European Solar Manufacturing Council AISBL
2 rue de Praetere | 1000 Brussels – Belgium

2. Juli 2025

Rückfragen
Christoph Podewils, Generalsekretär
podewils@emsc.solar

Konsultationsbeitrag des European Solar Manufacturing Councils zum NIS-2 - Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG

Der European Solar Manufacturing Council (ESMC) begrüßt die Möglichkeit, an der Verbändeanhörung „NIS-2 - Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG“ teilzunehmen. Er vertritt rund 70 Unternehmen und Organisationen aus dem Bereich der Solarproduktion in Europa, darunter mehrere Hersteller von Wechselrichtern, Batteriespeichersystemen und Energiemanagementsystemen.

Ausgangslage

Wir betrachten das Thema Cybersicherheit insbesondere aus der Perspektive der Sicherheit für das deutsche und europäische Stromsystem, das derzeit immer größere Mengen an Solarstrom aufnimmt und verteilt. Diese werden von Wechselrichtern bereitgestellt, welche den Gleichstrom der Solarmodule in netzkonformen Wechselstrom umwandeln. Zugleich bieten Wechselrichter zum Teil auch Systemdienstleistungen, etwa die Bereitstellung von Blindleistung an. Typischerweise ist jeder moderne Solarwechselrichter mit dem Internet verbunden, über das er sowohl Steuerbefehle als auch zum Beispiel Firmware-Updates erhält.

Problemlage

Ein Ausfall von mehr als 3 Gigawatt (GW) Stromerzeugungskapazität (einerlei, ob konventionell oder erneuerbar) kann erhebliche Auswirkungen auf das deutsche und europäische Stromnetz haben, bis hin zum (teilweisen oder großflächigen) Blackout. Das hat zuletzt der Stromausfall in Spanien am 28. April 2025 gezeigt.

Die bisher völlig unregulierte Fernsteuerbarkeit der Photovoltaikwechselrichter ist dabei als besonderes Risiko zu betrachten. So stammen bereits heute knapp 200 GW an Wechselrichterleistung im europäischen Stromsystem von zwei Herstellern aus einem autokratisch geführten Land. Der Marktführer, das chinesische Unternehmen Huawei, kontrolliert davon alleine Wechselrichter in europäischen PV-Anlagen mit einer Kapazität von rund 114 GW (SolarPower Europe). Chinesische Wechselrichter haben europaweit einen Marktanteil von rund 80 Prozent, ähnlich auch in Deutschland.

Rund 70 Prozent der an das europäische Stromnetz angeschlossenen Wechselrichter können ferngesteuert werden und sind somit potenzielle Ziele für feindliche Manipulationen. Ausführliche Informationen sind der Studie „Solutions for PV Cyber Risks to Grid Stability“ (DNV 2025) zu entnehmen.

Damit ist die Wechselrichterleistung, die chinesischen Unternehmen zuzuordnen ist, um ein Vielfaches größer als die Fehlerleistung, die das europäische Stromnetz kompensieren kann.

Beachtenswert ist, dass es unterschiedliche Aggregationsniveaus gibt: Sie reichen

1. von einzelnen Wechselrichtern einer Solarstromanlage im Kilowatt- oder niedrigerem Megawattbereich, über
2. eine Vielzahl von aggregiert ansteuerbarer Wechselrichter (etwa bei Direktvermarktern von Strom) mit hunderten von Megawatt Leistung bis hin zu
3. ganzen Produktserien unter direkter oder indirekter Kontrolle der Hersteller mit aggregierten Leistungen im Gigawatt-Bereich.

Maßnahmen

Zum Schutz dezentraler PV-Anlagen sowie zur Stärkung der Netzstabilität und somit der Energiesicherheit Deutschlands schlagen wir folgende Maßnahmen vor, welche im Rahmen des **NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes, NIS2UmsuCG** umgesetzt werden sollten:

1. Erweiterung der Definition „kritische Infrastruktur“

Die rechtliche Definition des Begriffs „kritische Infrastruktur“ sollte auf Hersteller kritischer Komponenten, wie beispielsweise Wechselrichter ausgeweitet werden, die über Fernzugriff (wie z.B. für Firmwareupdates) eine aggregierte dezentrale PV-Kapazität von über 104 MW direkt kontrollieren (Aggregationsniveau 2) und darüber letztlich die Funktionsfähigkeit der Anlagen beeinflussen können.

Generell ist es wichtig, dass der Gesetzgeber im Rahmen der Regulierung auch die Sicherheit und Vertrauenswürdigkeit einzelner (Aufdach-)PV-Anlagen garantiert, welche akkumuliert eine hohe Kapazität an Erzeugungsleitung generieren – die ausschließliche Kontrolle von Komponenten der Anlage oder des Systems zur Bündelung elektrischer Leistung und Steuerung von Erzeugungsanlagen oder dezentraler Energieerzeugungsanlagen (BSI-KritisV) ist nicht ausreichend.

2. Fernzugriff nur aus der EU und Staaten mit vergleichbarem Sicherheitsniveau

Für die Hersteller darf der (Fern-) Zugriff über das Internet auf die Wechselrichter in PV-Anlagen nur von innerhalb der EU oder von Staaten mit einem gleichwertigen Sicherheitsniveau erfolgen. Diese Regelung muss sowohl die direkte Steuerung als auch die indirekte Steuerung über Firmware- und Software-Updates umfassen. Entsprechende Gesetzesänderungen sollten im NIS2UmsuCG aufgenommen werden.

Identifikation und Anzeigepflicht

Die Identifikation und Anzeigepflicht kritischer Komponenten (§9b BSIG) sollte nicht dem Betreiber kritischer Energieanlagen obliegen, sondern wie in einer vorherigen Entwurfsfassung des NIS2UmsuCG (Entwurf datiert vom 02.12.2024) beim Bundesministerium des Inneren (BMI), liegen. Dabei sollte das BSI in der Bestimmung der kritischen Komponenten (basierend auf dem Funktionenkatalog der BNetzA in Absprache mit dem BSI), auch die

Hersteller (u.a. von Wechselrichtern) im Beratungsprozess konsultieren.

3. Branchenspezifische Cybersicherheitsregeln

Branchenspezifische Cybersicherheitsregelungen zum Schutz fernsteuerbarer PV-Anlagen sollten beispielsweise in Form einer Norm entwickelt werden. Um die Stromnetze in Deutschland und Europa zu schützen, sollten die Hersteller von Wechselrichtern somit ähnlich behandelt werden wie 5G-Mobilfunkhersteller. Mit der 5G-Toolbox setzen Mobilfunkbetreiber in allen EU-Mitgliedstaaten Maßnahmen zur Risikominderung um, um die gleichen Mindeststandards zur Sicherung ihrer 5G-Netze gegen Spionage, Sabotage und Risiken in der Lieferkette einzuhalten.

Die Standards sollte bei PV-Anlagen nicht nur die Wechselrichter umfassen, sondern auch die Cloud- und Kommunikationsinfrastruktur, die für die Überwachung und Verwaltung genutzt wird.