußgeldrahmens von 20.000.000 auf maximal 100.000 Euro anzustreben,
2. dass eine relative Höhe (4% vom weltweiten Jahresumsatz) gänzlich gestrichen wird, da durch die Anknüpfung an den

Umsatz Unternehmen mit geringeren Margen härter bestraft werden als Unternehmen mit hohen Margen und die Bußgelder schnell eine existenzielle Bedrohung darstellen können.

§ 14 Abs. 3 BSIG sieht eine Privilegierung in Bezug auf die Ahndung von Ordnungswidrigkeiten für solche Anbieter vor, die ihre Hauptniederlassung nicht in einem EU-Mitgliedstaat haben, nicht in einem anderen EU-Mitgliedstaat niedergelassen sind, dort aber einen Vertreter benannt haben und in diesem Mitgliedstaat dieselben digitalen Dienste anbieten. Gründe für diese Privilegierung lassen sich dem Entwurf nicht entnehmen.

Zu Artikel 2 – Änderung des Telekommunikationsgesetzes

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

Zu § 109a – Absatz 4

Diensteanbieter sind zukünftig verpflichtet, Nutzerinnen und Nutzer nicht nur über Störungen, sondern auch über Gefahren, die von Datenverarbeitungssystemen der Nutzer ausgehen oder diese betreffen, zu informieren. Die Verpflichtung, auch betroffene Nutzer zu informieren, nicht nur von tatsächlichen Störungen, sondern auch Gefahren ist unverhältnismäßig, unangemessen und nicht zielführend im Sinne des jetzigen § 109a Abs. 4 TKG. Zweck des § 109a Abs. 4 TKG ist, Störungen oder Gefahren, die von Nutzern ausgehen, zu unterbinden und dem Nutzer dabei – sofern technisch möglich und zumutbar – zu unterstützen, diese zu beheben. Betroffene Nutzer spielen in der Beseitigung der Störung keine Rolle.

Die deutsche Industrie schlägt vor, den § 109a Abs. 4 Satz 1 wie folgt zu fassen:
„Werden dem Diensteanbieter nach Absatz 1 Störungen *oder Gefahren* bekannt, die von Datenverarbeitungssystemen der Nutzer ausgehen ~~*oder diese betreffen*~~, so hat er die Nutzer, soweit ihm diese bereits bekannt sind, unverzüglich darüber zu benachrichtigen.“

Zu § 109a – Absatz 1a

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

Allerdings begegnet diese Vorschrift Bedenken in Hinblick auf ihre Umsetzbarkeit und Vereinbarkeit mit den Rechtsstaatsprinzipien der Bundesrepublik. Die rechtliche Bewertung, ob eine Nutzung von Daten rechtmäßig oder

rechtswidrig ist, setzt die Kenntnis des vollständigen Sachverhalts voraus. Dieser wird den Verpflichteten aber in der Regel nicht vorliegen, bspw. ob der Betroffene gegenüber dem Nutzer bzgl. der Nutzung seiner Daten zugestimmt hat. Der Verpflichtete hat auch keine Kenntnis von den Inhalten der Daten und darf sich diese aus rechtlichen Gründen auch nicht verschaffen. Zudem setzt die Feststellung der Unrechtmäßigkeit aufgrund der Schwierigkeit der rechtlichen Fragestellungen juristische Fachexpertise voraus, die die Verpflichteten in dem für solche Prüfungen erforderlichen Maßnahmen nicht vorhalten können, um unverzügliche Meldungen an das BKA abzusetzen zu können. Unter rechtsstaatlichen Gesichtspunkten ist anzumerken, dass die Ermittlung von Ordnungswidrigkeiten und Straftaten eine staatliche Aufgabe ist, die nicht in die Hände der Privatwirtschaft gelegt werden darf. Unsere Rechtsordnung sieht bislang eine Anzeige von Sachverhalten nur bei schwerwiegenden Straftaten, nicht aber leichten Straftaten und Ordnungswidrigkeiten vor. Dieser Grundsatz wird mit dem Entwurf gebrochen. Zum Schutz vor Denunziation muss an diesem Grundsatz aber festgehalten und auf die Einführung einer solchen Meldepflicht verzichtet werden.

