

Stellungnahme

**Entwurf eines Gesetzes zur Umsetzung
der Richtlinie (EU) 2022/2557 und zur
Stärkung der Resilienz von Betreibern
kritischer Anlagen**

**(KRITIS-Dachgesetz – KRITIS-
DachG)**

Bundesverband der Deutschen Industrie e.V.

Inhaltsverzeichnis

Vorbemerkung	3
Stellungnahme.....	4
1. KRITIS-Schutz als Teil der Gefahrenabwehr	4
2. Verzahnung mit NIS2UmsuCG und der Strategie zur Verbesserung der Resilienz kritischer Infrastrukturen	5
3. Begriffe: Einheitlich, eindeutig, konsistent definieren	6
4. Zuständigkeitsfragen klären	9
5. Erlass von Rechtsverordnungen, Anhörungsverfahren	10
6. Ausnahmeverfahren für die Öffentliche Verwaltung	11
7. Registrierung von kritischen Anlagen	12
8. Meldewesen und Informationsaustausch	13
9. Maßnahmen und Standards	15
10. Sicherheitsüberprüfungen	17
11. Nationale Risikoanalysen und Risikobewertungen	19
12. Erfüllungsaufwand.....	19
13. Streichung § 13	20
Über den BDI.....	21
Impressum	21

Vorbemerkung

Der BDI begrüßt die Möglichkeit, Stellung zum Entwurf des Gesetzes des Bundesministeriums des Innern und für Heimat (BMI) zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen (KRITIS Dachgesetz- KRITIS-DachG), kurz RefE, zu nehmen.

Gleichzeitig möchten wir erneut betonen, dass wir, wie in den „[10 Handlungsempfehlungen der deutschen Industrie zum KRITIS-Dachgesetz](#)“ vom Juni 2023 sowie der [BDI-Stellungnahme zum ersten Referentenentwurf des KRITIS-DachG](#) vom 24. August 2023 bereits ausgeführt, es weiterhin kritisch sehen, dass die Bundesregierung ein KRITIS-DachG zur Umsetzung der CER-Richtlinie und davon losgelöst ein NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) verfasst. Vorzugsweise wären die entsprechenden rechtlichen Vorgaben in einem Gesetz, mindestens aber in einem gemeinsamen Gesetzgebungsverfahren zu bündeln. Nur durch eine Bündelung kann Kohärenz – sowohl hinsichtlich der Anforderungen als auch in der Umsetzung – gewährleistet werden.

Wir bedauern sehr, dass das BMI die Verbändeanhörung in die Weihnachts- und Neujahrszeit gelegt hat. Mit der Versendung des zweiten Entwurfs am Nachmittag des 22. Dezember 2023 und der Frist zur Stellungnahme bis zum 24. Januar 2023 wurde es Unternehmen und Verbänden erschwert, sich umfassend zu dem Gesetzentwurf abzustimmen.

Zugleich wurden bislang noch nicht die Voraussetzungen geschaffen, um eine vollständige Bewertung (inhaltlich und monetär) des Gesetzesentwurfes vorzunehmen. So fehlt z.B. die nationale Risikoanalyse bzw. die Kenntnis darüber, in welchem Detaillierungsgrad welche Themen darin behandelt werden und damit auch, welche Szenarien für die Analyse der betrieblichen Risiken und die Ableitung von Maßnahmen und Kosten zu berücksichtigen sind. Eine Gesamtbewertung wird auch dadurch erschwert, dass die Rechtsverordnung nach § 16 noch nicht vorliegt.

Es ist daher sehr erfreulich, der E-Mail-Nachricht des BMI zum Start der Verbändeanhörung vom 22. Dezember 2023 zu entnehmen, dass im Anschluss an diese Beteiligungsrunde noch eine weitere Abstimmungsrunde erfolgen soll. Gerne beteiligt sich der BDI weiterhin an der Weiterentwicklung des Gesetzes, damit das gemeinsame Ziel, den physischen Schutz kritischer Infrastrukturen zu stärken, so gut wie möglich umgesetzt werden kann. In diesem Sinne fordert der BDI das BMI erneut dazu auf, direkt auf

Unternehmen und Verbände zuzugehen und mit diesen zu bestehenden Unklarheiten in den Austausch zu treten.

Stellungnahme

1. KRITIS-Schutz als Teil der Gefahrenabwehr

Resiliente und störungsfrei funktionierende KRITIS sind für das Funktionieren unseres Gemeinwesens von elementarer Bedeutung. Der Schutz von KRITIS ist daher ein Schlüssel zur Gewährleistung unserer nationalen Sicherheit.

In diesem Sinne begrüßt die deutsche Industrie den bereits durch die CER-Richtlinie verfolgten und einer in der Wirtschaft bereits etablierten Herangehensweise des All-Gefahren-Ansatzes, der sowohl Naturkatastrophen als auch vom Menschen verursachte, unbeabsichtigte oder vorsätzliche Gefährdungen berücksichtigt. Der Schutz vor derart vielfältigen, oft mehrdimensionalen Risiken erfolgt in der Prävention und der Abwehr, ob im physischen oder im Cyberraum. Es gilt, die seit Langem bestehenden und bekannten Defizite umfassend in einem ganzheitlichen, integrierten Ansatz auszuräumen. Ein Ansatz, der den unterschiedlichen Dimensionen von Sicherheitsrisiken – physisch, digital und hybrid – Rechnung trägt und somit Deutschland vorausschauend krisensicher – resilient – aufstellt. Die Umsetzung der CER-Richtlinie sollte als Chance genutzt werden, um die innere Sicherheit durch einen verbesserten ganzheitlichen Schutz von KRITIS zu erhöhen.

Sabotageakte, z. B. auf Gaspipelines und Bahninfrastruktur, haben indes gezeigt: Die Bedrohungslage hat sich im Kontext der geopolitischen Zeitenwende auch für Deutschland und Europa nochmals verschärft. Insbesondere kritische Infrastrukturen sind in den Fokus hybrider Strategien von Drittstaaten geraten.

