

Risiken für Wind- und Solarparks

[13.10.2026] Eine neue Studie hat Tausende über das Internet erreichbare Systeme im Umfeld europäischer Wind- und Solarparks identifiziert. Der Cyber-Sicherheitsrat Deutschland warnt vor wachsenden Risiken für die Energieversorgung durch die zunehmende Dezentralisierung.

Die Energiewende vergrößert die digitale Angriffsfläche der europäischen Energieinfrastruktur. Darauf weist der [Cyber-Sicherheitsrat Deutschland](#) unter Berufung auf eine Untersuchung des Unternehmens [Modat](#) und des niederländischen [National Cyber Security Centre](#) hin. Die auf der ONE Conference in Den Haag vorgestellte Studie „To see the wind and the sun“ identifizierte insgesamt über 8.500 über das öffentliche Internet erreichbare Systeme im Umfeld europäischer Wind- und Solarparks.

Deutschland liegt mit rund 210 exponierten Systemen im Bereich Windenergie an der Spitze der untersuchten Länder. Hinzu kommen 670 Systeme im Umfeld von Solaranlagen. An 180 Standorten stellten die Forscher Möglichkeiten zur weitreichenden Fernsteuerung fest. Eine untersuchte Benutzeroberfläche einer Windturbine bot beispielsweise Funktionen zum Starten, Stoppen und Zurücksetzen der Anlage. Die Autoren gehen davon aus, dass die tatsächliche Zahl betroffener Systeme höher liegt, da nur eindeutig zuordenbare Anlagen berücksichtigt wurden.

Wachsende Herausforderung für die Versorgungssicherheit

Hans-Wilhelm Dünn, Präsident des Cyber-Sicherheitsrats Deutschland, sieht darin eine wachsende Herausforderung für die Versorgungssicherheit. „Wir dezentralisieren unsere Energieversorgung – und dezentralisieren damit gleichzeitig ihre digitale Angriffsfläche“, erklärt Dünn. Der Schutz kritischer Energieinfrastruktur dürfe sich deshalb nicht auf große Kraftwerke und Netzbetreiber beschränken.

Dass Cyberangriffe auf dezentrale Energieanlagen reale Auswirkungen haben können, zeigte nach Angaben des Verbands ein Vorfall in Polen im Dezember 2025. Bei einem koordinierten Angriff wurden dort Kommunikationsverbindungen zu rund 30 Wind- und Solaranlagen beeinträchtigt.

Verbesserung der Cyber-Abwehr

Dünn fordert, die Erkenntnisse der Studie bei der Entwicklung des geplanten Cyberdome zu berücksichtigen. Das Konzept zur Verbesserung der Cyber-Abwehr setze mit Sensorik, Analyse und Früherkennung grundsätzlich an der richtigen Stelle an. Entscheidend sei jedoch, ob sich aus einem verbesserten Lagebild auch ein wirksamerer Schutz der Energieinfrastruktur ergebe. Insbesondere müsse untersucht werden, inwieweit zahlreiche dezentrale Schwachstellen zu einem übergreifenden Risiko für die Versorgungssicherheit werden könnten.

(al)

Stichwörter: Informationstechnik, Cybersicherheit