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

Zu § 109a – Absatz 8

Zur Abwehr erheblicher Gefahren für die Kommunikationstechnik einer Kritischen Infrastruktur erhält das BSI zukünftig weitgehende Anordnungsbefugnisse gegenüber dem Diensteanbieter. Anbieter haben selbst ein hohes Interesse an einem möglichst störungsfreien Betrieb ihrer Anlagen, um Leistungen gegenüber ihren Kunden vertragsgerecht erbringen zu können. Zudem verfügen die Anbieter über technische und organisatorische Fachkenntnisse zu ihren Anlagen, Diensten und Betriebsabläufen, die sie in die Lage versetzen, unverzügliche und angemessene Maßnahmen zur Störungsbeseitigung vornehmen zu können und die Störungsauswirkungen für Kunden möglichst gering zu halten. Diese Fachkenntnisse liegen dem Bundesamt heute nicht vor und können aus Gründen der Machbarkeit und des Aufwandes nicht erhoben werden. Vor diesem Hintergrund erscheint diese Eingriffsmöglichkeit weder hinsichtlich der Abwehr erheblicher Gefahren noch hinsichtlich des Interesses der Anbieter und der Kunden bzgl. einer möglichst störungsfreien Nutzung von Diensten als sachgerecht. Auf die Aufnahme eines solchen Anordnungsrechts sollte daher verzichtet werden.

Zu § 109b – Pflicht der Provider zur Meldung und Löschung

Löschpflicht nach § 109b lehnt die deutsche Industrie und hier insbesondere die Telekommunikationsdienstleister aufgrund der Gefahr des tiefen Eingriffs in das Fernmeldegeheimnis der betroffenen Nutzer sowie aufgrund des Risikos des Anbieters, gegen seine vertraglichen Pflichten zu verstoßen,

entschieden ab. Sofern nämlich die Feststellung der Unrechtmäßigkeit der in § 109b Abs. 2 TKG genannten Nutzungen nicht zutreffend ist, muss der Verpflichtete mit strafrechtlicher Sanktionierung seines Handelns, mit rechtlichen Ansprüchen des Betroffenen sowie mit dem Verlust der Kundenbeziehung rechnen. Die Verpflichtung zur Meldung und Löschung erscheint daher rechtlich nicht haltbar und ist aus Gründen der Unzumutbarkeit für Verpflichtete und Betroffene zu streichen.

Zudem gilt es zu klären, ob die Meldepflicht beim BKA ausschließlich für Provider oder auch z.B. für Mobilitätsdienstleister (im Sinne eines Dienstanbieters) gilt.

Zu § 149 Absatz 1

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

Zu Artikel 3 – Änderung des Telemediengesetzes

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

Zu § 13 Absatz 7a

Die Ausführungen zu § 109a Abs. 8 TKG gelten entsprechend. Auf die Aufnahme eines solchen Anordnungsrecht sollte daher verzichtet werden. Insbesondere gilt es detailliert zu klären, wie die Haftung des BSI im Falle von geschäftsschädigenden Auswirkungen dieser Anordnungen geregelt ist. Mit Blick auf Unternehmen, die Anlagen im besonderen öffentlichen Interesse betreiben, gilt es zudem zu klären, ob das BSI dieses Anordnungsrecht nur in Bezug auf Anlagen im besonderen öffentlichen Interesse oder für das gesamte Unternehmen hat.

Zu § 15 Absatz 2

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

Zu § 15b

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

Zu § 16 Absatz 2 Nummer 6 bis 9

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

Zu Artikel 4 – Änderung des Strafgesetzbuches

Eine Fortentwicklung des Strafgesetzbuchs (StGB) zur Anpassung des Strafrechts an Fallkonstellationen des digitalen Zeitalters ist aus Sicht der deutschen Industrie grundsätzlich zu begrüßen, um Recht auch im Cyberraum durchsetzen zu können. Bei der Fortentwicklung strafrechtlicher Normen sind insbesondere rechtliche Grauzonen für Unternehmen zu vermeiden, die beispielsweise aus uneindeutigen Anwendungsbereichen strafrechtlicher Regelungen resultieren können.