Aus Sicht des BDI ist es daher erforderlich, den Anwendungsbereich des KRITIS-Gesetzes dahingehend auszuweiten, dass neben den Betreibern kritischer Anlagen auch Bund und Länder beim Schutz kritischer Infrastrukturen in die Pflicht genommen werden. Betreiber kritischer Anlagen können terroristische oder gar militärische Bedrohungen nicht durch präventive Schutzmaßnahmen verhindern. Die letzte Instanz der Gefahrenabwehr können und dürfen nur die Gefahrenabwehrbehörden des Bundes und der Länder sein. Ohne eine entsprechende Erweiterung des Anwendungsbereichs und ggf. eine Neuregelung der Gefahrenabwehr insbesondere für Infrastrukturen,

**Bundesverband der
Deutschen Industrie e.V.**

Lobbyregisternummer
R000534

Hausanschrift
Breite Straße 29
10178 Berlin

Postanschrift
11053 Berlin

Ansprechpartner
Kerstin Petretto
T: +49 30 2028-1710

E-Mail:
k.petretto@bdi.eu

Internet
www.bdi.eu

die sich über das gesamte Bundesgebiet erstrecken, droht eine offene Flanke gegenüber derartigen Bedrohungen allein schon durch eine unzureichende Abschreckung.

2. Verzahnung mit NIS2UmsuCG und der Strategie zur Verbesserung der Resilienz kritischer Infrastrukturen

Durch die fortschreitende Digitalisierung wirtschaftlicher, technologischer gesellschaftlicher und politischer Prozesse werden die Risikolagen des Cyber- und des realen Raums immer mehr miteinander verschränkt.

Cyber-/IT- und physische Sicherheit lassen sich schon heute nicht isoliert voneinander betrachten und realisieren. Gerade im Bereich der physischen Sicherheit wird der Einsatz von IT-Lösungen weiter stark zunehmen, sodass sachlich überschneidungsfreie Regelungen künftig noch mehr als heute benötigt werden.

Es wäre aus Sicht des BDI dringend angezeigt gewesen, die NIS 2-Richtlinie und die CER-Richtlinie gemeinsam in einem Gesetz zu implementieren und so der hybriden Bedrohungslage sowie der Notwendigkeit zu einer eng verzahnten Kooperation unterschiedlicher Aufsichtsbehörden zu gewährleisten.

In diesem Zusammenhang ist es sehr bedauerlich, dass der neue Entwurf zum NIS2UmsuCG immer noch nicht vorliegt. Nur so wäre es möglich zu beurteilen, ob diese beiden Gesetze im Themenkomplex der nationalen Sicherheit miteinander verzahnt sind, sich gegenseitig ergänzen und keine Doppelregelungen enthalten.

In diesem Sinne kann das KRITIS-DachG schließlich für solche Unternehmen als Auffanggesetz greifen, für die die sektorspezifischen Regelungen bislang keine besonderen Pflichten zum Schutz der physischen Sicherheit vorsehen.

Dementsprechend sollten aus BDI-Sicht beispielsweise weiterhin die Sektoren Informationstechnik und Telekommunikation (TK) vollständig aus dem Anwendungsbereich des KRITIS-DachG herausgenommen werden soweit diese Unternehmen nicht unter spezialgesetzliche Pflichten fallen. Entsprechend der EU-rechtlichen Vorgaben gelten gemäß § 4 Abs. 6 RefE die §§ 7-12 RefE nicht für verschiedene Sektoren. Übrig bleibt letztlich die Registrierungspflicht nach § 6 RefE. Diese findet sich aber bereits schon in der NIS2 und dann auch in dem entsprechenden Umsetzungsgesetz. Insofern können die Sektoren auch direkt komplett ausgenommen werden. Die derzeitige teilweise Herausnahme aus dem Anwendungsbereich ist nicht unproblematisch.

Es entstehen rechtliche Unklarheiten, die vermieden werden könnten. Zum Beispiel scheint die Überwachungspflicht des § 14 auch für den TK-Sektor zu gelten, obwohl eine Überwachung nach § 14 Abs. 1 keinen Sinn ergibt. Denn hier soll die Überwachung der Vorgaben des § 10 erfolgen, der ja gerade nicht zu beachten ist. Gleiches gilt für § 16 Abs. 2: Diese Vorschrift enthält eine Verordnungsermächtigung zur Konkretisierung der Vorgaben des § 10, der keine Anwendung finden soll.

Zudem ist es nicht ersichtlich, warum der Luftverkehr mit seinen ebenfalls bestehenden umfangreichen europarechtlichen Vorgaben bei einer möglichen Ausnahmeregelung unberücksichtigt bleibt. Die umfangreichen Vorgaben an den Schutz der Anlagen und die Sicherheit des Betriebs (insb. VO (EU) 2018/1139 und VO (EU) 300/2008) qualifizieren ebenso für eine weiter vereinfachte Umsetzung des vorliegenden Gesetzes. Wie die bereits ausgenommenen Sektoren muss auch der Luftverkehr in diesem Rahmen „geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen“ ergreifen.

Laut § 1 des vorliegenden Entwurfs des KRITIS-DG beabsichtigt die Bundesregierung bis zum 17. Januar 2026 eine Strategie zur Verbesserung der Resilienz kritischer Infrastrukturen zu verabschieden. Trotz des durch die CER-Richtlinie vorgegebenen Zeitdrucks, das Gesetz bis Oktober 2024 zu verabschieden, ist es doch fragwürdig, dass die Strategie dem Gesetzesverfahren folgt. Eine Strategie sollte Leitplanken vorgeben, entlang derer Maßnahmen zur Erhöhung der Resilienz abgeleitet werden - nicht umgekehrt. Es ist zu befürchten, dass nach der Erarbeitung der Strategie eine schnelle Revision der gerade getroffenen Maßnahmen erfolgen könnte.

3. Begriffe: Einheitlich, eindeutig, konsistent definieren

Die in deutschen Gesetzen verwendeten Begrifflichkeiten sollten einheitlich gewählt, eindeutig definiert und konsistent genutzt werden. Der BDI hatte in seiner Stellungnahme vom 24. August 2023 bereits eine Vereinheitlichung der Begrifflichkeiten gefordert, vor allem die Streichung der Kategorie Kritische Infrastrukturen, der keine europarechtliche Entsprechung findet. Diese Streichung ist erfolgt. Auch insgesamt ist im jüngsten Entwurf eine deutliche Vereinheitlichung von Begrifflichkeiten und die Bestimmung der betroffenen Betreiber kritischer Anlagen niedergelegt.

