Kleine Anfrage zur schriftlichen Beantwortung
gemäß § 46 Abs. 1 GO LT
mit Antwort der Landesregierung

Anfrage der Abgeordneten Verena Kämmerling, Axel Miesner und Jonas Pohlmann (CDU)

Antwort des Niedersächsischen Ministeriums für Umwelt, Energie und Klimaschutz namens der Landesregierung

Sicherheit der Erzeugung erneuerbarer Energien: Sind die Anlagen ausreichend gegen Cyberattacken geschützt?

Anfrage der Abgeordneten Verena Kämmerling, Axel Miesner und Jonas Pohlmann (CDU), eingegangen am 05.02.2025 - Drs. 19/6447,
an die Staatskanzlei übersandt am 06.02.2025

Antwort des Niedersächsischen Ministeriums für Umwelt, Energie und Klimaschutz namens der Landesregierung vom 07.03.2025

Vorbemerkung der Abgeordneten

Die *Welt am Sonntag* berichtete am 19. Januar 2025 unter der Überschrift „Xi Jinping kann Deutschland den Strom abschalten“, dass sich viele in Deutschland installierte Photovoltaikanlagen per Internetsignal abschalten ließen. Da in vielen Anlagen Wechselrichter chinesischer Hersteller verbaut seien, würde dies der chinesischen Regierung im Krisenfall die Möglichkeit eröffnen, in Deutschland einen Blackout auszulösen. In anderen Ländern sei es in der jüngsten Vergangenheit demnach bereits zur Abschaltung von Photovoltaikanlagen durch chinesische Hersteller gekommen.

Verschärft werde das Problem durch die Absicht der Bundesregierung, chinesische Hersteller zwecks Netzstabilisierung in verbrauchsarmen Zeiten, etwa während Feiertagen, um die gezielte Trennung deutscher Photovoltaikanlagen vom Netz zu bitten. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt davor, ausländischen Herstellern Zugriff auf eine so große Zahl von Anlagen im europäischen Verbundnetz zu eröffnen.

Windenergieanlagen werden nach Aussage in der Welt am Sonntag oft mit Steuerungskomponenten aus chinesischer Produktion ausgestattet. Der Verband Deutscher Maschinen- und Anlagenbau e. V. (VDMA) warnt, dass dadurch jede Anlage von außen ansteuerbar und erheblichen Cyberrisiken ausgesetzt sei. Litauen habe angesichts der skizzierten Risiken den Einbau chinesischer Steuerungskomponenten bereits untersagt.

Vorbemerkung der Landesregierung

Unser vermaschtes, europäische Stromsystem ist so ausgelegt, dass es den plötzlichen Ausfall einzelner Erzeugungsanlagen auffangen kann. Der synchrone Ausfall von Anlagen mit einer Leistung von mehreren Gigawatt stellt das System hingegen vor große Herausforderungen, die im Extremfall zum Ausfall der Versorgung führen können. Da einzelne Photovoltaik-Anlagen (PV) mit derartigen Komponenten zwar eine im Vergleich zu Windparks oder Übertragungsnetzen geringe Leistung haben, die insgesamt installierte PV-Leistung jedoch beträchtlich zugenommen hat, ist der synchrone Ausfall aufgrund von Zugriffen von außen auf baugleichen Komponenten ein Risiko, das mit zunehmendem Ausbau abgestellt werden muss.

Das niedersächsische Stromnetz ist Teil des europäischen Verbundsystems. Für seinen sicheren Betrieb ist die Sicherheit des Gesamtnetzes entscheidend. Insofern sind die nachgefragten Risiken keine, die allein Niedersachsen betreffen oder die allein hier minimiert werden könnten. Vielmehr ist es Aufgabe der zuständigen Stellen auf Bundes- und europäischer Ebene dafür zu sorgen, dass die Risiken minimiert, bestenfalls abgestellt werden. Eine Zuständigkeit des Landes ist an dieser Stelle nicht gegeben.

