Nationales Testinstitut für Cybersicherheit

Cybersicherheit von Photovoltaikanlagen

Erkenntnisse und Empfehlungen

Version	1.0
Datum	17. September 2026
Klassifikation	Öffentlich

Autoren	Tobias Castagna, Stefan Gloor, Andreas Leisibach, Dilip Many, Raphael M. Reischuk, Lukas Sohrmann, Fabio Zuber
Verantwortlich	Tobias Castagna

Mit Unterstützung von energieschweiz

Inhaltsübersicht

Danksagung

Ein besonderer Dank gilt den Organisationen und Experten, die diese Untersuchung unterstützt haben, sei es durch die Bereitstellung von Testgeräten, durch Einblicke in die Verwendung solcher Geräte in unterschiedlichen Umgebungen oder durch eine Beteiligung an den Kosten. Mit ihrem Engagement haben sie massgeblich zum Gelingen dieser Sicherheitsanalyse beigetragen. Dazu gehören:

• EnergieSchweiz, Bundesamt für Energie BFE
• Bundesamt für Cybersicherheit BACS
• Bundesamt für Kommunikation BAKOM
• Eidgenössische Elektrizitätskommission ElCom
• Aziende Industriali di Lugano (AIL) SA
• ch-solar AG
• Flughafen Zürich AG
• HHM Gruppe (HEFTI. HESS. MARTIGNONI.)
• Stadt Zürich Organisation und Informatik (OIZ)
• Swisscom (Schweiz) AG
• Swissgrid AG
• Swissolar
• Verband Schweizerischer Elektrizitätsunternehmen (VSE)

• Prof. Dr. Christof Bucher, Berner Fachhochschule BFH
• Prof. Roger Buser, Hochschule Luzern HSLU
• Prof. Dr. Andreas Heinzelmann, ZHAW Zürcher Hochschule für Angewandte Wissenschaften
• Ruben Santamarta, selbstständiger Cybersicherheitsforscher
• Dr. Leonard Schliesser, Center for Security Studies CSS, ETH Zürich
• Arrigo Triulzi Lampugnani, selbständiger Cybersicherheitsexperte
• Bastian Widmer, selbständiger Cybersicherheitsexperte

Ein spezieller Dank geht an Robin Seidel, der im Rahmen seines Studiums an der ETH Zürich und in Kooperation mit dem NTC schwerwiegende Schwachstellen in einem vernetzten Gerät einer Photovoltaik-Anlage identifiziert hat. Diese Vorarbeit bestärkte das NTC im Handlungsbedarf und gab wesentliche Impulse für die vorliegende Analyse.

1 Management Summary

Das Wichtigste in Kürze

Photovoltaik ist systemrelevant: Ende 2025 waren in der Schweiz rund 338'000 netzverbundene Photovoltaikanlagen installiert. Ihre Jahresproduktion deckte 13,7 Prozent des Stromendverbrauchs. Zur sonnigen Mittagszeit decken die Anlagen regelmässig über die Hälfte des momentanen Verbrauchs.

Die Untersuchung: Das Nationale Testinstitut für Cybersicherheit NTC hat aus eigener Initiative sieben Wechselrichter und vier Energiemanagementsysteme geprüft. Unterstützt wurde das NTC dabei durch Branchenorganisationen und EnergieSchweiz.

Über 50 Befunde in elf Produkten: Sieben Befunde sind kritisch, sechs hoch. Fünf Produkte wiesen mindestens einen kritischen oder hohen Befund auf. Vier Geräte liessen sich vollständig übernehmen.

Hersteller reagieren rasch: Das NTC hat die Befunde den betroffenen Herstellern bereits vor der Publikation des vorliegenden Berichts mitgeteilt. Viele haben umgehend reagiert und Lücken bereits geschlossen.

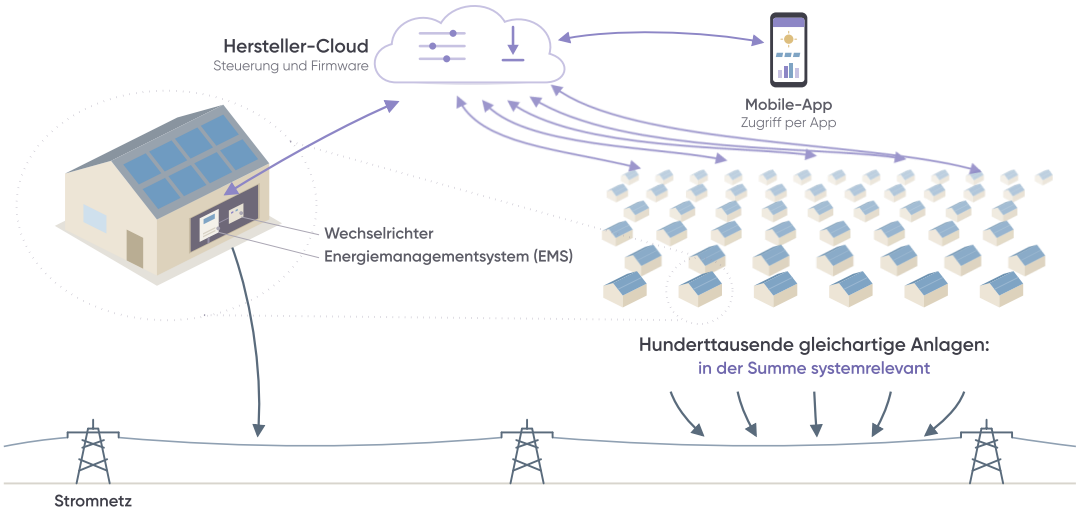
Nicht nur die Schwere entscheidet, sondern die Reichweite: Eine einzige Schwachstelle in einer relevanten Komponente kann Tausende angebundene Anlagen betreffen. Sechs Befunde sind von dieser Art. Die einzelne Anlage ist für das Netz unbedeutend, der Bestand als Ganzes ist kritische Infrastruktur.

Strukturelles Risiko: Das grösste Risiko lässt sich nicht durch verbesserte Produktsicherheit beheben. Es entsteht aus der Anbindung der Geräte an die Clouds der Hersteller, über die zum Beispiel Aktualisierungen der Firmware eingespielt werden.

Fehlende Zuständigkeit: Die Vorgaben greifen für Kleinanlagen zu kurz, und für das Risiko aus ihrer Summe ist niemand verantwortlich.

Ende 2025 waren in der Schweiz rund 338'000 netzverbundene Photovoltaikanlagen mit rund 9,5 Gigawatt (GW) Spitzenleistung installiert (zum Vergleich: das Kernkraftwerk Gösgen leistet rund 1 GW). Ihre Jahresproduktion von knapp 8 Terawattstunden (TWh) deckte 13,7 Prozent des Stromendverbrauchs, ungefähr auf dem Niveau des Kernkraftwerks Gösgen. Bis 2030 soll sich die Produktion gemäss den neuen Zwischenzielen des Bundesrats (18,7 TWh) mehr als verdoppeln. Für den Netzbetrieb zählt jedoch nicht die Jahressumme, sondern der Momentanbeitrag: Zur sonnigen Mittagszeit deckt die Photovoltaik regelmässig über die Hälfte des Verbrauchs, am 4. Juli 2026 um 14 Uhr gegen 85 Prozent.

Damit verändert sich die Struktur der Stromerzeugung: An die Seite weniger grosser, regulierter Kraftwerke treten Hunderttausende kleine, cloud-angebundene und weitgehend gleich konfigurierte Anlagen, einzeln unbedeutend, in der Summe systemrelevant.



Der Schweizer Bestand besteht dabei fast nur aus kleinen Anlagen auf Wohn- und Gewerbedächern, betrieben von Privatpersonen und kleineren Unternehmen ohne Expertise in Betrieb und Wartung von kritischer Infrastruktur. Was früher physischen Zugang zu einem Kraftwerk erforderte, ist heute über einen zentralen Fernzugang möglich. Das Risiko liegt dabei nicht in der Photovoltaik selbst, sondern in der Art, wie ihre Steuerung organisiert ist.

Privat betriebene Anlagen wurden bisher kaum unabhängig auf Schwachstellen geprüft: Es fehlen Anreize, klare Zuständigkeiten und eine passende Regulierung. Die Cybersicherheitsvorgaben der Strombranche (IKT-Minimalstandard) richten sich an Organisationen und greifen für Erzeuger erst ab 100 Megawatt, die über ein einziges System steuerbar sind. Auf die Anlage eines Einfamilienhauses sind sie weder anwendbar noch gedacht.

Das Nationale Testinstitut für Cybersicherheit NTC hat deshalb aus eigener Initiative elf in der Schweiz verbreitete digitale Produkte der Photovoltaik-Branche über rund ein Jahr geprüft: sieben Wechselrichter und vier Energiemanagementsysteme von insgesamt acht Herstellern. Das Prüfteam und ein wesentlicher Teil der finanziellen Mittel kamen vom NTC; mehrere Organisationen, mehrheitlich der Energiebranche, stellten Testgeräte bereit und beteiligten sich an den Kosten. Finanziell unterstützt wurde die Untersuchung zudem durch EnergieSchweiz. Weder die Hersteller noch die unterstützenden Organisationen nahmen Einfluss auf Auswahl, Prüfumfang oder Ergebnisse. Alle Befunde wurden den Herstellern vertraulich gemeldet. Dieser Bericht nennt grundsätzlich keine Produktnamen und keine technischen Details, sondern beschreibt typische Risikomuster und die daraus abgeleiteten Empfehlungen.

Insgesamt ergaben die Prüfungen über 50 Befunde, sieben davon kritisch und sechs weitere hoch. Fünf der elf Produkte wiesen mindestens einen hohen oder kritischen Befund auf. Bei vier Produkten erlangte das NTC die vollständige Kontrolle über das Gerät, teils durch das Einbringen fremden Programmcodes, teils über einen ungenügend geschützten Wartungszugang des Herstellers.

Wiederkehrend traten vier Muster auf:

- Mängel bei Authentifizierung und Zugriffskontrolle, etwa Standardpasswörter
- unsichere Wartungszugänge, etwa mit identischen Zugangsdaten für die ganze Geräteflotte
- fehlende oder schwache Verschlüsselung der Kommunikation über lokale Schnittstellen
- Schnittstellen, die sich nicht deaktivieren lassen

Bei nahezu allen geprüften Wechselrichtern lässt sich über die lokale Steuerschnittstelle ohne Anmeldung verändern, wie viel Leistung die Anlage einspeist, bis hinunter auf null. Aktiv ist diese Schnittstelle vor allem dort, wo ein Energiemanagementsystem die Anlage steuert. Für sich genommen betrifft ein solcher Zugriff nur eine Anlage. Werden jedoch viele Anlagen gleichzeitig manipuliert, kann dies die Stabilität des Stromnetzes gefährden. Das Netz muss jederzeit ein Gleichgewicht zwischen Erzeugung und Verbrauch sicherstellen. Netzrelevant wird eine Schwachstelle deshalb nicht durch ihre Schwere allein, sondern durch ihre Reichweite: Sechs Befunde wirken über eine zentrale Instanz auf einen ganzen Gerätebestand und damit auf viele Anlagen gleichzeitig.

Das Sicherheitsniveau der einzelnen Produkte ist nicht schlechter als bei anderen weitverbreiteten vernetzten Geräten, die das NTC in vergleichbaren Analysen geprüft hat. Hinweise auf absichtlich eingebaute Hintertüren oder versteckte Kommunikationskomponenten fanden sich keine. Die meisten Hersteller reagierten rasch auf die gemeldeten Schwachstellen; bei einem Teil der Befunde läuft das Offenlegungsverfahren noch, unter anderem weil für mehrere Modellreihen weltweit eine neue Firmware bereitgestellt werden muss. Was Solaranlagen von anderen vernetzten Geräten unterscheidet, ist nicht die Qualität der Produkte, sondern ihre Rolle: Was bei einem Haushaltsgerät meist ein Ärgernis bleibt, wiegt hier schwerer, denn die Anlagen sind in ihrer Summe systemrelevant.

Das massgebliche Risiko für das Schweizer Stromnetz liegt damit nicht im einzelnen Gerät, sondern in der Abhängigkeit von wenigen Herstellern: Über ihre Cloud-Infrastruktur werden die Anlagen gesteuert und mit Firmware versorgt, und daneben behalten die meisten Anbieter einen privilegierten Wartungszugang zu ihrem gesamten Gerätebestand.

Die Marktkonzentration vergrössert die Zahl der betroffenen Anlagen: 2025 entfiel über die Hälfte der neu verbauten Wechselrichter auf einen einzigen Hersteller, rund 80 Prozent auf vier (Huawei,

Fronius, Sungrow und SolarEdge). Behoben wird dieses Risiko nicht durch verbesserte Produktsicherheit, sondern nur durch eine Reduktion der Abhängigkeiten: nachprüfbare Zusicherungen, mehrere Anbieter am Markt und eine technische Begrenzung dessen, was aus der Ferne überhaupt möglich ist. International wird die verteilte Photovoltaik zunehmend als Frage der kritischen Infrastruktur behandelt, nicht mehr nur der Klimapolitik. Estland, Tschechien und Deutschland haben behördliche Warnungen veröffentlicht. Taiwan macht den Nachweis der Cybersicherheit zum Bestandteil der Produktzulassung, Litauen knüpft den Netzanschluss an Sicherheitsanforderungen. Die Schweiz hat diesen Schritt noch vor sich.

Aus den identifizierten Risiken leitet dieser Bericht Empfehlungen für fünf Adressaten ab.

Betreiberinnen und Betreiber von Kleinanlagen entscheiden am wirksamsten mit der Wahl eines etablierten Anbieters, dem sie neben der Installation auch den technischen Betrieb übertragen. Sie sollten sich bei der Übergabe bestätigen lassen, dass individuelle Passwörter gesetzt sind und die Anlage nicht direkt aus dem Internet erreichbar ist, vertraglich festhalten, wer für Updates und den Ereignisfall zuständig ist, und auf eine nicht benötigte Fernsteuerung verzichten.

Betreiber grösserer Anlagen verfügen über Fachwissen und Verhandlungsmacht, die Kleinanlagen fehlen. Sie sollten ihren Anlagenbestand samt Schnittstellen und Fernzugriffen inventarisieren, Photovoltaik, Energiemanagement und Ladeinfrastruktur vom übrigen Netz trennen, die zentrale Steuerbarkeit bewusst konfigurieren, Herstellerzugänge vertraglich fassen, und Sicherheitsanforderungen in ihre Ausschreibungen aufnehmen. Wo der IKT-Minimalstandard nicht greift, lohnt die freiwillige Anwendung.