Die im IT-SiG 2.0-E vorgeschlagenen Änderungen des StGB ergeben in diesem Zusammenhang Anlass zur Kritik, sodass an den nachfolgend aufgeführten Stellen Änderungsbedarf besteht. Da die Fortentwicklung des Strafrechts zudem nicht auf alle Tätergruppen gleichermaßen abschreckend wirkt, müssen parallel dazu Strafverfolgungs- und Sicherheitsbehörden mit den notwendigen Ressourcen ausgestattet werden, um Computerstraftaten effektiv verfolgen und die IT-Sicherheit in Deutschland nachhaltig stärken zu können. Von zentraler Bedeutung sind zudem verstärkte Bemühungen zur Prävention von Cyberangriffen.

Zu § 126a

Art. 4 Ziff. 2 IT-SiG 2.0 n.F. sieht die Schaffung des neuen Straftatbestands „Zugänglichmachen von Leistungen zur Begehung von Straftaten“ vor, der als § 126a ins StGB aufgenommen werden soll. Gem. § 126a Abs. 1 StGB-E stellt die neue Norm die Zugänglichmachung einer „internetbasierten Leistung“, die „darauf ausgerichtet ist, die Begehung von rechtswidrigen Taten zu ermöglichen, zu fördern oder zu erleichtern“, unter Strafe. Wie die Gesetzesbegründung (vgl. S. 81 IT-SiG 2.0-E) näher ausführt, zielt der neue Straftatbestand insbesondere auf Online-Plattformen, die Schadsoftware, Denial of Servie-Angriffe o.ä. anbieten.

Bei der Bereitstellung legaler Handelsplattformen oder legaler Softwareangebote (z.B. VPN-Lösungen) nicht in jedem Fall durch den Anbieter ausgeschlossen werden kann, dass diese bei missbräuchlicher oder nicht-intendierter Nutzung auch zur Begehung von Straftaten eingesetzt werden. Die Einführung des § 126a StGB-E soll im Wesentlichen Betreiber von Online-Plattformen erfassen. Die Einführung der eigenständigen strafrechtlichen Verantwortlichkeit dieser Betreiber in Fällen, in denen die Plattformen nicht nur untergeordnet zur Begehung von Straftaten genutzt werden, wird mit praktischen Problemen der Beweisbarkeit einer strafrechtlichen Beihilfe von Betreibern zu einzelnen Taten und einer aufgrund der durch Online-Plattformen angebotenen logistischen Strukturen erhöhten Gefahr der Begehung von Straftaten begründet (Begründung des Referentenentwurfs S. 79).

Praktische Beweisprobleme belegen, dass grundsätzlich Straftatbestände für das verfolgte Verhalten existieren. Warum ein neuer eigenständiger

Straftatbestand anstelle von Maßnahmen, wie Personalaufstockung oder Anpassung von Ermittlungsbefugnissen zur Behebung dieser Beweisprobleme notwendig ist, wird nicht deutlich.

Der neue Straftatbestand erfasst zudem nicht nur die zielgerichtete Bereitstellung von Infrastrukturen zur Erleichterung der Begehung von Straftaten. Wie aus der Begründung zum Referentenentwurf (S. 79 f.) deutlich wird, ist sich das BMI des über diese Fälle hinausgehenden Anwendungsbereich des Straftatbestandes bewusst, da sogar eingeräumt wird, dass zulässige Verhaltensweisen erfasst werden.

Warum der Wortlaut des § 126a Abs. 1 StGB-E dennoch derart weitreichend ist, erschließt sich nicht, zumal es in der Begründung des Referentenentwurfs zu § 126a StGB-E (S. 78) heißt: „*Der Entwurf zielt darauf, das Betreiben von auf die Förderung, Ermöglichung oder Erleichterung illegaler Zwecke ausgerichteten Plattformen unabhängig von dem Nachweis der Beteiligung an einzelnen konkreten Handelsgeschäften unter Strafe zu stellen.*“

Aus Sicht der Wirtschaft ist eine hinreichend bestimmte Abgrenzung zwischen dem intendierten sachlichen Anwendungsbereich des Straftatbestandes und der legalen Bereitstellung entsprechender Angebote von zentraler Bedeutung.

