Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
18(4)284 E

BDI

Bundesverband der Deutschen Industrie · 11053 Berlin

Digitalisierung und industrielle Wertschöpfungsstrukturen

An den
Vorsitzenden des Innenausschusses des
Deutschen Bundestages
Herrn Wolfgang Bosbach
Platz der Republik 1
11011 Berlin

Datum
16. April 2015

BDI-Stellungnahme zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) (BT-Drs. 18/4096)

Sehr geehrter Herr Bosbach,

mit Blick auf die öffentliche Anhörung im Innenausschuss möchte der Bundesverband der Deutschen Industrie (BDI) nochmals auf folgende für die deutsche Industrie wesentlichen Punkte hinweisen:

1. **Klare und transparente Definitionen, um Rechtssicherheit für die Unternehmen zu erreichen**
   Der BDI hält es für problematisch, dass zentrale Definitionen, wie z. B. die konkrete Definition „Kritischer Infrastrukturen“, nicht im Gesetz selber, sondern in einer gesonderten Rechtsverordnung geregelt werden. Auch der Umfang und der zeitliche Rahmen der Meldung sind im Entwurf nicht hinreichend bestimmt. Zudem sollte die Weitergabe von Daten gesetzlich ausgeschlossen werden, die über die allgemeine Darstellung des Sicherheitslagebildes hinausgehen und Rechte Dritter verletzten können.

2. **Win-win Situation für beide Seiten schaffen**
   Die Zusammenarbeit zwischen Unternehmen und Staat darf keine „Einbahnstraße“ sein. Informationen dürfen nicht nur, im Sinne einer Meldepflicht, von Unternehmen an die Behörden fließen und damit den Bürokratieaufwand der Unternehmen erhöhen. Vielmehr sollte das Bundesamt für Sicherheit in der Informationstechnik (BSI) künftig Informationen über Bedrohungen zeitnah, aktuell und praxisorientiert an die Unternehmen zurückgegeben. Nur so kann insgesamt ein erhöhtes Sicherheitsniveau erreicht werden.

Bundesverband der Deutschen Industrie e.V.
Mitgliedsverband
BUSINESSEUROPE

Hausanschrift
Breite Straße 29
10178 Berlin

Postanschrift
11053 Berlin

Telekontakte
T: +493020281461
F: +493020282461

Internet
www.bdi.eu

E-Mail
I.Ploeger@bdi.eu

3. **Doppelregulierung vermeiden**
   Doppelregulierung bzw. doppelte Zuständigkeiten müssen in jedem Fall vermieden werden. Betreiber Kritischer Infrastrukturen, die über bereits bestehende Rechtsvorschriften, z. B. das Telekommunikationsgesetz (TKG), das Energiewirtschaftsgesetz (EnWG) oder das Bundesdatenschutzgesetz (BDSG) reguliert werden, sollten nicht zusätzlich reguliert werden.

4. **Kompatibilität zwischen nationaler und europäischer Gesetzgebung herstellen**
   Der BDI tritt mit Nachdruck dafür ein, dass das IT-Sicherheitsgesetz mit der europäischen NIS-Richtlinie im Einklang steht. So können spätere Gesetzesanpassungen vermieden und Rechtssicherheit für die Unternehmen gewahrt werden. Die Bundesregierung sollte auf einen engen Anwendungsbereich der NIS-Richtlinie hinwirken. Auch sollte auf europäischer Ebene auf Sanktionen verzichtet werden. Um den Schutz von Unternehmensinteressen zu garantieren, sollte sich das Anhörungsrecht der Unternehmen bei einer potenziellen Meldeveröffentlichung stärken an dem Vorbild des IT-Sicherheitsgesetzes orientieren. Das Meldeverfahren sollte analog zum IT-Sicherheitsgesetz anonym erfolgreich.

