Bedenken zu China-Wechselrichtern

Wie die Photovoltaik in Europa sicherer werden kann

Um Cybersorgen vor unsicheren Photovoltaik-Komponenten aus China zu verringern, empfehlen deutsche Sicherheitsforscher mehr Transparenz und technische Maßnahmen. Dazu zählen offene Schnittstellen und Optionen für einen Offline-Modus. Ein chinesischer Anbieter zeigt sich grundsätzlich offen.

von **Oliver Ristau**

veröffentlicht am 22.12.2025

Hersteller von **PV-Komponenten** können die Sicherheit von Photovoltaikanlagen in Europa vor **Hackerangriffen** substanziell erhöhen, wenn sie bestimmte Features anbieten und technische Maßnahmen umsetzen. Darauf weisen Experten für **Cybersicherheit** gegenüber Tagesspiegel Background Energie hin. Das könnte auch das Vertrauen in Produkte aus Ländern wie China erhöhen.

Konkret geht es um die **Wechselrichter** von PV-Anlagen sowie **Batteriespeichern**. Sie sorgen physikalisch dafür, **Gleichstrom in Wechselstrom** umzuwandeln und damit den Strom kompatibel zur Aufnahme ins Stromnetz zu machen. Zugleich sind sie meist mit dem **Internet** verbunden, um so eine **bessere Steuerung der Anlagen** erreichen zu können. Doch diese Steuerbarkeit sorgt, wie berichtet *(https://background.tagesspiegel.de/energie-und-klima/briefing/fragezeichen-um-unklare-funkeinheiten-in-chinesischen-wechselrichtern)*, für **Unbehagen** in der Branche.

China dominiert Wechselrichter

So sieht der **Europäische Solarproduzentenverband ESMC** in der möglichen Fernsteuerbarkeit von Photovoltaikwechselrichtern ein besonderes Risiko. 70 Prozent der an das europäische Stromnetz angeschlossenen Wechselrichter ließen sich fernsteuern und seien somit „**potenzielle Ziele für Manipulationen**“, erklärte er unlängst in einer Stellungnahme *(https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/CI1/2-umsetzungs-cybersicherheit-2025/NIS2UmsuCG_RefE_ESMC.pdf?__blob=publicationFile&v=3)*.

Das Problem: „IT-Sicherheit lässt sich nicht vollständig ‚nachweisen‘“, sagt **Denis Feth**, Leiter für Security beim **Fraunhofer Institut für Experimentelles Software Engineering IESE** aus Kaiserslautern. Ob Produkte wie Wechselrichter als sicher angesehen werden, habe viel mit Vertrauen zu tun, denn **einhundertprozentige Sicherheit könne es prinzipiell kaum geben**. Hersteller könnten Vertrauen aber „durch technische Maßnahmen, Transparenz, Prüfungen, Zertifizierungen und Siegel“ aufbauen.

Wie das aussehen kann, dafür will der chinesische Elektronikspezialist **Sigenergy** ein Beispiel geben. Das Unternehmen vertreibt in China produzierte Speichersysteme und Wechselrichter für PV-

Anlagen. Das 2022 gegründete Unternehmen erwartet für das laufende Jahr bei Batteriespeichern im Privatkundengeschäft einen **Marktanteil von 10 Prozent in Deutschland** und will weiter expandieren.

Datenzentrum in Deutschland

Dafür sei es wichtig, die Sorgen in Europa rund um die IT-Sicherheit sehr ernst zu nehmen, sagte Gründer und Vorstandsvorsitzender **Tony Xu** kürzlich gegenüber **europäischen und chinesischen Journalisten** in Shanghai. Deshalb laufe sämtlicher Datenverkehr der Anlagen in Deutschland über ein **Amazon-Rechenzentrum** (AWS) in Frankfurt/Main. Das soll Sorgen vorbauen, dass Wechselrichter aus China gesteuert werden könnten.

Für Fraunhofer-Sicherheitsexperte Feth ist der Betrieb eines Cloud-Datenzentrums in Deutschland „grundsätzlich positiv, da damit der europäische Rechtsrahmen gilt. Gleichzeitig ist der **Standort des Rechenzentrums allein kein vollständiger Garan**t. Entscheidend ist, was die Software tut, wer administrativen Zugriff auf die Systeme hat und wie Updates, Zugriffsrechte und die Schlüsselverwaltung organisiert sind."

