Stellungnahme

BWE
Bundesverband WindEnergie

NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Referentenentwurf des BMI vom 23.06.2025

Juli
2025

Inhalt

1 Das Wichtigste in Kürze 3

2 Einleitung 3

3 Behördliche Zuständigkeit für Cybersicherheitsmaßnahmen im Energiesektor 4

4 Umsetzbarkeit aufgeführter Risikomanagementmaßnahmen 5

4.1 Mindestvorgaben für Risikomanagementmaßnahmen im IT- Sicherheitskatalog 5

4.2 Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen 6

5 Klarstellung der Zertifizierungspflicht ausschließlich für kritische Anlagen gemäß BSI-KritisV 7

6 Untersagung des Einsatzes kritischer Komponenten 8

1 Das Wichtigste in Kürze

Wir begrüßen:

- die behördliche Zuständigkeit der Bundesnetzagentur (BNetzA) als zentrale Stelle für Cybersicherheitsmaßnahmen im Energiesektor.
- umzusetzende Risikomaßnahmen für kritische Anlagen, um die Sicherheit und Resilienz unserer Energieinfrastruktur zu stärken.
- die Erweiterung der Befugnisse des BMI, insbesondere hinsichtlich der Untersagung des Einsatzes von kritischen Komponenten.

Wir kritisieren:

- Für kleinere Windparkgesellschaften sind die genannten Risikomaßnahmen nicht umsetzbar.

Wir regen an:

- Differenzierung der Anforderungen bei umzusetzenden Risikomaßnahmen für die unterschiedlichen Einrichtungskategorien.
- zeitnahe und präzise Umsetzung der umzusetzenden Risikomaßnahmen in Form konkret ausgestalteter Sicherheitskataloge durch die Bundesnetzagentur.
- BNetzA als zentrale Stelle auch bei der Kommunikation von Sicherheitsvorfällen zu installieren.
- Klarstellung der Zertifizierungspflicht ausschließlich für kritische Anlagen gemäß BSI-KritisV.

2 Einleitung

Das Bundesministerium des Innern und für Heimat (BMI) legt mit dem am 23. Juni 2025 veröffentlichten Referentenentwurf Regelungen zur Umsetzung der NIS-2-Richtlinie in Deutschland vor und gibt Gelegenheit zur Stellungnahme. Der Bundesverband Windenergie e.V. (BWE) hatte sich bereits zu dem im Mai 2024 veröffentlichten Referentenentwurf des BMI zur Umsetzung der NIS-2-Richtlinie geäußert. Der BWE begrüßt die Regelungsentwürfe des BMI im vorliegenden Referentenentwurf, sieht jedoch weiterhin einige offene Fragen und Unklarheiten, die im weiteren Gesetzgebungsprozess adressiert werden sollten.

Die Windenergiebranche unterstützt ausdrücklich das Ansinnen des BMI, weitere Maßnahmen zur Stärkung der Cybersicherheit in Deutschland zu verabschieden**.** Angriffe auf unsere IT-Infrastruktur und die Datenbestände von Unternehmen nehmen zu. Die Reform ist daher zentral für die Stärkung der Resilienz und IT-Sicherheit der deutschen Wirtschaft. Für Unternehmen in der Windenergiebranche gelten bereits seit Inkrafttreten der BSI-Kritisverordnung Anforderungen an die Umsetzung und den Nachweis von entsprechenden Maßnahmen. **Mit dem aktuellen Referentenentwurf zur Umsetzung der NIS-2-Richtlinie kommen zwei neue Kategorien hinzu: „besonders wichtige Einrichtung“ und „wichtige Einrichtung“.** Vor diesem Hintergrund werden weitere Mitgliedsunternehmen des BWE betroffen sein.

Bei der Umsetzung der Richtlinie ist es daher wichtig, dass keine neuen bürokratischen Hemmnisse für Betreibergesellschaften, Planer bzw. Projektierer und Hersteller von Windenergieanlagen entstehen. Hier bedarf es klarer und praxistauglicher Regelungen. Insbesondere bei möglichen Zertifizierungen auch für die neuen Einrichtungskategorien sieht der BWE Klärungsbedarf, die in dieser Stellungnahme erläutert sind.