Ob die Beschränkung der Strafbarkeit auf das Zugänglichmachen zu internetbasierte Leistungen mit bestimmtem Zwecken oder Tätigkeiten der Leistung eine in der Praxis handhabbare Beschränkung darstellt, ist zweifelhaft. Der Zweck ist ein subjektives Merkmal, der durch den Anbieter der internetbasierten Leistung bestimmt wird, nicht demjenigen der diese Leistung Dritten zugänglich macht. Dem möglichen Täter nach § 126a StGB-E wird der konkrete Zweck der „internetbasierten Leistung“ im Zeitpunkt des Zugänglichmachen daher i. d. R. nicht bekannt sein, denn Täter i. S. d. § 126a Abs. 1 StGB-E und Anbieter der Leistung müssen gerade nicht personenidentisch sein. Der Täter des § 126a Abs. 1 StGB-E hätte lediglich Einfluss auf den Zweck des Zugänglichmachens.

Unklar ist zudem, was die „Tätigkeit“ einer internetbasierten Leistung sein soll. Sofern auf die tatsächliche Nutzung der Leistung (zur Begehung von Straftaten) abgestellt wird, sollte der Wortlaut dies zum Ausdruck bringen und „Nutzung“ statt „Tätigkeit“ verwenden. Dennoch hätte der Betreiber der Plattform keinen Einfluss auf die tatsächliche Nutzung von Leistungen, die auf der Plattform von Dritten angeboten werden. Dem Plattformbetreiber wird die tatsächliche Nutzung der Leistungen noch weniger bekannt sein als der Zweck der Leistung.

Aus denselben Gründen wird daher auch die Praxistauglichkeit der Ausnahme nach § 126a Abs. 4 Nr. 1 StGB-E für lediglich untergeordnete Zwecke oder Tätigkeiten der internetbasierten Leistung zur Begehung von Straftaten bezweifelt. Wenn dem Täter (Zugänglichmachenden) der Zweck der

Leistung nicht bekannt ist, ist ihm auch nicht bekannt ob die Leistung mehreren Zwecken dienen soll und wie das Verhältnis zwischen diesen Zwecken ist. Unklar ist zudem wie ein Plattformbetreiber Kenntnis über die tatsächliche Tätigkeit bzw. Nutzung der auf der Plattform angebotenen Leistungen und dem Verhältnis der Nutzungen zueinander (Über- und Unterordnung) haben soll, wenn er diese Leistungen nicht anbietet und an konkreten Sachverhalten der Nutzung (z. B. konkreten Handelsgeschäften) nicht beteiligt ist.

In der vorliegenden Ausgestaltung würde § 126a StGB-E trotz der Beschränkung von „Zweck oder Tätigkeit" der internetbasierten Leistung, u. a. nach Abs. 4 Nr. 1, zu Rechtsunsicherheiten auf Seiten der Wirtschaft führen, da in der Norm keine ausreichende Differenzierung zwischen „legalem" Zugänglichmachen und dem von § 126a Abs. 1 erfasstem Zugänglichen vorgenommen wird. Die Differenzierung anhand von Zweck und Tätigkeit der zugänglichgemachten Leistung ist jedenfalls nicht ausreichend, da diese grundsätzlich vom Zugänglichmachenden nicht überblickt oder beeinflusst werden können. Nur der Anbieter der Leistung hat hierauf auf deren Zweck Einfluss und kann deren tatsächliche Nutzung beurteilen.

Zu § 202e

Ebenfalls neu eingeführt wird mit Art. 4 Ziff. 4 IT-SiG 2.0-E der Straftatbestand der „Unbefugten Nutzung informationstechnischer Systeme" (neuer § 202e StGB). Begründet wird die Einführung insbesondere mit der „mangelnden Effektivität der geltenden Normen." (vgl. S. 85 IT-SiG 2.0-E). Die Norm des § 202e Abs. 1 StGB-E stellt den unbefugten „Zugang" zu bzw. „Gebrauch" eines informationstechnischen Systems sowie das unbefugte „Beeinflussen" und „Ingangsetzen" informationstechnischer Prozesse unter Strafe, soweit hierdurch eine Eignung der Beeinträchtigung berechtigter Interessen eines anderen besteht. Laut Gesetzesbegründung (vgl. ebd., S. 84) können auch Apps in den Anwendungsbereich der Norm fallen, wenn „bei deren Installation die Nutzer mithin bewusst über die eingeräumten Zugriffsrechte getäuscht werden."