5. **Kohärenz mit internationalen Standards erreichen**
   Weder der Aktionsradius von international agierenden Unternehmen noch die Cyber-Angriffe machen an den Landesgrenzen halt. Eine deutsche Insellösung wäre nicht zielführend. Der BDI setzt sich daher für eine Kohärenz mit international bereits existierenden Standards ein. Eine Harmonisierung der Meldewege und Verfahren sowie der Definition der nationalen Zuständigkeiten ist anzustreben, um Doppelaufwendungen und Wettbewerbsnachteile zu vermeiden.

Die vollständige BDI-Kommentierung des Gesetzentwurfs entnehmen Sie bitte der Stellungnahme, die der BDI am 5. November 2015 im Rahmen der Verbändeanhörung an das Bundesinnenministerium übermittelt hat. Die Stellungnahme, die in der Anlage beigefügt ist, wurde vom BDI gemeinsam mit seinen Mitgliedsverbänden erarbeitet und bildet die branchenübergreifende Positionierung der Deutschen Industrie.

Mit freundlichen Grüßen

Plöger

Iris Plöger

Anlage
BDI-Stellungnahme zum Entwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 5. November 2015

Stellungnahme

zum Entwurf des Gesetzes zur „Erhöhung der Sicherheit informationstechnischer Systeme“ (ITSiG)

Sicherheit und Rohstoffe

Der BDI vertritt als Spitzenverband der deutschen Industrie und der industrienahen Dienstleister in Deutschland 37 Branchenverbände. Er repräsentiert die politischen Anliegen und Interessen von mehr als 100.000 Unternehmen mit rund acht Millionen Beschäftigten.

1. Grundsätzlich

- Der BDI unterstützt nachdrücklich das Ziel der Bundesregierung, das Industrieland Deutschland widerstandsfähiger gegen die steigende Anzahl von Cyberbedrohungen zu machen.
- Der vorliegende Entwurf wurde dem BDI am 4. November 2014 zur Kommentierung übermittelt. Aufgrund der, durch das BMI gesetzten, sehr kurzfristigen Rückmeldefrist, ist eine umfassende und detaillierte Bewertung nur bedingt möglich. Der BDI behält es sich daher vor, weitere Kommentierungen im Rahmen des mündlichen Anhörungsverfahrens zu übermitteln.
- Der BDI hat am 5. April 2013 eine erste Stellungnahme zum geplanten IT-Sicherheitsgesetz[1] an die Bundesregierung übermittelt und den Gesetzgebungsprozess seitdem eng und konstruktiv begleitet. Im Februar 2014 hat der BDI ein Positionspapier zur Ausgestaltung des IT-Sicherheitsgesetzes[2] veröffentlicht.
- Darüber hinaus hat der BDI gemeinsam mit BDLI, BDSV, BITKOM und ZVEI die Studie „IT-Sicherheit in Deutschland. Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes“[3] bei der Wirtschaftsprüfungsgesellschaft KPMG in Auftrag gegeben. Ziel der Studie war es, konkrete Handlungsempfehlungen für die Ausgestaltung eines IT-Sicherheitsgesetzes zu präsentieren, bevor die Bundesregierung einen neuen Entwurf vorlegt. Die Studie wurde am 3. Juli 2014 an Bundesinnenminister Thomas de Maizière übermittelt.
- Der BDI hält es für problematisch, dass zentrale Definitionen, wie z. B. die konkrete Definition Kritischer Infrastrukturen, nicht im Gesetz sel-

[1] BDI-Stellungnahme zum Referentenentwurf eines „Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme“, 5. April 2013, http://www.bdi.eu/images_content/SicherheitUndVerteidigung/BDI_Stellungnahme_IT-Sicherheitsgesetz_final.pdf

[2] BDI-Positionspapier „Erwartungen der deutschen Industrie an ein IT-Sicherheitsgesetz“, Feb. 2014, http://www.bdi.eu/download_content/SicherheitUndVerteidigung/Positionspapier_Sicherheitsgesetz_25_02.pdf

