Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland

Inhaltsverzeichnis

1 Einleitung

Das Bundesministerium des Innern und für Heimat (BMI) legt mit dem im September 2023 veröffentlichten Diskussionspapier Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland vor und gibt Gelegenheit zur Stellungnahme. Der Bundesverband Windenergie e.V. (BWE) begrüßt die Regelungsentwürfe des BMI zur Umsetzung der NIS-2-Richtlinie, sieht jedoch noch eine Reihe von offenen Fragen und Unklarheiten, die im weiteren Prozess adressiert werden sollten.

Die Windenergiebranche unterstützt ausdrücklich das Ansinnen des BMI, weitere Maßnahmen zur Stärkung der Cybersecurity in Deutschland zu verabschieden**.** Für Unternehmen in der Windenergiebranche gelten bereits seit Inkrafttreten der BSI-Kritisverordnung Anforderungen an die Umsetzung und den Nachweis von entsprechenden Maßnahmen. Zu unterscheiden sind hierbei die beiden Kategorien „Energieerzeugungsanlagen“ und „Anlagen oder Systeme zur Steuerung/Bündelung elektrischer Leistung“ (sog. Aggregatoren/Virtuelle Kraftwerke). **Mit dem jetzigen Entwurf zur Umsetzung der NIS-2-Richtlinie kommen zwei neue Kategorien „besonders wichtige Einrichtung“ und „wichtige Einrichtung“ hinzu.** Bei diesen geht es bei der Bestimmung der Betroffenheit nicht wie bislang um Schwellenwerte in Bezug auf die installierte Nettoleistung, sondern um eine Kombination aus Sektor- und Unternehmensgröße (Mitarbeiterzahl und Umsatz/Bilanz).

Vor diesem Hintergrund werden voraussichtlich weitere Mitgliedsunternehmen im BWE betroffen sein. Der BWE sieht hier Klärungsbedarf zu einer Reihe von Punkten, die in dieser Stellungnahme näher erläutert sind. Im Rahmen der Umsetzung der Richtlinie dürfen dabei keine neuen bürokratischen Hemmnisse für Betreibergesellschaften, deren Partnerunternehmen oder verbundene Unternehmen von Windenergieanlagen/Windparks entstehen, hier bedarf es klarer und praxistauglicher Regelungen. Unter anderem sollten diese mit dem KRITIS-Dachgesetz und den bestehenden Regelungen abgeglichen und gegebenenfalls angepasst werden. Weiterhin ist es zentral, dass etwaige Konkretisierungen der Regelungen in noch zu verabschiedenden Verordnungen rechtzeitig kommuniziert werden, damit die Unternehmen frühzeitig mit der Umsetzung beginnen können.

In dieser Stellungnahme beziehen wir uns auf den Stand des NIS 2 Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), das auszugsweise in dem Diskussionspapier vom 27.09.2023 veröffentlicht wurde.

Bei der Umsetzung der Richtlinie in nationales Recht erachtet der BWE daher insbesondere die folgenden Punkte für wichtig:

- Betroffenheit von Betreibergesellschaften, die Partnerunternehmen haben oder verbundene Unternehmen sind/ Definition der KMU
- Umsetzbarkeit der unter § 30 genannten Risikomaßnahmen
- Anpassung und Abgleich mit dem KRITIS-Dachgesetz/ Klarstellung von Fristen zur Umsetzung und Nachweisen
- Information über zu erlassende Verordnungen/ kritische Anlagen

2 Betroffenheit von Betreibergesellschaften, die Partnerunternehmen haben oder verbundene Unternehmen sind

Betreiber von Windenergieanlagen/Windparks (Betrieb von Erzeugungsanlagen gem. § 3 Nr. 18 d EnWG) sind in Deutschland sehr heterogen aufgestellt, teilweise mit unterschiedlichen Sparten (Planung/Projektierung, Windparkmanagement u.a.), mit Partnerunternehmen oder im Unternehmensverbund. Der Betrieb der Windenergieanlagen/Windparks wird vielfach in eigene Gesellschaften ausgelagert, wobei hier vorrangig Rechtsformen wie die GmbH, die GmbH & Co. KG, die GbR oder die eingetragene Genossenschaft (e.G.) gewählt werden.

Nach unserer Auffassung ist bei der Bestimmung, ob ein Unternehmen in den Anwendungsbereich des BSI-Gesetzes (BSI-G) fällt, jedes Unternehmen (jede rechtlich selbständige Einheit) einzeln zu betrachten. Unter Berücksichtigung der Mitarbeiterzahlen oder der Jahresumsätze/-bilanzsummen werden daher viele Betreibergesellschaften selbst nicht unmittelbar unter die Kategorien „wichtige Einrichtungen“ oder „besonders wichtige Einrichtungen“ fallen. Dies wird voraussichtlich lediglich für Betreibergesellschaften größerer Windparks gelten.

