POWER SYSTEMS

POSITIONSPAPIER

Umsetzung der NIS2-Richtlinie und Stärkung der Cybersicherheit von Energietechnologien

Registrierungsnummer im Register der Interessenvertreter: R000802

September 2025

Executive Summary

- Konsequente Umsetzung von NIS2 in Deutschland und Europa als Grundlage für die sichere Integration relevanter Anlagen und Systeme wie Windenergieanlagen, Wechselrichtern bei Solarenergie oder Netzkomponenten in die Energieversorgung und Verbindliche Einbeziehung aller kritischen Energietechnologien in die Definition kritischer Infrastrukturen.
- Zugriffe durch Dritte regulieren: Digitale Zugriffe durch Dritte, wie Hersteller oder Energiedienstleister auf Energieanlagen, müssen im regulatorischen Rahmen transparent und sicher gestaltet werden.
- Single-Operator-Prinzip wahren: Die Verantwortung für Cybersicherheit einer Anlage liegt beim Betreiber. Für Anlagen, die von der KRITIS erfasst werden, muss der regulatorische Rahmen jedoch klar Regeln, unter welchen Bedingungen Hersteller oder Dritte auf Anlagen zugreifen dürfen, insbesondere für Schalthandlungen oder bei der Aggregation kleinerer Anlagen.
- Lieferkettenresilienz stärken: Kritische Komponenten und digitale Dienste aus unsicheren Drittstaaten müssen hinsichtlich bestehender Risiken konsequent reguliert werden.
- Behördenkompetenzen erweitern: BMI, BSI und BNetzA benötigen durchsetzungsfähige Instrumente bis hin zu Nutzungs- und Betriebsverboten.
- Europäische Harmonisierung: Koordinierte Umsetzung der NIS2, Cyber Resilience Act (CRA) und CER-Richtlinie im Binnenmarkt, bei gleichzeitiger Nutzung nationaler Anpassungen zur Schließung regulatorischer Lücken und zur Präzisierung kritischer Anlagenkategorien.

Vorwort

VDMA Power Systems vertritt die führenden Hersteller von Energietechnologien in Deutschland und Europa – darunter Anbieter von Wind- und Solarenergieanlagen, thermischen Kraftwerkstechnologien, Speichern, Netzkomponenten sowie weiteren Schlüsseltechnologien für die Energiewende. Die Branche ist zentraler Lösungsanbieter für die künftige Energieversorgung und trägt wesentlich dazu bei, die europäischen Klimaziele, Versorgungssicherheit und wirtschaftliche Wettbewerbsfähigkeit zu sichern.

Mit dem massiven Ausbau erneuerbarer Energien und der zunehmenden Dezentralisierung der Stromerzeugung steigt zugleich die Komplexität und Verwundbarkeit des Energiesystems. Digitale Schnittstellen, Remote-Zugriffe und softwaregestützte Steuerungen sind heute integrale Bestandteile moderner Energietechnologien – sie ermöglichen einen effizienten Betrieb, eröffnen jedoch gleichzeitig Angriffsflächen für Cyberbedrohungen. Dies betrifft nicht nur Windenergieanlagen, sondern in besonderem Maße auch Wechselrichter und Netzkomponenten sowie weitere Systeme bspw. an Speichern, die tief in die Steuerung, Umwandlung und Verteilung elektrischer Energie eingreifen.

Grundlegende Einordnung

Zugriffe durch Dritte für Wartung, Firmware-Updates oder Ferndiagnose sind im Betrieb von Energieanlagen unverzichtbar – eröffnen jedoch potenziell kritische Eintrittspunkte für Manipulation, Sabotage oder Spionage. Ein erfolgreicher Angriff könnte nicht nur einzelne Anlagen, sondern ganze Netzbereiche destabilisieren sowie Informationen über Netzzustände sammeln.

Vor diesem Hintergrund sind politische Initiativen wie das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG) wichtig zur Verbesserung der Resilienz kritischer Infrastrukturen. Allerdings bestehen aus Sicht der Branche weiterhin Lücken und Präzisierungsbedarf, um einen durchgängig sicheren Betrieb von Energieanlagen über den gesamten Lebenszyklus hinweg zu gewährleisten.

Die Gewährleistung der Cybersicherheit und damit Resilienz von Energieanlagen ist nicht nur eine technische Notwendigkeit, sondern ein zentrales Thema der Energieversorgungssicherheit und nationalen Sicherheit. Anlagenbauer, Betreiber, Dienstleister und Zulieferer tragen gemeinsam Verantwortung, dass Angriffe auf Netzinfrastruktur – ob durch externe Cyberattacken oder über Schwachstellen in der Lieferkette – verhindert werden.

