Cybersicherheit und Steuerung von Photovoltaikanlagen – ein regulatorischer und technischer Lösungsansatz für Deutschland

Dr. Andreas Kubis[a], Peter Müller[a], Niklas Erle[a]

[a]*c.con Management Consulting GmbH, Altrottstraße 31, 69190 Walldorf*

Kurzfassung

Die zunehmende Digitalisierung des Energiesektors und der wachsende Anteil erneuerbarer Energien, insbesondere Photovoltaik (PV), erfordern eine robuste Cybersicherheitsstrategie. SolarPower Europe greift dieses Thema in seinem Bericht *A Harmonised Cybersecurity Baseline for Solar PV* [1] auf und schlägt zahlreiche Maßnahmen vor. Die Analyse dieses Positionspapiers zeigt, dass viele dieser Maßnahmen im deutschen Markt bereits durch bestehende Regulierungen und technische Standards adressiert sind. Die Untersuchung verdeutlicht, dass PV-Anlagen in Deutschland bereits durch ein starkes regulatorisches Sicherheitsnetz abgesichert sind. Das EEG und das MsbG gewährleisten eine sichere Steuerkommunikation über Smart Meter Gateways oder zertifizierte WAN-Infrastrukturen. Große Anlagen oder Aggregationen über 104 MW unterliegen der KRITIS-Regulierung und den IT-Sicherheitsanforderungen gemäß B3S und § 8a BSIG. Als wesentliche verbleibende Bedrohung wird die fehlende Regulierung von Wechselrichter-Backends identifiziert. Ohne zusätzliche Sicherheitsanforderungen könnten diese zur Schwachstelle für koordinierte Angriffe werden. Das Positionspapier empfiehlt daher verpflichtende Maßnahmen für sichere Firmware-Updates, gesicherte Kommunikationswege und eine stärkere Kontrolle von Hersteller-Backends. Nur durch eine vollständige Integration von Wechselrichter-Backends in das bestehende Sicherheitsregime kann das Risiko potenzieller Cyberangriffe minimiert und die Zuverlässigkeit der erneuerbaren Stromerzeugung langfristig gesichert werden.

Dieses Positionspapier ist ein Zwischenergebnis einer Studie zur Identifikation, Bewertung und Mitigation von Cyber-Sicherheitsrisiken im Kontext von PV-Systemen.

1 Motivation

Die zunehmende Digitalisierung des Energiesektors und die steigende Integration erneuerbarer Energien, insbesondere der Photovoltaik (PV), erfordern eine robuste Cybersicherheitsstrategie. SolarPower Europe greift dieses Thema in seinem Bericht „A Harmonised Cybersecurity Baseline for Solar PV“ [1] auf und schlägt umfangreiche Maßnahmen vor.

Dieses Positionspapier setzt sich mit den Vorschlägen von SolarPower Europe auseinander – insbesondere mit den Ausführungen in Kapitel 3.4 – und überträgt diese in ein deutsches Regulierungs- und Standardisierungsumfeld. Es wird ein Vorschlag unterbreitet, wie Messstellenbetreiber (MSB) und Aggregatoren[1] als zentrale Sicherheitsakteure zur sicheren Steuerung und Datenkommunikation beitragen können.

2 Einordnung der vorgeschlagenen Maßnahmen von Solar Power Europe

2.1 Schutzziele und Maßnahmen von Solar Power Europe

Solar Power Europe formuliert in seinem Bericht eine Reihe von Forderungen, die darauf abzielen, die Cybersicherheit für dezentrale Erzeugungsanlagen (DEA), konkret Photovoltaik, auf europäischer und nationaler Ebene zu verbessern. Die wichtigsten Forderungen lassen sich in vier Hauptkategorien unterteilen:

2.1.1 Verbesserung der Governance und Risikotransparenz im nationalen Cybersicherheitsrahmen

Verantwortung für Cyberangriffe: Die nationale Umsetzung der NIS2-Richtlinie muss klarstellen, dass der PV-Anlagenbetreiber für Cybersicherheitsvorfälle verantwortlich ist. Audits sollten risikobasiert erfolgen, anstatt pauschal *alle* Betriebsprozesse abzudecken.

[1] Aus Gründen der Lesbarkeit inklusive Direktvermarkter und Betreiber virtueller Kraftwerke.