Installationsbetriebe entscheiden in der Praxis über das Sicherheitsniveau der einzelnen Anlage, weil bei der Inbetriebnahme entsteht, was später angreifbar ist. Sie sollten bei jeder Anlage individuelle Zugangsdaten setzen und keine über ihren Kundenstamm hinweg einheitlichen Passwörter verwenden, den Wechselrichter nicht aus dem Internet erreichbar machen, nicht benötigte Schnittstellen deaktivieren und die Anlage vom übrigen Heim- oder Firmennetz trennen. Zur Übergabe gehören eine Dokumentation der Konfiguration und eine klare Abrede darüber, wer künftig Updates einspielt. In der Beschaffung sollten sie Produkte bevorzugen, die ohne Cloud funktionieren können, geschützte lokale Schnittstellen bieten und einen zugesicherten Update-Zeitraum haben.

Hersteller sollten Sicherheit als Konstruktionsprinzip verstehen: gerätespezifische und nicht rekonstruierbare Zugangsdaten, keine fest kodierten Geheimnisse, gesicherte lokale Schnittstellen sowie signierte Firmware-Updates. Wartungszugänge müssen zeitlich begrenzt, protokolliert und für die Betreiberin widerrufbar sein. Zentral ist eine werkseitige Sperre der netzrelevanten Fernsteuerung, die nur vor Ort aufgehoben werden kann. Sie begrenzt die skalierende Ebene technisch und nicht bloss organisatorisch. Und der Betrieb muss auch ohne Cloud möglich bleiben.

Politik und Behörden sollten die Lücke für Kleinanlagen schliessen. Wirksam sind Anforderungen, die am Produkt ansetzen und nicht an der Betreiberin: Mindestanforderungen für das Inverkehrbringen von Wechselrichtern und Energiemanagementsystemen, Sicherheitsanforderungen als Bedingung für den Netzanschluss und eine wiederkehrende Prüfung, die nicht mit einer einmaligen Zulassung endet. Ebenso nötig ist eine benannte Zuständigkeit für das Risiko, das erst aus der Summe der Kleinanlagen entsteht. Die wachsende Bündelung vieler Kleinanlagen bei Aggregatoren und virtuellen Kraftwerken ist dabei im Blick zu behalten. Für Anlagen besteht mit dem Sicherheitsnachweis bereits ein obligatorisches Kontrollverfahren, das sich um Cybersicherheitspunkte erweitern liesse.

Eine einfache und vollständige Lösung gibt es nicht; alle Ansätze haben Vor- und Nachteile, und Restrisiken bleiben.

Dieser Bericht ist kein Argument gegen die Photovoltaik, sondern eines für ihren sicheren Ausbau. Der Ausbau verringert die Notwendigkeit von Energieimporten. Diese Unabhängigkeit sollte aber nicht durch eine neue Abhängigkeit ersetzt werden, durch die Abhängigkeit von wenigen Herstellern mit Fernzugriff auf Tausende netzrelevante Geräte. Der Ausbau soll weitergehen, mit demselben Anspruch an Kontrollierbarkeit, der für andere kritische Infrastrukturen heute bereits selbstverständlich ist.

2 Ausgangslage und Motivation

2.1 Von wenigen grossen zu vielen kleinen Kraftwerken

Die Stromerzeugung der Schweiz beruhte lange überwiegend auf einer überschaubaren Zahl grosser, zentral betriebener und regulierter Kraftwerke. Kleinere Anlagen wie Kleinwasserkraftwerke gibt es zwar auch, sie fallen aber weder zahlenmässig noch in ihrer Vernetzung übermässig ins Gewicht. Mit dem Ausbau der Photovoltaik ist daneben eine zweite Welt entstanden: hunderttausende kleine, dezentrale «Kraftwerke» auf Dächern von Wohn- und Gewerbegebäuden. Mit dieser zweiten Welt entstehen neue Cyberrisiken mit Auswirkungen auf die gesamte Stromversorgung, die dieser Bericht behandelt.

2.2 Photovoltaik ist systemrelevant geworden

Die Photovoltaik hat sich in der Schweiz von einer Nischentechnologie zu einer tragenden Säule der Stromversorgung entwickelt. Ende 2025 waren rund 338'000 Anlagen mit einer kumulierten Spitzenleistung von rund 9,5 Gigawatt installiert. Ihre Jahresproduktion von knapp 8 Terawattstunden deckte 13,7 Prozent des Strom-Endverbrauchs[1] und entsprach damit ungefähr der geplanten Jahresproduktion des Kernkraftwerks Gösgen.[2]

Aussagekräftiger als diese Jahreswerte ist der momentane Beitrag zu Spitzenzeiten. Zur sonnigen Mittagszeit deckt die Photovoltaik regelmässig über die Hälfte des momentanen Verbrauchs, an Spitzentagen deutlich mehr. Am 4. Juli 2026 um 14:00 Uhr etwa waren es rund 6'100 Megawatt bei einer Last von rund 7'200 Megawatt und damit gegen 85 Prozent[3].

Damit ist die Photovoltaik für die Versorgungssicherheit relevant geworden. Einzeln betrachtet bleibt eine Anlage für das Netz unbedeutend. In der Masse fällt sie allerdings ins Gewicht, und weil diese Anlagen vernetzt und ähnlich konfiguriert sind, lassen sie sich auch gemeinsam beeinflussen, bestimmungsgemäss und netzdienlich durch den Netzbetreiber, missbräuchlich durch einen Angreifer. Zur kritischen Infrastruktur wird deshalb nicht die einzelne Anlage, sondern der Bestand als Ganzes.

Dieser Bestand wächst weiter. Der Bundesrat hat am 26. November 2025 in der Energieverordnung erstmals technologiespezifische Zwischenziele festgelegt: Von den 23 Terawattstunden, die die erneuerbaren Energien ohne Wasserkraft bis 2030 beitragen sollen, entfallen 18,7 auf die Photovoltaik. Gegenüber den knapp 8 Terawattstunden im Jahr 2025 ist dies mehr als eine Verdoppelung innerhalb von fünf Jahren. Das übergeordnete Ziel des Energiegesetzes verlangt für die erneuerbaren Energien ohne Wasserkraft bis 2035 35 und bis 2050 45 Terawattstunden. Technologiespezifische Zwischenziele hat der Bundesrat bisher nur für 2030 festgelegt.[4] Mit dem Bestand wächst damit auch der Bedarf, ihn steuerbar zu machen.

2.3 Warum das Thema bisher wenig beleuchtet wurde

International hat die Cybersicherheit von Photovoltaikanlagen zuletzt an Aufmerksamkeit gewonnen. Die in der Schweiz verbreiteten Geräte wurden bislang jedoch kaum unabhängig und systematisch geprüft. Dafür gibt es mehrere Gründe:

- **Wenig Anreiz bei den Anlagenbetreibern**: Die Anlagen werden überwiegend von Privatpersonen und kleineren Unternehmen betrieben. Gerade bei Privatpersonen dürfte

[1] Bundesamt für Energie, «Statistik Sonnenenergie 2025»: https://pubdb.bfe.admin.ch/de/sammlungen/statistik-sonnenenergie
[2] Swissolar, «Solarmonitor Schweiz 2025»: https://www.swissolar.ch/de/markt-und-politik/markt-schweiz/solarmonitor-schweiz
[3] Momentanwerte: energy-charts.info (Fraunhofer ISE), Nettostromerzeugung Schweiz, Woche 27/2026 (4. Juli 2026, 14:00 Uhr: Last 7'209 MW, Solar 6'121 MW): https://www.energy-charts.info/charts/power/chart.htm?c=CH&l=de&year=2026&week=27
[4] Bundesrat, Medienmitteilung «Bundesrat genehmigt Anpassungen von Verordnungen im Energiebereich», 26. November 2025: https://www.admin.ch/de/newnsb/dvb52hRdMmNdS3aNKL96C

dabei kaum im Vordergrund stehen, was ihre vernetzte Anlage angreifbar macht. Fällt eine Anlage durch einen Cyberangriff aus, kaufen sie den fehlenden Strom zu. Gemessen an diesen Stromkosten wäre eine Sicherheitsüberprüfung unverhältnismässig teuer. Das eigentliche Risiko entsteht erst, wenn viele Anlagen gleichzeitig manipuliert werden, und trifft dann nicht die einzelnen Betreiber, sondern die Stromversorgung insgesamt.

- **Keine Zuständigkeit bei den Netzbetreibern**: Sie verantworten die Stabilität des Gesamtsystems und tragen damit das Risiko. Über die Anschlussbedingungen können sie technische Anforderungen stellen, für die Cybersicherheit privater Kleinanlagen im Betrieb fehlt ihnen aber die Zuständigkeit (vgl. Kapitel 7.4).
- **Aufwändige Beschaffung und riskante Prüfung:** Die Geräte sind für unabhängige Prüfungen vergleichsweise teuer und aufwändig zu beschaffen, und das Testen erfordert Arbeiten an netzgekoppelten Geräten unter zum Teil hoher Spannung und damit besondere Vorsichtsmassnahmen und Fachkompetenz.
- **Begrenzte Übertragbarkeit internationaler Studien:** Bestehende Analysen aus dem Ausland bilden die Schweizer Marktgegebenheiten nur bedingt ab. Teils sind hierzulande andere Produkte verbreitet, und einzelne im Schweizer Markt relevante Anbieter kommen in internationalen Untersuchungen gar nicht vor.

2.4 Warum eine Cyberbedrohung besteht

Sicherheitsrelevant ist vor allem, dass moderne Anlagen meistens mit dem Internet und der Cloud des Herstellers verbunden sind. Das macht es praktikabel, eine grosse Zahl von Anlagen gleichzeitig und koordiniert zu beeinflussen. Auch der Verteilnetzbetreiber kann teilweise viele Anlagen zugleich ansteuern, etwa um die Einspeisung zu drosseln. Dieser Weg unterscheidet sich aber in mehreren Punkten: Er reicht nur so weit wie das Netzgebiet des jeweiligen Betreibers, er liegt in der Hand eines regulierten Unternehmens, und er nutzt häufig einen eigenen, vom Internet getrennten Steuerkanal (Rundsteuerung). Eine Herstellercloud erreicht eine Geräteflotte dagegen über das Internet über Netzgebiete und Landesgrenzen hinweg. Was eine gleichzeitige Manipulation vieler Anlagen für die Netzstabilität bedeuten würde, behandelt das Kapitel *6 Auswirkung auf die Netzstabilität*.

Diese Bedrohung trifft auf ungünstige Rahmenbedingungen. Die Betreiberinnen und Betreiber verfügen in der Regel über kein besonderes Cyber-Fachwissen und für den Betrieb ihrer Anlagen ist niemand verpflichtet, Cybersicherheit sicherzustellen. Während Netzbetreiber und sehr grosse Erzeuger Cybervorgaben wie dem IKT-Minimalstandard unterstehen, fallen Kleinanlagen und damit praktisch alle Schweizer Photovoltaikanlagen durch dieses Raster. Für Erzeuger greift der Standard erst ab 100 MW, also ab 100'000 kW. Eine typische Dachanlage liegt im zweistelligen Kilowattbereich und damit über tausendmal tiefer.

Diese Einschätzung teilt die nationale Netzgesellschaft. Swissgrid führt in ihrem White Paper «Systemverträgliche Integration Photovoltaik»[5] die Cyber-Security-Risiken ausdrücklich unter den Herausforderungen des Systembetriebs auf: Wechselrichter sowie weitere Anlagen wie Ladestationen und Energiemanagementsysteme seien zunehmend über das Internet fernsteuerbar. Unzureichende Vorgaben und ein mangelndes Problembewusstsein erhöhten das Risiko, dass externe Akteure das Stromsystem darüber destabilisieren.

2.5 Das sicherheitspolitische Umfeld

Diese technische Ausgangslage fällt mit einer sich verschärfenden sicherheitspolitischen Lage zusammen. Der Nachrichtendienst des Bundes (NDB) stellt in seinem Lagebericht «Sicherheit Schweiz 2026»[6] eine markante und nachhaltige Verschlechterung des sicherheitspolitischen Umfelds fest. Kritische Infrastrukturen werden dabei ausdrücklich als durch physische wie durch Cyberangriffe bedroht eingestuft. Der NDB hält zudem fest, dass die Infrastrukturen der europäischen Länder nicht isoliert betrachtet werden können. Ein Angriff auf Schweizer Infrastruktur, um von ihr abhängige andere Staaten zu treffen, sei ebenso denkbar wie umgekehrt

[5] Swissgrid AG, White Paper «Systemverträgliche Integration Photovoltaik», März 2026: https://www.swissgrid.ch/de/home/newsroom/blog/2026/20260330-01.html
[6] Nachrichtendienst des Bundes (NDB), «Sicherheit Schweiz 2026»: https://www.vbs.admin.ch/de/newnsb/jyRmuld1hBVy

Kollateralschäden durch Angriffe auf ausländische Infrastrukturen. Ebenso weist der NDB darauf hin, dass die Attraktivität solcher Ziele wächst, je stärker die Nato- und EU-Staaten ihre kritische Infrastruktur schützen, ohne dass die Schweiz gleichzieht.

Dass diese Einschätzung keine abstrakte ist, zeigt der koordinierte Cyberangriff auf die polnische Energie- und Wärmeversorgung vom Dezember 2025. Betroffen waren unter anderem mehr als 30 Wind- und Solarparks[7]. Das Vereinigte Königreich und die EU schrieben den Angriff im Juli 2026 offiziell dem russischen Geheimdienst FSB (Zentrum 16) zu.[8] Vor dem Hintergrund der eng verflochtenen europäischen Netze und der Einschätzung des NDB sind vergleichbare Entwicklungen auch für die Schweiz von Belang.

Dass die verteilte Photovoltaik dabei konkret im Blick steht, zeigt ein gemeinsamer Sicherheitshinweis des deutschen Bundesamts für Verfassungsschutz (BfV) und des Bundesamts für Sicherheit in der Informationstechnik (BSI) vom 3. Juni 2026[9]. Nach deren Erkenntnissen klären russische Cyberakteure aktiv Photovoltaikanlagen auf, die ungeschützt mit dem Internet verbunden sind. Im Fokus stehen Monitoring-Systeme, die auch steuernden Zugriff auf die Anlagen erlauben. Betroffen sind überwiegend Anlagen von Privatpersonen und Genossenschaften ohne energiewirtschaftlichen Hintergrund. Bei einem Teil dieser Anlagen ist der Zugriff ohne Zugangsdaten möglich, und die Softwarestände sind teilweise stark veraltet. Es handelt sich dabei um Auskundschaftung und nicht um einen Angriff. Der Hinweis zeigt aber, dass genau jene Anlagenklasse, die dieser Bericht untersucht, von staatlichen Akteuren systematisch erfasst wird.