[3] KPMG-Studie „IT-Sicherheit in Deutschland. Handlungsempfehlungen für eine zielorientierte Umsetzung des IT-Sicherheitsgesetzes“, Juli 2014, http://www.bdi.eu/images_content/SicherheitUndVerteidigung/KPMG_IT-Sicherheit_in_Deutschland.pdf

Bundesverband der Deutschen Industrie e.V.
Mitgliedsverband
BUSINESSEUROPE

Telekontakte
T: +493020281402
F: +493020282402
Internet
www.bdi.eu
E-Mail
D.Klein@bdi.eu

ber, sondern in einer gesonderten Rechtsverordnung geregelt werden. Um Rechtsklarheit für die betroffenen Unternehmen zu schaffen, sollte diese Rechtsverordnung zeitnah zum ITSiG verabschiedet werden. Gleichwohl begrüßt der BDI ausdrücklich die frühzeitige Einbindung der Industrie im Rahmen des Gesetzgebungsvorhabens. Das Angebot an die Verbände, bei der Erarbeitung der branchenspezifischen Mindeststandards und der Festlegung der Kriterien für die detaillierte Definition im Zuge einer nachgelagerten Verordnung umfangreich mitzuarbeiten, nimmt der BDI wahr. Die Beteiligung der Branchenvertreter zur Bestimmung der Kritischen Infrastrukturen sollte frühzeitig im Vorfeld der gesetzlichen Regelung stattfinden.

- Die deutsche Industrie tritt mit Nachdruck für eine höchstmögliche Kompatibilität zwischen dem deutschen IT-Sicherheitsgesetz und der europäischen NIS-Richtlinie ein. Das gilt insbesondere für die weitgehende Anonymisierung der Meldungen, wie sie im ITSiG vorgesehen ist. Der BDI plädiert dafür, dass eine solche Regelung auch in der NIS-Richtlinie berücksichtigt wird. Zumindest sollte den Mitgliedstaaten bei der Umsetzung der Richtlinie der Spielraum eingeräumt werden, dies eigenverantwortlich zu regeln.
- Doppelregulierung bzw. doppelte Zuständigkeiten müssen in jedem Fall vermieden werden. Betreiber Kritischer Infrastrukturen, die über bereits bestehende Rechtsvorschriften, z. B. das Telekommunikationsgesetz (TKG), das Energiewirtschaftsgesetz (EnWG) oder das Bundesdatenschutzgesetz (BDSG) reguliert werden, sollten nicht zusätzlich reguliert werden.
- Die Zusammenarbeit zwischen Unternehmen und Staat darf keine „Einbahnstraße“ sein. Informationen dürfen nicht nur, im Sinne einer Meldepflicht, von Unternehmen an die Behörden fließen. Vielmehr müssen Informationen über Bedrohungen zeitnah, aktuell und praxisorientiert von den staatlichen Stellen an die Unternehmen gegeben werden. Nur so kann insgesamt ein erhöhtes Sicherheitsniveau erreicht werden.
- Ein gutes Beispiel für eine enge und vertrauensvolle Zusammenarbeit zwischen Industrie und Behörden ist die Allianz für Cyber-Sicherheit. Diese leistet einen wichtigen Beitrag zur Prävention und Awareness. Sie gilt es weiter zu stärken. Die bereits vorhandene Möglichkeit zur freiwilligen Meldung eines Sicherheitsvorfalls an die Meldestelle der Allianz ist bei der Ausgestaltung des ITSiG zu berücksichtigen und mit den vorgesehenen Maßnahmen zu verzahnen.
- Weder der Aktionsradius von international agierenden Unternehmen noch die Cyber-Angriffe machen an den Landesgrenzen halt. Daher wäre eine deutsche Insellösung nicht zielführend. Der BDI setzt sich daher für eine Kohärenz mit international bereits existierenden Standards ein. Eine Harmonisierung der Meldewege und Verfahren sowie der Definition der nationalen Zuständigkeiten ist anzustreben, um Doppelaufwendungen und Wettbewerbsnachteile zu vermeiden. Weiterhin werden in zunehmenden Maße Dritte zur Bereitstellung von Diensten, als sogenannter „Sofware as a Service“ oder „Hardware as a Service“ genutzt, die ihre Dienste in der Regel über Staatsgrenzen erbringen. Doppelte Auditierungen müssen vermieden.