Dennoch fehlen weiterhin durchgängige einheitliche Definitionen der im KRITIS-DachG und dem NIS2UmsuCG verwendeten Begrifflichkeiten. So sind z.B. die in § 2 des vorliegenden Entwurfs des KRITIS-DachG genannten

Begrifflichkeiten „kritische Anlage“, „kritische Dienstleistung“ und „Vorfall“ nicht einheitlich definiert. Dabei ist es wichtig, den Begriff der „kritischen Anlage“ in den Kontext des Begriffs des „Betreibers“ zu stellen, der nun an prominenter Stelle in den Titel des Gesetzes aufgenommen wurde, ohne jedoch definiert zu werden. Äußerst fraglich ist, ob ein Betreiber selbst Resilienz gegenüber den anzunehmenden Risiken aufbauen kann. Ziel des Gesetzes sollte aus Sicht des BDI vielmehr die Stärkung der Resilienz kritischer Anlagen *durch* den Betreiber sein.

Während die CER- und die NIS-2-Richtlinie sich auf den Begriff „Einrichtungen“ fokussieren, stellt das KRITIS-DachG auf „Anlagen“ ab (vgl. insb. § 4 Abs. 1). Darüber hinaus können nach § 4 Abs. 2 „weitere Betreiber“ festgelegt werden. Dieser terminologische Bruch im Gesetz ist nicht nachvollziehbar. Auch die Begriffsbestimmungen in Verbindung mit § 4 und § 16 ergeben in der derzeitigen Fassung keinen Sinn. Es sollten einheitlich Betreiber kritischer Anlagen adressiert werden und dies gesetzesübergreifend konsistent. Letztlich ist auch die Definition der kritischen Anlage sprachlich ungenau verfasst (es müsste heißen: "eine Anlage, über die eine kritische Dienstleistung erbracht wird").

Die in § 4 enthaltene Sektorenbezeichnung erscheint unvollständig oder unpräzise. Vor allem entspricht sie weiterhin nicht dem in der CER-Richtlinie genutzten Wording (z.B. ist "Bankwesen" nicht enthalten, obwohl in § 4 Abs. 6 RefE Rückausnahme enthalten ist, "Digitalsektor" wird in Gesetzesbegründung häufiger erwähnt, obwohl er in § 4 Abs.1 RefE nicht genannt wird). Wie in Punkt sieben dieser Stellungnahme ausgeführt, ist zudem aus Sicht des BDI eine Ausnahmeregelung für Behörden auch gemäß CER-Richtlinie weiterhin nicht nachvollziehbar.

Auch die Kriterien zur Identifizierung von Betreibern kritischer Anlagen sind weiterhin unscharf definiert. § 4 Abs. 2 und 3 RefE führt als Kriterium beispielsweise an "die möglichen Auswirkungen von Ausfällen hinsichtlich Ausmaßes und Dauer auf wirtschaftliche und gesellschaftliche Tätigkeiten, die Umwelt, die öffentliche Ordnung und Sicherheit oder die Gesundheit der Bevölkerung". Die Flexibilisierungen innerhalb der Rechtsverordnung zur Identifizierung von KRITIS ist zwar zu unterstützen. Nichtsdestotrotz ist eine genaue Definition der Ausnahmen erforderlich.

Letztendlich muss darauf geachtet werden, dass die Ausgestaltung von „kritischen Anlagen“ und „kritischen Dienstleistungen“ in der Rechtsverordnung entsprechend § 16 RefE identisch mit der Ausgestaltung von „kritischen Anlagen“ und „kritischen Dienstleistungen“ entsprechend § 57 NIS2UmsuCG,

spricht der nächsten BSI-KRITIS-Verordnung, ist, wenn die zukünftige Verordnung nach § 16 RefE doch nicht wie geplant für beide Gesetze gelten soll. Dies betrifft im Besonderen auch die Ausgestaltung des in § 4 Abs.1 genannten Regelschwellenwertes. Dieser kann nur die Berechnungsgrundlage und somit Ausgangsbasis darstellen, anhand der unter Heranziehung der entsprechenden Korrekturfaktoren realistische Schwellenwerte ermittelt werden.

Der Begriff „Beratungsmission“ (u.a. § 7 Abs. 4 RefE) ist erläuterungsbedürftig und fehlt in den Begriffserläuterungen in § 2 RefE. Wünschenswert wäre eine Konkretisierung der in der CER-Richtlinie genannten Beratungsmission.

In § 8 RefE werden nach wie vor keinerlei nachvollziehbare Kriterien zum Begriff der „Wirtschaftsstabilität“ angelegt. § 10 Abs. 1 RefE verpflichtet Betreiber kritischer Anlagen, geeignete und verhältnismäßige technische, sicherheitsbezogene und organisatorische Maßnahmen zur Gewährleistung der Resilienz zu treffen. Die verwendeten Terminologien „geeignet“, „verhältnismäßig“ sowie „Gewährleistung“ sind hierbei nicht definiert. Der Zusatz zu § 10 ist nicht ausreichend. Demnach ist die Verhältnismäßigkeit gewahrt, wenn der Aufwand zur Verhinderung oder Begrenzung eines Ausfalls zum Risiko eines Vorfalls angemessen erscheint. Wie in der Begründung des RefE aufgeführt, können auch wirtschaftliche Aspekte berücksichtigt werden.

In § 11 Abs. 5 und 6 RefE werden ebenso unbestimmte Rechtsbegriffe wie „erhebliche Zweifel an der Einhaltung von Verpflichtungen“ verwendet. Diese undefinierten Begriffe lassen erhebliche Spielräume zu und müssen im Sinne einer Anwendungsklarheit spezifiziert werden. Die Begrifflichkeiten sollten aus Sicht des BDI unbedingt entsprechend angepasst vereinheitlicht werden.

In § 14 RefE werden nun auch „Billigungs -, Überwachungs -, und Schulungspflichten“ für Geschäftsleiter analog zu § 38 des Diskussionspapiers zum NIS2UmsuCG gefordert. Neben den vom BDI zum NIS2UmsuCG bereits geäußerten inhaltlichen Vorbehalten¹ sollten auch hier einheitliche Definitionen sichergestellt werden. Dabei ist in diesem Kontext zwingend zu definieren, was die Bezeichnung Geschäftsleiter / Geschäftsleiterin zum Ausdruck bringen soll und welche Funktion innerhalb eines Unternehmens /

¹ Vgl. <https://bdi.eu/publikation/news/nis-2-diskussionspapier-des-bundesinnenministeriums>

Konzernkonstrukts gemäß KRITIS-DachG künftig zur Haftung herangezogen wird.