Risikobewertungen für Niederspannungsnetze: Analog zu den bereits vorgesehenen Risikobewertungen für Netze mit grenzüberschreitender Relevanz (Network Code for Cybersecurity) sollen auch für Niederspannungsnetze systematische Risikobewertungen eingeführt werden [1] [2].

2.1.2 Cybersicherheit auf Produktebene

Höhere Sicherheitsanforderungen für netzrelevante Produkte: Produkte, die das Stromnetz wesentlich beeinflussen (z. B. Wechselrichter), sollen höheren Anforderungen im Rahmen des Cyber Resilience Act (CRA) unterliegen und als "wichtige Produkte mit digitalen Elementen, Klasse I" klassifiziert werden [1] [3].

Spezifischer Sicherheitsstandard für dezentrale Erzeugungsanlagen: Neben bestehenden IoT-Standards soll ein vertikaler Sicherheitsstandard für Wechselrichter und Steuerungssysteme geschaffen werden [1].

2.1.3 Cybersicherheit für den Betrieb von PV-Anlagen

Datenhoheit in der EU: Betriebsdaten von PV-Anlagen sollten entweder innerhalb der EU oder in Ländern mit vergleichbaren Sicherheitsstandards gespeichert werden [1].

Verbindliche Best Practices für große PV-Anlagen: Betreiber großer PV-Anlagen sollen verpflichtende Mindeststandards für sichere Betriebspraktiken einhalten [1].

Standardisierung der IT-Sicherheitsanforderungen für dezentrale Erzeugungsanlagen: Normierungsorganisationen sollen europaweite Mindeststandards für Cybersicherheit in der Betriebsführung von DEA einführen [1].

Sicherheitsüberwachung für aggregierte Steuerung von PV-Anlagen: Falls Aggregatoren oder Hersteller in der Lage sind, große PV-Flotten direkt zentral zu steuern, sollen zusätzliche Sicherheitskontrollen für Steuerkommandos eingeführt werden: Überwachung der Steuerbefehle über *Security Operations Centres* (SOCs) oder Übertragung der Fernsteuerungsfunktion an *regulierte Marktakteure* 1].

2.1.4 Bewusstseinsbildung und Sicherheitspraktiken für Betreiber von Klein-PV-Anlagen

Cybersicherheitsbewusstsein für Betreiber und Installateure: Klein-PV-Anlagen-Betreiber und Installateure sollen verpflichtet werden, Authentifizierungsverfahren einzuhalten und Sicherheitsupdates regelmäßig durchzuführen [1].

2.1.5 Schutzziele für die Steuerungs- und Aggregationssicherheit

Kapitel 3.4 des Solar Power Europe Reports widmet sich der sicheren Steuerung aggregierter PV-Anlagen, insbesondere in Szenarien, in denen Aggregatoren oder Hersteller zentrale Steuerbefehle an dezentrale Erzeugungsanlagen senden [1]. Ziel dieser Maßnahmen ist es, Manipulationen oder Cyberangriffe auf Steuerbefehle zu verhindern, die negative Auswirkungen auf Netzstabilität oder Marktmechanismen haben könnten.

Im Rahmen dieses Positionspapiers werden nicht alle zuvor aufgeführten Schutzziele der Solar Power Europe diskutiert. Stattdessen konzentriert sich dieses Positionspapier auf diejenigen Aspekte, die für die sichere Fernsteuerung von PV-Anlagenflotten durch Aggregatoren oder Hersteller entscheidend sind. Diese sind in Tabelle 1 aufgeführt.

Tabelle 1: Schutzziele und Maßnahmen

#	Schutzziel	Vorgeschlagene Maßnahmen
1	Absicherung von Steuerbefehlen und aggregierten Steuermechanismen	Einführung eines Sicherheitslayers, der zentrale Steuerkommandos an PV-Anlagen überwacht und unerwünschte Manipulationen erkennt. Sicherstellung, dass aggregierte Steuerbefehle keine kritischen Netzsituationen oder Marktverzerrungen auslösen.
2	Sicherheitsüberwachung für Aggregatoren und Fernsteuerung	Aggregatoren und Hersteller sollen keine uneingeschränkte Steuerungsmacht über PV-Anlagen erhalten, sondern durch technische und regulatorische Mechanismen überwacht werden. Sicherheitsmaßnahmen müssen sicherstellen, dass flächendeckende Angriffe oder unautorisierte Steuerungen erkannt und abgewehrt werden.
3	Normierung und Standardisierung für netzrelevante Steuerungssysteme	Einführung eines europaweit einheitlichen Cybersicherheitsstandards für vernetzte, ferngesteuerte PV-Anlagen. Klare Zertifizierungsanforderungen für Aggregatoren und Hersteller, um Sicherheitslücken zu vermeiden.
4	Einführung eines Sicherheitslayers für Steuerbefehle zwischen Aggregatoren und Anlagen	Option A: Überwachung der Steuerdatenströme durch Security Operations Centres (SOCs) zur Erkennung von Anomalien. Option B: Übertragung der Fernsteuerungsfunktion an regulierte Marktakteure, die als vertrauenswürdige Instanzen für Sicherheitskontrollen fungieren.