2. Im Einzelnen

- **Erfüllungsaufwand für die Wirtschaft**
  Anders als im vorliegenden Gesetzesentwurf angenommen, entstehen der Wirtschaft durchaus Mehraufwände durch die Anforderungen aus dem Gesetz. Auf Basis des damals vorliegenden Entwurfs hat KPMG die Kosten für die Umsetzung einer Meldepflicht untersucht. Die Berechnungen von KPMG zeigen, dass die Umsetzung der Meldepflicht zu signifikanten Erhöhungen der Personal- und Sachkosten für die betroffenen Unternehmen führt. Finanzielle Belastungen könnten sich zudem auch aus dem Risiko möglicher Reputationsschäden ergeben, die aus einem fehlerhaften Umgang mit den Meldedaten entstehen können. In Anlehnung an die Methode des Standardkostenmodells wurden zudem die Bürokratiekosten von KPMG abgeschätzt, die sich unmittelbar aus einer Meldepflicht für die Unternehmen ergeben. Diese spezifischen Kosten summieren sich auf Grundlage der für diese Studie getroffenen Annahmen auf insgesamt rund 1,1 Milliarde Euro pro Jahr.

- **Kritische Infrastrukturen, Artikel 1 § 2**
  In Artikel 1, Absatz 3 des Gesetzentwurfs wird versucht, eine Begriffsbestimmung der Kritischen Infrastrukturen vorzunehmen. Hier heißt es:

  > „(10) *Kritische Infrastrukturen im Sinne dieses Gesetzes sind Einrichtungen, Anlagen oder Teile davon, die*
  > *1. den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und*
  > *2. von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden.*
  > *Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 näher bestimmt. Kommunikationstechnik im Sinne des Absatzes 3 gehört nicht zu den Kritischen Infrastrukturen im Sinne dieses Gesetzes.“*

  In § 10 wird festgelegt, ab welchem Schwellenwert, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen gelten und wie diese bestimmt werden sollen:

  > *„Das Bundesministerium des Innern bestimmt nach Anhörung von Vertretern der Wissenschaft, betroffener Betreiber und der betroffenen Wirtschaftsverbände im Einvernehmen mit dem Bundesministerium für Wirtschaft und Energie (…) anhand der in den jeweiligen Sektoren erbrachten Dienstleistungen durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, ab welchem Schwellenwert welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne dieses Gesetzes gelten. Zugang zu Akten, die die Erstellung oder Änderung dieser Verordnung betreffen, wird nicht gewährt.“*

BDI-Kommentierung
Der Anwendungsbereich des Gesetzentwurfs ist nicht ausreichend konkret bestimmt. Deshalb erscheint es geboten in Artikel 1 bzw. der Begründung, konkrete Kriterien zu benennen, nach denen die Teilsegmente der aufgezählten Sektoren als kritisch eingestuft werden. Die Anforderungen an die Betreiber kritischer Infrastrukturen müssen einheitlich sein. Dies ist gegenwärtig durch die vorgesehenen Änderungen im EnWG und des TKG nicht der Fall.

Darüber hinaus hält der BDI es für äußerst problematisch, dass die wichtige Frage des Anwendungsbereichs auf eine spätere Rechtsverordnung delegiert wird. Das schadet der Rechtssicherheit und trifft auch auf wettbewerbsrechtliche Bedenken. Denn der Verordnungsermächtigung im Gesetzentwurf fehlt es an ausreichender Bestimmtheit, Normklarheit bei der Adressatenbestimmung und an der notwendigen Begrenzung der Ermächtigung. Es besteht außerdem ein erhebliches Risiko für die Investitionssicherheit und nimmt den Unternehmen das nötige Maß an Erwartungssicherheit.