Der Anwendungsbereich von § 202e StGB-E ist sehr weit gefasst und umfasst z.B. die bloße Einräumung von Zugriffsmöglichkeiten Dritter, die nicht durch vom Nutzer eingeräumten Zugriffsrechte erfasst ist, ohne dass tatsächlich Gebrauch von der Möglichkeit gemacht wurde. Der sachliche Anwendungsbereich von § 202e Abs. 1 StGB-E ist insbesondere in Hinblick auf die Tatbegehung nach § 202e Abs. 1 Nr. 1 i. V. m. Abs. 3 Nr. 1 Var. 1 StGB-E unverhältnismäßig weit. Allein das unbefugte Verschaffen eines Zugangs zu einem informationstechnischen System, das lediglich zur Verarbeitung personenbezogener Daten geeignet ist, stellt eine tatbestandlich erfasstes Verhalten dar.

Eine „Verarbeitung" personenbezogener Daten ist nach Art. 4 Nr. 2 i. V. m. Nr. 1 DS-GVO jeder mit oder ohne Hilfe automatisierter Verfahren

ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

Für eine Strafbarkeit nach § 202e Abs. 1 Nr. 1 StGB-E müsste das informationstechnische System zudem lediglich zur einer solchen Verarbeitung geeignet sein. Die Nutzung des Systems müsste die Verarbeitung personenbezogener Daten also lediglich fördern.

Wenn personenbezogener Daten verarbeitet werden, besteht für einen unbefugt verschafften Zugang – auch ohne tatsächliche Nutzung – stets die Eignung der Beeinträchtigung von berechtigten Interessen der datenschutzrechtlich geschützten Personen, da bereits die Möglichkeit des Zugangs von Nicht-Berechtigten zu personenbezogenen Daten eine Beeinträchtigung der datenschutzrechtlich geschützten Personen fördert.

Die Strafbarkeitsbeschränkung des § 202e Abs. 1 Satz 2 StGB-E, für Fälle in den durch die Tathandlungen keine Eignung zur Beeinträchtigung berechtigter Interessen Dritter besitzt, beschränkt den weiten sachlichen Anwendungsbereich entgegen der Begründung des Referentenentwurfs (S. 85) in den meisten Fällen nicht. Soweit informationstechnische System nach § 202e Abs. 3 Nr. 1 StGB-E betroffen sind, läuft die Beschränkung faktisch leer. Wann immer informationstechnische Systeme zur Verarbeitung personenbezogener Daten geeignet sind, ist eine tatbestandliche Handlung nach § 202 Abs. 1 Satz 1 Nr. 1-3 StGB-E auch grundsätzlich geeignet die datenschutzrechtlichen Interessen von Personen (berechtigte Interessen Dritter) zu beeinträchtigen.

Die Anforderungen an tatbestandlich geschützte informationstechnische Systeme nach § 202e Abs. 3 Nr. 2 StGB-E sind derart unbestimmt und weitgehend, dass unklar ist, welche informationstechnischen Systeme nicht geschützt sind. Es ist unklar worin die Beschränkungswirkung des § 202e Abs. 3 StGB-E liegt, die Begründung des Referentenentwurfs (vgl. S. 85) ist diesbezüglich ebenfalls unergiebig.

Die Einführung des § 202e StGB-E wird mit von unzureichenden Verurteilungszahlen abgeleiteter Ineffektivität der Straftatbestände der §§ 202a, 303a und 303b StGB belegt sowie der Erforderlichkeit des staatlichen Schutzes des aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleiteten Rechts auf Integrität und Vertraulichkeit informationstechnischer Systeme. Aufgrund geringer Verurteilungszahlen wegen der Straftaten nach §§ 202a, 303a und 303b StGB wird behauptet, dass diese Straftatbestände ineffektiv wären. Die geringen Verurteilungszahlen können jedoch genauso als Argument für die Effektivität dieser Straftatbestände herangeführt werden – „Die

Abschreckung der Straftatbestände führt zu weniger Tatbegehung und deshalb zu weniger Verurteilungen.“ Geringe Verurteilungszahlen belegen für sich genommen weder Effektivität noch Ineffektivität.