Mit anderen Worten: auch ein **einzelnes Datenzentrum lasse sich hacken** und fernsteuern als ein „single point of failure", wie es **Sadeeb Ottenburger** nennt, Leiter der Abteilung „Resiliente und Smarte Infrastruktursysteme" (RESIS) am Institut für Thermische Energietechnik und Sicherheit des **Karlsruher Instituts für Technologie (KIT)**.

Offene Schnittstellen

Sigenergy kündigt weitere Maßnahmen an. Die Optionen: die **Protokolle zu öffnen** und **Speicher und Wechselrichter von Dritten steuern zu lassen**, anstatt darauf zu bestehen, die Kontrolle zu behalten. Außerdem bietet das Unternehmen Kunden einen **vollständigen Offline-Betrieb** an, bei dem also die PV-Stromerzeugung und Batteriespeicherung unabhängig vom Datennetz erfolgen kann, auch wenn dann nicht 100 Prozent des Funktionsumfangs zur Verfügung stehen.

„Die Speicherung und Nutzung von Solarstrom wird aber auch **ohne Cloud funktionieren**", verspricht Xu. Mittelfristig soll es mittels KI aus dem Verbrauchsverhalten der Nutzer auch im Offline-Modus lernen können. Noch setzt KI die Kopplung mit der Cloud voraus.

Dazu Feth: „Die Öffnung der Kommunikationsprotokolle für Dritte ist aus technischer Sicht ein wichtiger Schritt, da sie Transparenz schafft und es ermöglicht, Wechselrichter und Speicher über alternative Energiemanagementsysteme zu betreiben." Eine **potenziell politisch motivierte Fernsteuerung** könne aber auch durch offene Schnittstellen **nicht ausgeschlossen werden**.

Offline-Betrieb

Deshalb sei der **Offline-Modus die sicherste Variante**, sofern dieser „dauerhaft und ohne funktionale Einschränkungen möglich bleibt und auch Wartung und Updates kontrolliert und idealerweise offline durchgeführt werden können."

KIT-Forscher Ottenburger gibt dabei aber zu bedenken, dass es **der systemischen Resilienz zuwiderlaufen würde**, betriebe man alle PV-Anlagen nur offline. Denn das Gelingen der Energiewende setze gerade die Vernetzung voraus. Ein Beispiel ist das Anfang 2025 beschlossene Solarspitzengesetz. Diese Novelle des **Energiewirtschaftsgesetz** (EnWG) verpflichtet größere PV-Anlagen unter anderem zur Fernsteuerbarkeit durch die Netzbetreiber.

Offene Schnittstelle als goldene Mitte

Für Ottenburger stellen deshalb die „offenen Schnittstellen im Rahmen des Machbaren die goldene Mitte“ dar. So bestehe die Möglichkeit, **Sicherheitsbedenken** auch an **nicht-europäische Produzenten aus China oder den USA** zu adressieren. PV-Produkte aus China müssten nicht pauschal unter Generalverdacht gestellt werden. Gleichzeitig eröffneten sie hiesigen Anbietern Marktchancen, etwa wenn sie die Steuerung der Anlagen übernehmen. „Wichtig ist aber, diese Schnittstellen regelmäßig mit Penetrationstests auf **Resilienz** zu überprüfen“, fordert er.

Für Unternehmen wie Sigenergy sind Cybersecurity-Maßnahmen auch eine Antwort auf die Anforderungen des **Cybersicherheitsgesetzes** NIS-2 *(https://www.bundestag.de/dokumente/textarchiv/2025/kw46-de-nis-2-1123138)*, das der Deutsche Bundestag im November 2025 verabschiedet hat. Das räumt dem **Bundesamt für Sicherheit in der Informationstechnologie** (BSI) unter anderem die Möglichkeit ein, cyberrelevante Komponenten wie Wechselrichter von nicht-europäischen Produzenten auf den Index zu stellen, wenn sie Sicherheitsprobleme verursachen könnten. Betreiber von Anlagenparks müssen außerdem die Cybersicherheit gewährleisten.

Teile der Recherche für diesen Text entstanden im Rahmen einer von Sigenergy organisierten Pressereise.

Verwandte Themen

Cybersicherheit