Andere Forderungen des Papiers, wie die Datenhoheit von PV-Anlagenbetreibern in der EU, die Bewusstseinsbildung für Klein-PV-Anlagenbetreiber oder die Klärung der gesetzlichen Verantwortlichkeit für Cyberangriffe, sind nicht Gegenstand dieser Analyse. Diese Themen sind zwar für die allgemeine Cybersicherheit im PV-Sektor von Bedeutung, haben jedoch keinen unmittelbaren Einfluss auf die Cybersicherheit der Steuerungs- und Aggregationssysteme, die Solar Power Europe adressiert.

2.2 Rechtliche Grundlagen für die Steuerung von PV-Anlagen

Die Anforderungen an die Steuerbarkeit von PV-Anlagen in Deutschland ergeben sich aus dem Zusammenspiel mehrerer nationaler Gesetzgebungen. Zentral sind das Erneuerbare-Energien-Gesetz (EEG) [4], das Messstellenbetriebsgesetz (MsbG) [5] sowie die Verordnung zur Bestimmung Kritischer Infrastrukturen (BSI-KritisV) [6]. Ergänzend greifen das Energiewirtschaftsgesetz (EnWG) [7] und das IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) [8], die für bestimmte Betreibergruppen technische Anforderungen und IT-Sicherheitsmaßnahmen definieren. Das EEG regelt in § 9 die Steuerbarkeit von PV-Anlagen. Betreiber von PV-Anlagen sind verpflichtet, sicherzustellen, dass ihre Anlagen unter bestimmten Bedingungen ferngesteuert werden können. Eine Übersicht liefert Tabelle 2.

Tabelle 2: Übersicht rechtlich-regulatorischer Anforderungen hinsichtlich der Steuerung von PV-Anlagen

Anlagengröße	Steuerungspflichten gemäß § 9 EEG
< 2 kWp	Keine Verpflichtung zur Steuerbarkeit.
2 – 7 kWp	Begrenzung der Wirkleistung auf 60 % der installierten Leistung, sofern kein intelligentes Messsystem (iMSys) vorhanden ist.
7 – 25 kWp	Begrenzung der Wirkleistung auf 60 % der installierten Leistung bis zum Einbau eines iMSys. Nach Installation eines iMSys: Steuerbarkeit durch Netzbetreiber oder Direktvermarkter erforderlich.
25 – 100 kWp	Übermittlung von Ist-Werten an den Netzbetreiber. Steuerung durch Netzbetreiber oder Direktvermarkter über ein iMSys oder eine andere technische Einrichtung erforderlich.
> 100 kWp	Steuerung durch Netzbetreiber oder Direktvermarkter über ein iMSys oder eine sonstige technische Einrichtung verpflichtend. Übermittlung von Ist-Werten an den Netzbetreiber.
> 104 MW	Einstufung als Kritische Infrastruktur gemäß BSI-KritisV. Betreiber müssen IT-Sicherheitsmaßnahmen gemäß § 8a BSIG umsetzen.

2.2.1 Steuerung von PV-Anlagen (< 104 MWp)

Das Messstellenbetriebsgesetz (MsbG) ergänzt die Regelungen des EEG, indem es die technische Infrastruktur für die Steuerung von PV-Anlagen vorgibt. Gemäß §29 Abs. 1 Satz 2 MsbG müssen sowohl PV-Anlagen ab einer Leistung von 7 kWp als auch Anlagen bei Letztverbrauchern, für die eine Vereinbarung nach § 14a EnWG besteht, mit einem intelligenten Messsystem (iMSys) ausgestattet sein, um eine sichere Kommunikation zwischen Anlagenbetreibern, Netzbetreibern und Direktvermarktern zu gewährleisten. Ein iMSys setzt sich aus zwei zentralen Komponenten zusammen: dem Smart Meter Gateway (SMGW) und einer modernen Messeinrichtung (mME) [9]. Das SMGW dient als zentrale Kommunikationsschnittstelle, über die Mess- und Steuerdaten sicher übertragen werden. Für die Übermittlung von Steuerbefehlen kommt das CLS-Modul (Controllable Local Systems) zum Einsatz, das eine gesicherte Anbindung zwischen Steuerungseinheiten und den PV-Anlagen ermöglicht [10].