Der Staat ist der größte Betreiber Kritischer Infrastrukturen. Gemäß dem vorliegenden Entwurf soll der Staat jedoch nicht unter das Gesetz fallen, obwohl die staatlichen Kritischen Infrastrukturbetreiber ebenso eine „hohe Bedeutung für das Funktionieren des Gemeinwesens“ haben. Der BDI setzt sich daher nachdrücklich dafür ein, dass die entsprechenden Meldepflichten und Sicherheitsstandards neben dem Bund auch für Länder und Kommunen gelten und vom Gesetz erfasst werden.

Gleichwohl begrüßt der BDI ausdrücklich, dass die Bestimmung der für die Anwendung der gesetzlichen Regelung relevanten kritischen Infrastrukturen sektor- und branchenspezifisch nach qualitativen und quantitativen Kriterien in enger Abstimmung mit den betroffenen Betreibern und Wirtschaftsverbänden erfolgen soll. Richtigerweise wird hierbei erkannt, dass sich die benannten Sektoren nicht nur wesentlich im Hinblick auf ihre Kritikalität und spezifischen Sicherheitsanforderungen zueinander unterscheiden, sondern diese mitunter auch innerhalb der Sektoren signifikant und abhängig vom Geschäftsmodell und Tätigkeitsbereich variieren.

Die geplante Konsultation mit Branchenvertretern zur Bestimmung der wesentlichen Kritischen Infrastrukturen bzw. des Adressatenkreises des Gesetzes sollte zeitnah stattfinden. Eine differenzierte Betrachtungsweise und eingehende Risikoanalyse ist im Vorfeld einer Gesetzesinitiative essentiell, um erfolgreich angemessene Sicherheitslösungen zu finden.

- **Mindeststandards, Artikel 1 § 8a**
  Der BDI begrüßt ausdrücklich die Möglichkeit zur Erarbeitung branchenspezifischer Sicherheitsstandards durch die Betreiber Kritischer Infrastrukturen und Branchenverbände im Wege der Selbstorganisation. Der BDI hat sich bereits im BDI-Positionspapier und in der KPMG-Studie explizit für diese Option ausgesprochen. Das wird dem Ziel gerecht, dass Mindeststandards für jede Branche passgenau sein müssen, um effektiv wirken zu können. Dem einzelnen Betreiber steht es

frei, abweichend von den branchenspezifischen Sicherheitsstandards, eigene den Stand der Technik berücksichtigende Maßnahmen umzusetzen. Dieser kooperative und vertrauensvolle Ansatz wird BDI-seitig mit Nachdruck unterstützt.

- **Bewertung und Veröffentlichung Sicherheit informationstechnischer Produkte, Systeme und Dienste, Artikel 1 § 7a**

  „(1) Das Bundesamt darf zur Erfüllung seiner Aufgaben auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte, Systeme und Dienste untersuchen. Es darf sich hierbei der Unterstützung Dritter bedienen.
  (2) Die aus den Untersuchungen gewonnenen Erkenntnisse dürfen nur zur Förderung der IT-Sicherheit genutzt werden.
  (3) Das Bundesamt darf seine Bewertung der Sicherheit der untersuchten informationstechnischen Produkte, Systeme und Dienste weitergeben und veröffentlichen. § 7 Absatz 1 Satz 3 und 4 ist entsprechend anzuwenden.“

  BDI-Kommentierung
  Diese Regelung greift tief in die privatwirtschaftliche Tätigkeit des betroffenen Unternehmens ein. Aus Sicht des BDI ist dies äußerst problematisch. Der bisher gültige Ansatz, dass Unternehmen bei Produkten, Systemen und Diensten um eine Zertifizierung durch das BSI ersuchen, wird umgekehrt. Das BSI erhielte damit die gesetzliche Befugnis noch vor Markteinführung eines Produkts, Prüfungen zu vollziehen. Darüber hinaus wird durch die geplante Form des Reverse Engineering eine Schwächung der Common Criteria (CC) durch die Hintertür befürchtet.