Warum der durch das Datenschutzrecht, insbesondere die DS-GVO, gewährleistete Schutz für personenbezogene Daten nicht den Schutzanforderungen des aus Art. 2 Abs. 1 i. V. m. 1 Abs. 1 GG abgeleiteten Allgemeinen Persönlichkeitsrecht sowie dem Grundrecht auf Integrität und Vertraulichkeit informationstechnischer Systeme nicht genügen soll, ist nicht ersichtlich. Insbesondere kommt den Sanktionsandrohungen der DS-GVO auch ausreichende Abschreckungswirkung zu.

Die zusätzliche Einbeziehung entsprechender Datenverarbeitungsvorgänge in den Anwendungsbereich strafrechtlicher Normen, über die bestehenden Straftatbestände hinaus, erscheint unverhältnismäßig und wird daher abgelehnt.

Die Einführung von § 202e StGB in seiner jetzigen Form wird von der deutschen Industrie abgelehnt.

Zu § 202f

§ 202f StGB-E (Besonders schwerer Fall einer Straftat gegen die Vertraulichkeit oder Integrität informationstechnischer Systeme) legt im Kern differenzierte Strafmaße für verschiedene Deliktarten fest. Laut der Gesetzgebegründung (vgl. S. 86 IT-SiG 2.0-E) sollen damit ebenfalls Regelungslücken im Strafrecht geschlossen werden, da „insbesondere das kollusive Zusammenwirken in Banden“ bei der Begehung von Computerstraftaten bis dato nicht angemessen im Strafrecht abgebildet werden könne.

Die Schließung bestehender Gesetzeslücken zur angemessenen Bestrafung schwerer Computerstraftaten ist grundsätzlich zu begrüßen. Insbesondere die generalpräventive Wirkung, die von einem ausdifferenzierten Strafrahmen ausgeht, dürfte dazu führen, dass bestimmte Tätergruppen stärker als bisher von der Begehung von Computerstraftaten abgeschreckt werden.

Artikel 5 – Änderung der Strafprozessordnung

Zu § 100a

Durch die Erweiterung des § 100a Abs. 2 StPO wird die Möglichkeit der Telekommunikationsüberwachung unangemessen stark auch auf Fälle ausgedehnt, die de facto dem Bereich der Alltagskriminalität zuzuordnen sind. Da es sich bei der Telekommunikationsüberwachung um einen schwerwiegenden Grundrechtseingriff handelt, sollte diese Möglichkeit der Überwachung auf den neu geschaffenen Qualifikationstatbestand des § 202f StGB begrenzt bleiben. Die mit der Telekommunikationsüberwachung verbundene hohe Intensität von Grundrechtseingriffen gebietet, dass diese Möglichkeit auf den Verdacht von hinreichend bestimmten und schwerwiegenden Straftaten beschränkt bleibt. Eine Erstreckung von Maßnahmen nach § 100a StPO auf Verdachtsfälle der § 126a und § 202e StGB-E würde daher, unter Berücksichtigung der geäußerten Kritik an diesen Normen, den Anforderungen an den Grundrechtseingriff nicht genügen.

Zu § 163g

Der Entwurf zu § 163g sieht vor, dass Staatsanwaltschaft und Polizeidienste zukünftig – auch gegen den Willen des Inhabers – auf Nutzerkonten oder Funktionen, die ein Anbieter eines Telekommunikations- oder Telemediendienstes einem Verdächtigen zur Verfügung stellt und mittels derer der Verdächtige eine dauerhafte virtuelle Identität unterhält, zugreifen.