4. Zuständigkeitsfragen klären

Die deutsche Industrie erkennt in dem Vorhaben des KRITIS-DachG eine große Chance, das seit Jahren bestehende „Zuständigkeitswirrwarr“ im KRITIS-Schutz zu durchbrechen und bundeseinheitliche Regelungen festzulegen sowie bestehende föderale Zersplitterungen zu beseitigen. Nur so kann ein „All-Gefahren-Ansatzes“ deutschlandweit erfolgreich implementiert werden.

Der vorliegende Gesetzesentwurf weist zwar bereits erhebliche Fortschritte auf, insbesondere durch die zentralen Rollen, die dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zugeordnet werden. Jedoch sind die Behördenzuständigkeiten bei der Durchsetzung und Aufsicht noch immer nicht eindeutig geregelt bzw. lassen die Vermutung zu, dass betroffene Unternehmen (insb. „Verbundunternehmen“) im Rahmen der Bundes- und Landeshoheit verschiedenen Regelungen z.B. bei der „Nachweiserbringung“ und den „Meldepflichten“ unterliegen.

So ist die Auflistung der zuständigen Bundesbehörden nach § 3 für den Vollzug des KRITIS-DachG in Bezug auf spezifische kritische Dienstleistungen in seiner jetzigen Fassung unklar. Es sollte zumindest in einer Anlage, deutlich aufgezeigt werden, welche Branchen und Dienstleistungen dem KRITIS-DachG unterstehen und welche Behörde auf Landes- oder Bundesebene die Zuständigkeit obliegt. Dies ist insbesondere in Hinblick auf die noch offenen Bund-Länder-Zuständigkeiten in Hinblick auf die zu erlassenen Rechtsverordnungen von großer Bedeutung. Das KRITIS-DachG zeichnet verantwortlich für die abschließende bundeseinheitliche und damit länderübergreifende Festlegung des betroffenen Kreises der Branchen und Dienstleister und muss dabei im Einklang mit dem NIS2UmsuG stehen. Tut es dies nicht, hat es sein Ziel verfehlt.

Zudem besteht aus Sicht des BDI auf Basis der aktuellen Formulierung von § 3 Abs. 4 das Risiko des bundesuneinheitlichen Vollzugs. Eine konkrete Definition der Verantwortlichkeit in den einzelnen Bundesländern fehlt. Die zusätzliche Bestimmung von kritischen Anlagen, Schwellenwerten sowie Anforderungen durch die Bundesländer würde zu erheblichen Mehraufwänden bei Betreibern kritischer Anlagen führen.

Die Behördenzuständigkeit muss klar geregelt und für die Wirtschaft erkennbar sein. Auch hier dürfen keine sich überschneidenden Zuständigkeiten geschaffen werden und die zuständige Behörde muss in die Lage versetzt werden diesen Pflichten nachzukommen. Nicht zuletzt, damit behördliche Prozesse, von denen die Betreiber abhängen, auch frist- und sachgerecht abgearbeitet werden können (z.B. nationale Risikoanalyse).

Für Unternehmen, die zukünftig sowohl nach NISUmsuCG als auch nach KRITIS-DachG Nachweispflichten unterliegen, muss eine Behörde mit der Aufgabe der Gesamtkoordination benannt werden. Diese muss bei etwaigen Überschneidungen, die sich ggf. auch bei sehr guter gesetzlicher Regelung der Zuständigkeiten nicht vollständig vermeiden lassen, eine für alle Seiten bindende Entscheidung treffen dürfen. Die Erbringung von Nachweisen durch Audits muss in Form von „Gesamtaudits“ für Anforderungen nach NISUmsuCG und nach KRITIS-DachG möglich sein.

5. Erlass von Rechtsverordnungen, Anhörungsverfahren

Der BDI begrüßt, dass wie angeregt § 16 Abs.1 KRITIS-DachG entsprechend § 57 Abs.2 des vorliegenden Entwurfs des NIS2UmsuCG formuliert wurde. Demnach werden die Rechtsverordnungen u.a. nach der Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber kritischer Anlagen und Einrichtungen der Bundesverwaltung und Wirtschaftsverbände erlassen.

Angesichts einiger noch bestehender Unklarheiten im vorliegenden Entwurf muss die Einbindung von Experten aus der Praxis in der nächsten Phase der Gesetzeserarbeitung unbedingt mit Priorität verfolgt werden. Dies gilt aus BDI-Sicht vorrangig für die aus Sicht der Wirtschaft noch völlig offenen Zuständigkeitsfragen für die Erarbeitung sektorspezifischer und sektorübergreifender Rechtsverordnungen (insbesondere die diesbezügliche Ermächtigung der Ministerien und Behörden des Bundes sowie der Länder, hier einzelne Kriterien über Verordnungen festzulegen) sowie der derzeit sehr engen und zum Teil inkonsistenten zeitlichen Vorgaben für die Umsetzung der Maßnahmen in der Praxis.

Soweit an der Einbeziehung weiterer Bundesministerien festgehalten wird, sollten auch die betroffenen Betreiber und Wirtschaftsverbände in die Anlagenbestimmung mit einbezogen werden.

