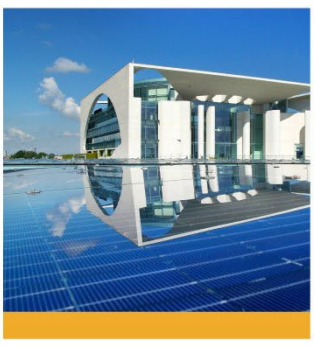
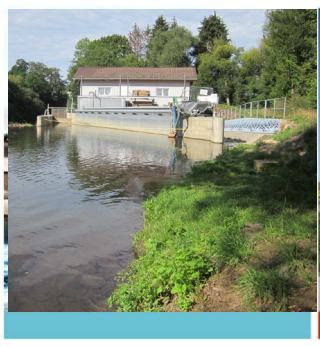
Bundesverband
Erneuerbare Energie e.V.

BEE-Stellungnahme

zum Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

Berlin, 4. Juli 2025




Inhaltsverzeichnis

Das Wichtigste in Kürze

Der Bundesverband Erneuerbare Energie e.V. (BEE) begrüßt, dass sich das Bundesministerium des Innern (BMI) im Rahmen eines Umsetzungsgesetzes zur zweiten Netzwerk- und Informationssicherheitsrichtlinie (NIS-2-Richtlinie) der Europäischen Union mit der Stärkung der Cybersicherheit in Deutschland beschäftigt. Der Verband unterstützt das Vorhaben, hier weitere Maßnahmen zu verabschieden.

Der BEE bewertet viele der angedachten Vorgaben als positiv und betrachtet das Gesetz insgesamt als zentral für die Stärkung der Resilienz und der IT-Sicherheit in der deutschen Wirtschaft. Besonders herauszuheben sind hierbei:

- die behördliche Zuständigkeit der **Bundesnetzagentur (BNetzA) als zentrale Stelle für Cybersicherheitsmaßnahmen** im Energiesektor
- umzusetzende **Risikomaßnahmen für kritische Anlagen** zur Stärkung der Resilienz der Energieinfrastruktur
- die Möglichkeit zur **Implementierung eines gemeinsamen Informationsmanagementsystems** bei Partner- oder verbundenen Unternehmen
- die explizite **Beteiligung der Betreiber und Branchenverbände** an der Festlegung und Aktualisierung der IT-Sicherheitskataloge

Demgegenüber bekräftigt der BEE in dieser Stellungnahme elementare Anforderungen, die in das NIS-2-Umsetzungsgesetz aufgenommen werden sollten:

- eine aktivere Rolle der zuständigen Behörden bei der **Einordnung von Unternehmen sowie bei der Information über deren Pflichten**
- **eine Klarstellung der jeweils zuständigen staatlichen Institution** an allen relevanten Stellen des Gesetzesentwurfs – insbesondere bei Zuständigkeit der BNetzA
- eine Unterscheidung nach Unternehmensgrößen bei der **Ausgestaltung der Mindestanforderungen** an die IT-Sicherheit im Anlagen- und Netzbetrieb nach § 5c EnWG
- Übertragung der Pflichten nach § 5c Abs. 4 EnWG auf externe Dienstleister, sofern das **Parkmanagement** von den Betreibergesellschaften an diese **ausgelagert** wurde
- **Konkretisierung und Vereinfachung** der Anforderungen an die Anlagenbetreiber bei den Vorgaben nach § 5c Absatz 4
- Präzisierung der **Ausführungen zu IT-Systemen, -Komponenten und -Prozessen**, die für die Funktionsfähigkeit der von ihnen betriebenen Anlagen maßgeblich sind
- Klarstellung, dass eine **Zertifizierungspflicht über den von der BNetzA erstellten IT-Sicherheitskatalog** ausschließlich kritische Anlagen betrifft, die unter der aktuell gültigen BSI-Kritis-Verordnung (BSI-KritisV) als solche klassifiziert werden

Obwohl die Zielsetzungen zur Stärkung der IT-Sicherheit grundsätzlich zu begrüßen sind, schlägt der BEE eine Überarbeitung des NIS-2-Umsetzungsgesetzes vor. Diese sollte **Unklarheiten beseitigen und die praktische Umsetzung erleichtern**, indem die beschriebenen Prozesse präzisiert und vereinfacht werden. Davon würden vor allem **kleine und mittelständische Unternehmen aus dem Energiesektor profitieren**.