Diese Vorschrift schafft den Grundsatz der Selbstbelastungsfreiheit ab. Insbesondere die Regelung, wonach gewonnene Erkenntnisse gegen den Verdächtigen nur mit seiner Zustimmung verwendet werden dürfen, täuscht den Unkundigen darüber hinweg, dass ein Verstoß selbst gegen diese Vorschrift wirkungslos bleibt, weil es ein generelles Verbot rechtswidrig erlangter Erkenntnisse nicht gibt. Darüber hinaus können die Erkenntnisse auch immer dazu verwendet werden, Parallelermittlungen gezielt anzustellen und so die unverwertbaren Ergebnisse in anderer Weise zu legitimieren.

Die deutsche Industrie spricht sich für die Streichung eines so weitreichenden Eingriffs in die Rechte von Tatverdächtigen, die durch die Unschuldsvermutung geschützt sind, aus.

Artikel 6 – Änderung des Gesetzes über die internationale Rechtshilfe in Strafsachen

Mit Blick auf die vorgeschlagene Änderung des Gesetzes über die internationale Rechtshilfe in Strafsachen sieht die deutsche Industrie – und hier insbesondere die Telekommunikationsprovider – die niedrige Anordnungsschwelle u.a. zum Zweck der Datensicherung kritisch.

Zu § 67 Absatz 5

§ 67 Abs. 5 des Entwurfs sieht eine Anordnungsbefugnis durch Staatsanwaltschaft und Polizei vor, statt wie bei Verkehrsdatenauskünften üblich durch den Richter. Diese niedrige Anordnungsschwelle wird u.a. damit begründet, dass eine Sicherung von Daten lediglich eine geringe Grundrechtsrelevanz aufweise. Dieser Einschätzung ist deutlich zu widersprechen.
Bereits durch das mit der Sicherung verbundene staatliche Veränderungsverbot stellt einen Eingriff in das Allgemeine Persönlichkeitsrecht und das Recht auf Integrität und Vertraulichkeit informationstechnischer Systeme dar. Aufgrund des Veränderungsverbots können die personenbezogenen Daten durch die betroffene Person beispielsweise nicht mehr gelöscht werden.

Um Daten sichern zu können, müssen diese zunächst durch eine Person identifiziert werden, was eine Verarbeitung personenbezogener Daten außerhalb der Einwilligung der betroffenen Person darstellt und damit ein Grundrechtseingriff.

Eine Datensicherung ist für den TK-Provider in keiner Weise betrieblich erforderlich und erfolgt einzig zum Zweck einer möglichen späteren Beauskunftung. Die Intensität dieses Eingriffs bemisst sich unabhängig davon, ob es noch zu einer Übermittlung der Daten an die Behörde kommt oder nicht. Denn für das Vertrauen des Grundrechtsträgers spielt es keine wesentliche Rolle, ob er die Preisgabe seiner Daten lediglich befürchten muss, oder diese eingetreten ist. Der Grundrechtsträger ist jedenfalls in seiner Verfügungsgewalt über seine Daten, u. a. der Löschung, beschränkt. Dies gilt erst recht, wenn man die Maximaldauer einer Sicherungsmaßnahme von 180 Tagen betrachtet, die wiederum um maximal 180 Tage verlängert werden können soll. Die maximale Sicherungsdauer von einem Jahr entspricht der doppelten Speicher-dauer der „Vorratsdatenspeicherung 2008“ und etwa dem Fünf- bzw. Dreizehnfachen der „Vorratsdatenspeicherung 2015“.

Die Befugnis Maßnahmen nach § 67 Abs. 5 IRG-E anzuordnen muss aufgrund der Grundrechtsintensität einem Richter vorbehalten sein. Eine besondere Eilbedürftigkeit der Sicherungsanordnung aufgrund Gefahr der Löschung oder Veränderung von Daten vermag entgegen der Begründung des Referentenentwurfs (vgl. S. 89) nicht die Zuständigkeit von Ermittlungsbehörden zu begründen. Die Einholung der richterlichen Genehmigung ist mit

heutigen technischen Möglichkeiten sowie aufgrund bestehender nächtlicher richterlicher Bereitschaftsdienste innerhalb kürzester Zeit möglich.