§ 16 Abs. 2 sollte wie folgt formuliert sein (Ergänzungen in rot): „Das Bundesministerium für Wirtschaft und Klimaschutz, das Bundesministerium für

Ernährung und Landwirtschaft, das Bundesministerium für Gesundheit, das Bundesministerium für Digitales und Verkehr und das Bundesministerium für Umwelt, Naturschutz, nukleare Sicherheit und Verbraucherschutz werden ermächtigt, **nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber kritischer Anlagen und Einrichtungen der Bundesverwaltung und Wirtschaftsverbände** im Einvernehmen mit dem Bundesministerium des Innern und für Heimat, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Rahmen ihrer jeweiligen Zuständigkeiten für kritische Dienstleistungen sektorspezifische Mindestvorgaben für Betreiber kritischer Anlagen zu bestimmen, die die Vorgaben des § 10 konkretisieren. Das Bundesministerium des Innern und für Heimat wird ebenfalls ermächtigt, **nach Anhörung von Vertretern der Wissenschaft, der betroffenen Betreiber kritischer Anlagen und Einrichtungen der Bundesverwaltung und Wirtschaftsverbände**, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, im Rahmen seiner Zuständigkeiten für kritische Dienstleistungen sektorspezifische Mindestvorgaben für Betreiber kritischer Anlagen zu bestimmen, die die Vorgaben des § 10 sektorspezifisch konkretisieren.“

6. Ausnahmeverfahren für die Öffentliche Verwaltung

Laut § 5 Abs. 2 RefE sind Einrichtungen der Bundesverwaltung, die Tätigkeiten ausüben in den Bereichen nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung, einschließlich der Ermittlung, Aufdeckung und Verfolgung von Straftaten, von den Verpflichtungen nach diesem Gesetz ausgenommen. Das Ausnahmeverfahren bestimmt sich nach § 17 RefE.

Dies ist aus BDI-Sicht sehr bedauerlich. Wie bereits in der Stellungnahme zum ersten Referentenentwurf und auch in den Anmerkungen zu diesem Referentenentwurf einleitend dargelegt, gilt es, die öffentliche Verwaltung nach gleichen Maßstäben als KRITIS zu definieren. Neben Bundesbehörden sollten auch Behörden der Länder und Kommunen – insbesondere Genehmigungs- und Überwachungsbehörden, die sensible Daten verarbeiten und für besonders wichtige und wichtige Einrichtungen essenzielle Verwaltungsleistungen erbringen, nicht durch Ausnahmeverfahren von den Verpflichtungen des KRITIS-DachG ausgenommen werden.

Darüber hinaus sind die Betreiber kritischer Anlagen im Falle einer Großschadenslage, die durch das BBK zu koordinieren ist, auch von diesem abhängig. In solchen Fällen muss das BBK auch in der Lage sein, dieser

Verpflichtung nachzukommen und darf nicht selbst durch sicherheitstechnische Probleme handlungsunfähig werden.

7. Registrierung von kritischen Anlagen

Grundsätzlich sollte sichergestellt werden, dass die in § 6 RefE enthaltene Registrierungspflicht gesetzesübergreifend einheitlich geregelt wird. Die Umsetzungsgesetze der CER- und der NIS2-Richtlinien sind aufeinander abzustimmen.

Der BDI begrüßt, dass § 6 des vorliegenden Referentenentwurfs eine Registrierung von kritischen Anlagen "über eine gemeinsam vom Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und dem Bundesamt für Sicherheit in der Informationstechnik eingerichtete Registrierungsmöglichkeit" vorsieht.

Die vorgesehenen Fristen sind indes unklar bzw. unrealistisch. Insbesondere ist die in § 6 Abs.6 genannte Frist von zehn Monaten zur Umsetzung von Maßnahmen gemäß §§ 10-12 RefE ist nicht realistisch, dies vor allem dann nicht, wenn die Planung gemäß § 9 RefE nur einen Monat weniger Zeit benötigen soll. Hier sollten längere Zeiträume vorgegeben werden, um ggf. nötigen Anpassungsmaßnahmen Rechnung tragen zu können.

Die deutsche Industrie fordert die Bundesregierung auf, ein volldigitales, datenschutzrechtlich gesichertes und risikoadäquat gegen Cyberbedrohungen geschütztes Registrierungswesen aufzusetzen, über das Unternehmen ihren Registrierungspflichten nach NIS2UmsuCG und KRITIS-DachG nachkommen können. Hier gilt es zu prüfen, inwiefern das Unternehmenskonto auf ELSTER-Basis als bereits bestehende Infrastruktur genutzt werden könnte. Dadurch würden unnötige Doppelstrukturen vermieden.

Auf die so gemeldeten Registrierungsdaten sollten die zuständigen staatlichen Stellen nach dem Need-to-know-Prinzip zugreifen können. Dadurch würden Erfüllungsaufwände für Unternehmen reduziert und Kapazitäten in der Wirtschaft geschaffen, die in den notwendigen Schutz vor Risiken fließen könnten.

Auf Unternehmensseite sollte keine Personen als Kontakt definiert werden können, sondern Funktionen. Dabei sollte klargestellt werden, dass *eine* zentrale Stelle für einen Unternehmensverbund angegeben werden kann und nicht jeder einzelne KRITIS-Betreiber eine 24/7-Kontaktstelle benennen und vorhalten muss.

8. Meldewesen und Informationsaustausch

Der BDI begrüßt, dass gemäß § 12 einheitliche Meldefristen sowie Meldewege für Meldungen gemäß KRITIS-DachG und NIS2UmsuCG, insbesondere inklusive eines einheitlichen Meldeportals sowie einer einheitlichen Meldestelle errichtet werden sollen.

Bei der Umsetzung ist zu beachten, dass das vorgesehene Meldewesen den Anlagenbetrieb nicht gefährden darf und auf Seiten des Anlagenbetreibers mit verhältnismäßigem Personalaufwand während des laufenden Betriebs zu bewältigen sein muss.

Der BDI begrüßt die gemäß § 12 erfolgte Einschränkung der Meldung von Vorfällen beim Vorliegen einer „erheblichen Störung“. Weitere, klare Einschränkungen und Vorgaben der Beurteilung von zu meldenden Vorfällen werden befürwortet, um hier eine Einheitlichkeit zu schaffen. Beispielsweise sollten sog. Beinahevorfälle nicht gemeldet werden müssen.

Der BDI begrüßt zudem die gemäß § 12 des vorliegenden Entwurfs geplanten, zweigeteilten Meldepflichten mit einer anfänglichen „Ad hoc“-Meldung und einer späteren ausführlichen Begründung – sofern diese im gleichen Formular zu leisten sind. Die „Ad-hoc“-Meldung im akuten Vorfall muss kurz gehalten werden können, damit die vorhandenen Ressourcen zur schnellstmöglichen Störungsbeseitigung und ggf. Betriebswiederaufnahme genutzt und nicht durch notwendige Meldepflichten gebunden werden. Dem wird in § 12 Abs. 3 zu Recht Rechnung getragen.