2.6 Abgrenzung: Batteriespeicher, Ladeinfrastruktur und weitere vernetzte Geräte

Nicht Gegenstand dieser Analyse, aber von wachsender Bedeutung sind vernetzte Verbraucher und Speicher wie Batteriespeicher, Ladestationen für Elektrofahrzeuge und Wärmepumpen. Gerade Batteriespeicher verbreiten sich rasch. Bei neuen Photovoltaikanlagen auf Schweizer Einfamilienhäusern ist inzwischen ein erheblicher Teil mit einem Speicher ausgestattet.[10] Aus Sicht der Cybersicherheit besonders relevant sind Angriffe, die Photovoltaik mit Batteriespeichern oder Ladeinfrastruktur kombiniert nutzen, da sich damit sowohl Einspeisung als auch Bezug manipulieren lassen. Die Ladeinfrastruktur hat das NTC bereits in einem früheren Bericht[11] untersucht.

[7] CERT Polska, «Energy Sector Incident Report – 29 December»: https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/
[8] OFSI/GOV.UK, Sanktionsmitteilung vom 13. Juli 2026: https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions
[9] Bundesamt für Verfassungsschutz (BfV) und Bundesamt für Sicherheit in der Informationstechnik (BSI), «Gemeinsamer Sicherheitshinweis: Auskundschaftung schlecht geschützter PV-Anlagen durch staatliche Cyberakteure», 3. Juni 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html
[10] Bundesamt für Energie, «Statistik Sonnenenergie 2025»: https://pubdb.bfe.admin.ch/de/sammlungen/statistik-sonnenenergie
[11] Nationales Testinstitut für Cybersicherheit NTC, Bericht zur Cybersicherheit von Ladeinfrastruktur, 2023: https://www.ntc.swiss/aktuelles/2023-analyse-ladeinfrastruktur-e-mobilitaet

3 Das Ökosystem einer Photovoltaik-Anlage

Dieses Kapitel beschreibt, aus welchen Bausteinen eine Photovoltaik-Anlage besteht. Es erklärt, wie diese untereinander und mit dem Internet kommunizieren und wer sie steuern kann. Die Darstellung bleibt bewusst beschreibend und zeigt, wo die Architektur eine Angriffsfläche bietet. Ob sich diese Flächen in der Überprüfung tatsächlich als Risiko erwiesen haben, ist nicht Thema dieses Kapitels. Welche Komponenten geprüft wurden und warum, steht im Kapitel *4 Methodik*. Die Ergebnisse folgen im Kapitel *5 Befunde und Risiken*.

3.1 Die Komponenten und ihr Zusammenspiel

Eine typische Photovoltaik-Anlage besteht aus einigen wenigen Grundbausteinen. Sie sind je nach Bauart unterschiedlich stark ineinander integriert. Für die folgende Betrachtung werden sie funktional getrennt dargestellt. Die **Solarmodule** erzeugen Gleichstrom (DC). Der **Wechselrichter** wandelt diesen in netzkonformen Wechselstrom (AC) um und speist ihn ins Netz ein. Er ist damit die zentrale, aktiv steuerbare Komponente der Anlage. Für die Fernüberwachung wird der Wechselrichter über ein **Kommunikationsmodul** (oft bereits im Wechselrichter integriert) mit dem Internet verbunden, meist per WLAN, Mobilfunk oder Kabel. Diese Anbindung ist technisch nicht zwingend, in der Praxis aber die Regel. Bei modernen Anlagen erfolgt die Überwachung meist über das Internet-Portal des Herstellers, und wo kein Kommunikationsmodul verbaut ist oder wo zusätzlich weitere Geräte wie Batteriespeicher, Ladestation oder Wärmepumpe gesteuert werden, übernimmt häufig ein **Energiemanagementsystem** die Kommunikation nach aussen. Über diese Anbindung fliessen die Betriebsdaten an eine **Herstellercloud**, die sie speichert und visualisiert. Je nach Hersteller ermöglicht sie darüber hinaus die Fernüberwachung, die Fernsteuerung und die Firmware-Aktualisierung der Anlage. Die **Mobile- oder Web-App** schliesslich ist die Bedienoberfläche für die Betreiberin oder den Betreiber und greift ihrerseits auf die Cloud zu. Ergänzend sind häufig weitere vernetzte Verbraucher und Speicher eingebunden, etwa **Batteriespeicher**, **Ladestationen für Elektrofahrzeuge oder Wärmepumpen**. Solche zusätzlichen Komponenten vergrössern die Angriffsfläche und die möglichen Auswirkungen weiter. Am Netzanschlusspunkt befindet sich zudem der Zähler des Verteilnetzbetreibers. Er misst die bezogene und die eingespeiste Energie und wird in der Schweiz schrittweise durch ein intelligentes Messsystem (**Smart Meter**) ersetzt, das die Messwerte fernauslesbar macht. Der Zähler gehört nicht der Betreiberin oder dem Betreiber, sondern dem Netzbetreiber, und bildet damit eine eigene, vom Hersteller unabhängige Verbindung nach aussen.

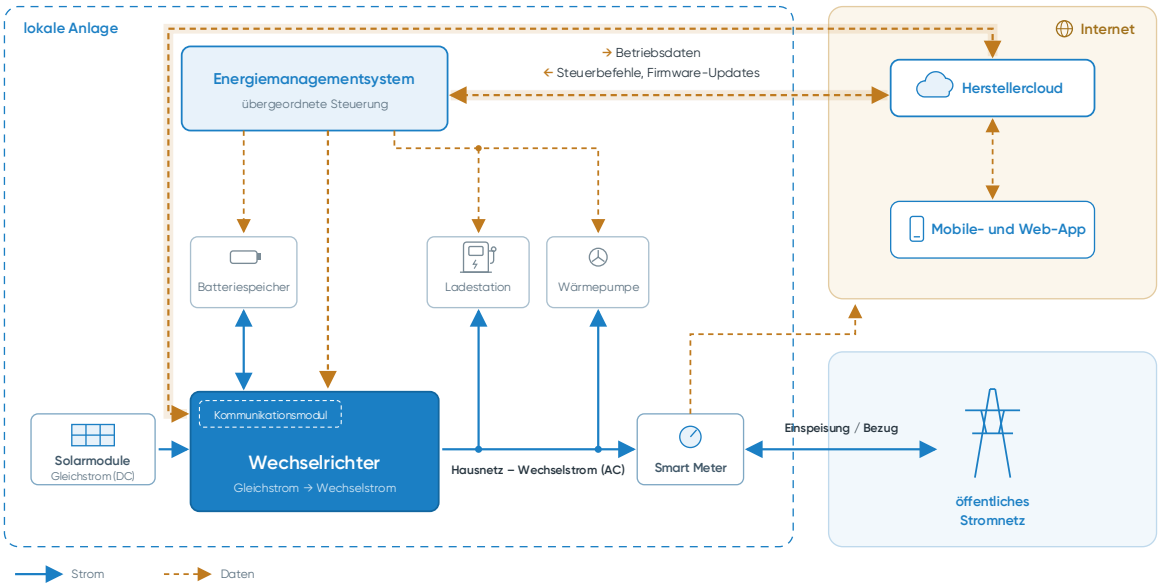


Abbildung 1: Schematische Übersicht einer typischen Photovoltaik-Anlage

3.2 Wechselrichter und Energiemanagementsystem

Für das Verständnis der Steuerbarkeit ist die Unterscheidung zwischen Wechselrichter und Energiemanagementsystem (EMS) zentral, weil beide Begriffe im Alltag oft vermischt werden.

Der **Wechselrichter** wandelt Strom und speist ihn ins Netz ein. Über seine netzdienlichen Funktionen wie Wirk- und Blindleistungsvorgaben oder Kennlinien ist er das Element, das die Einspeisung unmittelbar beeinflusst.

Das **Energiemanagementsystem** ist eine übergeordnete Steuerung. Sie koordiniert mehrere Geräte einer Anlage, typischerweise Wechselrichter, Batteriespeicher, Ladestation und Wärmepumpe, und optimiert deren Betrieb, etwa nach dem Eigenverbrauch.

Daraus ergibt sich ein Doppelcharakter, der das EMS für die Cybersicherheit besonders bedeutsam macht. Als Teil der Lösung kann ein EMS die Abhängigkeit von einzelnen Herstellerclouds verringern: Nicht jedes Gerät muss zwingend mit der Cloud seines Herstellers verbunden sein, und ein sinnvoll zwischen lokalem Netzwerk und Wechselrichter platziertes EMS kann die direkte Erreichbarkeit der Einzelgeräte begrenzen. Als Verschärfung des Problems gilt jedoch: Wer das EMS kontrolliert, kontrolliert alle daran angeschlossenen Geräte und kann damit mindestens ebenso viel Schaden anrichten wie über einen einzelnen Wechselrichter, potenziell mehr, weil das EMS auch weitere Komponenten wie Batteriespeicher und Ladestation steuert. Herstellerübergreifende EMS-Anbieter aggregieren diese Kontrolle zusätzlich über verschiedene Gerätemarken hinweg. Das EMS ist damit im Kern eine lokale Komponente, zugleich aber ein Bündelungspunkt, dessen Kompromittierung weiter reicht als die eines einzelnen Wechselrichters.

3.3 Kommunikationswege und bekannte Schwachstellen

Sicherheitsrelevant sind zwei Fragen: welche Komponenten miteinander kommunizieren und wie gut diese Verbindungen geschützt sind. Das Kommunikationsmodul meldet die Betriebsdaten an die Herstellercloud und empfängt von dort Befehle. Die App greift typischerweise ihrerseits auf die Cloud zu, nicht direkt auf die Anlage. Ist das Kommunikationsmodul im Wechselrichter integriert, spielt sich diese Verbindung geräteintern ab. Anders ist es, sobald ein externes Gerät den Wechselrichter direkt ansprechen soll, etwa ein Energiemanagementsystem. Dann verläuft die Verbindung lokal im Gebäude- oder Heimnetz.

Für diese lokale Verbindung sind Industrieprotokolle verbreitet, allen voran Modbus: früher über eine serielle Kabelverbindung (RS485), zunehmend über das Netzwerk (Modbus TCP). Daneben kommen herstellereigene Protokolle vor. Modbus wurde für abgeschottete Anlagen entworfen und bietet von sich aus weder Verschlüsselung noch Authentisierung. Einzelne Hersteller ergänzen proprietäre Autorisierungsmechanismen. Eine 2018 nachgereichte Sicherheitserweiterung auf TLS-Basis ist in der Praxis kaum verbreitet. Deshalb ist diese Schnittstelle für die späteren Befunde von Bedeutung.

Aus dem Internet ist der Wechselrichter nach dieser Architektur nicht direkt erreichbar. Der Weg von aussen führt stattdessen über die Herstellercloud. Die Herstellercloud wiederum kann konstruktionsbedingt sehr viele Anlagen zugleich überwachen, steuern und aktualisieren.

Dieses Bild deckt sich mit der vorhandenen Forschung. Eine Auswertung[12] von 93 seit 2012 offengelegten Schwachstellen mit CVE-Nummer bei 34 Herstellern ordnet den grössten Teil der Monitoring- und Cloud-Ebene zu, rund 38 Prozent dem Solar-Monitoring und rund 25 Prozent der Cloud, während der Wechselrichter mit Kommunikationsmodul bei knapp 30 Prozent betroffen war. Rund 80 Prozent aller Fälle gelten als hoch oder kritisch. Diese Zahlen sind mit Vorsicht zu lesen, denn sie zählen Fundstellen und nicht Risiko, und die vernetzte Ebene ist aus der Ferne ungleich leichter zu prüfen. Theoretisch bleiben sie aber nicht: Sechs der katalogisierten Schwachstellen werden seit 2022 regelmässig von Botnetzen ausgenutzt. Entscheidend ist am Ende weniger die Zahl der Schwachstellen als der Umstand, dass eine einzige Cloud sehr viele Anlagen zugleich erreicht.

[12] dos Santos, La Spina, Dashevskyi, «A Closer Look at the Gaps in the Grid», Black Hat Asia 2025: https://i.blackhat.com/Asia-25/Asia-25-dosSantos-A-Closer-Look-at-the-Gaps-in-the-Grid.pdf

3.4 Zentrale und lokale Steuerung

Die Bausteine lassen sich danach ordnen, wie viele Anlagen eine kompromittierte Komponente beeinflussen kann. Eine zentrale Instanz wie die Herstellercloud wirkt auf viele Anlagen gleichzeitig. Wer sie kontrolliert, kann an alle angebundenen Geräte Befehle senden. Eine lokale Instanz wie der Wechselrichter selbst, die Mobile-App oder ein lokales Steuergerät beeinflusst dagegen nur die eigene Anlage. Diese Unterscheidung trennt skalierende Angriffe, die viele Anlagen aus der Ferne treffen, von nicht-skalierenden Angriffen, die auf die Einzelanlage beschränkt bleiben. Sie ist der Grund, weshalb einzelne kleine Anlagen für sich unbedeutend sind, in der vernetzten Masse aber relevant werden. Für eine netzwirksame Manipulation ist die zentrale Ebene der lohnende Angriffspunkt. Diese zentrale Steuerbarkeit lässt sich technisch allerdings auch bewusst begrenzen. Dieser Bericht empfiehlt deshalb, Geräte so auszulegen, dass die Cloud die Anlage nur noch überwachen und mit signierten Updates versorgen, aber nicht mehr steuern kann (vgl. Kapitel *8.4.2*).

Neben der Herstellercloud tritt zunehmend eine zweite zentrale Steuerungsebene hinzu: Aggregatoren und virtuelle Kraftwerke. Dabei bündelt ein Anbieter viele verteilte Anlagen über Internet-Schnittstellen und vermarktet ihre gebündelte Leistung, etwa als Regelenergie. Ein Beispiel ist das Pilotprojekt «PV4Balancing»[13] der nationalen Netzgesellschaft Swissgrid, bei dem aggregierte Photovoltaikanlagen ihre Einspeisung auf Abruf als negative Tertiärregelleistung reduzieren. Noch näher an der Masse der Kleinanlagen liegt ein zweites Beispiel: Helion erhielt von Swissgrid die Bewilligung, private Photovoltaik-Kleinanlagen, Hausspeicher und Ladestationen über die eigene Plattform zu bündeln und die gebündelte Leistung am Regelenergiemarkt anzubieten[14]. Damit geraten genau jene Anlagen unter eine zentrale Fernsteuerung, die einzeln keinen Cybersicherheitsanforderungen unterliegen. Der Aggregator selbst ist dagegen erfasst, sobald er über ein einziges System auf mindestens 100 MW zugreifen kann (vgl. Kapitel *7.4).* Der «Flexpool»[15] der CKW etwa vereint bereits über 1'000 MW aus rund 1'700 Kundenanlagen an einem Steuerungspunkt, wenn auch technologisch gemischt und nicht allein aus Photovoltaik. Diese Entwicklung ist doppelschneidig: Netzdienlich eingesetzt sind steuerbare, gebündelte Anlagen ein Stabilisierungsinstrument. Zugleich entsteht mit dem Aggregator ein weiterer zentraler Steuerungspunkt, der bei Kompromittierung eine bereits koordinierte Fernsteuerung über viele Anlagen eröffnet. Diese Bündelung ist kein Nebenprodukt, sondern Teil der Zielarchitektur. Swissgrid hält fest, die Teilnahme dezentraler Einheiten an den Regelenergiemärkten solle über Aggregatoren möglichst niederschwellig erfolgen, und nennt eine zentrale Flexibilitätsplattform mit Koordinationsmechanismus als geeignetste Variante. Erprobt wird dies in einem weiteren Pilotprojekt, der «TSO-DSO-Koordination».[16] Die Zahl der über einen einzelnen Steuerungspunkt erreichbaren Anlagen, dürfte weiter wachsen. Umso wichtiger ist, die Sicherheitsanforderungen an diese Ebene zu klären, solange sie im Aufbau ist. Das NTC hat diese Plattformen nicht geprüft, die Einordnung betrifft die Struktur, nicht die Sicherheit einzelner Anbieter.