Mit dem EEG 2025 entfällt die 7-kWp-Schwelle als Kriterium für die Steuerbarkeitspflicht, jedoch bleibt das iMSys weiterhin die primäre Infrastruktur für die sichere Steuerkommunikation. Bestandsanlagen, die vor Inkrafttreten des EEG 2025 errichtet wurden, behalten ihre bisherigen Steuerbarkeitsanforderungen. Eine Nachrüstpflicht besteht nur in bestimmten Fällen, z. B. wenn eine Umstellung auf Direktvermarktung erfolgt oder durch eine neue Verordnung zur technischen Umsetzung der WAN-Anbindung zusätzliche Anforderungen entstehen.

Gemäß § 9 Abs. 4 EEG sind Regelungen zur Weitverkehrsnetzanbindung (WAN) für steuerbare PV-Anlagen unabhängig von den in § 9 Abs. 1 bis 3 EEG definierten Steuerungspflichten anzuwenden. Damit stellt das EEG sicher, dass Anlagen, die unter diese Vorschriften fallen, nicht nur fernsteuerbar sein müssen, sondern dass ihre Anbindung an das Netz bestimmten technischen Sicherheitsanforderungen entspricht. Diese Regelungen basieren auf einer gesonderten Verordnung gemäß § 19 Abs. 2 Satz 3 MsbG, die verbindliche Vorgaben zur sicheren WAN-Anbindung enthält.

Da § 9 Abs. 4 EEG keinen Spielraum für unsichere Kommunikationslösungen zulässt, müssen alle betroffenen Anlagen die im MsbG definierten technischen Anforderungen erfüllen. Besonders relevant sind dabei die BSI-Schutzprofile für Smart Meter Gateways (BSI-CC-PP-0073) und die BSI-TR-03109-Reihe, die Sicherheitsanforderungen für Steuer- und Kommunikationssysteme im Energiesektor festlegen [10].

2.2.2 Steuerung von Anlagen (> 104 MWp) und KRITIS-Regelungen

Während PV-Anlagen mit einer installierten Leistung von mehr als 104 MW gemäß § 1 BSI-KritisV als *Kritische Infrastruktur* (KRITIS) eingestuft werden und somit den IT-Sicherheitsanforderungen nach § 8a BSIG unterliegen, bleiben kleinere Anlagen formal außerhalb dieser Regulierung.

Allerdings kann auch die Vernetzung vieler kleinerer PV-Anlagen in Aggregations- und Steuerungssystemen einen kritischen Einfluss auf die Netzstabilität haben. Wenn ein Aggregator oder eine Steuerplattform eine große Anzahl dezentraler Erzeugungsanlagen (in Summe > 104 MWp) zentral steuert und dadurch einen signifikanten Einfluss auf das Stromnetz hat, wird sie nach der BSI-KritisV (Anhang 1, Teil 3, Tabelle 1.1.5) ebenfalls als KRITIS eingestuft [11] [12].

Um die IT-Sicherheit dieser Systeme zu gewährleisten, wurde der *Branchenspezifische Sicherheitsstandard* (B3S) für Steuerungs- und Bündelungsanlagen

entwickelt. Dieser Standard konkretisiert die Anforderungen an die IT-Sicherheit von Aggregatoren und zentralen Steuerungssystemen (> 104 MWp). Betreiber solcher Systeme, die unter die KRITIS-Definition der BSI-KritisV fallen, sind verpflichtet, den B3S als Maßstab für ihre IT-Sicherheitsmaßnahmen zu nutzen und die gesetzlichen Anforderungen aus § 8a BSIG zu erfüllen [13].