3 Behördliche Zuständigkeit für Cybersicherheitsmaßnahmen im Energiesektor

Der BWE begrüßt ausdrücklich, dass die Verantwortung für Cybersicherheitsmaßnahmen im Energiesektor zukünftig zentral bei der Bundesnetzagentur (BNetzA) liegt. Dies betrifft sowohl kritische Anlagen als auch die neu eingerichteten Kategorien „besonders wichtige“ und „wichtige“ Einrichtungen. Die Ausgestaltung erfolgt in den jeweiligen IT-Sicherheitskatalogen. In diesem Zusammenhang begrüßen wir auch die gestärkte Rolle des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Demnach werden Anforderungen an einen angemessenen Schutz in den IT- Sicherheitskatalogen im Einvernehmen mit dem BSI bestimmt.

Wir sehen den Mehrwert insbesondere darin, dass bei Partner- oder verbundenen Unternehmen ein gemeinsames Informationsmanagementsystem für einen definierten Geltungsbereich auf Basis von ISO/IEC 27001 implementiert werden kann. Dies ist vorteilhaft, da die Betriebsführungssparte häufig schon entsprechenden Anforderungen über die Kategorie „digitaler Energiedienst“ unterliegt. Somit muss nicht jede ausgegliederte Windparkgesellschaft eigenständig Anforderungen erfüllen und nachweisen (siehe auch BNetzA „Mitteilung zur Zertifizierung nach IT-Sicherheitskatalog § 11 Abs. 1a und 1b EnWG im Fall einer Betriebsführung durch Dritte“). Positiv hervorzuheben ist auch, dass die Betreiber und deren Branchenverbände explizit an der Festlegung und Aktualisierung der IT-Sicherheitskataloge beteiligt werden sollen.

Grundsätzlich ist aus unserer Sicht wichtig, dass im Gesetzentwurf an allen Stellen klar geregelt ist, welche Behörde oder welches Ministerium für welche Bereiche zuständig ist und für die betroffenen Unternehmen der relevante Ansprechpartner ist.

Vorschlag des BWE:

Aus unserer Sicht wäre es daher sinnvoll und folgerichtig, dass auch die Kommunikation bei Sicherheitsvorfällen mit der BNetzA geführt wird, insbesondere da es sich um eine gemeinsame Meldestelle handelt.

4 Umsetzbarkeit aufgeführter Risikomanagementmaßnahmen

4.1 Mindestvorgaben für Risikomanagementmaßnahmen im IT-Sicherheitskatalog

Aus Sicht des BWE sind die unter § 5c Absatz 4 EnWG aufgeführten Risikomaßnahmen für größere Unternehmen mit eigenem Windparkmanagement gut umsetzbar.

Für Betreibergesellschaften, die das Windparkmanagement an externe Dienstleister ausgelagert haben, sind die 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.

Im Folgenden gehen wir auf die aus unserer Sicht kritischen Punkte ein:

- § 5c Absatz 4 Nummer 3 benennt die **Aufrechterhaltung des Betriebs**. Wenn Maßnahmen im Rahmen des Wiederanlaufs und des Notfallmanagements definiert werden, wäre dies zu bewältigen. Wenn darüber hinaus jedoch Maßnahmen erzwungen werden, um den unterbrechungsfreien Betrieb zu gewährleisten (z. B. verbindliche Notstromaggregate), wäre das eine immense Mehrbelastung. Der Ausführungsgrad müsste im IT-Sicherheitskatalog konkretisiert werden.

- § 5c Absatz 4 Nummer 4 bezieht sich auf die **Sicherheit der Lieferkette**. Aus Sicht des BWE ist das ein wichtiger Punkt. Allerdings haben insbesondere kleine Unternehmen kaum Einfluss auf große (internationale) Zulieferer bzw. Dienstleister (z. B. Chiphersteller, Softwareunternehmen). Darüber hinaus sind mehrstufige Lieferketten meist intransparent. Eine vollständige Kontrolle oder Überprüfung auf Sicherheitsrisiken entlang der Lieferkette ist daher aus unserer Sicht nicht realistisch umsetzbar.

- § 5c Absatz 4 Nummer 9 benennt als umzusetzende Maßnahme, die **„Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen“**. Insbesondere zur Sicherheit des Personals ergibt sich die Frage: Ist hiermit die Überprüfung des Personals gemeint, 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?