  Die Übertragung dieser Prüfkompetenz auf „Dritte“ setzt voraus, dass diese „Dritten“ über das entsprechende Know-How verfügen, Produkte, Services und Dienste qualifiziert zu prüfen. Ein solches Wissen ist in der Regel nur bei Unternehmen derselben Branche verfügbar, was die Offenlegung von Geschäftsgeheimnissen oder Geschäftspotenzialen gegenüber direkten Konkurrenten zur Folge hätte. Speziell die Befugnis zur Weitergabe und Veröffentlichung der Informationen ohne angemessene Barrieren und Kontrollen kann zu einem neuen Sicherheitsrisiko führen oder zu einem Reputationsschaden für betroffene Unternehmen und ihre Produkte.

  Hier ist sicherzustellen, dass die Rechte der Hersteller gewahrt werden. Eine Weitergabe und Veröffentlichung der Bewertung des BSI sollte nur erfolgen, wenn das jeweilige Unternehmen ausdrücklich seine Zustimmung erteilt hat. Wir schlagen vor, einen solchen Zusatz in Absatz 3 zu ergänzen.

- **Weitergabe der Ergebnisse eines Sicherheitsaudits, Artikel 1 § 8a**
  In § 8a heißt es:

  > *„(3) (…) Die Betreiber übermitteln dem Bundesamt eine Aufstellung der durchgeführten Audits, Prüfungen oder Zertifizierungen einschließlich der dabei aufgedeckten Sicherheitsmängel. Bei Sicherheitsmängeln kann das Bundesamt die Übermittlung der gesamten Audit-, Prüfungs- oder Zertifizierungsergebnisse und, soweit erforderlich, im Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes oder im Benehmen mit der sonst zuständigen Aufsichtsbehörde die Beseitigung der Sicherheitsmängel verlangen.“*

  BDI-Kommentierung
  Eine gesetzliche Verpflichtung zur Detailmeldung der Ergebnisse der geforderten Sicherheitsaudits, Prüfungen oder Zertifizierungen an das BSI wird als bedenklich erachtet. Das Recht über die detaillierten Informationen eines Audits oder einer Überprüfung verfügen zu dürfen, sollte prinzipiell ausschließlich dem Auftraggeber obliegen.

  Unklar bleibt zudem, welche Konsequenzen eine Übermittlung der Auditergebnisse ans BSI nach sich zieht. Dies gilt insbesondere dann, wenn eine Zertifizierungspflicht hergestellt würde. Über die Verpflichtung zur Zertifizierung wäre eine Konformität zu geforderten Anforderungen bereist ausreichend sichergestellt. Weitergehende Berichterstattungen würden den bereits erheblichen Bürokratieaufwand weiter steigern.

- **Meldepflichtige Ereignisse, Artikel 1 § 8b**
  Gemäß dem Referentenentwurf haben

  > *„(4) Betreiber kritischer Infrastrukturen (…) bedeutende Störungen ihrer informationstechnischen Systeme, Komponenten oder Prozesse, die zu einem Ausfall oder einer Beeinträchtigung der von ihnen betriebenen Kritischen Infrastrukturen führen können, über die Kontaktstelle unverzüglich an das Bundesamt mitzuteilen.“*

  In den Erläuterungen zu § 8b (Seiten 39 und 40) wird erstmals versucht meldepflichtige Ereignisse zu definieren:

  > *„Eine Störung im Sinne des BSI-Gesetzes liegt daher vor, wenn die eingesetzte Technik die ihr zugedachte Funktion nicht mehr richtig oder nicht mehr vollständig erfüllen kann oder versucht wurde, entsprechend auf sie einzuwirken. Dazu zählen insbesondere Fälle von Sicherheitslücken, Schadprogrammen und erfolgten, versuchten oder erfolgreich abgewehrten Angriffen auf die Sicherheit in der Informationstechnik sowie außergewöhnliche und unerwartete technische Defekte mit IT-Bezug (z. B. nach Softwareupdates oder ein Ausfall der Serverkühlung). Die Störungen sind dann meldepflichtig, wenn sie bedeutend sind. Eine bedeutende Störung liegt vor, wenn die Funktionsfähigkeit des Betreibers oder die von diesem betriebene Kritische Infrastruktur bedroht sind.“*