Rechtlicher Rahmen

- IT-Sicherheitsgesetz 2.0 (2021) und BSIG regeln Betreiberpflichten und BSI-Kompetenzen.
- EnWG (§ 11 ff.) enthält Sicherheits- und Zuverlässigkeitsvorgaben für Energieanlagen.
- NIS2UmsuCG (Entwurf 2025) präzisiert Betreiberpflichten für den Energiesektor und schafft Eingriffsmöglichkeiten des BMI/BSI.
- KRITIS-Dachgesetz (Umsetzung CER-Richtlinie) stärkt die physische Resilienz.
- Cyber Resilience Act (CRA, EU-Verordnung 2024) definiert Sicherheitsanforderungen für Produkte mit digitalen Elementen.
- Maschinenverordnung legt Anforderungen der Anlagen gegen Korrumpierung fest.
- Netzkodex für Cybersicherheit (EU) konkretisiert sektorale Anforderungen für Energieanlagen.

Diese Regelungen bilden eine solide Grundlage, weisen jedoch zentrale Lücken bei Herstellerzugriffen und Lieferkettenrisiken auf.

Kernherausforderungen

1. Single-Operator-Prinzip beibehalten und Dritte berücksichtigen

Akteure wie Hersteller haben häufig lebenslangen digitalen Zugriff auf Anlagen, auch ohne permanente Datenverbindung (z. B. über Fernwartung, Updates, Steuerungsbefehle). Damit können diese Akteure im Extremfall direkt in die Stromerzeugung eingreifen.

Forderung:

- Das Single-Operator-Prinzip muss gewahrt bleiben: Betreiber sind für die Cybersicherheit ihrer Anlagen verantwortlich, Dritte müssen aber in die KRITIS-Definition einbezogen werden.
- Alle Energieanlagen, bei welchen Dritten Schaltzugriffe ermöglicht werden, sind als Kritische Infrastrukturen einzustufen und sollten uneingeschränkt den KRITIS-Sicherheitsanforderungen unterliegen.
- Alternativ: Absenkung der Schwellenwerte bspw. für Windenergieanlagen, da integrierte Konvertertechnologie schon auf niedrigen Ebenen Einfluss auf die Netzstabilität hat.

2. Lieferkettensicherheit in den Fokus rücken

Energieanlagen sind nicht nur externen Angriffen, sondern auch Lieferkettenrisiken ausgesetzt.

Kritisch sind:

- Herkunft von Netz- und Steuerungskomponenten,

- kontinuierlicher Support und Wartung,
- Firmware-/Software-Updates, die direkt Einfluss auf Netz und Anlagen haben.

Forderungen:

- Nur Komponenten und Dienstleistungen zulassen, die europäischen und transatlantischen Sicherheitsanforderungen entsprechen.
- Hersteller und Akteure aus Drittstaaten, die (potenziell) staatlicher Einflussnahme unterliegen, sind als unzuverlässig einzustufen. Die Zertifizierung einzelner Komponenten reicht nicht aus, um Risiken angemessen zu minimieren. Darüber hinaus erfasst die Umsetzung der NIS2-Richtlinie die Gefahren durch einen steuernden Zugriff auf Anlagen/Systeme durch Externe nicht angemessen genug. Dies gilt insbesondere für den versorgungskritischen Bereich Energie
- Dauerhafte Risikobewertungen durch BMI unter Einbeziehung technischer und nicht-technischer Faktoren.

3. Verbot kritischer Komponenten und Dienste spezifizieren

Akteure aus rivalisierenden oder unsicheren Drittstaaten können Anlagen manipulieren, überwachen oder stilllegen. Digitale Zugriffe durch Dritte, insbesondere Schalthandlungen welche durch Hersteller, Energiedienstleister oder andere externe Akteure erfolgen, müssen klar geregelt und als Gefährdung des Energiesystems und der Versorgungssicherheit behandelt werden. Auch durch Dritte kontrollierte oder aggregierte Anlagen, die aus vielen kleinen Einheiten bestehen, sollten als kritische Infrastruktur eingestuft werden und den vollen KRITIS-Sicherheitsanforderungen unterliegen. Die Aufsichtsbehörden müssen im NIS2-Umsetzungsgesetz (§23a, §41) dementsprechend befugt werden, digitale Dienste und kritische Funktionen zu untersagen oder einzuschränken. Nur so können Sicherheitsrisiken wirksam adressiert und die Resilienz der nationalen und europäischen Energiesysteme gestärkt werden.