- § 5c Absatz 4 Nummer 10 fordert dedizierte, gesicherte **Notfallkommunikationssysteme**. Je nach Ausführungsgrad im Rahmen des IT-Sicherheitskatalogs wären die meisten Unternehmen wohl gezwungen, eine zweite Kommunikationsinstanz aufzubauen, die im besten Fall unabhängig von der kompletten IT-Infrastruktur des Unternehmens ist. Das kann eine größere finanzielle und personelle Mehrbelastung darstellen, wobei der Nutzen in keinem Verhältnis zum Aufwand steht.

- § 5c Absatz 4 Nummer 12 ist wenig verständlich formuliert, bleibt sehr vage und stellt unserer Einschätzung nach ein hohes Umsetzungsrisiko dar. Nach unserem Verständnis müssten über diese Anforderungen EUCC-zertifizierte Produkte und Dienste eingesetzt werden, wobei der Einsatzbereich nicht genau abgegrenzt wird. Dies muss im Rahmen des IT-Sicherheitskatalogs genauer ausgestaltet werden, um den genauen Aufwand abschätzen zu können. Zudem ist eine

EUCC-Zertifizierung noch so neu, dass es zum jetzigen Zeitpunkt schwerfällt, überhaupt Produkte mit entsprechender Zertifizierung zu finden.

4.2 Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen

Gemäß § 31 Absatz 2 BSI- Gesetz sind Betreiber kritischer Anlagen dazu verpflichtet, für die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, Systeme zur Angriffserkennung einzusetzen. Die Definition dieser Systeme, Komponenten und Prozesse, ist jedoch zu ungenau definiert. Hier sind konkrete Vorgaben für deren Erhebung und Bewertung vorzugeben.

Vorschlag des BWE (Ergänzung fett markiert):

Betreiber kritischer Anlagen sind verpflichtet, für die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, Systeme zur Angriffserkennung einzusetzen. **Die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen maßgeblich Anlagen, sind durch eine Business Impact Analyse zu ermitteln. Die maximal tolerierbare Ausfallzeit dieser Systeme, Komponenten und Prozesse ist zu bestimmen.** Die eingesetzten Systeme zur Angriffserkennung müssen geeignete Parameter und Merkmale aus dem laufenden Betrieb kontinuierlich und automatisch erfassen und auswerten. Sie sollten dazu in der Lage sein, fortwährend Bedrohungen zu identifizieren und zu vermeiden sowie für eingetretene Störungen geeignete Beseitigungsmaßnahmen vorzusehen, **die innerhalb der maximal tolerierbaren Ausfallzeit abgeschlossen werden**. Dabei soll der Stand der Technik eingehalten werden. Der hierfür erforderliche Aufwand soll nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage stehen.

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

Aus Sicht des BWE sind die Vorgaben für eine Zertifizierung in den jeweiligen IT-Sicherheitskatalogen für kritische Anlagen - Energieanlagen und digitale Energiedienste - richtig und nachvollziehbar. Für kleinere Unternehmen sehen wir dafür jedoch keine Notwendigkeit und befürchten erhöhte Kosten und die Gefahr eines Zertifizierungsstaus. Das liegt vor allem an der Kombination aus neuen Pflichten, engen Fristen und begrenzten Ressourcen für Prüfungen und Zertifizierungen.

- **Neue Pflichten:** Der Entwurf erweitert die Anzahl der betroffenen Unternehmen erheblich. Viele mittelständische Unternehmen aus dem Energiebereich werden nun als „wichtige Einrichtungen“ erfasst. Diese müssten erstmals umfangreiche Cybersicherheitsmaßnahmen nachweisen oder diese sogar zertifizieren lassen (z. B. nach ISO 27001).

  Viele Anforderungen müssen zudem noch durch das BSI per Rechtsverordnung konkretisiert werden. Die Unternehmen wissen also nicht, ob und welche konkreten Zertifizierungen erforderlich sein werden, was ihre Vorbereitung verzögert. Sobald die Anforderungen veröffentlicht sind, entsteht zudem ein „Run“ auf Zertifizierungsstellen – alle auf einmal.

