Berlin, Juli 2025

Stärkung der Sicherheit europäischer Windenergie durch eine lückenlose NIS-2-Umsetzung

Mit fortschreitendem Ausbau der Windenergie und anderer dezentraler Erzeugungsanlagen sowie der zunehmenden Vernetzung im Energiesektor erlangt die Cybersicherheit immer größere Bedeutung. Vor diesem Hintergrund begrüßen die europäischen Hersteller von Windenergieanlagen (WEA) den vorliegenden Entwurf des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes vom 23.06.2025 (im Folgenden: Gesetzentwurf) als wichtigen Schritt in die richtige Richtung. Gleichwohl sehen wir an verschiedenen Stellen Klarstellungs- bzw. Verbesserungsbedarf, um die Sicherheit von WEA als zentralen Baustein der europäischen Energieversorgung zu erhöhen:

1. Ein-Betreiber-Prinzip wahren – kritische Erzeugungsanlagen auch auf die aggregierte Erzeugungsleistung eines Herstellers ausweiten

Windenergieanlagen enthalten eine große Anzahl steuerbarer Kontrollsysteme und sind größtenteils mit der Netzinfrastruktur verbunden, um Produktions- oder Zustandsdaten zu teilen. Neben dem Netzbetreiber, dem Anlagenbetreiber und Servicedienstleistern ist der Hersteller wesentlich für den Betrieb der Anlagen und hat einen digitalen Zugang zu den Windenergieanlagen, um die erforderlichen Dienstleistungen während des gesamten Lebenszyklus zu erbringen. Dies kann auch dann der Fall sein, wenn keine direkte Datenverbindung besteht. WEA-Hersteller könnten faktisch über ihre Anlagen in die Stromerzeugung eingreifen, bspw. indem sie Anlagen oder Steuerungssysteme abschalten und durch nicht ordnungsmäßigen Betrieb oder die Übermittlung falscher Netzsignale Schäden verursachen. **Bei der Definition kritischer Erzeugungsanlagen sollte daher nicht nur auf die aggregierte Leistung eines Betreibers, sondern auch auf die Erzeugungsleistung, auf die ein Hersteller Zugriff hat, abgestellt werden. In der Konsequenz sind Windenergieanlagen als kritische Erzeugungsanlagen einzustufen, unabhängig von der Größe des Windparks, in dem sie sich befinden. Der Betreiber müsste für die entsprechende Erzeugungsanlage folglich die Anforderungen der IT-Sicherheitskataloge sowie die Vorgaben des Katalogs kritischer Funktionen/Komponenten erfüllen.**

Der Gesetzentwurf adressiert Hersteller von WEA gemäß §5c EnWG-E bislang als „Betreiber digitaler Dienste“, die, sofern sie den KRITIS-Schwellenwert überschreiten, für die Sicherheit ihres Systems garantieren müssen, welches Zugriff auf die Steuerung von WEA ermöglicht (d.h. die Leitwarte in Deutschland). Die eigentliche WEA, für die der jeweilige Betreiber Verantwortung trägt, bleibt jedoch unreguliert. Dies stellt eine Sicherheitslücke dar, die im Gesetzentwurf geschlossen werden muss.

Forderung 1: Jede Windenergieanlage, auf die Betreiber digitaler Dienste wie WEA-Hersteller per Fernsteuerung zugreifen können, sollte als kritische Anlage definiert und reguliert werden. Das Ein-Betreiber-Prinzip der Windenergieanlage ist dabei zu wahren, die Verantwortung für die Cybersicherheit der jeweiligen WEA verbleibt also bei dem Betreiber.

Alternativ sollte die Einführung niedrigerer Schwellenwerte für kritische (Windenergie-) Anlagen geprüft werden. Aufgrund der spezifischen technischen Gegebenheiten der Windenergie kann die integrierte Umrichtertechnologie bereits bei einem wesentlich niedrigeren Schwellenwert Auswirkungen auf die Verteilnetzebene haben.

2. Neue Werkzeuge zum Verbot kritischer Komponenten und Dienstleistungen müssen konkretisiert und konsequent genutzt werden

Hersteller, die unter dem Einfluss eines rivalisierenden oder potenziell feindlichen Staates stehen, können dazu benutzt werden, die Windenergieanlagen, die Stromerzeugung und das Stromnetz zu manipulieren, zu überwachen oder zu beschädigen. Selbst lokale Stromausfälle oder Überkapazitäten können dabei zu Netzinstabilität führen und damit auch entlegene Regionen betreffen.

Wie in der Formulierungshilfe der Bundesregierung vom 02.12.2024 vorgesehen, sollte es dem BMI gemäß §56 (7) BSIG-E im Einvernehmen mit dem BMWE und dem AA aktiv ermöglicht werden, per Rechtsverordnung kritische Komponenten zu definieren und ihren Einsatz in kritischen Anlagen zu untersagen, sofern dies die öffentliche Ordnung oder Sicherheit Deutschlands voraussichtlich beeinträchtigt (§41 BSIG-E). Laut Gesetzentwurf soll hierbei insbesondere berücksichtigt werden, ob der Hersteller kritischer Komponenten unmittelbar oder mittelbar von der Regierung eines Drittstaates kontrolliert wird oder zur Zusammenarbeit verpflichtet ist bzw. verpflichtet werden kann. **Dieses Instrument sollte zur Gewährleistung der nationalen Sicherheit konsequent genutzt werden.**

Forderung 2a: Der Einsatz kritischer Komponenten von nicht vertrauenswürdigen Herstellern und von Herstellern, die unter der Kontrolle eines Drittstaates stehen, sollte in allen kritischen Anlagen untersagt werden.

Die Möglichkeit zur Untersagung des Einsatzes kritischer Komponenten ist wichtig, aber nicht ausreichend. Auch kritische Prozesse und Funktionen, wie der Zugriff auf WEA-Anlagen, sind für die Sicherheit von Energieanlagen relevant und müssen entsprechend reguliert werden.

Auf Grundlage von §30 und §31 in Verbindung mit §39 BSIG-E sollten neben kritischen Komponenten auch Prozesse und Funktionen untersagt werden können, wenn sie den Risikomanagementpflichten nicht ausreichend entsprechen. Ein solcher Fall liegt z.B. vor, wenn Zertifizierungen nicht erteilt wurden. Gemäß §52 BSIG-E kann das BMI die Zertifikaterteilung für bestimmte Produkte oder Leistungen untersagen, wenn „überwiegende öffentliche Interessen, insbesondere sicherheitspolitische Belange der Bundesrepublik Deutschland, der Erteilung entgegenstehen“.

Forderung 2b: Die Möglichkeit zur Untersagung kritischer Dienstleistungen ist im NIS2UmsuCG angelegt, sollte jedoch konkretisiert werden. Folglich sollte die Ausübung kritischer Dienstleistungen aus nicht vertrauenswürdigen Drittstaaten untersagt werden.

ENERCON
Ansprechpartner:
Philipp Vohrer | philipp.vohrer@enercon.de
Andreas Becker | andreas.becker@enercon.de

Nordex
Ansprechpartner:
Tony Adam | tadam@nordex-online.com

Vestas
Ansprechpartner:
Johannes Schiel | joshi@vestas.com

Siemens Energy
Ansprechpartner:
Jon Lezamiz Cortazar | jon.lezamiz-cortazar@siemens-energy.com
Maximilian Fricke | maximilian.fricke@siemens-energy.com

VDMA Power Systems
Ansprechpartner:
Malte Peters | malte.peters@vdma.org