Jedoch sind für den Fall, dass eine Tochtergesellschaft eine Betreibergesellschaft eines Windparks ist und die Muttergesellschaft das technische und kaufmännische Windparkmanagement übernommen hat, zwei Betrachtungen vorzunehmen.

In § 28 Abs. 3 wird für die Bestimmung von Mitarbeiterzahl, Jahresumsatz und Jahresbilanzsumme auf die Empfehlung 2003/361/EG verwiesen, um festzustellen, ob ein Unternehmen unter die in § 28 des Regelungsentwurfs genannten Kategorien („besonders wichtige Einrichtungen“ und „wichtige Einrichtungen“) fällt. Diese sieht grundsätzlich vor, dass die Kennzahlen von sog. „Partnerunternehmen“ oder „verbundenen Unternehmen“ – zumindest anteilig – zugerechnet werden können. Nach dieser Berechnungsmethode würden viele Betreibergesellschaften, die Tochtergesellschaften größerer Unternehmen sind, aufgrund der Hinzurechnung der Mitarbeiterzahlen oder Jahresumsätze/-bilanzsummen mindestens unter die Kategorie „wichtige Einrichtung“, wenn nicht sogar unter die Kategorie „besonders wichtige Einrichtung“, einzuordnen sein.

Eingeschränkt wird dies gemäß § 28 Abs. 3 Satz 2 des Regelungsentwurfs zum BSI-G, indem die Hinzurechnung der Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung dann nicht gelten soll, wenn das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse unabhängig von seinem Partner oder verbundenen Unternehmen ist. Eine solche Unabhängigkeit dürfte jedoch größtenteils bei Betreibergesellschaften, die Tochtergesellschaften von größeren Unternehmen sind, nicht zutreffen. Vielmehr werden diese von der Muttergesellschaft über deren informationstechnische Systeme, Komponenten und Prozesse verwaltet. Folglich fallen Betreibergesellschaften, die Tochtergesellschaften größerer Mutterunternehmen sind, in den Anwendungsbereich des § 28 und sind somit betroffen (teilweise können sie sogar unter die Kategorie „besonders wichtige Einrichtungen“ fallen).

Die Muttergesellschaft selbst könnte im Bereich des Windparkmanagements unter eine „(besonders) wichtige Einrichtung“ subsumiert werden, wenn sie Dienstleistungen anbietet, die z. B. dem Betrieb von Erzeugungsanlagen gem. § 3 Nr. 18 d EnWG zuzuordnen sind. Zudem könnte sie auch als „Betreiber

kritischer Anlagen“ gelten und somit gemäß § 28 Abs. 1 Nr. 4 eine „besonders wichtige Einrichtung“ sein. Folglich könnte auch das übergeordnete Unternehmen betroffen sein.

Im Übrigen bleibt für uns die Abgrenzung, wann die „Hinzurechnung“ von Zahlen anderer Gesellschaften nach der o.g. Kommissionsempfehlung stattfinden soll und wann nicht, unklar. Denn bislang wird im deutschen Recht die Frage, welche juristische Person Adressatin der Pflichten aus dem BSI-G ist, ohnehin danach bestimmt, ob eine Gesellschaft „rechtlich, wirtschaftlich und tatsächlich“ Einfluss auf eine in der NIS-1-Richtlinie definierte Anlage hat. Wir gehen davon aus, dass diese Kriterien auch unter NIS-2 erhalten bleiben. Daher bleibt in § 28 Abs. 3 Satz 2 nur das Kriterium „Unabhängigkeit“ als substanzielles Kriterium übrig – denn wenn eine Konzerngesellschaft gar keinen eigenen „wirtschaftlichen, rechtlichen und tatsächlichen“ Einfluss hätte, käme sie ohnehin schon gar nicht als NIS-2-/BSI-G-Adressatin in Betracht. Der Begriff „Unabhängigkeit“ ist bislang allerdings so wenig konkretisiert, dass die Subsumtion, ob hinzugerechnet werden soll oder nicht, nach dem jetzigen Entwurf sehr schwerfallen wird.

Zusammenfassend ist Folgendes festzustellen: Sollten bei der Berechnung der Kriterien Mitarbeiterzahl und Umsatz/Bilanz die in § 28 genannten Schwellenwerte überschritten sein, wäre das jeweilige Unternehmen betroffen.