Einleitung

Das Bundesministerium des Innern (BMI) hat am 23. Juni 2025 den Referentenentwurf zur nationalen Umsetzung der NIS-2-Richtlinie in Deutschland veröffentlicht. Die neue Bundesregierung holt damit schon früh in der neuen Legislaturperiode ein Gesetzesvorhaben nach, das nach dem Bruch der Ampel-Koalition im November 2024 nicht mehr vor der Bundestagswahl fertiggestellt werden konnte.

Der BEE begrüßt weitere Maßnahmen zur Stärkung der Cybersicherheit in Deutschland. Erneuerbare Energien sind systemsetzend für die Energieversorgung der Zukunft. Um den Weg zu 100 Prozent Erneuerbaren Energien in allen Sektoren bestreiten zu können, muss die Digitalisierung konsequent ausgeweitet und beschleunigt werden. Dabei muss die Sicherheit der IT-Systeme dauerhaft gewährleistet sein.

Der BEE sieht im Gesetzesentwurf noch Optimierungspotenzial. Insbesondere für kleine und mittelständische Unternehmen im Energiesektor, die unter die neuen Anlagenkategorien „besonders wichtige Einrichtung“ und „wichtige Einrichtung“ fallen, entstehen neue Herausforderungen. Außerdem sorgen die neuen Vorgaben mehrfach für Unklarheiten und offene Fragen.

Im Folgenden legt der BEE seine vorläufige Einschätzung des Referentenentwurfs dar.

1 Aktivere Rolle der zuständigen Behörden bei der Einordnung von Unternehmen

Der Referentenentwurf sieht vor, dass Unternehmen nach §§ 30–32 BSI-Gesetz-E selbst prüfen müssen, ob sie unter die Definition von „Besonders wichtigen Einrichtungen“ oder „Wichtigen Einrichtungen“ fallen. Nach § 33 sind sie außerdem dazu verpflichtet, eine Selbsterklärung bzw. Selbsteinordnung an das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu übermitteln. Diese muss alle relevanten Unternehmensdaten enthalten, zudem ist eine dreimonatige Frist zu beachten. Eine zentrale Benachrichtigung durch das BSI erfolgt nicht.

Viele EU-Länder wählen abweichende Ansätze, zum Beispiel durch eine stärkere zentrale Steuerung oder eine automatische Behördenzuweisung. In Frankreich erfolgt die zentrale Erfassung und offizielle Benachrichtigung durch die nationale Cybersicherheitsbehörde ANSSI (Agence nationale de la sécurité des systèmes d'information). Auch in Italien und in den Niederlanden übernehmen die jeweils zuständigen Behörden ACN (Agenzia per la Cybersicurezza Nazionale) und RDI (Rijksinspectie Digitale Infrastructuur) eine aktivere Rolle. Sie führen zentrale Listen oder nehmen für die Unternehmen eine automatisierte Einstufung vor.

Eine verpflichtende Selbsteinordnung **sorgt bei vielen Unternehmen in Deutschland für Unsicherheit** darüber, ob sie von den Regelungen der NIS-2-Richtlinie überhaupt betroffen sind. Insbesondere viele kleine und mittelständische Unternehmen unterschätzen die Bedeutung der neuen Rechtslage oder kennen ihre Einstufungskriterien nicht genau.

Das BSI sollte Unternehmen auf Nachfrage eine rechtsverbindliche Auskunft darüber erteilen, ob sie von den Vorgaben der NIS-2-Richtlinie betroffen sind. Noch besser wäre es, die Rolle des BSI so auszugestalten, dass es Unternehmen **aktiv über ihre Pflichten informiert und offiziell einer der Kategorien zuteilt**.

2 Ausgestaltung der IT-Sicherheitskataloge nach § 11 Abs. 1a und 1b EnWG

Der BEE begrüßt ausdrücklich, dass die **Verantwortung für Cybersicherheitsmaßnahmen** im Energiesektor **zukünftig zentral bei der Bundesnetzagentur (BNetzA) liegt** – sowohl für kritische Anlagen als auch für die neu eingerichteten Kategorien „Besonders wichtige Einrichtungen“ und „Wichtige Einrichtungen“.

