

### ENERGIEVERSORGUNG

## Die Sorge vor Hackern steigt

**Tausende Windräder sind aktuell gestört. Dahinter könnte eine Cyberattacke stehen. Experten warnen: Deutschlands Energiesysteme sind für Hacker ein attraktives Ziel.**

Ein besorgniserregendes Szenario drängt dieser Tage wieder ins Bewusstsein von Behörden, Unternehmen und Bürgern: Ein flächendeckender Stromausfall in Deutschland oder gar Europa, ausgelöst durch einen Cyberangriff. Seit Beginn des Ukrainekrieges gibt es eine Störung bei Tausenden deutschen Windrädern, das Bundesamt für Sicherheit in der Informationstechnik (BSI) schließt einen Hackerangriff als Ursache nicht aus.

Die Angst vor gezielten Cyberattacken auf die Energie-Infrastruktur ist in der Branche zu spüren. So beobachtet etwa der Eon-Konzern, der das größte Stromverteilnetz in Deutschland betreibt, parallel zur russischen Invasion am Boden vermehrt Angriffe auf die digitale Infrastruktur. "Unsere Detektions- und Reaktionsfähigkeiten haben wir erhöht", teilt Eon mit. Aber könnten russische Hacker tatsächlich die Stromversorgung in Deutschland abschalten?

IT-Expertinnen und -Experten warnen vor zu schlechten Schutzmaßnahmen. "Deutschland ist perspektivisch nicht ausreichend auf Cyberangriffe auf erneuerbare Energiesysteme vorbereitet. Windkraftanlagen und Solarenergieunternehmen können hierdurch in Mitleidenschaft gezogen werden", sagt Sadaf Momeni, Beraterin für IT-Sicherheit bei der Ginkgo Cybersecurity GmbH. Für den Zugriff auf viele verschiedene Wind- und Solaranlagen werde beispielsweise ihrer Erfahrung nach oftmals nur ein einziges Passwort genutzt - statt mehrere verschiedene, warnt Momeni.

Probleme sieht auch Lothar Renner, EMEAR-Geschäftsführer für Security beim US-Technologiekonzern Cisco: "Viele Industriebetriebe nutzen noch alte, proprietäre Protokolle" - also Lösungen, die ausschließlich bei diesem Unternehmen zum Einsatz kommen. Finde ein Angreifer heraus, wie der Datenaustausch innerhalb solcher Unternehmen funktioniert, gebe es kaum Experten, die gegen einen Angriff vorgehen könnten.

In der aktuellen Bedrohungslage können veraltete Systeme besonders problematisch sein. Hans-Walter Borries ist stellvertretender Vorstandsvorsitzender des Bundesverbands für den Schutz Kritischer Infrastrukturen und glaubt: "Es ist realistisch, dass russische Hacker versuchen, unser Energiesystem anzugreifen." Borries ist auch Dozent an der Universität Witten/Herdecke sowie Reserveoffizier bei der Bundeswehr.

### Leitwarten als sensibles Angriffsziel

Laut Borries gibt es in Deutschland ein paar besonders schutzbedürftige Orte, die für eine funktionierende Stromversorgung essenziell sind und die aus Hackersicht "lohnende Ziele" wären. Zum einen seien da die zentralen Leitwarten der großen Übertragungsnetzbetreiber in Deutschland. An diesen Stellen halten die Betreiber Stromerzeugung und -verbrauch im Gleichgewicht. Nur wenn die Frequenz im Netz nahe ihrem Sollwert von 50 Hertz liegt, funktioniert die Stromversorgung zuverlässig. Fließt hingegen zu viel oder zu wenig Strom ins Netz, kann es zu Stromausfällen kommen.

"Jemand, der die Kontrolle über eine zentrale Leitwarte erlangt, könnte die Energieversorgung in Europa nachhaltig stören", warnt Borries. "In einer militärischen Auseinandersetzung würden solche Stellen womöglich vorrangig angegriffen."

Zum Schutz solcher kritischer Komponenten äußern sich Übertragungsnetzbetreiber wie Tennet oder 50Hertz derzeit nicht. Das Thema erscheint ihnen - angesichts der Entwicklung in der Ukraine - zu riskant, um nähere Auskunft darüber zu geben. 50Hertz teilt lediglich mit, dass das Unternehmen Vorsorge treffe, um Einrichtungen und Personal zu schützen.

Tennet gibt an, die eigenen Systeme jederzeit auf dem neuesten Stand zu halten und ein dediziertes Risikomanagement durchzuführen. Zudem sei die Energie-Erzeugung redundant ausgelegt. Es gibt also Ersatzverbindungen und -komponenten für Notfälle.

Hinweise darauf, wie gut das Stromnetz gegen Cyberangriffe geschützt ist, gibt aber Fabian Potratz, Chief Technology Officer des Start-ups Envelio, das auf digitales Stromnetzmanagement spezialisiert ist und seit einigen Monaten mehrheitlich Eon gehört. Sein Start-up habe eine Zertifizierung zur Informationssicherheit erwerben müssen, erklärt Potratz. Das werde jährlich überprüft, obwohl sein Start-up gar nicht Teil des Leitsystems sei.