3.5 Anlagentypen und Betreiber

Die Netzwerkanbindung und das Schutzniveau hängen stark vom Anlagentyp ab. In Anlehnung an die Förderkategorien des Bundes gelten Anlagen bis 100 kW als **Kleinanlagen**: Sie umfassen Einfamilienhäuser, Mehrfamilienhäuser und kleinere Gewerbebauten. Kleinanlagen sind meist im normalen Gebäude- oder Heimnetz und werden von Privatpersonen oder kleineren Unternehmen betrieben, die in der Regel kein besonderes Cyber-Fachwissen mitbringen. **Grossanlagen** über 100 kW sind häufiger professionell betreut und hinter einer Firewall segmentiert. Die grössten Anlagen sind an ein eigenes Umspannwerk und den Verteilnetzbetreiber angebunden und verzichten häufiger auf eine Anbindung an die Herstellercloud. Umgekehrt ist die Cloud-Anbindung bei Kleinanlagen zwar die Regel, aber auch dort nicht zwingend.

[13] Swissgrid, Pilotprojekt «PV4Balancing»: https://www.swissgrid.ch/de/home/newsroom/blog/2025/die-sonne-als-ressource-fuer-einen-stabilen-netzbetrieb.html
[14] Helion Energy AG, virtuelles Kraftwerk für Privatkunden auf Basis der Plattform «Helion ONE»: https://www.gebaeudetechnik.ch/de/news/virtuelles-kraftwerk-fuer-die-schweiz--252
[15] CKW (Axpo-Gruppe), «Flexpool»: https://www.ckw.ch/ueber-ckw/medienstelle/medienmitteilungen/2025/1000-megawatt-virtuelles-grosskraftwerk-von-ckw-erreicht-meilenstein
[16] Swissgrid AG, White Paper «Systemverträgliche Integration Photovoltaik», März 2026: https://www.swissgrid.ch/de/home/newsroom/blog/2026/20260330-01.html

2025	Anz. Anlagen	Leistung in MW	Ø Leistung in kW
bis 4 kW	1'132	3.0	2.7
über 4 kW bis 10 kW	9'073	68.9	7.6
über 10 kW bis 20 kW	14'864	211.9	14.3
über 20 kW bis 30 kW	4'831	117.8	24.4
über 30 kW bis 50 kW	3'134	119.8	38.2
über 50 kW bis 100 kW	1'977	138.9	70.3
über 100 kW bis 1000 kW	2'175	536.2	246.6
über 1000 kW	72	136.4	1'882.5
Total Netzverbundanlagen	**37'257**	**1'332.9**	**35.8**

Abbildung 2: Netzverbundanlagen nach Grösse. Quelle: Statistik Sonnenenergie 2025[17], BFE

Die Grössenverteilung zeigt das Missverhältnis deutlich. Von den 2025 neu installierten 37'257 Netzverbundanlagen lagen 35'011 und damit 94 Prozent bei höchstens 100 kW. Auf sie entfiel rund die Hälfte der neu installierten Leistung. Die durchschnittliche Anlage misst rund 25 kW, der Median rund 11 kW. Zugleich stammen rund 40 Prozent der Schweizer Photovoltaik-Produktion aus Anlagen unter 30 kW. Der Bestand, für den keine betrieblichen Cybersicherheitsvorgaben gelten, trägt damit einen erheblichen Teil der Erzeugung.

3.6 Marktkonzentration

Sicherheitsrelevant ist nicht nur, wie viele Anlagen installiert sind, sondern von wie vielen verschiedenen Herstellern sie stammen: Firmware, Wartungszugänge und Update-Kette bestimmt der Hersteller, weshalb ein einzelner Befund für dessen gesamten Gerätebestand gelten kann, auch für Anlagen ohne Cloud-Anbindung. In der Schweiz hat sich dieses Feld mehrfach verschoben. Das PV-Barometer 2026[18] wertet dazu Projektdesigns aus: 2017 lag Fronius bei 45,7 Prozent Marktanteil; 2020 verteilte sich der Markt auf drei ähnlich grosse Anbieter (FIMER 23,5 Prozent, Fronius 22,9, SolarEdge 22,8); 2025 entfielen auf Huawei 52,3 Prozent, auf Fronius 13,3, auf Sungrow 9,2 und auf SolarEdge 8,2 Prozent. Der Anteil des grössten Anbieters ist damit heute höher als je zuvor im Beobachtungszeitraum. Die Zahl der Anbieter ist dabei nicht gesunken, verändert hat sich die Verteilung.

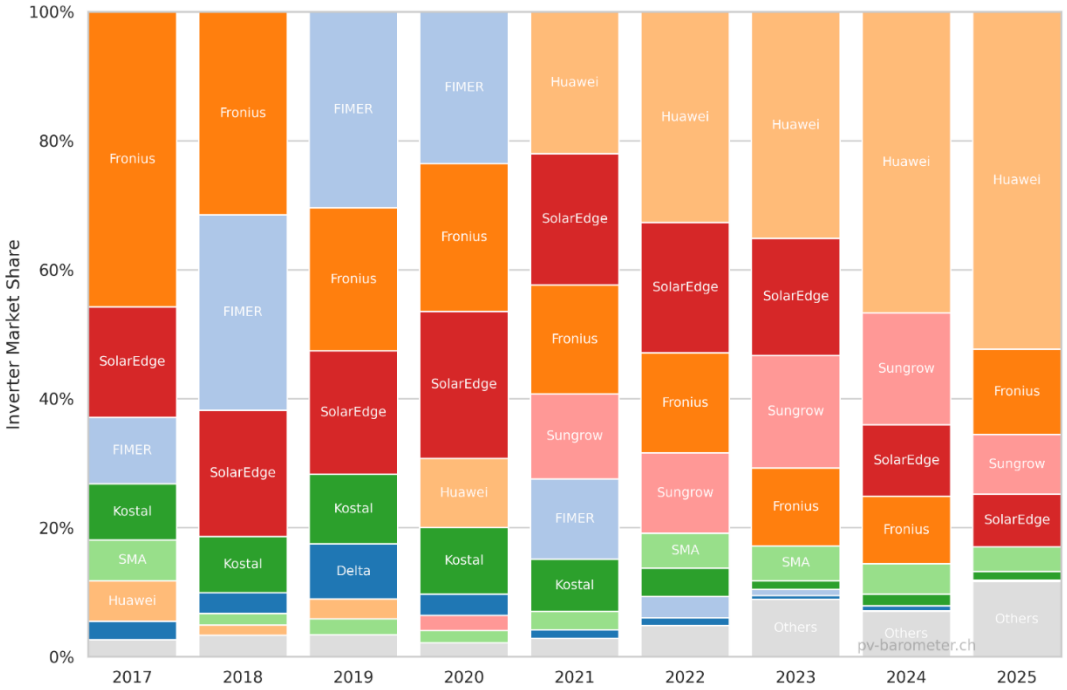


Abbildung 3: Marktanteile der Wechselrichterhersteller in der Schweiz. Quelle: PV-Barometer 2026

[17] Bundesamt für Energie, «Statistik Sonnenenergie 2025»: https://pubdb.bfe.admin.ch/de/sammlungen/statistik-sonnenenergie
[18] Berner Fachhochschule & Eturnity AG, «PV-Barometer 2026»: https://www.pv-barometer.ch/

4 Methodik

Das NTC hat Wechselrichter und Energiemanagementsysteme einer umfassenden technischen Sicherheitsanalyse unterzogen. Die Überprüfung war auf drei Grundsätze ausgerichtet:

- **Marktnähe:** eine an der Verbreitung im Schweizer Markt orientierte Auswahl der Geräte.
- **Unabhängigkeit:** kein Einbezug der Hersteller in Auswahl, Durchführung und Finanzierung; Kontakt ausschliesslich im Rahmen der Schwachstellenmeldung.
- **Skalierung:** Konzentration auf Schwachstellen, mit denen sich viele Anlagen zugleich manipulieren lassen.

Über einen Zeitraum von rund einem Jahr wendete das NTC insgesamt rund 1'300 Arbeitsstunden für die Untersuchung auf. Unterstützt wurde sie durch zahlreiche Organisationen aus dem Energiesektor, die Testgeräte bereitstellten und sich an den Kosten beteiligten. Die Hersteller der geprüften Produkte waren daran nicht beteiligt. Die folgenden Abschnitte beschreiben den Untersuchungsgegenstand und dessen Abgrenzung, die Auswahl und Beschaffung der Geräte, den Testaufbau, den analytischen Schwerpunkt sowie den Umgang mit den gefundenen Schwachstellen.

4.1 Untersuchungsgegenstand und Abgrenzung

Der Fokus der Überprüfung lag bewusst auf Wechselrichtern und Energiemanagementsystemen sowie auf Anlagen in Wohn- und kleineren Gewerbebauten. Beides folgt aus der im Kapitel *3 Das Ökosystem einer Photovoltaik-Anlage* beschriebenen Architektur: Wechselrichter und Energiemanagementsysteme sind die zentralen, netz- und cloud-angebundenen Komponenten einer Photovoltaik-Anlage und können die Einspeisung aktiv steuern. Solche Kleinanlagen wiederum unterliegen keinen betrieblichen Cybersicherheitsvorgaben. Produktseitig gelten für neu in Verkehr gebrachte Geräte seit August 2025 die Cybersicherheitsanforderungen der EU-Funkanlagenrichtlinie, falls diese eine Funkschnittstelle aufweisen (vgl. Kapitel *7.3.2*). Diese setzen ein Grundniveau, sagen aber nichts über Konfiguration, Betrieb und Wartung der installierten Anlage aus und beruhen auf der Selbstdeklaration des Herstellers. Betrieben werden die Anlagen meist von Privatpersonen oder kleineren Unternehmen ohne besonderes Cyber-Fachwissen, und unabhängig geprüft wurden sie bislang kaum.

Bewusst nicht untersucht wurden die Solarmodule. Zwar enthalten manche Module aktive Elektronik wie Moduloptimierer. Diese sind aber, wenn überhaupt vernetzt, nur mit dem Wechselrichter verbunden und liegen damit ausserhalb des skalierenden Angriffsbildes. Nicht Teil der Untersuchung waren zudem Komponenten wie Smart Meter, Batteriespeicher und Ladestationen für Elektromobilität. Auch diese Komponenten sind sicherheitsrelevant und gewinnen an Bedeutung: Batteriespeicher etwa sind, ähnlich wie Wechselrichter, netz- und cloud-angebunden, und ein koordiniertes Laden oder Entladen vieler Speicher hätte eine vergleichbare Wirkung auf das Netz.

Ausserhalb des Untersuchungsumfangs lagen zudem sehr kleine Steckersolargeräte («Balkonkraftwerke»). Sie sind im Schweizer Markt deutlich weniger verbreitet als in Deutschland und sind bereits Gegenstand unabhängiger Untersuchungen. Dass auch in dieser Kategorie ernstzunehmende Schwachstellen bestehen, zeigen z.B. die vom Chaos Computer Club (CCC) offengelegten Funkschwachstellen[19] der Hoymiles-Mikrowechselrichter (2026) (vgl. Kapitel *5.3.4*).

Der rechtliche Rahmen bestimmte die Prüftiefe mit. Die Geräte selbst hat das NTC beschafft und konnte sie ohne Einschränkung untersuchen. Die Herstellerclouds sind dagegen fremde, produktiv betriebene Systeme: Zugriffe darauf können ohne Einwilligung des Betreibers nach Art. 143bis StGB strafbar sein. Ein 2023 im Auftrag des NTC erstelltes Rechtsgutachten[20] grenzt ab, welche

[19] Chaos Computer Club (B. Heinz «Hunz»), «Analyse der Funk- und Firmware-Schwachstellen von Hoymiles-Wechselrichtern», 2026: https://www.ccc.de/updates/2026/blinkenlights-hoymiles
[20] Walder Wyss AG, «Rechtsgutachten zur Strafbarkeit von Ethical Hacking»: https://www.walderwyss.com/de/news/2023-06-26_rechtsgutachten-zur-strafbarkeit-von-fuer-das-nationale-testinstitut-fuer-cybersicherheit-ntc

Prüfhandlungen ohne solche Einwilligung zulässig sind.

Eine Einwilligung wäre nur über die Hersteller zu erhalten gewesen. Das hätte deren Einbezug in die Untersuchung bedeutet und stünde im Widerspruch zum Grundsatz der Unabhängigkeit. Das NTC hat sich deshalb bewusst auf den ohne Einwilligung zulässigen Rahmen beschränkt und auf eine vertiefte Prüfung der Cloud-Ebene verzichtet.

Dieser Bericht beurteilt die technische Machbarkeit, nicht die Absicht möglicher Akteure und nicht den Verlauf einer Krisenbewältigung.

4.2 Geräteauswahl

Eine vollständige Statistik der hierzulande verbauten Wechselrichter gibt es nicht. Zur Anlagenzahl und Leistungsverteilung stehen offizielle Daten zur Verfügung (Pronovo-Statistiken[21], Statistik Sonnenenergie[22] des BFE). Für die Marktanteile der Hersteller existiert dagegen nur die Erhebung des PV-Barometers, die von einem Marktteilnehmer verantwortet wird, die Anteile dafür aber seit 2017 jährlich ausweist und so die Entwicklung über die Zeit sichtbar macht. Exakte Zahlen lassen sich daraus nicht ableiten, wohl aber Grössenordnungen, und diese sind eindeutig. 2025 entfiel gut die Hälfte der neu verbauten Wechselrichter auf einen einzigen Hersteller, rund zwei Drittel auf zwei und rund 80 Prozent auf vier. Untersucht wurden deshalb sieben Wechselrichter von sechs Herstellern, darunter die marktbestimmenden Anbieter.

Für Energiemanagementsysteme ist die Datenlage noch dünner. Eine vergleichbare Statistik existiert nicht. Massgebend waren hier Gespräche mit Fachpersonen aus der Branche. Geprüft wurden vier Systeme.

Die Auswahl deckt damit beide Zeithorizonte ab. Rückblickend hilft die Mehrjahresbetrachtung: Weil der grösste Teil des Schweizer Bestands erst in den vergangenen Jahren gebaut wurde, bilden die Marktanteile dieser Jahre den installierten Bestand näherungsweise ab. Vorausblickend prägt das, was heute installiert wird, das Risiko über mehr als ein Jahrzehnt.