- **Enge Fristen:** Den angepassten Zeitraum von drei Jahren zum Nachweis von Risikomanagementmaßnahmen bei kritischen Anlagen halten wir für einen realistischen und pragmatischen Ansatz. So werden sowohl die BNetzA als auch Zertifizierungs- und Auditierungsstellen und nicht zuletzt die Unternehmen selbst personell entlastet. Nach dem derzeitigen Entwurf müssen betroffene Unternehmen jedoch auch für Nicht-kritische Anlagen innerhalb von wenigen Monaten nach Inkrafttreten ihre Pflichten erfüllen, etwa beim Nachweis der Sicherheitsvorkehrungen und der Risikoanalyse. Das ist für viele Unternehmen zeitlich nicht machbar, wenn zusätzlich ein Zertifizierungsverfahren durchlaufen werden muss.

- **Begrenzte Ressourcen:** Zertifizierungsstellen (z. B. für ISO 27001) haben bereits jetzt lange Wartezeiten. Zudem müssen sich viele Auditor*innen erst für neue Anforderungen qualifizieren oder durch das BSI akkreditieren lassen. Dadurch entsteht ein **Flaschenhals**, sodass selbst vorbereitete Unternehmen im Falle einer verpflichtenden Zertifizierung den Nachweis nicht rechtzeitig abschließen können.

Der Änderungsvorschlag in § 5c Abs. 2 EnWG-E besagt, dass auch Betreiber von Energieanlagen, die als „besonders wichtige“ oder „wichtige“ Einrichtungen im Sinne des § 28 BSI- G zu klassifizieren sind, die Vorgaben aus dem IT-Sicherheitskatalog der BNetzA einhalten müssen. Der aktuelle IT-Sicherheitskatalog gemäß § 11 Absatz 1b des EnWG beinhaltet eine Zertifizierungspflicht bei einer akkreditierten Zertifizierungsstelle.

Vorschlag des BWE:

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.

6 Untersagung des Einsatzes kritischer Komponenten

Der BWE betont die herausragende Bedeutung des sicheren Betriebs jeder einzelnen Windenergieanlage über ihre gesamte Lebensdauer hinweg. Die Gewährleistung höchster Sicherheitsstandards ist unerlässlich, da Windenergieanlagen nicht nur potenziellen Angriffen von außen, sondern auch Risiken innerhalb der Lieferkette ausgesetzt sein können. Vor diesem Hintergrund begrüßt der BWE ausdrücklich die im aktuellen Entwurf des NIS-2-Umsetzungsgesetzes erweiterten Befugnisse des BMI und die vorgesehene Möglichkeit, den Einsatz kritischer Komponenten zu untersagen, sofern diese nicht von einem vertrauenswürdigen Hersteller stammen.

Gleichzeitig möchten wir darauf hinweisen, dass die Definition kritischer Komponenten in § 2 Nr. 23 BSI-Gesetz sehr allgemein ist. Auch die Festlegung kritisch bestimmter Funktionen der BNetzA[2] (veröffentlicht im Amtsblatt 12/25) lässt vieles offen. Sowohl bei der Anzeige beim geplanten erstmaligen Einsatz einer kritischen Komponente als auch bei einer möglichen Untersagung besteht Unsicherheit, da unklar ist, welche Komponenten konkret gemeint sind. Die in der Windenergie eingesetzten IKT-Produkte, IKT-Dienste und IKT-Prozesse sind in der Regel branchenspezifische Produkte und speziell für den Windparkbetrieb konzipiert (SCADA-Systeme wie Windparkregler, Parkrechner, Condition-Monitoring-Systeme, Betriebsführungssoftware usw.). Hier würde es helfen, wenn es Whitelists gäbe, also Listen, in denen die Geräte und ihre erlaubten Einsatzgebiete dokumentiert sind. Darüber hinaus sind, abhängig von der Art der betroffenen Komponenten, angemessene Vorlaufzeiten für Windenergieanlagenhersteller, Planer und Projektierer zu berücksichtigen.

[1] IT-Sicherheitskatalog gemäß § 11 Absatz 1b Energiewirtschaftsgesetz – LINK

[2] BNetzA- Festlegung kritisch bestimmter Funktionen/ Amtsblatt/ 12/2025 – 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, kiri

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

Autoren in alphabethischer Reihenfolge

Stefan Grothe | Fachreferent Technik
Katharina Schuler | Referentin Politik Europa

Einbezogenen Gremien

- Gesamtvorstand
- AK Energiepolitik
- Betreiberbeirat
- Betriebsführerbeirat
- Juristischer Beirat

Datum

04.07.2025