Die später folgende ausführliche Meldung sollte in Bezug auf Art und Umfang klar geregelt sein und nur die absolut notwendigen Informationen abfragen. Die Betreiber der Anlage müssen auch diese Verpflichtung während des laufenden Betriebs bewältigen können. Entsprechend sollten derartige grundsätzliche Anforderungen an Kriterien für die Inhalte der Meldungen der betroffenen Betreiber noch als Maßgabe für die Festlegung des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe Eingang in die Regelungen des § 12 Abs. 4 finden.

In dieser Hinsicht bedauert der BDI, dass gemäß § 12 RefE die Anbindung der Landesbehörden an die Meldestelle nicht vorgesehen ist. Erfolgt eine solche Regelung nicht, müssten bei landesgrenzüberschreitenden Vorfällen mehrere Behörden durch die Betreiber kritischer Anlagen informiert werden und diese Landesbehörden sich miteinander koordinieren. Dies würde im

direkten Widerspruch zu dem Anspruch des KRITIS-DachG stehen, das Meldewesen so zu verschlanken, dass Betreiber kritischer Anlagen bestenfalls nur eine Meldung für einen Vorfall tätigen müssen.

Ferner würde die Nichtanbindung die behördliche Koordination und Lagebilderstellung im Falle bundesweiter Vorfälle oder von umfassenden Sektor-Angriffen erheblich erschweren und einen Anstieg an Kosten auf Bundes- und Länderebene nach sich ziehen.

Auch ist es bedauerlich, dass RefE bislang nicht vorsieht, umgekehrt auch einen rückläufigen Informationsfluss vom BBK und anderen Behörden an die Betreiber der kritischen Anlage einzurichten. Dies ist insbesondere aus Präventionszwecken unbedingt geboten und ist entsprechend im BSI-Gesetz bzw. NIS2UmsuCG bereits so geregelt.

Klares Ziel muss sein, mit den unter das NIS2UmsuCG und das KRITIS-DachG fallenden Unternehmen Informationen und Einschätzungen über Risikolagen zwischen Staat und Wirtschaft in beide Richtungen systematisch auszutauschen, um im Sinne der Prävention ein tagesaktuelles, kostenfreies Lagebild zu digitalen und physischen Bedrohungen zu erstellen.

Der BDI schlägt erneut vor, einen zentralen Single Point Of Contact (SPOC) einzurichten, der die Behörden institutionalisiert einbindet, die für den Schutz von KRITIS (digital und physisch) Sorge tragen müssen. Der SPOC selbst fungiert als Schnittstelle (Dispatcher Hub) zwischen Unternehmen sowie Bundes- und Landessicherheitsbehörden: Er verteilt die eingehenden Meldungen entsprechend der Zuständigkeit nach dem Prinzip „ein Vorfall ein Formular“ und stellt sicher, dass der „Need-to-know“-Ansatz umgesetzt wird. Auf unterschiedlichen Zugriffsebenen gilt es, beispielsweise im Rahmen einer durch den Bund bereitgestellten sicheren virtuellen Plattform, Betreibern von Kritischen Infrastrukturen und Sicherheitsbehörden des Bundes und der Länder Zugriff zu erteilen.

Um einen derartigen SPOC zu ermöglichen, ist weiterhin eine durch den Gesetzgeber zu erfolgende Überprüfung der bestehenden Regeln der Geheimhaltung notwendig, damit Sicherheitsbehörden für den Schutz von KRITIS relevante Information sowohl untereinander als auch mit Sicherheitsbetrauten der Unternehmen direkt und zeitnah teilen können.

9. Maßnahmen und Standards

Der BDI begrüßt, dass der neue Referentenentwurf die Forderung der Industrie nach der Vermeidung von Doppelverpflichtungen insbesondere in § 4 Abs.8 aufgegriffen hat. Demgemäß können Betreiber kritischer Anlagen künftig mit Risikoanalysen und Risikobewertungen sowie Dokumenten und Maßnahmen zur Stärkung der Resilienz, die sie bereits auf der Grundlage anderer öffentlich-rechtlicher Verpflichtungen ergriffen haben, ihren Verpflichtungen nach §§ 9 bis 11 nachkommen. Die zuständigen Aufsichtsbehörden des Bundes oder die zuständigen Behörden der Länder stellen die Gleichwertigkeit im Benehmen mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und dem Bundesamt für Sicherheit in der Informationstechnik fest (Äquivalenzprüfung).

Allerdings führt der RefE nach wie vor nicht aus, was mit einem „Resilienzplan“ adressiert ist. Dies sollte konkretisiert werden. Es sollte darauf hingewiesen werden, dass bereits eine zielführende und praxisgerechte Planung von notwendigen Maßnahmen und deren entsprechende spätere Umsetzung ausreicht, um dem Ziel dieses Gesetzes gerecht zu werden. Bauliche Maßnahmen können Monate / Jahre in Anspruch nehmen.

Es ist zudem unklar, in welchen Zyklen die Resilienzpläne überprüft bzw. aktualisiert werden müssen. Hier müssen gesetzliche Vorgaben festgelegt werden, die mit den Betreibern von kritischen Anlagen abgestimmt werden. Das Offenhalten von Fristen birgt grundsätzlich für die Betreiber das Risiko unzureichender Vorbereitung und sollte daher unterbleiben.

Auch sind die benannten Muster und Mindestanforderungen weiterhin ausstehend. Bei dem Verweis auf den „Stand der Technik“ sollten entsprechende Hinweise auf Normen bzw. Vorgaben aufgenommen werden. Offen bleibt in § 10 Abs.1, in welchen Fällen ein angemessener physischer Schutz der Liegenschaften und kritischen Anlagen vorliegt und welche Maßnahmen hierzu verhältnismäßig sind. Insbesondere wirtschaftliche Aspekte bleiben im Entwurfstext bisher unberücksichtigt, obwohl ihnen sowohl in der Begründung aber in Satz 2 § 30 (1) des Diskussionspapiers zum NIS2UmsuCG Rechnung getragen wird. Klarstellend schlagen wir daher folgende Formulierung vor. § 10 Abs.1, Satz 2 RefE sollte wie folgt formuliert werden:

„Bei den von den Betreibern kritischer Anlagen zu treffenden technischen, sicherheitsbezogenen und organisatorischen Maßnahmen ist die Verhältnismäßigkeit zu wahren. Diese ist gewahrt, wenn der Aufwand zur

Verhinderung oder Begrenzung eines Ausfalls zum Risiko eines Vorfalls angemessen erscheint. Dabei können auch wirtschaftliche Aspekte berücksichtigt werden.“

Gemäß § 10 Abs.10 kann das BBK Betreibern kritischer Anlagen Vorlagen und Muster für einen Resilienzplan zur Verfügung stellen. Im Sinne der Einheitlichkeit und Handhabung sollte die Erstellung dieser Vorlagen und Muster als „kann“-Anforderung, durch eine „muss“-Vorschrift ersetzt werden. Die Verwendung dieser Vorlagen und Muster muss jedoch weiterhin freiwillig erfolgen, um Unterschieden im Sicherheitsmanagement Rechnung tragen zu können.