4.3 Beschaffung

Die Geräte wurden über Partnerorganisationen und auf demselben Weg beschafft, wie ihn auch eine reguläre Kundschaft nutzen würde. Dieses Vorgehen stellt sicher, dass reale Auslieferungszustände und Konfigurationen geprüft wurden und nicht eigens vorbereitete Prüfmuster. Kontakt zu den Herstellern gab es ausschliesslich im Rahmen der Schwachstellenmeldung.

Die Überprüfung erfolgte auf Initiative des NTC. Konzeption, Durchführung und Auswertung lagen vollständig beim NTC und fanden im eigenen Labor statt. Finanziert wurde sie zu einem wesentlichen Teil aus Mitteln des NTC, ergänzt durch mehrere Partnerorganisationen aus dem Energiesektor, die sich an den Kosten beteiligten und Testgeräte beisteuerten. Hersteller waren daran nicht beteiligt und die Partnerorganisationen hatten keinen Einfluss auf den Prüfumfang und die Ergebnisse.

4.4 Testaufbau

Für den Betrieb der Wechselrichter ist eine eingangsseitige Gleichstromversorgung nötig. Da der Betrieb echter Solarmodule im Labor nicht praktikabel ist, wurden die Module durch eine steuerbare Gleichstromquelle ersetzt. So liessen sich die Geräte unter reproduzierbaren Bedingungen prüfen. Der Schwerpunkt lag auf der Analyse von Firmware, Schnittstellen, Cloud-Anbindung und Konfiguration. Ein grundsätzlicher Vorbehalt bleibt: Ein Gerät könnte sein Verhalten ändern, sobald es erkennt, dass es geprüft wird. Ein solcher Prüfstandsmodus wäre mit einem laborgestützten Ansatz nicht zwingend erkennbar. Das NTC ist sich dieser Möglichkeit

[21] Pronovo AG, Statistiken: https://pronovo.ch/de/services/berichte/
[22] Bundesamt für Energie, «Statistik Sonnenenergie 2025»: https://pubdb.bfe.admin.ch/de/sammlungen/statistik-sonnenenergie

bewusst und hat ihr entgegengewirkt, soweit das machbar war: Die Geräte wurden über reguläre Vertriebswege bezogen und im Auslieferungszustand betrieben, und der Prüfaufbau wurde so gestaltet, dass er sich möglichst wenig von einer realen Installation unterscheidet.

4.5 Fokus auf skalierende Schwachstellen

Im Mittelpunkt der Analyse standen Schwachstellen, mit denen sich eine grosse Zahl von Anlagen zugleich manipulieren lässt. Schwachstellen, die nur die Einzelanlage betreffen, etwa solche, die physischen Zugang zum Gerät voraussetzen, waren nicht der Schwerpunkt. Diese Unterscheidung zwischen skalierenden und nicht-skalierenden Schwachstellen zieht sich durch den gesamten Bericht und bestimmt, wie die einzelnen Befunde gewichtet werden.

4.6 Schwachstellen-Meldeprozess

Alle identifizierten Schwachstellen wurden den betroffenen Herstellern im Rahmen eines koordinierten Offenlegungsverfahrens (Responsible Disclosure) vertraulich gemeldet, um deren Behebung vor der Veröffentlichung zu ermöglichen. Dieses Vorgehen entspricht der Responsible-Disclosure-Policy[23] des NTC und der gängigen Praxis in der Branche. Der vorliegende öffentliche Bericht verzichtet daher bewusst auf technische Details und die Nennung betroffener Produkte und stellt stattdessen die zugrunde liegenden Risikomuster dar.

[23] NTC Vulnerability Disclosure Policy: https://www.ntc.swiss/hubfs/ntc-vulnerability-disclosure-policy.pdf

5 Befunde und Risiken

5.1 Überblick

Das NTC hat elf Produkte untersucht: sieben Wechselrichter von sechs Herstellern und vier Energiemanagementsysteme. Zwei der Energiemanagementsysteme stammen von Herstellern, die auch einen der geprüften Wechselrichter herstellen, sodass sich die elf Produkte auf acht Hersteller verteilen. Insgesamt wurden über 50 Schwachstellen identifiziert, davon sieben mit der Kritikalität «kritisch» und sechs mit «hoch». Mindestens ein hoher oder kritischer Befund entfiel auf fünf der elf Produkte.

Bei vier Produkten erlangte das NTC die vollständige Kontrolle über das Gerät, also die höchste Rechtestufe (Root-Zugriff). Bei einem Produkt führten dorthin drei Schwachstellen, die das Ausführen von beliebigem Programmcode auf dem Gerät erlauben (Remote Code Execution) und alle als kritisch eingestuft sind. Bei drei Produkten genügte dafür ein unzureichend geschützter Wartungszugang des Herstellers. Diese Rechtestufe ist deshalb bedeutsam, weil sie nicht nur das Steuern der Anlage erlaubt, sondern das Verändern der Firmware und damit des Geräteverhaltens insgesamt.

Sechs der über 50 Befunde wirken über eine zentrale Instanz auf viele Anlagen zugleich und skalieren damit. Die übrigen bleiben auf die Einzelanlage beschränkt. Diese sechs sind der für die Netzstabilität entscheidende Teil der Statistik, denn netzrelevant wird eine Schwachstelle nicht durch ihre technische Schwere, sondern dadurch, dass sie sich auf eine ganze Geräteflotte anwenden lässt. Auch das BSI nennt in seinem Hinweis[24] vom Juni 2026 die «Nutzung von Skalierungseffekten» ausdrücklich als Weg von der Einzelanlage zur Netzstabilität. Zwei der sechs Befunde sind als «kritisch» eingestuft, einer als «hoch» und drei als «mittel». Diese Einstufung bewertet die Auswirkung auf das geprüfte Produkt und nicht die Folgen für das Stromnetz. Ein als «mittel» eingestufter Befund in einer Cloud, die eine Geräteflotte steuert, kann netzseitig schwerer wiegen als ein kritischer Befund am einzelnen Gerät. Fünf der sechs Befunde stammen aus der Ebene mit der grössten Hebelwirkung, der Herstellercloud, und zwar aus von aussen erreichbaren Schnittstellen. Eine vertiefte Prüfung der Cloud selbst war aus rechtlichen Gründen nicht möglich (vgl. Kapitel *4.1*). Bereits die Aussensicht genügte jedoch, um Schwachstellen mit netzweiter Reichweite zu finden.

Bei einem Teil der Befunde, darunter mehrere der kritischen, ist das koordinierte Offenlegungsverfahren zum Zeitpunkt der Veröffentlichung noch nicht abgeschlossen. Das liegt in der Sache und nicht an mangelnder Kooperation: Betroffen sind teils mehrere Modellreihen weltweit, die eine neue Firmware benötigen.

Das Sicherheitsniveau der einzelnen Produkte ist dabei generell nicht schlechter als bei anderen weitverbreiteten Geräten des «Internet of Things» (IoT), in einzelnen Aspekten sogar besser. Diese Einordnung stützt sich auf die Prüferfahrung des NTC mit vergleichbaren Geräteklassen, namentlich aus den Überprüfungen von Peripheriegeräten[25] und von Produkten im Anwendungsbereich der RED-Richtlinie[26]. Ernst zu nehmen sind jedoch die wiederkehrenden Muster und vor allem die strukturellen Risiken, die das Gesamtbild dominieren und in diesem Kapitel im Mittelpunkt stehen. Genau darin liegt der Kern: Was bei vernetzten Haushaltsgeräten ein Ärgernis bleibt, betrifft hier eine Geräteklasse, die in ihrer Summe systemrelevant ist.

Dass diese Schwächen nicht nur im Labor bestehen, bestätigen deutsche Sicherheitsbehörden: Sie beobachten Photovoltaikanlagen, bei denen ein Zugriff teilweise ohne Zugangsdaten möglich ist und deren Softwarestände stark veraltet sind (vgl. Kapitel *2.5*).

---

[24] Bundesamt für Verfassungsschutz (BfV) und Bundesamt für Sicherheit in der Informationstechnik (BSI), «Gemeinsamer Sicherheitshinweis: Auskundschaftung schlecht geschützter PV-Anlagen durch staatliche Cyberakteure», 3. Juni 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html

[25] NTC, Summarischer Bericht zur Cybersicherheit von Peripheriegeräten: https://www.ntc.swiss/aktuelles/2026-bericht-peripheriegeraete

[26] NTC, Bericht zur Cybersicherheit vernetzter Geräte hinsichtlich RED-Richtlinie: https://www.ntc.swiss/aktuelles/2025-bericht-red

5.2 Zwei Perspektiven auf die Bedrohung

Die Befunde sind vor dem Hintergrund zweier grundsätzlich verschiedener Bedrohungsperspektiven zu lesen:

- **Die Angreifbarkeit durch Dritte**: technische Schwachstellen, die ein externer Angreifer ausnutzt. Sie tritt bei allen Herstellern auf und lässt sich durch bessere Produktqualität und unabhängige Prüfungen verringern.
- **Der Hersteller oder seine Lieferkette als Angreifer:** Hier geht es nicht um technische Schwachstellen, sondern um Abhängigkeiten. Die legitimen Mittel der Fernwartung und der Firmware-Verteilung können vom Hersteller selbst missbraucht werden, von einem Angreifer, der den Hersteller kompromittiert, von böswilligen Mitarbeitenden oder aufgrund staatlicher Anordnung gegenüber dem Hersteller. Dieses Risiko ist herstellerspezifisch und lässt sich nicht durch technische Sicherheitsvorkehrungen beheben. Verringern lässt es sich nur, indem die Abhängigkeit selbst kleiner wird: durch nachprüfbare Zusicherungen statt blossem Vertrauen, durch Diversifizierung und durch technische Begrenzung dessen, was aus der Ferne überhaupt möglich ist (vgl. Kapitel 7.6).

Beide Perspektiven ziehen sich durch die folgenden Befunde. Diese Unterscheidung ist nicht ungewöhnlich. Das deutsche BSI führt in seinem Positionspapier[27] zur Cybersicherheit im Energiesektor unter den neuen Angriffsvektoren ausdrücklich die «Manipulation von Energieinfrastruktur durch Hersteller oder Dritte» auf und nennt dabei Wechselrichter als Beispiel.

5.3 Ergebnisse der technischen Überprüfung

5.3.1 Herstellerclouds

Für skalierende Angriffe ist die Cloud-Ebene am gewichtigsten. Eine Cloud verwaltet eine ganze Geräteflotte, weshalb eine einzelne Schwachstelle dort potenziell eine grosse Zahl von Anlagen betrifft, anders als eine Lücke am einzelnen Gerät.

Gerade diese Ebene liess sich jedoch nur eingeschränkt prüfen. Tests an einer Herstellercloud greifen auf ein fremdes, produktiv betriebenes System zu und sind ohne Einwilligung des Betreibers nach Art. 143bis StGB nur mit Einschränkungen zulässig[28]. Eine solche Einwilligung einzuholen hätte bedeutet, die Hersteller in die Untersuchung einzubeziehen, was dem Grundsatz der Unabhängigkeit widersprochen hätte. Die Prüfung beschränkte sich deshalb auf den ohne Einwilligung zulässigen Rahmen. Umso bemerkenswerter ist das Ergebnis: Bereits in diesem engen Rahmen wurden bei mehreren Herstellerclouds Schwachstellen gefunden, unter anderem solche der Kategorien SQL-Injection und Cross-Site-Scripting. Die Hersteller haben sie nach der Meldung behoben.

Darin zeigt sich zugleich ein strukturelles Problem: Die Ebene mit der grössten Hebelwirkung ist ausgerechnet diejenige, die unabhängige Prüfstellen ohne Mitwirkung des Herstellers nicht vollständig untersuchen können.

Ein Befund aus dieser Prüfung ist in mehrfacher Hinsicht aufschlussreich. Eine als kritisch eingestufte Schwachstelle betraf das Energiemanagementsystem des Schweizer Herstellers Solar Manager. Sie hätte einem Angreifer aus der Ferne den Zugriff auf einzelne Systeme erlaubt, allerdings nicht nur auf eines, sondern nacheinander auf weitere Systeme. Der Hersteller reagierte vorbildlich und schloss die Lücke innerhalb weniger Stunden. Darüber hinaus erteilte er dem NTC die Einwilligung, auch seine Cloud zu prüfen. Damit entfiel die weiter oben beschriebene rechtliche Schranke, die eine Prüfung der Cloud-Ebene sonst erschwert. Der Fall zeigt, dass sich diese Schranke auflösen lässt, wenn ein Hersteller Transparenz als Chance versteht. Anders als sonst nennen wir den Hersteller hier namentlich, mit seinem Einverständnis und als positives Beispiel

[27] Bundesamt für Sicherheit in der Informationstechnik (BSI), «Positionspapier: Cybersicherheit im Energiesektor Deutschlands»: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Positionspapier_Cybersicherheit_Energiesektor.html

[28] Walder Wyss AG, «Rechtsgutachten zur Strafbarkeit von Ethical Hacking»: https://www.walderwyss.com/de/news/2023-06-26_rechtsgutachten-zur-strafbarkeit-von-fuer-das-nationale-testinstitut-fuer-cybersicherheit-ntc

beim Umgang mit dieser Schwachstellenmeldung.

Aufschlussreich ist der Fall auch aus einem zweiten Grund. Solar Manager ist vor allem in der DACH-Region verbreitet, mit schätzungsweise 50'000 Installationen. Produkte mit einer solchen regionalen Verbreitung kommen in internationalen Untersuchungen, die meist aus den USA oder von global tätigen Sicherheitsfirmen stammen, in der Regel nicht vor. Sie fallen durch das Raster, obwohl sie hierzulande zehntausende Anlagen steuern. Diese Lücke lässt sich nur durch Prüfungen schliessen, die am tatsächlichen Schweizer Markt ansetzen.