Ein Energieerzeuger ist zunächst nach § 49 EnWG für die (Betriebs-)Sicherheit seiner Anlage verantwortlich. Nach § 49 Abs. 1 EnWG sind Energieanlagen so zu errichten und zu betreiben, dass die technische Sicherheit gewährleistet ist. Dabei sind vorbehaltlich sonstiger Rechtsvorschriften die allgemein anerkannten Regeln der Technik zu beachten.

Auch hat die Europäische Union inzwischen strenge Sicherheitsanforderungen eingeführt, um den Schutz kritischer Infrastrukturen vor Cyber-Bedrohungen zu gewährleisten. Ab dem 1. August 2025 wird der RED Delegated Act VO (EU) 2022/30 zur Ergänzung der RL 2014/53/EU über die Harmonisierung von Funkanlagen-Bereitstellungen in der EU gesetzlich verpflichtend. Für die Hersteller von PV-Anlagen hat das zur Folge, dass alle Geräte mit eingebauter Funktechnologie, die sie ab dem 1. August 2025 auf dem europäischen Markt anbieten möchten, die Vorgaben aus dem Funkanlagengesetz vollständig einhalten müssen. Relevant ist hierbei vor allem Artikel 3.3 der RL 2014/53/EU, der verbindliche Vorschriften für Cybersicherheit für alle in Europa verkauften IoT-Produkte enthält. Photovoltaik-Anlagen, die auf drahtlose Verbindungen angewiesen sind, müssen danach eine neue und umfassende Reihe von Cybersicherheitsanforderungen erfüllen. Diese Anforderungen konzentrieren sich auf die Verbesserung der Netzschutzfunktionen, den Schutz personenbezogener Daten und die Verringerung von Betrugsrisiken (vgl. Art. 3.3. d-f der RL 2014/53/EU). Die Richtlinie sieht vor, dass alle von in die EU importierten oder dort hergestellten Produkte mit Funktechnologie ab August 2025 zwingend diese Anforderungen erfüllen müssen, um eine CE-Kennzeichnung zu erhalten. Diese Kennzeichnung signalisiert, dass ein Produkt konform mit den Vorgaben der RED-Richtlinie ist und es somit rechtmäßig in den Mitgliedstaaten der EU vertrieben werden darf.

Darüber hinaus ist am 10. Dezember 2024 der sogenannte Cyber Resilience Act der EU (Verordnung [EU] 2024/2847 vom 23. Oktober 2024 über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnungen [EU] Nr. 168/2013 und [EU] 2019/1020 sowie der Richtlinie [EU] 2020/1828 [Cyberresilienz-Verordnung]) in Kraft getreten. Der Cyber Resilience Act ist die erste europäische Verordnung, die ein Mindestmaß an Cybersicherheit für alle vernetzten Produkte festlegt, die auf dem EU-Markt erhältlich sind.

Nach Artikel 6 der Verordnung werden Produkte mit digitalen Elementen nur dann auf dem Markt bereitgestellt, wenn sie den grundlegenden Cybersicherheitsanforderungen der Richtlinie genügen und ordnungsgemäß installiert, gewartet und bestimmungsgemäß verwendet werden. Zudem müssen die vom Hersteller festgelegten Verfahren den grundlegenden, in Anhang I und II der Verordnung festgelegten, Cybersicherheitsanforderungen entsprechen sowie die gegebenenfalls erforderlichen Sicherheitsaktualisierungen installiert sein. Herstellern, Importeuren und Händlern werden mit der Verordnung daher strenge Pflichten auferlegt.