Genaue Angaben zum Meldeprozess fehlen im vorliegenden Entwurf weiterhin. Der Referentenentwurf enthält keine Angaben über inhaltliche Anforderungen an eine Meldung, Detailtiefe und Zeitrahmen.

Aus BDI-Sicht führt eine Meldung über jede Störung, die zu einer „Beeinträchtigung führen könnte", zu weit. Gemäß dieser Definition liegt bereits eine Störung vor, wenn nur versucht wurde auf die Technik einzuwirken. Die Tatsache, dass diese dann bereits bedeutend ist, wenn die Funktionsfähigkeit auch nur bedroht ist, umfasst bei einer unverzüglichen Meldeverpflichtung im Zweifel jegliche Störungen. Um Rechtssicherheit zu schaffen, ist eine Konkretisierung aus BDI-Sicht dringend geboten. Außerdem sollten die Vorgaben zur Meldepflicht mit anderen bestehenden nationalen gesetzlichen Regelungen, wie z. B. dem Energiewirtschaftsgesetz, sowie der NIS-Richtlinie auf europäischer Ebene und internationalen Standards („Cybersecurty Framework" in den USA"), übereinstimmen.

Die gesetzliche Vorgabe in § 8a

> *„(4) (…) Die Meldung muss Angaben zu den Störungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache, der betroffenen Informationstechnik und zur Branche des Betreibers enthalten"*

steht der im selben Absatz geforderten „unverzüglichen" Meldung entgegen. Unternehmen sollten grundsätzlich die Möglichkeit haben, IT-Beeinträchtigungen zunächst intern zu analysieren. Insofern erscheint die Pflicht zur unverzüglichen Feststellung und Weitermeldung von Beeinträchtigungen durch die betroffenen Unternehmen nicht gerechtfertigt.

Darüber hinaus erschweren die vorgesehene Inhalte einer Meldung (ausgenutzte Sicherheitslücken, vermutete oder tatsächliche Ursachen, die betroffene Informationstechnik auf System- und Komponentenebene) erschweren weiterhin eine schnelle und gleichzeitig unternehmensinterne Compliance konforme Meldung. Die Meldung der eindeutigen Identifikationsmerkmale von gefundenen Schadensmerkmalen und Programmen erscheinen zielführender. Die Weitergabe erlaubt es anderen Unternehmen, schnell zu prüfen, ob sie ebenfalls betroffen sind. Das schafft einerseits einen praxistauglichen Mehrwert und andererseits eine Basis für ein Sicherheitslagebild gegeben.

Der BDI schlägt folgende Formulierung zu § 8a (4) vor:

> *„(…) Die Meldung sollte vorrangig Angaben zu den Signaturen oder sonstigen Identifikationsmerkmalen von gefundenen Schadensmerkmalen und Programmen sowie Angaben zur Branche enthalten und sollte nachträglich durch Informationen zu den Störungen sowie zu den technischen Rahmenbedingungen, insbesondere der vermuteten oder tatsächlichen Ursache und der betroffenen Informationstechnik ergänzt werden."*

Außerdem bleibt unklar, was im Falle eines Verstoßes gegen die Meldepflicht zu befürchten ist. Mit Blick auf die parallelen Vorgaben der NIS-Richtlinie ist damit zu rechnen, dass die Verletzung einer Meldepflicht die Erhebung eines Bußgeldes nach sich ziehen wird. Vor diesem Hintergrund wäre der Tatbestand der Meldepflichtverletzung unbedingt zu spezifizieren.