Aus BDI-Sicht ist es von höchster Relevanz, dass bestehende Sicherheitssysteme auf Seiten der Anlagenbetreiber weitestgehend erhalten und notwendigenfalls unter Einsatz des vorhandenen Personals optimiert werden sollten. Eine Schaffung neuer, anderer oder zu umfangreicher Standards könnte den Anlagenbetrieb gefährden. Wir unterstützen insofern die Regelung des § 4 Abs.8, wonach auf Seiten der Anlagenbetreiber auf Basis anderer Gesetze bereits vorgenommene Risikobewertungen und anlagenspezifische Gefährdungsbeurteilungen nach diesem Gesetz anerkannt werden können, wenn diese gleichwertig sind, um Anlagenbetreibern eine zusätzliche Auslastung des Personals sowie Kosten zu ersparen.

In diesem Kontext begrüßt der BDI insbesondere auch die Möglichkeit nach § 10 Abs.6 zur Entwicklung von branchenspezifischen Resilienzstandards.

Bei der Entwicklung und Anerkennung von Resilienzstandards und Mindestanforderungen gemäß § 10 Abs. 4, 5 und 7 sollten die zuständigen Behörden vor allem auf ein angemessenes Kosten-Nutzen-Verhältnis achten.

Dabei gilt es, die Lebenswirklichkeit der Anlagenbetreiber zu berücksichtigen und die Nutzung von Synergieeffekten zu ermöglichen. Diese können sich z.B. aus brancheneinheitlichen bzw. sogar -übergreifenden Standards, ergeben.

Gleichzeitig sollten aber auch anlagenspezifische Abweichungen ermöglicht werden, soweit dies vor dem Hintergrund der örtlichen Gegebenheiten gerechtfertigt ist. Üblicherweise haben Anlagenbetreiber bereits eigene Sicherheitsmaßnahmen eingeführt. Eine Schaffung neuer, erheblich abweichender Standards, kombiniert mit einem bürokratischen Meldewesen könnte den reibungslosen Anlagenbetrieb gefährden. Etwaige neue Maßnahmen müssen im laufenden Betrieb mit dem vorhandenen Personalpool umsetzbar sein.

Die im RefE in § 10 beispielhaft aufgeführten Maßnahmen erwecken den Eindruck, als wären sie zufällig ausgesucht und den entsprechenden Absätzen zugeordnet. Da es sich in erster Linie um Maßnahmen des Kontinuitätsmanagements handelt, die in aller Regel sowohl physische als auch IT-relevante Sicherheitsmaßnahmen umfassen, hilft eine dem Anschein nach willkürliche Aufzählung beliebiger Maßnahmen und Prozesse nicht. Zentrales Anliegen hier wäre eine Kategorisierung physischer Resilienzmaßnahmen gewesen.

Der BDI schlägt vor, dass dieser Katalog weiterhin nur beispielhaften Charakter entfaltet, er dabei jedoch sinnvoll strukturiert wird. Eine Option wäre es physische Resilienzmaßnahmen in die folgenden Kategorien aufzuteilen. Zudem können sie mit konkreten Beispielen beschrieben werden, um so ein einheitliches Verständnis bei Betreibern und Behörden herzustellen.

- a.) Elektronischer Schutz (z.B.: Zutrittskontrolle, Einbruchsschutz, Videoüberwachung, Perimeterschutz, Einsatz von Detektionsgeräten)
- b.) Mechanischer Schutz: Maßnahmen des Objektschutzes, darunter das Aufstellen von Zäunen, Sperren, Mauern oder Türen
- c.) Personeller Schutz: Bereitstellung von Sicherheitspersonal

Darüber hinaus ist die Aufnahme einer Wirksamkeitsprüfung für Anlagen dringend erforderlich.

10. Sicherheitsüberprüfungen

Sicherheit wird nicht nur durch Regulierungen, durch technische Maßnahmen des Werk- oder des IT-Schutzes erreicht. Ebenso wichtig ist eine entsprechende Schulung der Mitarbeiterinnen und Mitarbeiter zu Präventionszwecken – und die Überprüfung der Vertrauenswürdigkeit von Mitarbeiterinnen und Mitarbeitern, die in besonders sicherheitssensiblen Bereichen tätig sind. Letzteres ist eine Leistung, die vorrangig durch staatliche Sicherheitsbehörden geleistet werden kann – im Rahmen des Geheimschutzes aber auch darüber hinaus, insbesondere in Bezug auf den Schutz von KRITIS. Das Dachgesetz muss dieser Anforderung Rechnung tragen.

Der Referentenentwurf geht auf diese Herausforderung nicht ein.

§ 10 Abs. 3 RefE enthält in der Auflistung potenzieller Maßnahmen lediglich eine Klarstellung, dass das von den Betreibern kritischer Anlagen zu berücksichtigende Sicherheitsmanagement im Hinblick auf Zuverlässigkeitsüberprüfungen der Mitarbeitenden unbeschadet der Vorschriften des

Sicherheitsüberprüfungsgesetzes (SÜG) in Verbindung mit der Sicherheitsüberprüfungsfeststellungsverordnung (SÜFV) sowie unbeschadet weiterer Fachgesetze wie dem Atomgesetz, dem Luftsicherheitsgesetz (LuftSiG), [dem Sicherheitsgewerbegesetz] und der Hafensicherheitsgesetze erfolgt.

Dies ist aus Sicht der deutschen Industrie nicht ausreichend, um den notwendigen Schutzbedarf zu realisieren.