Fazit:

Die Einordnung von Betreibergesellschaften, die Tochtergesellschaften großer Mutterunternehmen sind, als „(besonders) wichtige Einrichtungen“ ist aus unserer Sicht unklar und so wie wir sie aktuell interpretieren nicht zielführend. Gerade ihre Abhängigkeit im Hinblick auf die informationstechnischen Systeme, Komponenten und Prozesse, auf die die Tochtergesellschaften keinen Einfluss haben, führt dazu, dass eine Hinzurechnung der Daten der Muttergesellschaft erfolgt – die Tochtergesellschaften somit nicht in den Genuss der Ausnahme des § 28 Abs. 3 Satz 2 kommen – und somit die Tochtergesellschaften zu einer „(besonders) wichtigen Einrichtung“ werden. Den Tochtergesellschaften werden damit Pflichten aufgebürdet, auf deren Umsetzung sie keinen Einfluss nehmen können. Sie können dies lediglich durch vertragliche Verpflichtungen an ihre Muttergesellschaft sicherstellen. Dies könnte in der Vertragsgestaltung problematisch im Hinblick auf das Über-/Unterstellungsverhältnis sein.

Der von dem Gesetz gewollte Effekt läuft hier unseres Erachtens ins Leere und verpflichtet (zusätzlich) die falschen Unternehmen. Die eigentlichen Akteure, nämlich Betreiber großer Windparks sowie Windparkmanager im Rahmen der Anlagenüberwachung (falls ein Fernsteuereingriff möglich ist), fallen größtenteils unter das BSI-G und sind somit selber verpflichtet, die Vorgaben einzuhalten.

Zudem stellt die Betroffenheit von Tochtergesellschaften als Betreibergesellschaften eine Ungleichbehandlung im Vergleich zu anderen selbständigen Betreibergesellschaften dar. Diese haben ebenfalls keinen Einfluss auf die IT-Sicherheit, da sie die Steuerung und Verwaltung ihrer Windenergieanlage ebenfalls in die Hände von Windparkmanagern gegeben haben. Die Verpflichtungen des BSI-G treffen sie aber nicht.

Vorschlag des BWE:

In der NIS-2-Richtlinie selbst findet sich keine Regelung, die der Regelung in § 28 Abs. 3 entspricht. Lediglich in Nr. 16 der Erwägungsgründe der NIS-2-Richtlinie steht die Empfehlung, die Unverhältnismäßigkeiten, die durch eine Hinzurechnung der Daten der Partner- oder verbundenen Unternehmen entstehen könnten, zu berücksichtigen. Zudem wird vorgeschlagen, wie Mitgliedstaaten dies regeln könnten. Dieser Vorschlag hat nun Einzug in § 28 Abs. 3 des Regelungsentwurfs des BSI-G gefunden.

Aus unserer Sicht ist es richtig, dass der Gesetzgeber der Empfehlung gefolgt ist, jedoch ist diese Regelung unvollständig und lässt diejenigen Betreibergesellschaften unberücksichtigt, die vollständig in der Abhängigkeit ihrer Muttergesellschaft stehen (da keine Mitarbeiter und Infrastruktur).

Hier könnte der Gesetzgeber eine weitere Regelung einfügen, um diese Unverhältnismäßigkeit zu berücksichtigen. Dies wäre auch nicht im Widerspruch zur NIS-2-Richtlinie, sondern würde der Empfehlung in Nr. 16 der Erwägungsgründe folgen.

2.1 Definition der KMU

Bei der Bestimmung von Mitarbeiterzahl, Jahresumsatz und Jahresbilanzsumme und der Definition von „besonders wichtigen Einrichtung“ und „wichtige Einrichtung“ (§ 28 Abs. 1 und § 28 Abs. 2) verweist der Gesetzgeber auf die Kommissionsempfehlung 2003/361 EG.

In Artikel 2 der Kommissionsempfehlung 2003/361 EG – Mitarbeiterzahlen und finanzielle Schwellenwerte zur Definition der Unternehmensklassen – wird neben der Mitarbeiterzahl bei der Erreichung eines finanziellen Schwellenwertes entweder der Jahresumsatz **oder** die Jahresbilanzsumme herangezogen. Abweichend hierzu wird im NIS-2UmsuCG (§ 28 Abs. 1 Nr. 1b und § 28 Abs. 2 Nr. 1b) der Jahresumsatz **und** die Jahresbilanzsumme zur Erreichung eines finanziellen Schwellenwertes und damit zur Bestimmung der „besonders wichtigen Einrichtung“ und „wichtigen Einrichtung“ herangezogen. Beide Schwellenwerte müssen also erreicht sein.