2.3 Fazit und Bewertung der Maßnahmen

Die bestehende Regulierung stellt sicher, dass alle steuerbaren PV-Anlagen über eine sichere Kommunikationsinfrastruktur angebunden sind. Die sichere Steuerung erfolgt über das SMGW oder alternative BSI-konforme WAN-Infrastrukturen. Große oder aggregierte Anlagen über 104 MWp sind als KRITIS eingestuft und unterliegen dann den IT-Sicherheitsanforderungen nach § 8a BSIG. Damit sind alle neu installierten PV-Anlagen entweder über die Infrastruktur des MsbG oder, falls sie als KRITIS eingestuft werden, über die KRITIS-Regelungen abgesichert. Unsichere oder unregulierte Steuerungslösungen sind somit im Zielzustand ausgeschlossen.

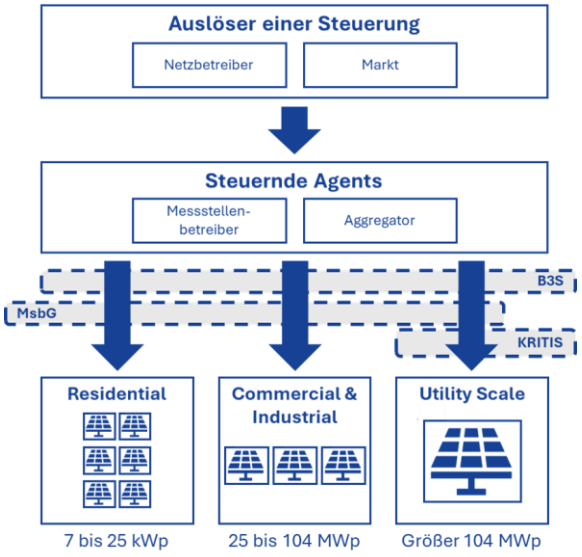

Abbildung 1: Übersicht der rechtlichen Anforderungen an PV-Systeme

Solar Power Europe hat in seinem Bericht vier zentrale Schutzziele für die Absicherung von aggregierten Steuermechanismen definiert [1]. Die Überprüfung der aktuellen regulatorischen Rahmenbedingungen zeigt, dass die ersten drei Schutzziele bereits weitgehend erfüllt sind:

Absicherung von Steuerbefehlen und aggregierten Steuermechanismen: Durch § 9 Abs. 4 EEG und § 19 Abs. 2 MsbG sind alle steuerbaren Anlagen verpflichtet, eine sichere WAN-Anbindung zu nutzen [9] [10]. Die Nutzung von Smart Meter Gateways (SMGW) oder zertifizierten WAN-Infrastrukturen stellt sicher, dass keine unregulierten Steuerbefehle gesendet werden können. Netzbetreiber und Direktvermarkter sind über die bestehenden regulatorischen Vorgaben dazu verpflichtet, sicherzustellen, dass keine Manipulation von Steuerbefehlen erfolgt.

➔ Schutzziel 1 ist durch die bestehende Regulierung weitgehend erfüllt.

Sicherheitsüberwachung für Aggregatoren und Fernsteuerung: Aggregatoren haben keine unkontrollierte Steuerungsmacht über PV-Anlagen, da für große Aggregatoren regulatorische Einschränkungen bestehen. Wenn eine Steuerplattform mindestens 104 MWp aggregiert, fällt sie unter die §1 BSI-KritisV und wird als Kritische Infrastruktur (KRITIS) eingestuft. Damit gelten für Betreiber verpflichtende IT-Sicherheitsmaßnahmen gemäß § 8a BSIG. Zusätzlich sind für Aggregatoren die BSI-Schutzprofile und der Branchenspezifische Sicherheitsstandard (B3S) für Steuerungs- und Bündelungsanlagen verbindlich [13]. Hersteller haben in **keinem Fall** eine *legitimierte Steuerungsmacht* über PV-Anlagen.

➔ Schutzziel 2 ist durch die bestehenden gesetzlichen und regulatorischen Vorgaben erfüllt.

Normierung und Standardisierung für netzrelevante Steuerungssysteme: Die BSI-TR-03109-Reihe und die BSI-Schutzprofile für SMGWs setzen bereits verbindliche technische Standards für die sichere Steuerung von PV-Anlagen [10]. [9]

➔ Schutzziel 3 ist weitgehend erfüllt.

Einführung eines Sicherheitslayers für Steuerbefehle zwischen Aggregatoren und Anlagen: Das ursprüngliche Schutzziel forderte die Einführung eines zusätzlichen Sicherheitslayers, z. B. durch Security Operations Centres (SOCs) oder die Übertragung der Fernsteuerung an regulierte Marktakteure [1]. Die bestehenden Regelungen gewährleisten bereits eine sichere, überwachte Infrastruktur für Steuerbefehle, sodass eine zusätzliche Echtzeitüberwachung von Steuerbefehlen als obsolet erachtet werden kann.

