Deutscher Bundestag **Drucksache 21/9338**

21. Wahlperiode 23.11.2026

Vorabfassung - wird durch die lektorierte Version ersetzt.

Kleine Anfrage

der Abgeordneten Ruben Rupp, Robin Jünger, Alexander Arpaschi, Sebastian Maack, Tobias Ebenberger, Lars Haise, Edgar Naujok, Steffen Janich, Prof. Dr. Michael Kaufmann, Carina Schießl, Beatrix von Storch, Micha Fehre, Peter Bohnhof, Ronald Gläser, Martin Hess, Sascha Lensing und der Fraktion der AfD

Zur Gefährdung der deutschen Energieinfrastruktur durch ungesicherte Verwaltungssysteme bei Windparks und Solaranlagen im Internet

Die Stabilität und die Sicherheit der bundesdeutschen Energieversorgung hängen im Zuge der voranschreitenden sogenannten Energiewende in erheblichem Maße von der Verfügbarkeit dezentraler Erzeugungsanlagen ab. Mit der politisch gewollten massenhaften Einspeisung von Strom aus Windkraft- und Photovoltaikanlagen wächst zugleich die Anfälligkeit des Gesamtsystems gegenüber Cyberangriffen und Sabotageakten.

Aktuelle Untersuchungen niederländischer Sicherheitsforscher offenbaren erhebliche Sicherheitslücken: Demnach wurden europaweit mehr als 8 500 Verwaltungs- und Steuerungssysteme von Wind- und Solarparks identifiziert, die ohne hinreichende Schutzmechanismen frei über das öffentliche Internet erreichbar waren (vgl. www.heise.de/news/Tausende-europaeische-Windanlagen-und-Solarparks-offen-im-Internet-11482262.html). Deutschland nimmt hierbei eine unrühmliche Spitzenposition ein: Allein 212 Steuerungssysteme von Windenergieanlagen sowie mindestens 672 Verwaltungsschnittstellen von Photovoltaikanlagen waren hierzulande ungeschützt online zugänglich (vgl. https://modat.io/blog/modat-research-exposed-systems-wind-and-solar/). Über solche exponierten Schnittstellen könnten unter anderem Steuerbefehle, Produktionsdaten, Netzkopplungspunkte und teilweise Standard-Zugangskennungen eingesehen oder manipuliert werden (https://publica-rest.fraunhofer.de/server/api/core/bitstreams/378d4c9c-326e-41ec-b4b6-2f6c8c616e96/content).

Ein unbefugter Zugriff auf Steuerungssysteme von Anlagen erneuerbarer Energien birgt das reale Risiko koordinierter Abschaltungen, gezielter Frequenz- und Spannungsmanipulationen und folglich schwerer Störungen bis hin zu großflächigen Netzüberlastungen und Ausfällen. Verschärfend kommt der mutmaßliche Einsatz von Komponenten und Steuerungselektronik aus Drittstaaten, deren Integrität und Missbrauchspotenzial wiederholt Gegenstand von Sicherheitsbedenken waren, hinzu.

Wir fragen die Bundesregierung:

1. Wie viele Verwaltungssysteme, Leit- und Fernwirkschnittstellen von Windenergieanlagen (Onshore und Offshore) sowie gewerblichen Photovoltaikanlagen (ab 100 KW) in Deutschland sind nach Kenntnis der Bun-

desregierung aktuell ungeschützt über das öffentliche Internet erreichbar oder waren es in den vergangenen 24 Monaten?