Der zeitliche Aufwand eines Anrufs rechtfertigt es jedenfalls nicht, vor Eingriff in die Grundrechte des Allgemeinen Persönlichkeitsrechts und Rechts auf Integrität und Vertraulichkeit von informationstechnischen System die Beurteilung der Zulässigkeit eines solchen Eingriffs einem Ermittlungsbeamten zu überlassen. Wenn der Ermittlungsbeamte über den Grundrechtseingriff entscheidet, der ihm gleichzeitig seine Ermittlungen überhaupt erst ermöglicht, entspricht dies nicht dem rechtstaatlichen Prinzip der Gewaltenteilung.

Zu Artikel 8 – Änderung des Artikel-10-Gesetzes

Mit der vorgeschlagenen Änderung des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz - G 10) wird der in § 3 G 10 normierte Katalog an Voraussetzungen erweitert, unter denen die Nachrichtendienste von Bund und Ländern berechtigt sind, Kommunikation zu überwachen und aufzuzeichnen. Die Erweiterung umfasst den mit Art. 4 Ziff. 4 IT-SiG 2.0-E neu eingeführten § 202f StGB (Besonders schwerer Fall einer Straftat gegen die Vertraulichkeit oder Integrität informationstechnischer Systeme).

Deutsche Sicherheitsbehörden müssen über die notwendigen Kompetenzen und Ressourcen verfügen, um die IT-Sicherheit in Deutschland zu stärken. Die Handlungsfähigkeit staatlicher Institutionen im Cyberraum dient nicht zuletzt auch dazu, berechtigte Interessen deutscher Unternehmen und Bürger zu schützen.

Grundrechtseingriffe, so wie sie mit der vorgeschlagenen Ergänzung des § 3 G 10 verbunden sind, bedürfen dabei einer besonders sorgfältigen Rechtsgüterabwägung und Begründung. Zudem bedarf es eindeutiger Definitionen der Eingriffsbefugnisse von Sicherheitsbehörden. Aus der Begründung im IT-SiG 2.0-E geht nicht hervor, warum die vorgeschlagene Erweiterung des § 3 G 10 im konkreten Fall erforderlich ist. Unklar ist zudem, wie im Falle einer Anwendung der neuen Eingriffsbefugnisse Geschäftsgeheimnisse von Unternehmen geschützt werden, die einer Cyberstraftat zum Opfer gefallen sind. Die deutsche Industrie sieht daher an dieser Stelle noch erheblichen Klärungsbedarf.

Zu Artikel 10 – Änderung der Außenwirtschaftsverordnung

Als Bestandteil der holistischen Gesamtstrategie zur Stärkung der Cyberresilienz Deutschlands plant die Bundesregierung im Rahmen des Zweiten IT-Sicherheitsgesetzes auch eine Anpassung der Außenwirtschaftsverordnung. Mit Blick auf die Wahrung der digitalen Souveränität Deutschlands sollen zukünftig alle Hersteller von KRITIS-Kernkomponenten nach § 2 Abs. 13 des BSI-Gesetzes unter die Investitionskontrollen des BMWi fallen.

Zu § 55 Absatz 1 Satz 2 Nummer 2 und § 55 Absatz 1 Satz 3

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

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

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

Offene Grenzen und Auslandsinvestitionen sind von großer Wichtigkeit für die international ausgerichtete deutsche Industrie. In Deutschland arbeiten mehr als 3 Millionen Menschen für Unternehmen, die ganz oder teilweise in der Hand ausländischer Investoren sind. Der BDI steht verschärften Investitionskontrollen seit Jahren kritisch gegenüber. Investitionsprüfungen und Investitionsverbote belasten Unternehmen mit Bürokratie, schrecken Investoren ab und beschleunigen die Spirale des weltweit zunehmenden Investitionsprotektionismus. Auch vor dem Hintergrund von zwei Verschärfungen

der Investitionsprüfungen in den letzten beiden Jahren (AWV-Novellen 2017 und 2018) ist eine weitere Verschärfung im Zuge des 2. IT-Sicherheitsgesetzes abzulehnen.

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 36 Branchenverbände und mehr als 100.000 Unternehmen mit rund 8 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
T: 030-2028-1523
s.heckler@bdi.eu

Oliver Klein
Referent
T: 030/2028-1502
o.klein@bdi.eu

BDI Dokumentennummer: D 1056