Bezüglich der aktuellen Ausgestaltung der IT-Sicherheitskataloge nach § 11 Abs. 1a und 1b EnWG sieht es der BEE als positiv an, dass **bei Partner- oder verbundenen Unternehmen ein gemeinsames Informationsmanagementsystem** für einen definierten Geltungsbereich auf Basis von ISO/IEC 27001 implementiert werden kann. Damit wird aufgegriffen, dass die Betriebsführungssparte vielfach schon entsprechenden Anforderungen über die Kategorie „Digitaler Energiedienst“ unterliegt. Somit muss nicht jede ausgegliederte Betreibergesellschaft die Anforderungen eigenständig erfüllen und nachweisen.[1]

Zusätzlich wird festgelegt, dass die Anforderungen an einen angemessenen Schutz in den IT-Sicherheitskatalogen im Einvernehmen mit dem BSI bestimmt werden. Damit übernimmt auch diese Behörde eine starke Rolle. Darüber hinaus sollen die **Betreiber und deren Branchenverbände explizit an der Festlegung und Aktualisierung der IT-Sicherheitskataloge beteiligt** werden, was der BEE ausdrücklich befürwortet.

Jedoch finden sich im Gesetzesentwurf weiterhin eine Reihe von Regularien, in denen nicht eindeutig bestimmt wird, welche Behörde oder welches Ministerium genau zuständig ist. Hier muss nachgebessert werden, sodass **für alle Bereiche die entsprechenden Zuständigkeiten unmissverständlich geklärt** sind. Die betroffenen Unternehmen wären somit eindeutig über ihre jeweiligen Anlaufstellen informiert.

Sollten Sicherheitsvorfälle auftreten, sollte aus Sicht des BEE die **Kommunikation mit der BNetzA** vorgesehen sein. Dies wäre es sinnvoll und folgerichtig, insbesondere da es sich um eine gemeinsame Meldestelle handelt.

[1] siehe BNetzA: „Mitteilung zur Zertifizierung nach IT-Sicherheitskatalog § 11 Abs. 1a und 1b EnWG im Fall einer Betriebsführung durch Dritte“

3 Ausgestaltung der Mindestanforderungen an die IT-Sicherheit im Anlagen- und Netzbetrieb nach § 5c EnWG

Der BEE hält die unter § 5c EnWG aufgeführten Vorgaben für größere Unternehmen, insbesondere aus der Windbranche, für gut umsetzbar. Für kleinere Unternehmen aus der Erneuerbaren-Branche stellen die Anforderungen nach § 5c EnWG hingegen eine große Herausforderung dar. Dies sieht der Verband aufgrund der folgenden Punkte kritisch:

- Für Betreibergesellschaften, die das Parkmanagement 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.
- § 5c Absatz 4 Nummer 3 benennt die **Aufrechterhaltung des Betriebs**. Dies lässt sich umsetzen, wenn Maßnahmen im Rahmen des Wiederanlaufs und Notfallmanagements definiert werden. Wenn darüber hinaus jedoch Maßnahmen erzwungen werden, um den unterbrechungsfreien Betrieb zu gewährleisten (z. B. verbindliche Nutzung von Notstromaggregaten), 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**. Der BEE erkennt die Relevanz dieser Betrachtung an, sieht jedoch nur geringe Möglichkeiten zum Einfluss kleiner Unternehmen auf große, internationale Zulieferer und Dienstleister. Darüber hinaus sind mehrstufige Lieferketten oft intransparent. Eine vollständige Kontrolle oder Überprüfung auf Sicherheitsrisiken entlang der Lieferkette ist daher aus Sicht des BEE nicht realistisch umsetzbar.
- § 5c Absatz 4 Nummer 9 benennt als umzusetzende Maßnahme die **Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen**. Hier bleiben Fragen offen, beispielsweise, ob mit „Sicherheit des Personals“ womöglich die Überprüfung des Personals unter Punkt A.7.1 im Annex der DIN ISO 27001 oder Nr. 56 der Konkretisierung der Anforderungen an die gemäß § 8a Abs. 1 BSIG umzusetzenden Maßnahmen gemeint ist.
- § 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. Im besten Fall sollte diese zusätzlich unabhängig von der kompletten IT-Infrastruktur des Unternehmens sein. Das kann eine größere finanzielle und personelle Mehrbelastung darstellen, sodass der Nutzen ggf. in keinem Verhältnis mehr zum Aufwand steht.
- § 5c Absatz 4 Nummer 12 ist sehr vage und damit missverständlich formuliert, wodurch sich ein hohes Umsetzungsrisiko ergibt. Nach Verständnis des BEE müssten hier EUCC-zertifizierte Produkte und Dienste eingesetzt werden, allerdings ist der **Einsatzbereich nicht genau abgegrenzt**. Es braucht eine genaue Ausgestaltung im Rahmen des IT-Sicherheitskatalogs, um den Aufwand besser abschätzen zu können. Zudem besteht die EUCC-Zertifizierung erst seit Kurzem, sodass Produkte mit dieser Zertifizierung bisher nur schwer zu finden sind.