Selbst wenn ein Angreifer das Start-up Envelio hacken würde, könne er von dort aus nicht auf die Stromleitsysteme zugreifen, denn die Büro-IT der Netzbetreiber sei strikt von der Steuerung der Netze getrennt. Aber: "Ohne Security-Mindset kommt man keinen Meter weit in der Branche", sagt Potratz. "Das nehmen die Netzbetreiber sehr ernst." Sogar einen klassischen

physischen Angriff auf die Leitstellen hält Potratz für erfolgversprechender als einen Cyberangriff.

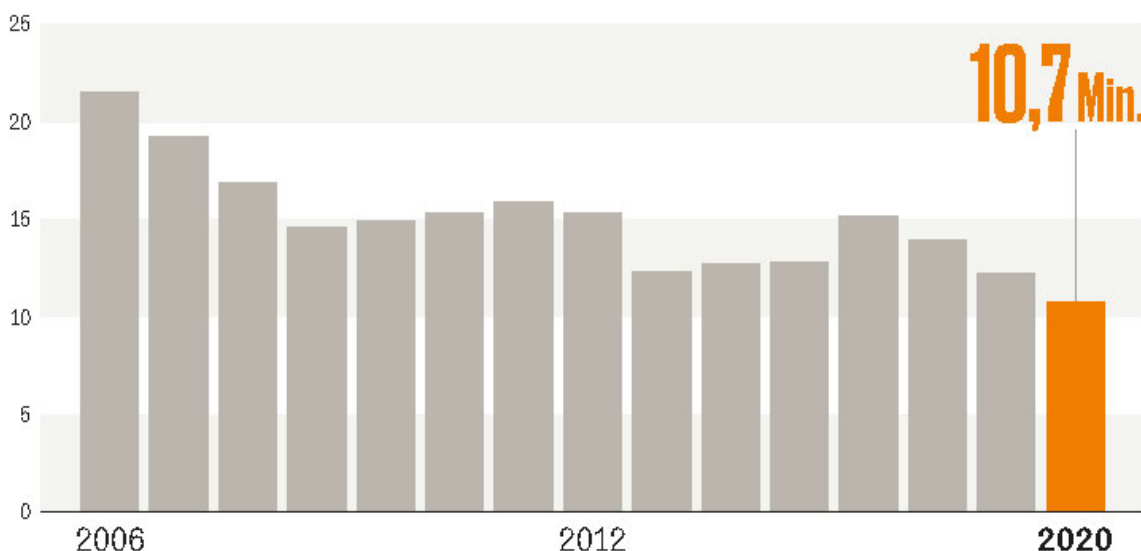
Experte Borries benennt indes noch ein weiteres, potenzielles Angriffsziel: die sogenannten Funkrundsteuersender der Europäischen Funkrundsteuerung GmbH (EFR). Europaweit gibt es drei solcher Sender - zwei davon in Deutschland und einen in Ungarn. Sie können per Langwelle Signale über 500 Kilometer versenden und ermöglichen es Stromnetzbetreibern, Wind- und Solarparks sowie Kraftwärmekopplungsanlagen zu steuern - und im Zweifel daran zu hindern, Strom einzuspeisen.

Ein Angreifer, der Zugriff auf die Sender bekäme, könnte damit Wind- und Solaranlagen immer wieder vom Netz nehmen, sagt Christoph Sorge, Professor am Lehrstuhl für Rechtsinformatik an der Universität des Saarlandes. Tatsächlich bestätigt das Bundesamt für Sicherheit in der Informationstechnik: "Sollte ein Angreifer die Kontrolle über das Funk-Rundsteuerungssystem erlangen, kann nicht ausgeschlossen werden, dass diese Anlagen durch den Angreifer zu einem Einspeisestopp veranlasst werden."

Laut Sorge müssten Angreifer Schwachstellen bei der Sendeeinrichtung oder bei den Empfängern suchen. Er sagt: "Beides ist vermutlich nicht einfach, aber ausschließen würde ich beides nicht."

### Stromversorgung mit Lücken

Länge der Versorgungsunterbrechung je Stromverbraucher  
in Deutschland in Minuten



HANDELSBLATT

Quelle: Bundesnetzagentur

Handelsblatt Nr. 047 vom 08.03.2022  
© Handelsblatt Media Group GmbH & Co. KG. Alle Rechte vorbehalten.  
Zum Erwerb weitergehender Rechte wenden Sie sich bitte an [nutzungsrechte@vhb.de](mailto:nutzungsrechte@vhb.de).

*Energiebranche: Stromversorgung - Länge der Versorgungsunterbrechung pro Jahr je Stromverbraucher in Deutschland in Minuten 2006 bis 2020 (MAR / Grafik)*


Krapp, Catiana

Quelle:	Handelsblatt print: Heft 47/2022 vom 08.03.2022, S. 28
Ressort:	Unternehmen
Branche:	ENE-01 Alternative Energie ENE-16 Strom ENE-16-03 Stromversorgung P4910
Dokumentnummer:	4D692F68-BF20-45BE-B540-E4C313414096

Dauerhafte Adresse des Dokuments:

[https://www.wiso-net.de/document/HB\\_4D692F68-BF20-45BE-B540-E4C313414096%7CHBPM\\_4D692F68-BF20-45BE-B540-E](https://www.wiso-net.de/document/HB_4D692F68-BF20-45BE-B540-E4C313414096%7CHBPM_4D692F68-BF20-45BE-B540-E)

Alle Rechte vorbehalten: (c) Handelsblatt GmbH

 © GBI-Genios Deutsche Wirtschaftsdatenbank GmbH