Zurzeit sind personelle Sicherheitsüberprüfungen nur sehr eingeschränkt möglich (außer Telekommunikation / ÜNB / teilweise VNB), wobei zudem mehrmonatige Wartezeiten die Regel und nicht die Ausnahme sind. Dies hemmt die Wirtschaft und ist im Hinblick auf den Fachkräftemangel nicht tolerierbar.

Nur die Nutzung von Terrorlisten / Sanktionslisten bei Bestandspersonal und polizeiliche Führungszeugnisse bei Einstellung sind Optionen, die den Unternehmen zur Verfügung stehen. Der BDI fordert daher, Unternehmen, welche nicht ohnehin dazu verpflichtet sind, die Möglichkeit einzuräumen, Personal mit sicherheitskritischen Aufgaben zu überprüfen / überprüfen zu lassen bzw. in die Lage zu versetzen, sich mit Sicherheitsbehörden auszutauschen. Hierzu bedarf es einer gesetzlichen Grundlage mit justiziablen Mindeststandards und klaren Ausführungsbestimmungen unter Berücksichtigung der Widerspruchsfreiheit auf gesetzlicher und verordnungsrechtlicher Ebene zu schaffen. Ohne eine solche sind „Überprüfungsmaßnahmen“ nach DSGVO untersagt.

Von herausragender Bedeutung bei Überprüfungen von aktuellem oder künftigem Personal ist der Zeitrahmen der Überprüfung. Dieser muss zwingend eng gesetzt sein, da der Fachkräftemangel nicht nur in der deutschen Wirtschaft dazu führt, dass in einem dynamischen Bewerbermarkt Entscheidungen schnell getroffen werden müssen. Denkbar wäre daher auch eine Regelung, die ähnlich dem Atomrecht oder dem LuftSiG eine Überprüfung der Zuverlässigkeit, ggfs. auch unter Entrichtung einer für den Anlagenbetreiber verhältnismäßigen Verwaltungsgebühr, zulässt.

Gleichzeitig unterstützen wir, dass entsprechende bereits existierende Vorschriften über Zuverlässigkeitsüberprüfungen unberührt bleiben.

Die deutsche Industrie würde es sehr begrüßen, wenn Verbände, Unternehmen und Experten eng in den Prozess zur Etablierung und Entwicklung von Überprüfungsverfahren einbezogen würden, um das Verfahren an den Bedarfen der Unternehmen auszurichten. Hierfür bieten die Wirtschaftsverbände ihre einschlägigen Gremien als Foren des Austauschs an.

11. Nationale Risikoanalysen und Risikobewertungen

Der BDI begrüßt die Einführung sektorspezifischer nationaler Risikoanalysen, um die Besonderheiten des jeweiligen Sektors berücksichtigen zu können. Bei den nationalen Risikoanalysen und -bewertungen sollten Wirtschaftsverbände beteiligt werden, um die behördliche Sicht mit den Praxiserfahrungen zu spiegeln und Sektor- und Branchenspezifische Risiken zu ergänzen. Dieses ist auch im Rahmen der CER-Richtlinie vorgesehen.

Bestimmte durch die nationalen Risikoanalysen und -bewertungen identifizierte Risiken (z.B. Sabotageakte, die durch terroristische Vereinigungen oder durch Drittstaaten verübt werden) können durch die Betreiber kritischer Anlagen in ihren Resilienzplänen indes nur bedingt berücksichtigt werden. In diesen Fällen sollten Bund und Länder, wie im Punkt 2 dieser Stellungnahme bereits dargelegt, auch im Sinne der EU-Richtlinien zum Schutz Kritischer Infrastrukturen (CER-Richtlinie) und der allgemeinen Gefahrenabwehr die Betreiber kritischer Anlagen bzw. die kritischen Anlagen angemessen schützen,

Die Risikobetrachtung laut Referentenentwurf ist indes bisher sehr statisch. Es muss die Möglichkeit bestehen, Anpassungen an aktuelle Risikolagen vorzunehmen und unbürokratisch Maßnahmen zu implementieren.

12. Erfüllungsaufwand

Der Entwurf blendet weiterhin Fragen einer Finanzierung aus, der Erfüllungsaufwand wird deutlich unterschätzt.

Finanzierungsmöglichkeiten für zusätzliche Sicherheitsmaßnahmen für Betreiber kritischer Anlagen gilt es daher bereits jetzt genauer abzuschätzen und möglichst rasch zu regeln. Es ist erkennbar, dass die Umsetzung des KRITIS-DachG für die Betreiber erhebliche Kosten verursachen wird, bspw. durch kostspielige Mitarbeiterüberprüfungen, die Umsetzung neuer physischer Sicherheitsmaßnahmen sowie durch den Einsatz von ggfs. zusätzlichem Personal für die Planung erforderlicher Maßnahmen, regelmäßiger Risikoanalysen und den Aufsatz eines Meldesystems sowie weiterer Erfüllungsaufwände, die sich aus dem Gesetz ergeben.

Betreiber kritischer Anlagen dürfen nicht mit zusätzlichen Kosten belastet werden, vor allem da die vergangenen Jahre durch inflationäre Kostensteigerungen in vielen Bereichen geprägt waren. Daher sollte für § 13 des

vorliegenden Entwurfs des KRITIS-DachG eine Kostenerstattungsregelung ergänzt werden.

13. Streichung § 13

Der BDI erkennt im Bereich der physischen Sicherheit keinen Regelungsbedarf, was die Verwendung kritischer Komponenten angeht. Der BDI begrüßt daher ausdrücklich die Streichung von §13 (Einsatz kritischer Komponenten) aus dem neuen RefE.

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 39 Branchenverbände und mehr als 100.000 Unternehmen mit rund acht Mio. Beschäftigten. Die Mitgliedschaft ist freiwillig. 15 Landesvertretungen vertreten die Interessen der Wirtschaft auf regionaler Ebene.

Impressum

Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29, 10178 Berlin
www.bdi.eu
T: +49 30 2028-0

Lobbyregisternummer: R000534

Ansprechpartner

Kerstin Petretto
Senior Manager Sicherheit und Verteidigung
T: +49 30 2028-1710
k.petretto@bdi.eu

BDI Dokumentennummer: D1876