Inwiefern können die in der Kommissionsempfehlung 2003/361 EG (hier zur Definition der Unternehmensklassen) genannten Größenschwellen für Mitarbeiterzahl, Jahresumsatz und Jahresbilanzsumme zur Definition der „besonders wichtigen Einrichtung“ und „wichtigen Einrichtung“ angewandt werden?

3 Umsetzbarkeit der unter § 30 genannten Risikomaßnahmen

Für die betroffenen Betreibergesellschaften sind die in § 30 genannten Risikomaßnahmen nicht umsetzbar, da sie keinen Einfluss auf die informationstechnischen Systeme, Komponenten und Prozesse haben, wenn sie das Windparkmanagement an geeignete Dienstleister ausgelagert haben. Die Pflichten müssten vertraglich auf die Dienstleister übertragen werden.

Für größere Unternehmen sind diese Maßnahmen unseres Erachtens umsetzbar.

3.1 „Sicherheit des Personals“ aus § 30 Abs. 2 Nr. 9

In § 30 Abs. 2 Nr.9 wird als umzusetzende Maßnahme die „Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen“ gefordert.

Insbesondere zur Sicherheit des Personals ergeben sich Fragen. Ist hiermit die Überprüfung des Personals, wie z.B. unter Punkt A.7.1 des Annexes der DIN ISO 27001 oder Nr. 56 der Konkretisierung der Anforderungen an die gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen gemeint?

3.2 Cybersicherheitszertifizierung aus § 30. Abs. 6

In § 30 Abs. 6 heißt es: Besonders wichtige Einrichtungen und wichtige Einrichtung dürfen durch Rechtsverordnung nach § 57 Abs. 4 bestimmte IKT-Produkte, IKT-Dienste und IKT-Prozesse nur verwenden, wenn diese über eine Cybersicherheitszertifizierung gemäß europäischer Schemata nach Artikel 49 der Verordnung (EU) 2019/881 verfügen. Wir verstehen § 30 Abs. 6 i.V.m. § 57 Abs. 2 des Entwurfes so, dass der deutsche Gesetzgeber von der Öffnungsklausel in Art. 24 Abs. 1 der NIS-2-Richtlinie Gebrauch machen möchte und das BMI dies in einer entsprechenden Verordnung konkretisieren soll. Eine solche Zertifizierungspflicht würde betroffene Unternehmen sehr streng regulieren und ihre Umsetzung würde einen großen Zeitvorlauf erfordern. Daher wäre es wichtig, dass betroffene Unternehmen rechtzeitig wissen, ob, wann und welche Pflichten sie zur Cybersicherheitszertifizierung treffen werden.

Die in der Windenergie eingesetzten IKT-Produkte, IKT-Dienste und IKT-Prozesse sind i.d.R. branchenspezifische Produkte und speziell für den Windparkbetrieb konzipiert (SCADA – Systeme wie Windparkregler, Parkrechner, Condition Monitoring Systeme, Betriebsführungssoftware u.a.).

Angesichts der Tatsache, dass noch kein Entwurf für die nach § 57. Abs. IV geforderte Ministeriumsverordnung bekannt ist und die Schemata nach Artikel 49 der Verordnung (EU) 2019/881 nach unserem Wissen noch nicht finalisiert sind, herrscht jedoch noch viel Unklarheit, was diese verpflichtende Cybersicherheitszertifizierung konkret für Unternehmen bedeuten würde.

Für unsere Mitglieder wäre daher wichtig, über folgenden Punkte rechtzeitig informiert zu werden: Welche Produkte und Dienstleistungen plant das BMI in seiner Verordnung hier einzubeziehen? Wie genau sähe der Zertifizierungsprozess aus und wie können hierdurch Verzögerungen, bspw. für die Errichtung und den Betrieb von Windenergieanlagen/Windparks vermieden werden? Welche Timeline gibt es für die Schemata und die Verordnung nach § 57 Abs. 4 des Entwurfes und wird diese zeitgleich mit dem BSI-G neu in Kraft treten oder erst später, ggf. mit einer Übergangsfrist?

