Stellungnahme

BWE
Bundesverband WindEnergie

NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Referentenentwurf des BMI vom 26.06.2024

Juli
2024

Inhalt

1 Einleitung 3

2 Betroffenheit von Betreibergesellschaften mit Partnerunternehmen oder als Teil verbundener Unternehmen 4

3 Umsetzbarkeit der unter § 30 genannten Risikomaßnahmen 6

3.1 „Sicherheit des Personals“ aus § 30 Abs. 2 Nr. 9 6

3.2 Cybersicherheitszertifizierung aus § 30 Abs. 6 6

3.3 Schnittstelle zum Net Zero Industry Act 7

4 Anpassung und Abgleich mit dem KRITIS-Dachgesetz/ Fristen zur Umsetzung und Nachweisen 8

5 Information über zu erlassende Verordnungen/ Beteiligung der Verbände 8

6 Klarstellung der Zertifizierungspflicht ausschließlich für kritische Anlagen gemäß BSI-KritisV 9

1 Einleitung

Das Bundesministerium des Innern und für Heimat (BMI) legt mit dem am 26. Juni 2024 veröffentlichten Referentenentwurf 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 im vorliegenden Referentenentwurf (siehe auch Stellungnahmen zu dem im September 2023 veröffentlichen Diskussionspapier und zu dem am 07. Mai 2024 veröffentlichten Referentenentwurf), sieht jedoch weiterhin einige offene Fragen und konkreten Änderungsbedarf, auf den wir im Einzelnen in dieser Stellungnahme eingehen. Zunächst das Wichtigste in Kürze:

Der BWE unterstützt:

- Das Ansinnen des BMI, weitere Maßnahmen zur Stärkung der Cybersicherheit in Deutschland zu verabschieden.

Der BWE kritisiert:

- Bei der Klärung der Betroffenheit von Unternehmen ist der Begriff „Unabhängigkeit“ nicht konkretisiert; zudem ist die Abgrenzung, wann eine „Hinzurechnung“ der Daten von Partner- oder verbundenen Unternehmen erfolgen soll, unklar.
- Fehlende Konkretisierung der Maßnahme zur Prüfung des Personals nach § 30 Abs. 2 Nr. 9.

Der BWE regt an:

- Bei der Bestimmung, ob ein Unternehmen in den Anwendungsbereich des BSI-Gesetzes fällt, ist jedes Unternehmen einzeln zu betrachten.
- Vor allem braucht es eine Differenzierung für den Fall, dass eine Tochtergesellschaft eine Betreibergesellschaft eines Windparks ist und die Muttergesellschaft das technische und kaufmännische Windparkmanagement übernommen hat.
- Es sollte klargestellt werden, dass die Zertifizierungspflicht ausschließlich für kritische Anlagen gemäß BSI-KritisV gilt.
- Die Unternehmen brauchen rechtzeitige Informationen, wann und welche Pflichten sie zur Cybersicherzeitszertifizierung treffen.
- Es sollte die Chance genutzt werden, dass NIS-2-Umsetzungs- und Cybersicherheits-stärkungsgesetz mit dem Net Zero Industry Act und den dazugehörigen Präqualifikationskriterien zu verbinden.
- Bei der bevorstehenden Entwicklung der verschiedenen Umsetzungsverordnungen sollten in jedem Fall die Wirtschaftsverbände beteiligt werden.

2 Betroffenheit von Betreibergesellschaften mit Partnerunternehmen oder als Teil verbundener Unternehmen

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. 1 Nr. 4 a und b und § 28 Abs. 2 Nr. 3 a und b i.V.m. § 28 Abs. 3 des Regelungsentwurfs zum BSI-G 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. Ob diese Kriterien auch bei der Bestimmung der „Einrichtung“ unter NIS-2 erhalten bleiben, ist bisweilen ungeklärt. Sofern dies der Fall sein sollte, 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, nach dem jetzigen Entwurf sehr schwerfallen wird.

Weitere Abgrenzungsschwierigkeiten ergeben sich dadurch, dass der Regelungsentwurf gegenwärtig auf die Gesellschaft abstellt, „die anderen natürlichen oder juristischen Personen entgeltlich Waren oder Dienstleistungen anbieten, die einer der in Anlage 1 bestimmten Einrichtungsarten zuzuordnen ist“ (vgl. § 28 Abs. 1 Nr. 4). Dies kann jedenfalls so auszulegen sein, dass jeweils die mit dem Kunden vertragsschließende Gesellschaft als „Einrichtung“ und damit unter dem BSI-G Verpflichtete abzustellen wäre. Hierbei wird es sich aber nicht zwingend auch um diejenige Gesellschaft handeln, die „rechtlichen, wirtschaftlichen und tatsächlichen“ Einfluss auf die relevanten Anlagen hat.

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 selbst 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.

3 Umsetzbarkeit der unter § 30 genannten Risikomaßnahmen

Für die betroffenen Betreibergesellschaften, die das Windparkmanagement an geeignete Dienstleister ausgelagert haben, sind die in § 30 genannten Risikomaßnahmen nicht umsetzbar, da sie keinen Einfluss auf die informationstechnischen Systeme, Komponenten und Prozesse 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 ergibt sich die Frage: 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 Einrichtungen dürfen durch Rechtsverordnung nach § 58 Absatz 3 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 in Verbindung mit § 58 Absatz 3 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 strenger als zuvor regulieren und ihre Umsetzung würde einen gewissen 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 § 58 Absatz 3 geforderte Ministeriumsverordnung bekannt ist und die Schemata nach Artikel 49 der Verordnung (EU) 2019/881 nach unserem Wissen noch nicht finalisiert sind, herrscht zurzeit 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, beispielsweise 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?