Wie gross die Hebelwirkung einer einzigen Cloud sein kann und wie schwierig sich die Behebung gestalten kann, zeigt ein international dokumentierter Fall[29]. Das Dutch Institute for Vulnerability Disclosure (DIVD), das ähnlich wie das NTC Schwachstellen sucht und meldet, stiess bei der Monitoring-Plattform Solarman auf Zugangsdaten für ein Administrationskonto, die offen in einem öffentlichen Software-Verzeichnis (GitHub) lagen und nicht durch eine zweite Sicherheitsstufe (Mehrfaktor-Authentisierung) geschützt waren. Über dieses eine Konto liessen sich weltweit fast eine Million Anlagen mit zusammen über 10 GW Leistung einsehen und steuern, bis hin zum Auslesen und Überschreiben der Firmware. Bezeichnend war der Umgang damit: Der Betreiber reagierte monatelang nicht, das exponierte Passwort wurde nach einer ersten Korrektur sogar wieder auf den offengelegten Wert zurückgesetzt, und eine Lösung gelang erst über diplomatische Kanäle und die Einbindung des chinesischen CERT. Der Fall steht damit für zwei Muster zugleich: die enorme Reichweite einer zentralen Cloud und die in der Praxis manchmal schwierige Zusammenarbeit mit Herstellern bei der Behebung. In den Niederlanden führte er in der Folge zu parlamentarischen Anfragen und verstärkter behördlicher Aufmerksamkeit für die Cybersicherheit von Wechselrichtern. Dass es sich nicht um einen einmaligen Ausreisser handelte, zeigt eine spätere, deutlich grössere Offenlegung[30]: 2024 fand die Sicherheitsfirma Bitdefender in denselben Solarman- und Deye-Plattformen neue Schwachstellen, die nach Medienberichten theoretisch eine noch grössere Flotte betroffen hätten (rund 195 GW Leistung über mehr als zwei Millionen Anlagen).

5.3.2 Lokale Schnittstellen und Herstellerzugänge

Die übrigen Befunde verteilen sich auf wiederkehrende Klassen. Am häufigsten, und über viele der geprüften Geräte hinweg, traten Mängel bei Authentifizierung und Zugriffskontrolle auf (etwa fehlender Sitzungsablauf sowie fehlende oder unveränderte Standardpasswörter), dazu eine fehlende oder schwache Verschlüsselung lokaler Schnittstellen. Weitere Befunde betrafen nicht deaktivierbare Schnittstellen (etwa einen nicht abschaltbaren WLAN-Hotspot) sowie unsichere Hersteller-Wartungszugänge über einen Fernzugang (SSH, teils mit flottenweit identischen Zugangsdaten).

Dass es sich nicht um Einzelfälle handelt, bestätigen unabhängige Untersuchungen. Forescout dokumentierte in der Studie SUN:DOWN[31] vergleichbare Schwächen bei mehreren Marktführern (unter anderem unsichere Cloud-Schnittstellen, fest im Gerät hinterlegte, unveränderbare Zugangsdaten sowie Firmware-Aktualisierungen ohne kryptografische Signatur). Der auf Cybersicherheit im Energiesektor spezialisierte Forscher Ruben Santamarta beschreibt[32] unsichere Fernwartungszugänge bei europäischen Herstellern.

Wie wenig solche Wartungszugänge mitunter geschützt sind, zeigt ein Befund besonders deutlich. Bei einem Gerät liess sich über den geräteeigenen WLAN-Zugangspunkt das Passwort des Installateur-Kontos ohne jede Anmeldung zurücksetzen und neu vergeben. Mit den so erlangten administrativen Rechten liess sich anschliessend der Fernzugang (SSH) und Root-Zugriff aktivieren. Dieser ist im Auslieferungszustand mit einem Standardpasswort geschützt, das bei der ersten Anmeldung geändert werden muss. Im Normalbetrieb bleibt der Zugang jedoch ungenutzt,

[29] Dutch Institute for Vulnerability Disclosure (DIVD), Fall «Solarman» (DIVD-2022-00009): https://csirt.divd.nl/cases/DIVD-2022-00009/
[30] Bitdefender, Untersuchung zu Schwachstellen in den Plattformen Solarman und Deye, August 2024: https://blogapp.bitdefender.com/labs/content/files/2024/08/Bitdefender-PReport-solarman-creat7907.pdf
[31] Forescout (dos Santos et al.), «SUN:DOWN» : https://www.forescout.com/research-labs/sun-down-a-dark-side-to-solar-energy-grids/
[32] Santamarta, «Cyber-Physical Attacks on Solar Inverters», Mai 2026: https://www.reversemode.com/2026/05/a-practical-analysis-of-cyber-physical.html

und damit bleibt auch das Standardpasswort in Kraft. Wer sich als Erster anmeldet, vergibt das neue Passwort selbst. Für die vollständige Kompromittierung genügte Zugriff auf das geräteeigene WLAN.

Aufschlussreich ist die Verkettung: Drei Schutzmechanismen sind vorhanden: eine Kontoanmeldung, ein abschaltbarer Fernzugang und ein Passwortwechsel bei der Erstanmeldung. Keiner greift, weil der erste ohne Authentisierung umgangen werden kann und der dritte erst wirkt, wenn sich jemand anmeldet, was nicht vorausgesetzt werden kann.

Andere Schwachstellen traten erst durch die Analyse der Gerätefirmware zutage. Bei einem Produkt fanden sich Dienste, die mit den höchsten Rechten laufen und Eingaben bereits verarbeiten, bevor eine Anmeldung erfolgt ist. In einem Fall war in der ausgelieferten Firmware noch ein Debug-Dienst aktiv, der einen Parameter einer Netzwerkanfrage ungeprüft in einen Speicherbereich fester Grösse übernimmt (Buffer-Overflow). Weil dieser Dienst mit den höchsten Rechten läuft, lässt sich über einen solchen Überlauf eigener Programmcode einbringen und ausführen. Ohne Zugangsdaten und mit blossem Zugang zum lokalen Netzwerk war damit die vollständige Kontrolle über das Gerät erreichbar (Root-Zugriff). Dabei ist bemerkenswert, dass der Dienst im Betrieb nicht benötigt wird, und er in der ausgelieferten Firmware dennoch erreichbar war. Genau darauf zielt der Grundsatz, den die in Kapitel *8.4.2 Werkseitige Steuerungssperre für netzrelevante Funktionen* zitierten Leitlinien formulieren: Was nicht in jeder Einsatzart gebraucht wird, sollte ab Werk deaktiviert sein.

Besonders folgenreich ist die lokale Steuerschnittstelle. Über sie lassen sich bei nahezu allen geprüften Wechselrichtern nicht nur Messwerte auslesen, sondern auch die netzrelevanten Einstellungen des Geräts verändern, und das oft ohne Authentifikation. Technisch geschieht dies über das Industrieprotokoll Modbus. Ob der Hersteller dafür die standardisierten SunSpec-Registermodelle oder ein eigenes Schema verwendet, ändert daran nichts: SunSpec[33] beschreibt nur die Bedeutung der Register und ist keine Sicherheitsschicht. Diese Schnittstelle ist bei mehreren Herstellern werkseitig deaktiviert. Für den Betrieb mit einem Energiemanagementsystem muss sie jedoch aktiviert werden. Ist sie aktiv, erfolgt der Zugriff ohne jede Anmeldung, sodass jedes Gerät im selben Netzwerk Befehle senden kann. Zwischen Energiemanagementsystem und Wechselrichter besteht damit sehr häufig keine Sicherheit.

Allen in diesem Abschnitt beschriebenen Befunden ist gemeinsam, dass sie Zugang zum lokalen Netzwerk voraussetzen. Sie erlauben die vollständige Kontrolle über ein einzelnes Gerät, nicht über viele.

5.3.3 Vom lokalen zum skalierenden Angriff

Lokale Schwachstellen betreffen für sich genommen nur die Einzelanlage und skalieren nicht. Eine Überlegung relativiert diese Entwarnung: Ein Angreifer, der sich bereits im lokalen Netz befindet, kann Wechselrichter über das ungeschützte Modbus TCP steuern. Dort ist die Wirkung konstruktionsbedingt sogar ohne Schwachstelle erreichbar. In das lokale Netz gelangt ein Angreifer etwa über befallene IoT-Geräte. Dass Heimgeräte in grossem Stil kompromittiert werden, zeigen sowohl klassische Botnetze aus infizierten Computern und IoT-Geräten (etwa vom Typ Mirai) als auch der rasche Anstieg sogenannter Residential Proxy Networks, bei denen gekaperte Heimanschlüsse als Zugangsknoten weitervermietet werden.[34] Auch der NDB beschreibt Anonymisierungsnetzwerke aus schlecht geschützten, internetexponierten Heimgeräten wie Routern, teils über in der Schweiz gemietete Infrastruktur.[35] Werden viele Heimnetze auf diese Weise kompromittiert, wird aus einem lokalen ein breit wirksamer Vektor.

[33] SunSpec Alliance, «Modbus»-Spezifikation: https://sunspec.org/modbus/
[34] BSI, Bericht zu Residential-Proxy-Missbrauch, «Steckbriefe aktueller Botnetze: Mirai», 2026: https://www.bsi.bund.de/dok/12820010
[35] Nachrichtendienst des Bundes (NDB), «Sicherheit Schweiz 2026»: https://www.vbs.admin.ch/de/newnsb/jyRmuld1hBVy

5.3.4 Was nicht untersucht wurde: dauerhafte Beschädigung von Geräten

Nicht Gegenstand der eigenen Untersuchung war die Möglichkeit, Geräte durch den Betrieb in bestimmten Zuständen dauerhaft zu beschädigen. Dass dies keine rein hypothetische Gefahr ist, zeigt der Hoymiles-Fall. Forschende des Chaos Computer Club demonstrierten 2026, dass sich Mikrowechselrichter über das ungeschützte Funkprotokoll durch das Einspielen manipulierter Firmware dauerhaft unbrauchbar machen lassen.[36] Das NTC erlangte bei vier Geräten die vollständige Kontrolle über das Gerät (Root-Zugriff, die höchste Rechtestufe), hat eine dauerhafte Beschädigung jedoch nicht getestet. Zudem können weitere Schutzmechanismen zum Beispiel auf Elektronik-Ebene greifen. Ein solcher Angriff hätte, anders als eine vorübergehende Netzstörung, langfristige Folgen.

5.3.5 Was nicht gefunden wurde

Ebenso bedeutsam wie die identifizierten Schwachstellen ist, was nicht festgestellt wurde. Es fanden sich keine Hinweise auf absichtlich eingebaute Hintertüren oder versteckte, undokumentierte Kommunikationskomponenten, wie sie in der internationalen Berichterstattung diskutiert werden.[37] In einem Gerät wurde zwar zunächst ein Mikrofon entdeckt, was Anlass zur Abklärung gab. Die Analyse ergab jedoch eine dokumentierte Bedienfunktion (Interaktion über Klopfzeichen) und keinen Hinweis auf eine verdeckte Funktion. Erledigt ist der Fall damit aber nicht: Das Bauteil kann mehr erfassen, als die Bedienung erfordert, und liesse sich nach einem Firmware-Update womöglich missbrauchen. Da dieselbe Funktion auch ohne ein Mikrofon möglich wäre, ist diese Wahl als Schwachstelle zu werten, ganz ohne böswillige Absicht. Genau das ist das Muster des Berichts: die festgestellten Risiken sind struktureller Natur und erfordern keine Annahme böswilliger Absicht, um ernst zu sein.

5.4 Strukturelle Risiken

Die eigentliche Botschaft dieses Berichts liegt nicht in den Einzelbefunden, sondern in fünf strukturellen Risiken, die unabhängig von der Qualität einzelner Produkte bestehen.

5.4.1 Abhängigkeit von der Herstellercloud

Die im Kapitel «Das Ökosystem einer Photovoltaik-Anlage» beschriebene zentrale Steuerbarkeit ist funktional gewollt, verlagert aber die Kontrolle über eine grosse Zahl von Anlagen an einen einzelnen Punkt. Daraus ergibt sich ein Risiko bei Fehlfunktionen oder Kompromittierung des Herstellers, im Extremfall auch die mögliche Nutzung als geopolitisches Druckmittel. Verstärkt wird die Abhängigkeit dadurch, dass viele Geräte dauerhaft mit der Cloud verbunden sind, teils gefördert durch Anreize wie verlängerte Garantien. Zur selben Ebene gehört der Firmware-Update-Kanal: Er ist notwendig, wirkt aber ebenfalls gleichzeitig auf die gesamte Flotte, und was über ihn verteilt wird, verändert das Gerät tiefgreifend.

Dass dieser Kanal real ausgenutzt wird, zeigte der Angriff auf das Satellitennetzwerk KA-SAT vom Februar 2022. Die Angreifer gelangten auf den Server, über den Software-Updates an die Modems verteilt werden, und spielten darüber eine Schadsoftware aus, die den Speicher der Geräte überschrieb. Betroffen war unter anderem die Fernüberwachung von 5'800 Windenergieanlagen des Herstellers Enercon mit zusammen 11 Gigawatt. Die Anlagen speisten weiter ein, liessen sich aber nicht mehr aus der Ferne überwachen oder zurücksetzen. Der Angriff galt der Ukraine, die deutschen Anlagen waren Kollateralschaden, also genau jenes Szenario, das der NDB für die Schweiz ebenfalls für möglich hält (vgl. Kapitel *2.5*).[38]

---

[36] Chaos Computer Club (B. Heinz «Hunz»), «Analyse der Funk- und Firmware-Schwachstellen von Hoymiles-Wechselrichtern», 2026: https://www.ccc.de/updates/2026/blinkenlights-hoymiles
[37] Reuters, Berichterstattung zu undokumentierten Kommunikationsmodulen, Mai 2025: https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/
[38] SentinelOne: «AcidRain – A Modem Wiper Rains Down on Europe», 31. März 2022: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/

5.4.2 Privilegierter Fernwartungszugang

Unabhängig von der Cloud behalten die meisten Hersteller einen privilegierten Zugang zu ihrer Geräteflotte, etwa über Wartungskonten oder Fernzugänge. Das ist kein Einzelfehler, sondern ein Konstruktionsprinzip: Ein einziges kompromittiertes oder rekonstruierbares Zugangsverfahren betrifft potenziell die gesamte Flotte, und ein solcher Zugang lässt sich nicht wie eine gewöhnliche Schwachstelle beheben. Betroffen sind auch Grossanlagen, die nicht an eine Herstellercloud angebunden sind, aber über eigene, aus der Ferne erreichbare Steuer- und Wartungsschnittstellen verfügen. Wie real diese Möglichkeit ist, zeigte im November 2024 der Fall der Deye-Wechselrichter: Der Hersteller schaltete im Rahmen eines Vertriebsstreits zahlreiche eigene, nicht autorisiert vertriebene Geräte in mehreren Ländern gezielt ab, ganz ohne Schwachstelle.[39]

Dasselbe Muster reicht über den Hersteller hinaus: Auch Installationsbetriebe, Serviceanbieter und Aggregatoren haben häufig Fernzugang zu sämtlichen von ihnen betreuten Anlagen, ohne dass für sie Cybersicherheitsvorgaben gelten. Wie weit das reicht, zeigte im April 2022 ein gezielter Angriff auf den Bremer Wartungsdienstleister Deutsche Windtechnik, der über 7'600 Windenergieanlagen betreut: Das Unternehmen schaltete daraufhin sämtliche Verbindungen der Datenfernüberwachung ab, sodass für ein bis zwei Tage keine Fernüberwachung mehr möglich war. Die Anlagen selbst waren nicht betroffen.[40] Angegriffen wurde weder ein Hersteller noch ein Betreiber, sondern der Dienstleister dazwischen.