4 Anpassung und Abgleich mit dem KRITIS-Dachgesetz/ Klarstellung von Fristen zur Umsetzung und Nachweisen

Die Anpassung und der Abgleich zu bestehenden Regulierungen/Gesetzen wie dem zukünftig geplanten KRITIS-Dachgesetz oder spezialrechtlichen Regelungen (z.B. Network Code on Cybersecurity, IT-Sicherheitskatalog der BNetzA) ist aus unserer Sicht dringend erforderlich. Betroffene Unternehmen können somit eindeutig identifiziert werden und geeignete branchenspezifische Maßnahmen umsetzen.

Den angepassten Zeitraum von drei Jahren zum Nachweis von Cybersecurity-Maßnahmen bei kritischen Anlagen halten wir für einen realistischen und pragmatischen Ansatz, da hier sowohl BSI als auch Zertifizierungs- und Auditierung-Stellen und nicht zuletzt die Unternehmen selber personell entlastet werden. Wir gehen davon aus, dass damit die aktuelle Gesetzeslage (§ 8b Abs. 3 BSI-G in Verbindung Anhang 1 Teil 1 Nr. 3 der KritisV) mit einer Nachweispflicht alle zwei Jahre ersetzt würde. Uns ist jedoch nicht klar, wie der Übergang unter der jetzigen KritisV zu der neu zu erlassenden Verordnung mit längeren Nachweisfristen gestaltet werden wird. Darüber würden wir uns nähere Informationen wünschen.

Ebenfalls heißt es in der Gesetzesbegründung (zu Artikel 29 (Inkrafttreten, Außerkrafttreten, zu Abs. 1)), dass bei einer Verkündung im März 2024 den Einrichtungen noch sechs Monate für die Umsetzung der in diesem Gesetz enthaltenen Verpflichtungen zur Verfügung stehen. Der hier genannte Zeitpunkt ist der letzte Quartalsbeginn vor Ablauf der Umsetzungsfrist des Artikel 41 NIS-2-Richtlinie am 17. Oktober 2024. Diese Frist halten wir in Anbetracht der notwendigen vorherigen Feststellung der Betroffenheit, der umzusetzenden Maßnahmen und ggf. einer erforderlichen Hinzuziehung von Fachfirmen bzw. Fachpersonal für zu kurz gewählt.

5 Information über zu erlassende Verordnungen/ kritische Anlagen

Der Entwurf verweist in wichtigen Teilen auf Verordnungen, die nach der Verordnungsermächtigung in § 57 noch zu erlassen sind. In diesen Verordnungen werden für unsere Mitglieder wesentliche Pflichten konkretisiert, etwa die Frage, wer eine „kritischen Anlage“ betreibt und damit deutlich mehr Pflichten hat, oder für welche IKT-Produkte verpflichtende Cybersicherheitszertifizierungen verordnet werden (siehe dazu bereits oben). Beispielsweise ist aus dem aktuellen BSI-G-Entwurf nicht ersichtlich, ob in der neuen Kategorie „Kritische Anlagen“ die bisherigen „kritischen Infrastrukturen“ nahtlos weitergeführt werden sollen oder ob sich hier Änderungen im Vergleich zur BSI-KritisV ergeben (z.B. bei den betroffenen Anlagen in einzelnen Sektoren oder Schwellenwerten siehe auch unsere Frage zu Übergangsregelungen bezüglich des Turnus bei den Nachweispflichten). Unklar ist z.B. auch, ob es wie bislang weiterhin „gemeinsame Betreiber“ einer kritischen Anlage oder einer wichtigen/besonders wichtigen Einrichtung geben soll.

Dasselbe gilt für die Verordnungen, die nach § 15 des jetzigen Entwurfes des KRITIS-Dachgesetzes (Referentenwurf vom 25.07.2023) zu erlassen sind. Auch hier stehen die konkreten Angaben zur sachlichen Anwendung erst in einer Verordnung, über die bislang weder der Inhalt noch die geplante

Timeline bekannt sind. Es besteht ein dringendes Interesse der betroffenen Unternehmen, diese wichtigen Konkretisierungen zu erfahren, um ggf. rechtzeitig mit der Umsetzung zu beginnen.

Impressum

Bundesverband WindEnergie e.V.
EUREF-Campus 16
10829 Berlin
030 21234121 0
info@wind-energie.de
www.wind-energie.de
V.i.S.d.P. Wolfram Axthelm

Foto
Pixabay (CCO)

Der Bundesverband WindEnergie e.V. ist als registrierter Interessenvertreter im Lobbyregister des Deutschen Bundestages unter der Registernummer R002154 eingetragen.
Den Eintrag des BWE finden Sie hier.

Ansprechpartner

Stefan Grothe
Abteilung Facharbeit Wind
Fachreferent Technik
fachgremien@wind-energie.de

Datum

17. Oktober 2023