➔ Schutzziel 4 ist bereits erfüllt, da der Sicherheitslayer für Steuerbefehle von Smart-Meter-Gateway-Administratoren und/oder unter die KRITIS-Regelung fallenden Aggregatoren abgesichert ist.

Die bestehende Regulierung gewährleistet, dass alle steuerbaren PV-Anlagen über eine sichere Steuerkommunikation verfügen, entweder durch das Messstellenbetriebsgesetz (MsbG) oder – bei großen Aggregationen – durch die KRITIS-Regelungen der BSI-KritisV. Unsichere oder unregulierte Steuerungslösungen sind somit ausgeschlossen, wodurch die wesentlichen Sicherheitsanforderungen bereits gesetzlich und technisch umgesetzt sind.

3 Die Sicherheitsbedrohung – Ungesicherte Wechselrichter-Backends

Die bisherige Analyse zeigt, dass die regulatorischen und technischen Anforderungen in Deutschland bereits ein hohes Maß an Sicherheit für die Steuerung von PV-

Anlagen gewährleisten. Steuerbefehle müssen über gesicherte WAN-Infrastrukturen erfolgen, unregulierte oder unsichere Steuermechanismen sind ausgeschlossen, und kritische Aggregationssysteme unterliegen strengen Sicherheitsanforderungen [9] [10] [13].

Die verbleibende Sicherheitslücke: Wechselrichter-Backends als Angriffsvektor

Trotz dieser umfassenden Sicherheitsmaßnahmen gibt es eine zentrale Bedrohung, die durch die bisherige Regulierung nicht vollständig adressiert wird: die Sicherheit von Wechselrichter-Backends und cloudbasierten Update-Mechanismen.

3.1 Warum sind ungesicherte Wechselrichter-Backends problematisch?

Als eines der größten Risiken im Bereich der PV-Anlagen wird die unzureichende Absicherung von Hersteller-Backends und Firmware-Updates der Wechselrichter gesehen [1] [3]. Während die Steuerung von PV-Anlagen in Deutschland weitgehend reguliert ist und über gesicherte Infrastrukturen erfolgt, bleiben viele Wechselrichter weiterhin über zentrale Cloud-Plattformen der Hersteller manipulierbar [1]. Diese stellen potenzielle Angriffsvektoren dar, da sie oft nicht den hohen nationalen oder EU-weiten Sicherheitsstandards unterliegen. Die wesentlichen Schwachstellen sind:

Fehlende Signaturüberprüfung und Authentifizierung: Eine der Hauptbedrohungen ist die fehlende Signaturprüfung und Authentifizierung von Firmware-Updates [3]. Ohne eine kryptographische Signierung und Zertifizierung durch eine unabhängige Instanz besteht das Risiko, dass manipulierte Softwarepakete auf die Wechselrichter eingespielt werden. Angreifer könnten über kompromittierte Update-Server gefälschte Updates oder modifizierte Steuerbefehle einschleusen, die zu unkontrolliertem Verhalten der Geräte und damit zu erheblichen Netzstabilitätsrisiken führen.

Unsichere Übertragungswege: Ein weiteres Problem sind unsichere Übertragungswege für Firmware-Updates [3]. Falls Updates über ungesicherte Kanäle oder nicht zertifizierte Server bereitgestellt werden, besteht die Gefahr sogenannter Man-in-the-Middle-Angriffe, bei denen ein Angreifer zwischen den Kommunikationspartnern sitzt und die übertragene Firmware verändert. In einem solchen Szenario könnte ein Wechselrichter gezielt mit fehlerhafter oder schädlicher Software ausgestattet werden, die seine Funktionalität einschränkt oder die der Angreifer zu einer koordinierten Netzstörung missbrauchen kann.

Unregulierte Backend-Systeme: Besonders kritisch ist die zentrale Kontrolle über Wechselrichter durch Dritte über unregulierte Hersteller-Backends. Viele dieser Plattformen ermöglichen potenziell eine direkte Fernsteuerung von Wechselrichtern, ohne dass die Steuerung über zertifizierte nationale Infrastrukturen wie das Smart Meter Gateway erfolgt [1]. Sollte ein Angreifer Zugriff auf diese zentralen Systeme erlangen, wäre es theoretisch möglich, eine große Anzahl von Wechselrichtern gleichzeitig zu beeinflussen. Dies könnte gezielt genutzt werden, um Lastspitzen zu erzeugen, Netzfrequenzschwankungen herbeizuführen und somit regionale Stromausfälle zu provozieren.