5.4.3 Unsichere lokale Steuerprotokolle als Konstruktionsmerkmal

Die lokale Steuerung vieler Wechselrichter beruht auf verbreiteten Industrieprotokollen, die keine Authentisierung vorsehen. Das ist kein Fehler einzelner Geräte, sondern der Standard einer ganzen Gerätekategorie. Verschärft wird er durch die Verlagerung dieser Steuerung von physisch zugangsbeschränkten Verbindungen (RS485) auf vernetzte Schnittstellen (Ethernet, WLAN), weil damit jedes Gerät im selben Netz zum möglichen Absender von Steuerbefehlen wird.

5.4.4 Marktkonzentration als Klumpenrisiko

Die im Kapitel «Das Ökosystem einer Photovoltaik-Anlage» beschriebene Konzentration wirkt sicherheitstechnisch als «Single Point of Failure»: Je grösser der Anteil eines Herstellers, desto mehr Geräte erreicht ein einzelner Befund. Wie konkret dieses Risiko ist, zeigt eine Einschätzung der niederländischen Cybersicherheitsfirma Secura: In den Niederlanden haben zwei Hersteller (Huawei und Sungrow) je für sich einen so grossen Marktanteil, dass ein Angriff auf die Systeme eines einzigen von ihnen genügen würde, um die für eine Netzwirkung nötige Grössenordnung zu erreichen. Europaweit kämen laut Secura mehrere Hersteller über diese Schwelle.[41]

5.4.5 Standort und Herkunft als Scheinsicherheit

Verschiedene Hersteller werben damit, ihre Cloud werde in europäischen Rechenzentren betrieben und von europäischen Organisationen verwaltet. Der Hosting-Standort allein sagt jedoch wenig über die tatsächliche Kontrolle über das Gerät aus, unter anderem weil Firmware und Software vom Hersteller stammen und nicht am Hosting-Standort entwickelt werden. In den eigenen Tests bestätigte sich zwar, dass der beobachtete Datenverkehr an EU-Endpunkte ging. Eine ausschliesslich europäische Kontrolle oder Datenhaltung lässt sich daraus nicht ableiten. Ebenso wenig löst die Herkunft des Geräts das Problem: Auch Geräte europäischer Anbieter enthalten häufig Chips oder Software-Bausteine aus Drittstaaten oder werden dort gefertigt.

---

[39] Berichterstattung zu aus der Ferne abschaltbaren Deye-Wechselrichtern, 2024: https://www.heise.de/news/Photovoltaik-Deaktivierte-Deye-und-Sol-Ark-Wechselrichter-in-den-USA-10183706.html
[40] heise online, «Cyber-Angriff: Fernüberwachung von Windkraftanlagen lahmgelegt», 27. April 2022:, https://www.heise.de/news/Cyber-Angriff-legte-offenbar-Windturbinen-lahm-7066606.html
[41] Secura, «Cybersecurity threats and measures for the solar power sector», 2024: https://www.energy-innovation.nl/documents/1299/2024-Secura_Report-Cybersecurity_threats_and_measures_for_the_solar_power_sector.pdf

6 Auswirkung auf die Netzstabilität

6.1 Grundprinzip: das Gleichgewicht von Erzeugung und Verbrauch

Ein Wechselstromnetz muss dauerhaft nahe seiner Nennfrequenz (in Europa 50 Hz) betrieben werden. Dies setzt ein Echtzeit-Gleichgewicht zwischen Erzeugung und Verbrauch voraus. Weicht die Frequenz ab, greifen im europäischen Verbundnetz gestufte Reserven: eine primäre Reserve, die binnen Sekunden anspringt (rund 3'000 MW), sowie eine sekundäre und eine tertiäre Reserve mit längeren Vorlaufzeiten.[42] Ein plötzlicher Leistungssprung über den sogenannten Referenzstörfall von 3'000 MW hinaus kann von der primären Reserve allein nicht mehr aufgefangen werden. Bei 49 Hz erfolgt ein regulatorisch vorgeschriebener Lastabwurf.[43]

Ein erschwerender struktureller Faktor ist der Rückgang der Netzträgheit. Klassische Kraftwerke stabilisieren die Frequenz über die rotierenden Schwungmassen ihrer Generatoren, während wechselrichterbasierte Erzeugung diese Trägheit nicht von sich aus bereitstellt.[44] Moderne Wechselrichter sollen dies über netzbildende («grid-forming») Funktionen zunehmend ausgleichen. Dieser Aspekt wird weiter unten bei den relativierenden Faktoren aufgegriffen.

6.2 Reale Evidenz: das Netz kann auch ohne Cyberangriff kippen

Wie fragil ein System bei hoher wechselrichterbasierter Erzeugung sein kann, zeigte der iberische Blackout vom 28. April 2025, und zwar ohne böswillige Beteiligung. Zeitweise stammte ein sehr hoher Anteil des Stroms aus erneuerbaren Quellen. Eine Kette von Problemen bei Spannung und Blindleistung, einer netzstützenden Grösse, die die Spannung im Netz mitbestimmt und weiter unten beim Wirkebenen-Typ B genauer erklärt wird, führte zu rasch steigender Spannung, kaskadierenden Abschaltungen von Erzeugung und schliesslich zum vollständigen Systemkollaps in Spanien und Portugal. Für die Verhältnismässigkeit wichtig ist die Ursacheneinordnung von ENTSO-E, dem Verband der europäischen Übertragungsnetzbetreiber: Nicht ein «Zuviel» an erneuerbarer Erzeugung war ausschlaggebend, sondern Lücken in der Spannungs- und Blindleistungsregelung.[45]

Dass viele gleichartig konfigurierte Anlagen gleichzeitig reagieren, ist kein Gedankenexperiment. In Deutschland schrieb eine Richtlinie von 2005 vor, dass sich Photovoltaikanlagen bei einer Netzfrequenz von 50,2 Hz unverzüglich vom Netz trennen. Mit dem Ausbau wurde daraus ein Systemrisiko: Bei Erreichen dieser Frequenz hätten sich schlagartig Anlagen mit mehreren Gigawatt Leistung getrennt. Die Systemstabilitätsverordnung von 2012 verpflichtete die Netzbetreiber deshalb zur Nachrüstung von rund 300'000 bestehenden Anlagen mit etwa einer Million Wechselrichtern, damit die Trennung gestaffelt statt gleichzeitig erfolgt.[46]

6.3 Drei Angriffstypen eines kompromittierten Wechselrichters

Die verbreitete Vorstellung, ein Angriff bestehe im massenhaften «An- und Abschalten», greift zu kurz. Der Sicherheitsforscher Ruben Santamarta unterscheidet drei Typen cyber-physischer Angriffe mit zunehmender Komplexität.[47]

---

[42] Goerke et al., Karlsruher Institut für Technologie, «Who Controls Your Power Grid? On the Impact of Misdirected Distributed Energy Resources on Grid Stability», 2024: https://publikationen.bibliothek.kit.edu/1000173186
[43] Verordnung (EU) 2017/2196 der Kommission vom 24. November 2017 zur Festlegung eines Netzkodex über den Notzustand und den Netzwiederaufbau des Übertragungsnetzes, Artikel 15 (automatischer Unterfrequenzlastabwurf) und Anhang: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32017R2196
[44] ENTSO-E: «Frequency stability in long-term scenarios», Untersuchung zum Rückgang der Systemträgheit im Synchrongebiet Kontinentaleuropa, Dezember 2021: https://www.entsoe.eu/news/2021/12/06/entso-e-assesses-the-impact-of-reduction-of-inertia-on-frequency-stability-in-long-term-scenarios/
[45] ENTSO-E, «Expert Panel Final Report on 28 April 2025 Blackout in Spain and Portugal»: https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/
[46] BDEW: 50,2-Hertz-Problem: https://www.bdew.de/energie/systemstabilitaetsverordnung/502-hertz-problem/
[47] Santamarta, «Cyber-Physical Attacks on Solar Inverters», Mai 2026: https://www.reversemode.com/2026/05/a-practical-analysis-of-cyber-physical.html

6.3.1 Typ A: Wirkleistung und Frequenz (Zu- und Abschalten)

Durch abgestimmtes Trennen oder Zuschalten vieler Anlagen wird das Gleichgewicht zwischen Erzeugung und Verbrauch gestört und die Frequenz verschoben. Erreichen lässt sich das über direkte Trennbefehle, über die Manipulation der Schutzfunktion, die eine Anlage bei einem Netzausfall automatisch vom Netz trennt (Anti-Islanding), oder über veränderte Vorgaben dazu, bei welcher Spannung eine Anlage am Netz bleiben oder sich trennen soll (die sogenannten Durchfahr-Kurven HVRT und LVRT, «High/Low Voltage Ride-Through»). Besonders wirksam ist ein Angriff, der die Manipulation im Takt der netzeigenen Ausregelung wiederholt und die Schwingung so aufschaukelt, ähnlich wie beim Anstossen einer Schaukel im richtigen Rhythmus.

Dass Gleichzeitigkeit auch ohne Angriff netzwirksam ist, zeigt ein Phänomen aus dem Marktbetrieb. Passen viele Anlagen ihre Einspeisung beim Wechsel des Marktintervalls sprunghaft an, entstehen Frequenzabweichungen jeweils zum Stunden- oder Viertelstundenwechsel, bekannt als «deterministic frequency deviations». Swissgrid will deshalb vorschreiben, dass auch Photovoltaikanlagen solche geplanten Änderungen über eine Rampe fahren. Ein Angreifer, der viele Anlagen gleichzeitig schaltet, nutzt denselben Effekt, nur absichtlich und ohne Rampe.[48]

6.3.2 Typ B: Blindleistung und Spannung

Dies ist nach Santamartas Einschätzung der wirksamste Weg zu örtlichen Ausfällen. Wechselrichter stützen das Netz nicht nur mit Wirkleistung, sondern auch mit Blindleistung, die die Spannung im Netz mitbestimmt. Wie ein Wechselrichter reagieren soll, legen Kennlinien fest, etwa die Volt-Var-Kurve: Steigt die Spannung, nimmt der Wechselrichter Blindleistung auf und senkt die Spannung wieder. Das stabilisiert das Netz. Ein Angriff kehrt diese Reaktion um. Eine manipulierte Kennlinie zwingt den Wechselrichter, bei bereits hoher Spannung zusätzlich Blindleistung einzuspeisen und die Spannung so weiter hochzutreiben. Schon wenige Anlagen können die örtliche Spannung damit über die zulässigen Grenzen treiben, worauf Schutzeinrichtungen benachbarter Anlagen und Umspannwerke abschalten und eine Kaskade anstossen können. Zur Realitätsnähe: Über eine veränderte Steuerlogik, etwa nach einer Kompromittierung der Firmware, ist eine solche Umkehr plausibel. Der Angriff braucht weder komplexen Schadcode noch grosse Skala. Zum selben Schluss kommen Netzsimulationen, die DNV im Auftrag von SolarPower Europe mit den Netzmodellen von ENTSO-E durchgeführt hat:[49] Werden grosse Kapazitäten gleichzeitig zwischen induktiver und kapazitiver Blindleistung umgeschaltet, entstehen rasche Spannungssprünge, die Schutzeinrichtungen benachbarter Erzeugungsanlagen und Umspannwerke auslösen und eine Kaskade anstossen können. Die Untersuchung hält zugleich fest, dass unklar bleibt, wie schnell und wie weit die vorhandenen Mechanismen zur Spannungshaltung dem entgegenwirken würden.

6.3.3 Typ C: Umrichtergetriebene Instabilität (Oszillationen)

Das gezielte Anregen netzeigener Schwingungen bis hin zu erzwungenen Oszillationen ist der komplexeste Vektor. Er gilt, auch nach Santamartas eigener Einschätzung, als derzeit unrealistisch, insbesondere als koordinierter Angriff über eine Vielzahl kleiner, heterogener Heim-Wechselrichter. Als Phänomen ist er dennoch real. Beim iberischen Blackout regte eine erzwungene Schwingung aus einem einzelnen grossen Photovoltaik-Kraftwerk (nach der Analyse von Santamarta die Anlage Núñez de Balboa), nicht aus verteilten Kleinanlagen, eine überregionale Oszillation an.[50]

[48] Swissgrid AG, White Paper «Systemverträgliche Integration Photovoltaik», März 2026: https://www.swissgrid.ch/de/home/newsroom/blog/2026/20260330-01.html
[49] SolarPower Europe / DNV: «Solutions for PV Cyber Risks to Grid Stability», 2025: https://www.solarpowereurope.org/insights/thematic-reports/solutions-for-pv-cyber-risks-to-grid-stability
[50] ENTSO-E, «Expert Panel Final Report on 28 April 2025 Blackout in Spain and Portugal»: https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/

6.3.4 Einordnung: der gefährlichste Vektor ist nicht der aufwändigste

Überraschend ist dabei: Der gefährlichste Vektor ist nicht der aufwändigste. Gegenüber reinen Erzeugungsverlusten ist das Netz vergleichsweise robust. Der spannungsgetriebene Angriff über Blindleistung dagegen kommt mit kleiner Skala und geringer Komplexität aus, was die Bedrohung realer macht, wie der iberische Blackout auf genau dieser Ebene zeigt (vgl. Kapitel *6.2*).

6.4 Das Cyber-Szenario: koordinierte Last- und Erzeugungsmanipulation

Die Vorstellung, kompromittierte, mit dem Internet verbundene Geräte liessen sich zu einem netzwirksamen Verbund bündeln, ist in der Forschung seit rund einem Jahrzehnt etabliert (unter den Begriffen «load-altering» beziehungsweise MaDIoT, «Manipulation of Demand via IoT»). Die Arbeiten reichen von frühen Modellen über Dabrowski et al.[51] (2017) und Soltan et al.[52] (2018) bis zu Goerke et al.[53] (2024), die detailliert quantifizieren, wie viele Anlagen je Typ für eine Netzwirkung im europäischen Verbundnetz nötig wären. Die erste photovoltaikspezifische Ausformulierung dieser Grundidee stammt aus dem «Horus-Szenario»[54] von Willem Westerhof, das im August 2017 veröffentlicht wurde und auf einer Offenlegung an den Hersteller vom Dezember 2016 beruht.

Wechselrichter sind für solche Angriffe besonders geeignet, weil sie als Echtzeitsysteme die Netzfrequenz präzise verfolgen und einen Angriff dadurch sehr genau ausführen können.

Über die reine Netzdestabilisierung hinaus ist ein zweiter Schadenspfad zu nennen. Angreifer mit weitreichendem Zugriff können Geräte über eine bösartige Firmware dauerhaft ausser Betrieb setzen, sodass sie vor Ort ersetzt oder neu bespielt werden müssen. Denkbar ist auch eine Erpressung («Ransomware auf Wechselrichtern»). Solche destruktiven Wirkungen hätten deutlich längerfristige Folgen als eine vorübergehende Netzstörung.