2. Kennt und wie bewertet die Bundesregierung die konkreten Befunde der einleitend zitierten Sicherheitsforscher hinsichtlich der in Deutschland identifizierten 212 Windenergie- und 672 Solarpark-Verwaltungssysteme, und welche weitergehenden Erkenntnisse liegen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) hierzu vor?
3. Wurden die betroffenen Anlagenbetreiber über das BSI, das Nationale Cyber-Abwehrzentrum (Cyber-AZ) oder die zuständigen Computer Emergency Response Teams (CERT) bereits identifiziert und über die Sicherheitslücken informiert, und wie viele Betreiber haben diese Schwachstellen nach Kenntnis der Bundesregierung bislang nachweislich und mit welchen Maßnahmen geschlossen (bitte ausführen)?
4. Welche konkreten gesetzlichen und regulatorischen Vorgaben (insbesondere nach dem BSI-Gesetz) gelten derzeit für die Absicherung von Verwaltungs-, Wartungs- und Fernsteuerungsschnittstellen bei Anlagen Erneuerbarer Energien, und ab welchen Leistungsschwellen greifen diese Pflichten im Einzelnen?
5. Welche behördlichen Kontroll-, Prüf- oder Sanktionsmechanismen existieren seitens der Bundesnetzagentur oder des BSI, um sicherzustellen, dass Betreiber von Wind- und Solarparks administrative Steuerungsschnittstellen nicht fahrlässig oder gar vorschriftswidrig im öffentlichen Internet exponieren?
6. Plant die Bundesregierung Maßnahmen, um bestehende Regulierungslücken bei kleineren und mittleren Erzeugungsanlagen zu schließen, die formell nicht unter den Schwellenwert Kritischer Infrastrukturen (KRITIS) fallen, in ihrer Summe jedoch netzrelevante Gesamtkapazitäten steuern (bitte ausführen)?
7. Welche Erkenntnisse liegen der Bundesregierung über die Hersteller, Fabrikate und Herkunftsländer (insbesondere der Volksrepublik China) der in deutschen Wind- und Solarparks verbauten Wechselrichter, Fernwirkeinheiten (RTU), SCADA-Systeme und Speichersteuerungen vor (bitte ausführen und auflisten)?
8. Sieht die Bundesregierung ein abstraktes oder konkretes Sicherheitsrisiko darin, dass Komponenten aus Drittstaaten über integrierte Mobilfunk- oder Cloud-Schnittstellen durch ausländische Akteure manipuliert oder aus der Ferne abgeschaltet werden könnten, und wenn ja, wie wird dieses Risiko operativ überwacht (bitte ausführen)?
9. Prüft die Bundesregierung die Einführung verbindlicher Zertifizierungsstandards oder den Ausschluss nicht vertrauenswürdiger Hersteller bei kritischen IT- und Steuerungskomponenten für Anlagen Erneuerbarer Energien (bitte ausführen)?
10. Wie viele Cyberangriffe, unbefugte Fernzugriffe oder gravierende Sicherheitsvorfälle auf Wind- und Solarparks beziehungsweise deren Betreibergesellschaften wurden seit 2022 beim BSI oder weiteren Sicherheitsbehörden des Bundes registriert (bitte nach Jahren, Energieträger und Art des Vorfalls aufschlüsseln)?
11. Welche konkreten Erkenntnisse besitzt die Bundesregierung über erfolgreiche Sabotageversuche oder Ransomware-Angriffe auf deutsche Anlagenbetreiber oder deren Zulieferer (wie beispielsweise Fernwartungsdienstleister oder Satellitenkommunikationssysteme) seit 2022?

Vorabfassung - wird durch die lektorierte Version ersetzt.

Zu welchen Schäden inklusive eines Datenabflusses ist es dabei im Einzelnen gegebenenfalls gekommen?

12. Sind der Bundesregierung Fälle bekannt, bei denen es infolge von IT-Sicherheitsvorfällen an Anlagen Erneuerbarer Energien zu tatsächlichen Einspeiseunterbrechungen, Netzinstabilitäten oder Fehlschaltungen kam (bitte ausführen)?

13. Welche Anforderungen stellt die Bundesregierung an die Notfall- und Schwarzstartkonzepte der Übertragungs- und Verteilnetzbetreiber für den Fall, dass eine erhebliche Anzahl dezentraler Erzeugungsanlagen durch einen koordinierten Cyberangriff zeitgleich vom Netz getrennt oder unkontrolliert hochgefahren wird?

14. In welchem Umfang sind Betreiber von Windparks und Solaranlagen verpflichtet, autarke Notabschaltmechanismen und manuelle Steuerungsfähigkeiten vorzuhalten, die im Falle eines Cyberangriffs unabhängig von Internet- und Cloudverbindungen vor Ort bedient werden könnten (bitte ausführen)?

15. Welche behördlichen Vorgaben existieren für den Einsatz und die Überwachung von Standard-Zugangsdaten, und wie will die Bundesregierung das fortgesetzte Inverkehrbringen von Anlagen mit unsicheren Werkseinstellungen unterbinden?

Berlin, den 17. November 2026

Dr. Alice Weidel, Tino Chrupalla und Fraktion

Vorabfassung - wird durch die lektorierte Version ersetzt.

Vorabfassung - wird durch die lektorierte Version ersetzt.

Gesamtherstellung: H. Heenemann GmbH & Co. KG, Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin, www.heenemann-druck.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.bundesanzeiger-verlag.de
ISSN 0722-8333