- **Anonymisierte bzw. pseudonymisierte Meldung, Artikel 1 § 8b**
  Die grundsätzliche Möglichkeit zur anonymisierten bzw. pseudonymisierten Meldung unterstützt der BDI mit Nachdruck. Diese Regelung muss für alle Kritischen Infrastrukturbetreiber gleichermaßen gelten. Gegenwärtig ist sie für die Energiewirtschaft allerdings völlig ausgeschlossen:

  > *„Die Nennung des Betreibers ist nur dann erforderlich, wenn die Störung tatsächlich zu einem Ausfall oder einer Beeinträchtigung der Kritischen Infrastrukturen geführt hat."*

  BDI-Kommentierung
  Der BDI hatte in der KPMG-Studie bereits einen entsprechenden Vorschlag erarbeitet. Die Studie empfiehlt eine „Pseudonymisierung der Meldepflicht via Treuhänder". Eine solche Lösung ermöglicht es dem BSI uneingeschränkt, ein Lagebild zu erstellen und minimiert zugleich das Risiko von Reputationsschäden für die meldenden Unternehmen. Ein unabhängiger Treuhänder könnte dabei die vermittelnde Rolle annehmen und bei Bedarf auch einen gesicherten Weg zum meldenden Unternehmen zur Verfügung stellen.

- **Anwendungsbereich, Artikel 1 § 8c**
  Der BDI begrüßt, dass nach §8c Absatz 2 Satz 1 Betreiber Kritischer Infrastrukturen, die über bereits bestehende Rechtsvorschriften reguliert werden, diesen auch weiterhin unterliegen sollen (Vermeidung doppelter Regulierung und Zuständigkeiten).

- **Auskunftsverlangen, Artikel 1 § 8d**
  In § 8d regelt die Auskunft des BSI zu Informationen

  > *„(1) Das Bundesamt kann auf Antrag Auskunft zu den im Rahmen von § 8a Absatz 2 und 3 erhaltenen Informationen sowie zu den Meldungen nach § 8b Absatz 4 erteilen, wenn keine schutzwürdigen Interessen des betroffen Betreibers Kritischer Infrastrukturen dem entgegenstehen und durch die Auskunft keine Beeinträchtigung des Verfahrens oder sonstiger wesentlicher Sicherheitsinteressen zu erwarten ist."*

  BDI-Kommentierung
  Die Auswirkungen einer Bekanntgabe der Informationen und Meldungen kann für den konkreten Betreiber der Kritischen Infrastruktur massive Auswirkungen, wie z. B. Preisgabe von Betriebsgeheimnissen, Wettbewerbsnachteile, Umsatzeinbußen oder Imageverlust zur Folge haben. Es besteht Seitens der deutschen Industrie die Befürchtung, dass bei einer Beeinträchtigung oder einem Ausfall Kritischer Infrastrukturen die ebenfalls schutzwürdigen Interessen des betroffenen Betreibers dem

Informationsbedürfnis nachgelagert werden.

Der BDI schlägt daher vor, dass die Auskunft lediglich in anonymisierter Form erteilt werden sollte. Eine Formulierung wie folgt wäre daher das Minimum, welches Eingang in die gegenwärtige Klausel finden sollte:

> „*nach Anhörung und ohne namentliche Nennung des konkreten Betreibers der Kritischen Infrastruktur.“*

- **Umsetzungsfrist**
  Die vorgesehene Umsetzungsfrist von zwei Jahren ist zu knapp bemessen. Für die Energiewirtschaft soll sogar eine noch kürzere Umsetzungsfrist von lediglich einem Jahr gelten. Je nach individueller Betroffenheit ist eine Vielzahl an zusätzlichen Verpflichtungen zu erfüllen. Die betroffenen Unternehmen benötigen ausreichend Zeit, um neue Informationsabläufe, Sicherheitsprozesse und Auditverfahren abzustimmen. Der BDI spricht sich dafür aus, die Umsetzungsfrist des Gesetzes für alle Betreiber Kritischer Infrastrukturen auf drei Jahre zu verlängern.