VDMA
Power Systems

VDMA POWER SYSTEMS

STELLUNGNAHME

Stellungnahme zum Entwurf eines Gesetzes zur Stärkung der Cybersicherheit von VDMA Power Systems

Registrierungsnummer im Register der Interessenvertreter: R000802

März 2026

VDMA
Power Systems

Executive Summary

- Konsequente gesetzliche Grundlage für die sichere Integration von Anlagen wie Windenergieanlagen, Wechselrichtern bei Solarenergiesystemen oder Netzkomponenten in das Energiesystem als Teile kritischer Infrastruktur.
- Zugriffe durch Dritte regulieren: Digitale Zugriffe durch Dritte, wie Hersteller oder Energiedienstleister auf Energieanlagen, müssen im regulatorischen Rahmen transparent und sicher gestaltet werden.
- Zugriff aus der Lieferkette darf nur von vertrauenswürdigen Herstellern / Lieferanten erfolgen.

VDMA
Power Systems

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 Energieversorgung und trägt wesentlich dazu bei, die europäischen Klimaziele, Versorgungssicherheit und wirtschaftliche Wettbewerbsfähigkeit zu sichern. Die Sicherheit der Energieversorgung ist entscheidende Grundvoraussetzung für die nationale Sicherheit und darf daher keinesfalls Risiken ausgesetzt werden. Dies gilt auch für die Technologien, die zur Erzeugung und Verteilung zum Einsatz kommen.

Mit dem massiven Ausbau erneuerbarer Energien und der zunehmenden Dezentralisierung der Stromerzeugung steigt 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 Gesetz zur Stärkung der Cybersicherheit wichtig zur Verbesserung der Resilienz kritischer Infrastrukturen. Allerdings bestehen 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 verhindert werden. Egal ob durch externe Cyberattacken oder über Schwachstellen in der Lieferkette entstehen.

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. Dritte angemessen berücksichtigen

Akteure wie Hersteller haben häufig berechtigten lebensdauerlangen Zugriff auf Anlagen, auch ohne permanente Datenverbindung (z. B. über Fernwartung, Updates, Steuerungsbefehle). Damit können diese Akteure im Extremfall bspw. 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.

2. Lieferkettensicherheit in den Fokus rücken

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

VDMA
Power Systems

Kritisch sind:

- Herkunft von Netz- und Steuerungskomponenten sowie auch Gesamtsystemen
- 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 von Gesamtsystemen und Akteure aus Drittstaaten, die (potenziell) staatlicher Einflussnahme unterliegen, sind als unzuverlässig einzustufen. Die Zertifizierung einzelner Komponenten und Zugriffmöglichkeiten des BSI reichen nicht aus, um Risiken angemessen und vollständig zu minimieren.
- Darüber hinaus erfasst die bisherige Gesetzeslage die Gefahren durch einen steuernden und/oder parametrisierenden Zugriff auf Anlagen/Systeme durch Externe nicht angemessen genug. Dies gilt insbesondere für den versorgungskritischen Bereich Energie – der von anderen Bereichen wie der Telekommunikation gesondert zu betrachten ist.
- Dauerhafte Risikobewertungen durch BMI unter Einbeziehung technischer und nicht-technischer Faktoren.

Akteure aus rivalisierenden oder unsicheren Drittstaaten können Anlagen manipulieren, überwachen oder stilllegen. Digitale Zugriffe durch Dritte, insbesondere Schalt- und parametrisierende Handlungen welche durch Hersteller, Energiedienstleister oder andere externe Akteure erfolgen, müssen klar geregelt und als kritische Interaktion im Energiesystems und der Versorgungssicherheit behandelt werden.