Unsichere Firmware-Updates: Zudem fehlt in vielen Fällen eine robuste Integritätsüberprüfung und Update-Authentifizierung. Ohne eine zweistufige Update-Verifizierung oder ein Firmware-Register, das von einer vertrauenswürdigen Instanz verwaltet wird, kann nicht sichergestellt werden, dass ein Wechselrichter die erhaltene Softwareversion tatsächlich von einem autorisierten Hersteller oder Dienstleister erhalten hat. Dadurch bleibt die Gefahr bestehen, dass bösartige Software eingeschleust wird, die entweder einzelne Anlagen außer Betrieb setzt oder durch massenhafte Koordination eine Systemstörung verursacht [1].

Diese Schwachstellen zeigen, dass trotz der bestehenden Regulierung zur sicheren Steuerung von PV-Anlagen weiterhin eine erhebliche Bedrohung durch ungesicherte Wechselrichter-Backends besteht. Die fehlende Kontrolle über Hersteller-Clouds, die unzureichende Absicherung von Firmware-Updates und die Möglichkeit der zentralisierten Manipulation stellen Risiken dar, die dringend adressiert werden müssen. In den folgenden Kapiteln wird daher untersucht, welche zusätzlichen Sicherheitsmaßnahmen erforderlich sind, um Wechselrichter-Backends und deren Update-Infrastrukturen effektiver abzusichern.

3.2 Handlungsempfehlungen zur Absicherung von Wechselrichter-Backends

Die Analyse zeigt, dass Wechselrichter-Backends ein potenzielles Sicherheitsrisiko darstellen, da durch sie i.d.R. Einfluss auf eine große Anzahl von Erzeugungsanlagen genommen werden kann, sie aber nicht denselben regulatorischen Vorgaben unterliegen wie die Steuerung über das Smart Meter Gateway oder KRITIS-Infrastrukturen. Um diese Schwachstelle zu schließen, sind gezielte Maßnahmen erforderlich, die eine sichere Bereitstellung, Übertragung und Implementierung von Firmware-Updates sowie eine stärkere Kontrolle über Hersteller-Backends gewährleisten [3] [9] [10]. Tabelle 3 fasst die Mitigationsmaßnahmen zusammen.

4 Fazit

Die Analyse zeigt: Die Steuerung von PV-Anlagen in Deutschland ist größtenteils durch bestehende Regelungen wie EEG, MsbG und KRITIS gut abgesichert. Eine wesentliche Lücke besteht jedoch bei den Wechselrichter-Backends. Ohne klare Sicherheitsvorgaben drohen Cyberangriffe über Hersteller-Clouds. Der Bericht von SolarPower Europe liefert hierzu wertvolle Impulse und unterstreicht die Bedeutung eines ganzheitlichen Sicherheitsansatzes [1]. Das Positionspapier empfiehlt daher verbindliche Anforderungen für Updates, Kommunikation und die Kontrolle von Backend-Systemen, um die Resilienz der Stromerzeugung zu stärken.