3.3 Schnittstelle zum Net Zero Industry Act

Diese Fragen sind insbesondere vor dem Hintergrund der voraussichtlichen finalen Verabschiedung des Net Zero Industry Act (NZIA) durch den Rat der Europäischen Union am 27. Mai 2024 von großer Relevanz: Laut NZIA müssen die EU-Mitgliedstaaten nach Inkrafttreten der Verordnung innerhalb von 18 Monaten sogenannten Präqualifikations- und Zuschlagskriterien für Ausschreibungen von Erneuerbaren Energien einführen.

Wenngleich die Details der Ausgestaltung dieser Kriterien noch offen sind und unter anderem mit einem Durchführungsrechtsakt der Europäischen Kommission präzisiert werden sollen, ist Cyber- und Datensicherheit als ein Präqualifikationskriterium im NZIA festgelegt.

Aus Sicht des BWE sollte Cybersicherheit daher auf dem risiko-basierten Ansatz wie beispielsweise der NIS2-Richtlinie beruhen und leicht überprüfbar sein. Das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz kann dieses Ziel erreichen, wenn bestimmte Rahmenbedingungen erfüllt werden. Hersteller von Windenergieanlagen (wie auch unabhängige Serviceanbieter, Netzbetreiber, Stromvermarkter, je nach Zugriffsberechtigung auch Betriebsführer) haben die Möglichkeit aus der Ferne auf ihre Anlagen zuzugreifen und diese auch im Bedarfsfall abzuschalten. Der deutsche Gesetzgeber sollte hier mit dem Instrument des NZIA und nachgelagerten Umsetzungsgesetzen wie zur NIS-2-Richtlinie und entsprechenden Präqualifikationskriterien auf 100% der EE-Ausschreibungsvolumina für Windenergie dafür Sorge tragen, dass Akteuren aus nicht-demokratischen Ländern keine Möglichkeit des Fernzugriffs auf elementare Bestandteile der deutschen Energieversorgung gegeben wird.

Die im Referentenentwurf genannte mögliche Rechtsverordnung zu einer Cybersicherheitszertifizierung von IKT-Produkten, IKT-Diensten und IKT-Prozessen sollte daher sicherstellen, dass der Datenverkehr

beim Betrieb von Windenergieanlagen ausschließlich über Datenverarbeitungssysteme innerhalb der EU erfolgt.

4 Anpassung und Abgleich mit dem KRITIS-Dachgesetz/ 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 selbst 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.

5 Information über zu erlassende Verordnungen/ Beteiligung der Verbände

Der Entwurf verweist in wichtigen Teilen auf Verordnungen, die nach der Verordnungsermächtigung in § 58 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 Abschnitt 3.2). Eine Anhörung von Vertretern der Wissenschaft, der betroffenen Einrichtungen und der betroffenen Wirtschaftsverbände ist aus unserer Sicht dringend erforderlich.

Dasselbe gilt für die Verordnungen, die nach § 15 des jetzigen Entwurfes des KRITIS-Dachgesetzes (Referentenwurf vom 25. Juli 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.

6 Klarstellung der Zertifizierungspflicht ausschließlich für kritische Anlagen gemäß BSI-KritisV

Der Änderungsvorschlag in § 5c Abs. 2 EnWG-E besagt, dass Betreiber von Energieerzeugungsanlagen, die als besonders wichtige und wichtige Einrichtungen im Sinne des § 28 BSI- G zu klassifizieren sind, ebenfalls den IT-Sicherheitskatalog gemäß § 11 Absatz 1a des EnWG einhalten und sich nach gegenwärtiger Fassung des IT-Sicherheitskatalogs auch zertifizieren lassen müssen.

Da sich die Zertifizierungspflicht nicht aus dem Gesetz, sondern aus dem IT-Sicherheitskatalog)[1] selbst ergibt, bitten wir um Klarstellung, dass eine Zertifizierungspflicht über den von der BNetzA erstellten IT-Sicherheitskatalog ausschließlich kritische Anlagen betrifft, die unter der aktuell gültigen BSI-KritisV hierunter klassifiziert werden.

[1] Bundesnetzagentur (2005): IT-Sicherheitskatalog 08 2015 Abschnitt F.I. – LINK.

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

AdobeStock

Haftungsausschluss

Die in diesem Papier enthaltenen Angaben und Informationen sind nach bestem Wissen erhoben, geprüft und zusammengestellt. Eine Haftung für unvollständige oder unrichtige Angaben, Informationen und Empfehlungen ist ausgeschlossen, sofern diese nicht grob fahrlässig oder vorsätzlich verbreitet wurden.

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 | Fachreferent Technik| s.grothe@wind-energie.de

Autor*innen

Stefan Grothe | Fachreferent Technik
Luca Liebe | Referent Politik Europa
Kristina Hermann | Leiterin Facharbeit Windenergie

Datum

03. Juli 2024