- § 5c Absatz 7 Nr. 1 fordert von Anlagenbetreibern innerhalb von 24 Stunden eine Einschätzung darüber, **ob ein Sicherheitsvorfall auf eine rechtswidrige oder eine böswillige Handlung zurückzuführen ist**. Weiterhin müssen Anlagenbetreiber innerhalb von 72 Stunden eine Einschätzung über den Schweregrad und die Auswirkungen des Sicherheitsvorfalls abgeben. An dieser Stelle braucht es eine Klarstellung, dass Anlagenbetreiber nicht dafür haftbar gemacht werden, wenn sie bei der Meldung eines Sicherheitsvorfalls unwissentlich eine fehlerhafte Einschätzung abgeben.
- § 5c Abs. 9 legt fest, dass Betreiber sicherzustellen haben, dass sie über die benannte oder durch das BSI festgelegte **Kontaktstelle** jederzeit erreichbar sind. Diese Vorgabe ist bei kleinen Anlagen nur schwer einzuhalten und sollte vereinfacht werden.

4 Besondere Anforderungen an die Risikomanagementmaßnahmen von Betreibern kritischer Anlagen nach § 31 Abs. 2 BSI-G

In § 31 Absatz 2 BSI-G 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“. Jene informationstechnischen Systeme, Komponenten und Prozesse sind im Gesetzesentwurf **zu ungenau definiert**. Es braucht konkrete Vorgaben für deren Erhebung und Bewertung. Der BEE macht dafür den folgenden Formulierungsvorschlag:

“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 Anlagen maßgeblich sind, 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 Anwendung der Zertifizierungspflicht ausschließlich für kritische Anlagen gemäß BSI-KritisV

Aus Sicht des BEE sind die Vorgaben an eine Zertifizierung in den jeweiligen IT-Sicherheitskatalogen **für kritische Anlagen richtig und nachvollziehbar**. Dies umfasst sowohl Energieanlagen als auch digitale Energiedienste.

Für kleine und mittelständische Unternehmen sieht der Verband jedoch keine Notwendigkeit, da erhöhte Kosten und die Gefahr eines Zertifizierungsstaus zu befürchten sind. Das liegt vor allem an der Kombination aus neuen Pflichten, engen Fristen und begrenzten Ressourcen für Prüfungen und Zertifizierungen. Im Folgenden wird dies genauer erläutert:

- Neue Pflichten: Der Entwurf erweitert die Anzahl der betroffenen Unternehmen erheblich. Viele mittelständische Energieunternehmen werden nun als „Wichtige Einrichtungen“ erfasst. Diese müssen erstmals umfangreiche Cybersicherheitsmaßnahmen nachweisen oder sich sogar neu zertifizieren lassen (z. B. nach ISO 27001). Da viele Anforderungen zudem noch durch das BSI per Rechtsverordnung konkretisiert werden müssen, wissen die Unternehmen nicht immer, welche Zertifizierungen konkret erforderlich sein werden. Dadurch verzögert sich die Vorbereitung und sobald die Anforderungen veröffentlicht werden, sind die Zertifizierungsstellen schnell überlaufen.
- Enge Fristen: Den angepassten Zeitraum von drei Jahren zum Nachweis von Risikomanagementmaßnahmen bei kritischen Anlagen hält der BEE für einen realistischen und pragmatischen Ansatz. Dadurch werden die BNetzA und die Zertifizierungs- und Auditierung-Stellen sowie die Unternehmen personell entlastet. Nach dem derzeitigen Entwurf müssen betroffene Unternehmen jedoch bereits innerhalb weniger Monate nach Inkrafttreten bestimmte Nachweise erbringen. Diese beziehen sich beispielsweise auf Sicherheitsvorkehrungen und die Risikoanalyse. Das ist für viele Unternehmen zeitlich nicht machbar, insbesondere, wenn zusätzlich ein Zertifizierungsverfahren durchlaufen werden muss.
- Begrenzte Ressourcen: Beauftragungen von Zertifizierungsstellen (z. B. für ISO 27001) sind schon jetzt mit langen Wartezeiten verbunden. Viele Auditoren müssen sich zudem erst für neue Anforderungen qualifizieren oder durch das BSI akkreditiert werden. Dadurch hätten es selbst gut vorbereitete Unternehmen schwer, einen verpflichtenden Nachweis fristgerecht zu erbringen. Der BEE spricht sich hier für eine Erleichterung aus.

Da sich die Zertifizierungspflicht nicht aus dem Gesetz, sondern aus dem IT-Sicherheitskatalog ergibt, bittet der BEE um Klarstellung, dass eine Zertifizierungspflicht über den von der BNetzA erstellten IT-Sicherheitskatalog **ausschließlich kritische Anlagen betrifft, die unter der aktuell gültigen BSI-KritisV als solche klassifiziert werden.**

Hinweis:
Diese BEE-Positionierung erfolgt ausnahmsweise nicht im Namen des Bundesverbandes Solarwirtschaft e.V. Die Erarbeitung einer einvernehmlichen Position war innerhalb der Solarbranche in der Kürze der Konsultationsfrist nicht möglich. Interessierte Mitgliedsunternehmen aus der Solarbranche werden sich daher ggf. mit eigenen Stellungnahmen einbringen. Diese entsprechen nicht zwingend der Position von BSW-Solar oder BEE.

Ansprechpartner*innen:
Bundesverband Erneuerbare Energie e.V. (BEE)
EUREF-Campus 16
10829 Berlin

Dr. Matthias Stark	Florian Widdel
Leiter Fachbereich Erneuerbare Energiesysteme	Referent für Digitalisierung, Sektorenkopplung und Energienetze
matthias.stark@bee-ev.de	florian.widdel@bee-ev.de

Weitere Autor*innen:

Stefan Grothe, Bundesverband Windenergie e.V.

Manuel Maciejczyk, Fachverband Biogas e.V.

Als Dachverband vereint der Bundesverband Erneuerbare Energie e.V. (BEE) Fachverbände und Landesorganisationen, Unternehmen und Vereine aller Sparten und Anwendungsbereiche der Erneuerbaren Energien in Deutschland. Bei seiner inhaltlichen Arbeit deckt der BEE Themen rund um die Energieerzeugung, die Übertragung über Netz-Infrastrukturen, sowie den Energieverbrauch ab.

Der BEE ist als zentrale Plattform aller Akteur*innen der gesamten modernen Energiewirtschaft die wesentliche Anlaufstelle für Politik, Medien und Gesellschaft.

Unser Ziel: 100 Prozent Erneuerbare Energie in den Bereichen Strom, Wärme und Mobilität.

Impressum
Bundesverband Erneuerbare Energien e.V.
EUREF-Campus 16
10829 Berlin

Tel.: 030 2758 1700
info@bee-ev.de
www.bee-ev.de
V.i.S.d.P. Wolfram Axthelm

Der Bundesverband Erneuerbare Energien e.V. ist als registrierter Interessenvertreter im Lobbyregister des Deutschen Bundestages unter der Registernummer R002168 eingetragen.
Den Eintrag des BEE finden Sie hier.

Datum
4. Juli 2025