Die Verordnung gilt für alle Produkte, die direkt oder indirekt mit einem anderen Gerät oder Netzwerk verbunden sind, mit Ausnahme bestimmter quelloffener Software- oder Dienstleistungsprodukte, die bereits unter bestehende Vorschriften fallen (wie z. B. Medizinprodukte, Luftfahrt und Autos). Produkte tragen die CE-Kennzeichnung, um anzuzeigen, dass sie die CRA-Anforderungen erfüllen. Hersteller, Importeure und Händler müssen daher sicherstellen, dass ihre Produkte mit digitalen Elementen den Cybersicherheitsstandards für den EU-Markt entsprechen.

1. Wie groß ist in Niedersachsen der Anteil von Anlagen zur Erzeugung erneuerbarer Energien, in denen chinesische Wechselrichter oder Steuerungskomponenten verbaut wurden?

Hierzu liegen der Landesregierung keine belastbaren Daten vor.

2. Teilt die Landesregierung die Einschätzung, dass sich aus der Nutzung chinesischer Wechselrichter und Steuerungskomponenten sowie der Ansteuerbarkeit der Anlagen über das Internet ein Cyberrisiko für Anlagen zur Erzeugung erneuerbarer Energien ergibt? Falls nein, warum kommt die Landesregierung zu einer anderen Einschätzung als das BSI und der VDMA? Falls ja, welche Maßnahmen wird die Landesregierung gegebenenfalls ergreifen, um den Schutz der Energieerzeugung vor Cyberrisiken in Niedersachsen zu verbessern?

Die Landesregierung hat keine Gründe zu einer anderen Einschätzung bezüglich der Sicherheit der Anlagen mit derartigen Wechselrichtern zu kommen. Vielmehr teilt sie die Sorgen bezüglich Cyberattacken von außen. Daher unterstützt die Landesregierung auch höhere Sicherheitsstandards bis hin zum Ausschluss von sicherheitsrelevanten Komponenten aus bestimmten Staaten. Grundsätzlich ist es erforderlich, dass unabhängig vom Herkunftsland alle verbauten Komponenten, auf die von außen zugegriffen werden kann, diejenigen hohen Sicherheitsstandards erfüllen, welche die EU für künftige Produkte definiert hat bzw. auf dieser Basis definiert werden.

3. Wie sind Anlagen zur Erzeugung erneuerbarer Energien in Niedersachsen derzeit gegen Cyberattacken und Einflussnahmen durch ausländische Unternehmen und Regierungen geschützt?

Siehe Vorbemerkung.

4. Unterstützt die Landesregierung das Vorhaben der amtierenden Bundesregierung, chinesische Hersteller um die Abregelung in Niedersachsen installierter Photovoltaikanlagen zu bitten? Falls nein, welche Maßnahmen wird die Landesregierung ergreifen, um dies zu verhindern?

Die Landesregierung unterstützt die Bundesregierung in ihrem Bemühen, jedwede Fernwartungs- und Steuerungsmöglichkeit von Komponenten vor unbefugtem Zugriff zu sichern. Sie befürwortet, Zugriffe allein auf solche aus dem EU-Raum zu beschränken. Mit den Regelungen, die die EU getroffen hat, ist eine Erhöhung der Sicherheit zu erwarten.

5. Hält die Landesregierung den Einbau chinesischer Steuerungskomponenten und Wechselrichter in Anlagen zur Erzeugung erneuerbarer Energien weiterhin für vertretbar? Falls ja, warum kommt sie insoweit zu einer anderen Einschätzung als z. B. die litauische Regierung? Falls nein, was gedenkt die Landesregierung zu tun?

Die Landesregierung unterstützt ein Höchstmaß an Sicherheit und die höheren Anforderungen der EU. Aus Sicht der Landesregierung muss jeder unbefugte Zugriff von außerhalb des EU-Raums sicher ausgeschlossen werden. Ob der Einbau chinesischer Steuerungskomponenten und Wechselrichter vor dem Hintergrund von Erkenntnissen der Sicherheitsbehörden vertretbar ist, muss die Bundesregierung bewerten.

(Verteilt am 11.03.2025)