VDMA
Power Systems

Um diese zentralen Lücken zu schließen, sollten die folgenden konkreten Ansatzpunkte gesetzlich umgesetzt werden:

Die im Nis2UmsuCG gegebene Möglichkeit, den Einsatz kritischer Komponenten zu untersagen, ist ein wichtiger Schritt, reicht jedoch nicht aus, um Sicherheitsrisiken im Energiesektor angemessen zu reduzieren. Insbesondere der Fernzugriff von Herstellern auf Energieanlagen stellt ein relevantes Risiko für die Versorgungssicherheit dar und sollte daher reguliert werden. Daher muss der Fernzugriff nicht-vertrauenswürdiger Hersteller aus Drittstaaten adressiert werden. Analog kann so das BMI im Benehmen mit dem BMWE und dem Auswärtigen Amt befugt sein, den Einsatz einer Anlage zu untersagen, wenn der technisch mögliche Fernzugriff des Herstellers auf kritische Komponenten ein Sicherheitsrisiko für Deutschland darstellt. Als Fernzugriff gilt dabei die Möglichkeit des Herstellers, Anlage oder Komponenten zu steuern. Im Falle einer Untersagung kann das BMI zudem den Einsatz weiterer Anlagen desselben Herstellers oder Typs untersagen. Bei der Risikoprüfung ist insbesondere zu berücksichtigen, ob der Hersteller direkt oder indirekt von einer Drittstaatenregierung kontrolliert wird oder zur Zusammenarbeit mit staatlichen Stellen verpflichtet ist.

Bei der Risikoprüfung sind insbesondere folgende Kriterien gesetzlich zu verankern:

- Ob der Hersteller einer unmittelbaren oder mittelbaren Kontrolle durch staatliche Stellen oder Streitkräfte eines Drittstaates unterliegt oder hierzu verpflichtet werden kann.
- Ob der Hersteller bereits an Aktivitäten beteiligt war, die nachteilige Auswirkungen auf die öffentliche Ordnung oder Sicherheit Deutschlands, eines EU-Mitgliedstaates, eines EFTA-Staates oder eines NATO-Staates hatten oder haben könnten.
- Ob weitere Anhaltspunkte bestehen, die Zweifel an der Vertrauenswürdigkeit des Herstellers begründen.
- Ob ein technisch möglicher Fernzugriff im Einklang mit den sicherheitspolitischen Interessen Deutschlands, der Europäischen Union oder der NATO steht.

Im Falle einer Untersagung muss das BMI zudem die Möglichkeit haben, auch den zukünftigen Einsatz weiterer Anlagen desselben Herstellers sowie baugleicher oder verwandter Anlagentypen zu untersagen. Die Entscheidung hierüber sollte in Form einer Allgemeinverfügung ergehen.

Widerspruch und Klage gegen solche Maßnahmen dürfen keine aufschiebende Wirkung entfalten, um akute sicherheitsrelevante Risiken zu verhindern.
Zur effizienten Sachverhaltsermittlung ist der Betreiber gesetzlich zur umfassenden Mitwirkung zu verpflichten. Dies umfasst die vollständige und wahrheitsgemäße Angabe aller relevanten Informationen sowie die Benennung und Bereitstellung aller bekannten Beweismittel.

Fazit

Deutschland und Europa sind abhängig 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,
- Striktes Management auch von Risken aus der Lieferkette,

kann die Versorgungssicherheit langfristig gewährleistet werden.

Wichtig ist nun:

- Eine wirksame Gesetzeslage im Bereich der Sicherheit des Energiesystems ist zwingend erforderlich, im überparteilichen Interesse und mit Blick auf die Sicherheit Deutschlands.
- Anlagen wie Windenergieanlagen, Wechselrichter, Batteriespeicher oder weitere für die Energieversorgung relevante Systeme sind aufgrund ihrer systemrelevanten Funktionen kritische Anlagen.
- Die Gesetzgebung muss zukünftig berücksichtigen, dass Sicherheit nicht allein durch den Einsatz vertrauenswürdiger Komponenten gewährleistet werden kann. Sie erfordert insbesondere die konsequente Regulierung aller digitalen Zugriffe durch Dritte, etwa Hersteller oder Dienstleister, die systemnahe Funktionen wie Fernwartung oder Steuerung ausüben.

VDMA
Power Systems

Kontakt:

[redacted]
[redacted] Technik & Innovation
Telefon: [redacted]
E-Mail: [redacted]

[redacted]
[redacted] Energiepolitik
Telefon: [redacted]
E-Mail: [redacted]

Lobbyregister: R000802
EU-Transparenzregister ID: 9765362691-45

vdma.eu