Forderungen:

- §41 BSIG: Ministerien müssen die Befugnis haben, die Nutzung kritischer Komponenten und kritischen Digitalen Diensten von unzuverlässigen Herstellern zu untersagen.
- §5c EnWG: Auch digitale Energiedienstleistungen müssen reguliert werden, Betreiber sind zu angemessenem Schutz zu verpflichten.

4. Durchsetzung und Handlungsfähigkeit der Behörden

Behörden wie BMI und BNetzA müssen personell und organisatorisch so ausgestattet sein, dass sie ihre Eingriffsbefugnisse effektiv wahrnehmen können. Sie benötigen durchsetzungsfähige Instrumente, um Sicherheitsrisiken bei KRITIS-Anlagen wirksam zu adressieren, einschließlich der Möglichkeit, digitale Dienste, systemkritische Funktionen oder durch Dritte kontrollierte/aggregierte Anlagen zu untersagen oder einzuschränken, sowie

Eingriffe bis hin zu Nutzungs- und Betriebsverboten durchzuführen. Dazu gehören insbesondere:

Notwendig sind:
- klare Eingriffsbefugnisse (z. B. dauerhafter Entzug von Netzzugangslizenzen),
- kontinuierliche Überprüfung von Herstellern und Dienstleistern,
- verbesserte Meldemöglichkeiten für unzuverlässige Hersteller, um auch Handlungen der Wirtschaft anzustoßen,
- ressortübergreifende Zusammenarbeit und Einbeziehen relevanter Ressorts (BMI, BMWK, AA).

Fazit

Die Energiewende macht Deutschland und Europa abhängiger von einer stabilen, sicheren und resilienten Energieinfrastruktur. Mit zunehmender Digitalisierung wächst die Verwundbarkeit durch Cyberrisiken.

Nur durch:

- Einbeziehung aller relevanten Energietechnologien,
- klare Regulierung von Zugriffen durch Dritte,
- eine Klarstellung im NIS2-Umsetzungsgesetz (§23a, §41), dass Aufsichtsbehörden auch digitale Dienste und kritische digitale Funktionen untersagen oder beschränken können,
- Striktes Management auch von Risken aus der Lieferkette,

kann die Versorgungssicherheit langfristig gewährleistet werden.

Wichtig ist nun:
- Die schnelle Verabschiedung des NIS2UmsuCG ist zwingend erforderlich – im überparteilichen Interesse und mit Blick auf die Sicherheit Deutschlands.
- Rechtsverordnungen und Begriffsbestimmungen müssen sicherstellen, dass Anlagen wie Windenergieanlagen, Wechselrichter, Batteriespeicher oder weitere für die Energieversorgung relevante Systeme aufgrund ihrer systemrelevanten Funktionenwals kritische Anlagen behandelt werden.
- Handlungsspielräume in §9 BSIG, §§30/41 NIS2UmsuCG müssen konsequent ausgestaltet und angewandt werden.
- Auch das Inkrafttreten und die Umsetzung des CRA muss die Möglichkeit stärken, kritische Produkte europaweit einheitlich zu regulieren.

- Die Gesetzgebung muss zukünftig berücksichtigen, dass Sicherheit nicht allein durch den Einsatz vertrauenswürdiger Komponenten gewährleistet werden kann. Sie erfordert ebenso die konsequente Überprüfung aller digitalen Zugriffe durch Dritte, etwa Hersteller oder Dienstleister, die systemnahe Funktionen wie Fernwartung oder Steuerung ausüben.

Die NIS2-Umsetzung ist nicht somit nur für das Risikomanagement von Unternehmen relevant, sondern wird zunehmend zu einem zentralen Instrument, um die Stabilität und Resilienz der nationalen und europäischen Energiesysteme zu sichern.

Kontakt:
Sebastian Steul
Referent Power Systems Technik & Innovation
Telefon: +49 69 6603-1748
E-Mail: sebastian.steul@vdma.eu

Malte Peters
Referent Power Systems Energiepolitik
Telefon: +49 30 306946-21
E-Mail: malte.peters@vdma.eu

Steffen Zimmermann
Leiter Competence Center Industrial Security
Telefon: +49 69 6603-1978
E-Mail: steffen.zimmermann@vdma.eu

Lobbyregister: R000802
EU-Transparenzregister ID: 9765362691-45

vdma.eu