Tabelle 3: Maßnahmen zur Absicherung von Backends

#	Maßnahme	Beschreibung	Effektivität
1	Regulierung und Kontrolle von Hersteller-Backendsystemen	Eine Abhängigkeit von zentralisierten Hersteller-Clouds muss verhindert werden und über gesetzliche Vorgaben ausgeschlossen werden.	Sehr hoch
2	Signierte und zertifizierte Firmware-Updates	Firmware-Updates müssen kryptographisch signiert (z.B. RSA- oder ECC-Signatur) und vor der Verteilung geprüft werden. Die Prüfung erfolgt durch eine unabhängige Stelle im Rahmen einer Typzertifizierung (vgl. Cyber Resilience Act). Diese Stelle überprüft: (a) Sicherheitsfunktionen, (b) Integrität der Software, (c) Abwehrmechanismen gegen Manipulationen.	Sehr hoch
3	Gesicherte Übertragung von Firmware-Updates über SMGW, PKI-gesicherte Server oder zertifizierte Installateurssysteme	Um Manipulationen beim Firmware-Update zu verhindern, muss die Übertragung über zertifizierte und sichere Kommunikationskanäle erfolgen. Je nach technischer Infrastruktur kommen drei Wege in Betracht: (1) Direkte Serververbindung mit PKI-Authentifizierung, (2) Übertragung über das Smart Meter Gateway (SMGW) mit CLS-Kanal, (3) Update durch zertifizierte Installateure mit abgesichertem Equipment.	Sehr hoch
4	Hardware-gestütztes Secure Boot, gesicherte Update Quellen	Nur autorisierte Firmware darf gebootet werden (TPM 2.0 oder HSM für Root-of-Trust). Wechselrichter dürfen nur von zertifizierten Servern oder geschützten USB-Dongles Updates beziehen (keine Downloads von beliebigen URLs oder Ausführung beliebiger Dateien).	Hoch
5	Zweistufige Update-Verifizierung	Vor dem Update erfolgt eine Sicherheitsüberprüfung durch ein unabhängiges System (z.B. SMGW-A oder Aggregator) – z.B. Signierungsaustausch nach #1.	Hoch
6	Firmware-Register bei einem „Agent“ (ggf. MSB)	Ein „Agent“ führt ein Register, das den aktuellen Firmware-Stand jedes Wechselrichters dokumentiert und verifiziert. Das SMGW nutzt dieses Register zur Authentifizierung und Steuerung von Updates.	Mittel

Literaturverzeichnis

[1] SolarPower Europe, *A Harmonised Cybersecurity Baseline for Solar PV,* Brüssel, 2024.

[2] Amtsblatt der Europäischen Union, *Verordnung (EU) 2024/1366: Netzkodex mit sektorspezifischen Vorschriften für Cybersicherheitsaspekte grenzüberschreitender Stromflüsse - Network Code Cybersecurity (NCCS),* Brüssel, 2024.

[3] Amtsblatt der Europäischen Union, *Verordnung (EU) 2024/2847: Horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen - Cyber Resilience Act (CRA),* Brüssel, 2024.

[4] Bundesgesetzblatt, *Erneuerbare-Energien-Gesetz (EEG),* zuletzt geändert 21. Februar 2025.

[5] Bundesgesetzblatt, *Messstellenbetriebsgesetz (MsbG),* zuletzt geändert 21. Februar 2025.

[6] Bundesgesetzblatt, *BSI-Kritisverordnung (BSI-KritisV),* zuletzt geändert 29. November 2023.

[7] Bundesgesetzblatt, *Energiewirtschaftsgesetz (EnWG),* zuletzt geändert 21. Februar 2025.

[8] Bundesgesetzblatt, *Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0),* 2021.

[9] Bundesamt für Sicherheit in der Informationstechnik (BSI), *BSI-Schutzprofile für Smart Meter Gateways (BSI-CC-PP-0073 V2),* Bonn, 2024.

[10] Bundesamt für Sicherheit in der Informationstechnik (BSI), *Technische Richtlinie BSI-TR-03109-5 (Kommunikationsadapter),* Bonn, 2023.

[11] Bundesnetzagentur, *Netzausbau Strom: Bedarfsermittlung 2023-2037/2045 (Bestätigung Netzentwicklungsplan Strom),* Bonn, 2024.

[12] R. Elsland, T. Boßmann, A.-L. Klingler, A. Herbst, M. Klobasa und M. Wietschel, „Netzentwicklungsplan Strom - Entwicklung der regionalen Stromnachfrage und Lastprofile,“ Fraunhofer-Institut für System- und Innovationsforschung ISI, Karlsruhe, 2016.

[13] Bundesverband der Energie- und Wasserwirtschaft (BDEW), *Branchenspezifischer Sicherheitsstandard für Anlagen oder Systeme zur Steuerung / Bündelung elektrischer Leistung (B3S Aggregatoren),* Berlin, 2023.

Die **c.con Management Consulting GmbH** ist eine spezialisierte Unternehmensberatung für die Energie- und Versorgungswirtschaft. Ihre Schwerpunkte liegen in der Fachberatung für Energieversorgungsunternehmen, im strategischen Projektmanagement, Prozessoptimierung und Transformation. c.con hat seit 2007 über 400 Projekte bei mehr als 30 Kunden erfolgreich begleitet und wurde von brand eins und Statista bereits mehrfach als „Beste Unternehmensberatung“ ausgezeichnet.

Kontakt: ccon@ccon.com