6.5 Grössenordnung (illustrative Überschlagsrechnung)

Zur Einordnung, ausdrücklich nicht als eigenständige Blackout-Prognose, lässt sich die Grössenordnung aus der Literatur ableiten. Nach Dabrowski et al. genügt unter für einen Angreifer günstigen Bedingungen die Kontrolle über rund 4'500 MW, um die Frequenz im europäischen Verbundnetz unter die Lastabwurfschwelle von 49 Hz zu drücken, das Anderthalbfache des Referenzstörfalls. Der Wert gilt für einen Angriff, der die Leistung im Takt der Netzregelung moduliert und die Abweichung so aufschaukelt; ein einmaliger Leistungssprung müsste bei gleichen Netzbedingungen rund 6'000 MW umfassen. Die Schwelle bezeichnet ein Leistungsungleichgewicht, das sich von der Verbrauchs- wie von der Erzeugungsseite erreichen lässt: Dabrowski leitet sie von der Lastseite ab, Goerke et al. und dos Santos et al. übertragen sie auf die Photovoltaik. Für die Photovoltaik heisst das konkret ein sonniger Tag mit tiefer Last, etwa an einem Sommerwochenende oder Feiertag.

Zur Einordnung: 4'500 MW entsprechen knapp der Hälfte der in der Schweiz installierten 9,5 GW. Die Schwelle ist damit eine europäische und keine schweizerische. Im europäischen Massstab genügt umgekehrt ein kleiner Anteil: Gemessen am Ende 2025 in der EU installierten Bestand von rund 406 GW machen 4'500 MW gut ein Prozent aus, und auch die konservative Variante mit 6'000 MW bleibt unter zwei Prozent; dieser Anteil sinkt mit jedem weiteren Ausbaujahr.[55] Eine unabhängige Simulation kommt auf eine ähnliche Grössenordnung: DNV nennt für das europäische Netz eine gezielte Kompromittierung von 3 GW als Schwelle, ab der erhebliche

[51] Dabrowski, Ullrich, Weippl, «Grid Shock: Coordinated Load-Changing Attacks on Power Grids», 2017: https://dl.acm.org/doi/10.1145/3134600.3134639
[52] Soltan, Mittal, Poor, «BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid», 2018: https://www.usenix.org/conference/usenixsecurity18/presentation/soltan
[53] Goerke et al., Karlsruher Institut für Technologie, «Who Controls Your Power Grid? On the Impact of Misdirected Distributed Energy Resources on Grid Stability», 2024: https://publikationen.bibliothek.kit.edu/1000173186
[54] Westerhof, «Horus Scenario», 2017: https://horusscenario.com/
[55] SolarPower Europe, «EU Solar Market Outlook 2025-2030», Dezember 2025: https://www.solarpowereurope.org/insights/outlooks/eu-solar-market-outlook-2025-2030

Auswirkungen möglich sind.[56]

Für die Schweiz folgt daraus keine Beruhigung, sondern eine andere Frage: wie stark der Schweizer Bestand an einzelnen Steuerungspunkten gebündelt ist. Weil auf einen einzigen Hersteller gut die Hälfte des Marktanteils entfällt (vgl. Kapitel *3.6*), erreicht bereits eine einzige Herstellercloud einen erheblichen und wachsenden Teil des Schweizer Bestands. Eine ähnliche Bündelung entsteht durch Aggregatoren und virtuelle Kraftwerke (vgl. Kapitel *3.4*). Für einen europaweit koordinierten Angriff ist nicht die nationale Summe entscheidend, sondern die Zahl der Plattformen, über die sie erreichbar ist.

Eine belastbare, eigenständige Berechnung für das Schweizer Netz liegt ausserhalb des Untersuchungsumfangs. Belastbar bleibt die Kernaussage: Bereits ein Anteil von unter zwei Prozent des europäischen Wechselrichter-Bestands genügt rechnerisch, um relevante Netzeffekte auszulösen, wobei die konkrete Zahl stark von Geräteverteilung und Netzzustand abhängt. Der Blindleistungs-Vektor (Typ B) benötigt nach Santamarta deutlich weniger kontrollierte Leistung, wirkt dafür örtlich und nicht überregional.

6.6 Realer Präzedenzfall: Polen, 29. Dezember 2025

Ein koordinierter Cyberangriff traf mehr als 30 Wind- und Solarparks sowie ein Heizkraftwerk und ein Industrieunternehmen. Bei den Erneuerbaren-Anlagen ging die Kommunikation zu den Verteilnetzbetreibern verloren. Die Stromerzeugung selbst wurde nicht beeinträchtigt, und der Übertragungsnetzbetreiber sah die Stabilität des polnischen Systems zu keinem Zeitpunkt gefährdet. Die Erzeugung lief zwar weiter, war aber von den Anforderungen des Netzes entkoppelt. Der polnische Übertragungsnetzbetreiber hielt fest, es seien Unregelmässigkeiten im Betrieb kleinerer Erzeuger beobachtet und behoben worden, das System habe aber mit den verfügbaren Mitteln ausgeglichen werden können. Die eingesetzte Schadsoftware war destruktiv (Wiper). Der Bericht der zuständigen Stelle vergleicht die Angriffe mit vorsätzlicher Brandstiftung.

Die Bedeutung des Vorfalls liegt nicht in einem knapp abgewendeten Blackout, sondern darin, dass ein fähiger Akteur nachweislich Zugriff auf die Steuerungsebene (Operational Technology, OT) zahlreicher Erneuerbaren-Parks erlangte und Zerstörungsabsicht zeigte. Damit verliert das Szenario seinen rein theoretischen Charakter. Am 13. Juli 2026 schrieben das Vereinigte Königreich und die EU den Angriff offiziell dem russischen Geheimdienst FSB (Zentrum 16) zu und verhängten ein gemeinsames Sanktionspaket. Nach britischer Einschätzung hätte der Angriff im Winter rund 500'000 Menschen von der Stromversorgung abschneiden können.[57] Die technische Dokumentation liefert CERT Polska.[58]

6.7 Einschätzung unabhängiger Fachleute

Auch ausserhalb staatlicher Stellen wird die Gefahr ernst genommen. Das niederländische DIVD (vgl. Kapitel *5*) untersucht in einem eigenen Programm Wechselrichter, Ladestationen, Smart Meter und zunehmend Energiemanagementsysteme. Im Juli 2026 warnten Fachleute im Anschluss an den Angriff in Polen öffentlich, im schwersten Szenario könne ein erfolgreicher Angriff zu grossflächigen, über Tage anhaltenden Stromausfällen führen.[59]

6.8 Relativierende Faktoren

Das Netz ist nicht wehrlos. Gestufte Reserven, Schutzsysteme und weiterhin vorhandene Trägheit fangen viele Störungen ab, und nicht jede Manipulation kaskadiert. Die Heterogenität der Flotte

[56] SolarPower Europe / DNV: «Solutions for PV Cyber Risks to Grid Stability», 2025: https://www.solarpowereurope.org/insights/thematic-reports/solutions-for-pv-cyber-risks-to-grid-stability
[57] OFSI/GOV.UK, Sanktionsmitteilung vom 13.7.2026: https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions
[58] CERT Polska, «Energy Sector Incident Report – 29 December»: https://cert.pl/en/posts/2026/01/incident-report-energy-sector-2025/
[59] Dutch Institute for Vulnerability Disclosure (DIVD), öffentliche Warnung zur Verwundbarkeit des Stromnetzes (Chris van 't Hof), Juli 2026: https://www.nu.nl/klimaat/6403086/stroomnet-kwetsbaar-voor-cyberaanval-geen-kwestie-van-of-maar-wanneer.html

mit ihren vielen Herstellern, Firmware-Ständen und Konfigurationen erschwert zudem einen einzigen, herstellerübergreifenden Exploit. Innerhalb einer dominanten Herstellercloud bleibt die Konzentration allerdings real, und in der Schweiz ist sie ausgeprägt (vgl. Kapitel *3).*

Gleichzeitig sinkt mit dem Rückgang klassischer Kraftwerke die Netzträgheit. Netzbildende Wechselrichter sollen dies ausgleichen. Wenn jedoch genau diese Wechselrichter das Angriffsziel sind, entfällt mit der Erzeugung auch die Stabilisierungskomponente. Insgesamt dürfte das Grundschutzniveau durch fortlaufende Aktualisierungen der Hersteller sowie die geltende und kommende EU-Produktregulierung (RED, CRA) steigen. Die strukturellen und geopolitischen Risiken werden dadurch jedoch nicht ausgeräumt.

7 Internationaler Vergleich und Regulierung

Die Cybersicherheit von Photovoltaikanlagen ist in den letzten rund zwei Jahren international auf die regulatorische Agenda gerückt. Dieses Kapitel gibt einen Überblick über die Massnahmen anderer Staaten und der EU und ordnet die Schweiz darin ein. Die dargestellten Einschätzungen stammen von den jeweiligen Behörden und Regierungen. Sie werden hier erläutert, nicht bewertet.

7.1 Ein gemeinsames Muster

Auffällig ist, dass die Vorstösse verschiedener Länder auf dieselben zwei Punkte zielen: die Möglichkeit der Fernsteuerung über Hersteller-Clouds und die starke Konzentration des Marktes auf wenige, überwiegend chinesische Hersteller. Neun der zehn weltweit grössten Wechselrichter-Hersteller stammten 2024 aus China, auf Huawei und Sungrow allein entfielen rund 55 Prozent der weltweiten Lieferungen.[60] Diese Ausgangslage wird von mehreren nationalen Sicherheitsbehörden als strategisches Risiko eingestuft.

Zur Einordnung gehört auch die Gegenposition. Das chinesische Handelsministerium bezeichnete die Einstufung als Hochrisiko-Staat im Mai 2026 als ohne konkrete Belege erfolgt und als Stigmatisierung chinesischer Produkte.[61] Die chinesische Handelskammer bei der EU wies ihrerseits den Vorwurf zurück, China könne Energie als Druckmittel einsetzen, und verwies auf den Beitrag chinesischer Unternehmen zur europäischen Energiewende.[62]

7.2 Die eingesetzten Instrumente im Überblick

Die Vorstösse lassen sich nach ihrer Eingriffstiefe ordnen, vom blossen Informieren bis zur Verweigerung des Netzanschlusses.

- **Warnen:** Estland und Tschechien setzen auf behördliche Warnungen. Der estnische Auslandsnachrichtendienst warnte[63] im Februar 2024 ausdrücklich vor chinesischen Wechselrichtern und hielt fest, je stärker Estland auf Solarenergie setze, desto grösser wäre die Wirkung einer möglichen Manipulation. Der Nachrichtendienst-Chef sprach von einem Erpressungsrisiko.[64] Die tschechische Cyberbehörde NÚKIB warnte am 3. September 2025 vor Datentransfer nach und Fernverwaltung aus China bei kritischer Infrastruktur und nannte Photovoltaik-Wechselrichter als eines von mehreren Beispielen. Es handelt sich um eine Warnung, nicht um ein Verbot: Regulierte Stellen müssen sie in ihrer Risikoanalyse berücksichtigen.[65] Deutschland warnte im Juni 2026 in einem gemeinsamen Hinweis von Verfassungsschutz und BSI vor der Auskundschaftung ungeschützt mit dem Internet verbundener Photovoltaikanlagen durch russische Akteure.[66]
- **Empfehlen:** Australien adressierte das Thema früh. Das Cyber Security Cooperative Research Centre veröffentlichte im August 2023 den Bericht «Power Out? Solar Inverters and the Silent Cyber Threat» und empfahl drei Massnahmen: Cyber-Risikobewertungen für alle verkauften Wechselrichter, verpflichtende Cybersicherheits-Ratings sowie den Rückruf oder die

[60] EUISS, Caspar Hobhouse, «The dragon in the grid: Limiting China's influence in Europe's energy system», Januar 2026: https://www.iss.europa.eu/publications/briefs/dragon-grid-limiting-chinas-influence-europes-energy-system
[61] Ministry of Commerce, China, «Remarks on the EU's Prohibition of Funding for Projects Using Chinese Inverters», Mai 2026: https://english.mofcom.gov.cn/News/SpokesmansRemarks/art/2026/art_29f372ba6bfc4cde81fd567ea440cc60.html
[62] Euronews, «EU moves to ban high-risk inverters from China over cybersecurity threats», 4. Mai 2026: https://www.euronews.com/my-europe/2026/05/04/eu-moves-to-ban-high-risk-inverters-from-china-over-cybersecurity-threats
[63] Estonian Foreign Intelligence Service (Välisluureamet): «International Security and Estonia 2024», Februar 2024: https://raport.valisluureamet.ee/2024/en/6-china/6-3-the-advance-of-chinese-technology/
[64] Reuters, Berichterstattung zu undokumentierten Kommunikationsmodulen, Mai 2025: https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/
[65] Tschechische Cyberbehörde NÚKIB, September 2025: https://nukib.gov.cz/en/infoservis-en/news/2295-nukib-warns-against-the-transfer-of-the-data-to-and-remote-administration-from-people-s-republic-of-china/
[66] Bundesamt für Verfassungsschutz (BfV) und Bundesamt für Sicherheit in der Informationstechnik (BSI), «Gemeinsamer Sicherheitshinweis: Auskundschaftung schlecht geschützter PV-Anlagen durch staatliche Cyberakteure», 3. Juni 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html

Nachbesserung von Geräten mit schweren Schwachstellen.[67] Unabhängig davon gilt in Australien seit dem 4. März 2026 eine allgemeine Produktanforderung für vernetzte Konsumgeräte: Der Cyber Security Act 2024 und die darauf gestützten Security Standards for Smart Devices Rules verlangen unter anderem eindeutige Passwörter, eine Meldestelle für Schwachstellen und die Angabe des Unterstützungszeitraums.[68]

- **Prüfen und offenlegen:** Die Niederlande kamen über die Forschung zur Aufsicht. Die Rijksinspectie Digitale Infrastructuur prüfte zwischen 2021 und 2023 neun handelsübliche Wechselrichter von acht Marken gegen die Norm ETSI EN 303 645, eine europäische Basisnorm, die lediglich Mindestanforderungen an vernetzte Konsumgeräte stellt und ausdrücklich nur gegen elementare Angriffe auf grundlegende Konstruktionsschwächen schützen soll, etwa gegen herstellerweit identische Standardpasswörter. Kein einziges Gerät erfüllte sämtliche Anforderungen. Die Behörde warnte, dass sich Geräte aus der Ferne abschalten oder für Angriffe missbrauchen liessen.[69] Unabhängig davon lösten die im Kapitel «Befunde und Risiken» beschriebenen Offenlegungen in den Niederlanden parlamentarische Anfragen aus.
- **Zum eigenen Gesetzesvorhaben Stellung nehmen:** Deutschland zeigt den Zielkonflikt zwischen netzdienlicher Steuerung und Cybersicherheit besonders deutlich (vgl. Kapitel *7.3.1*).
- **Fördermittel binden:** Die Europäische Union schliesst Wechselrichter von Hochrisiko-Lieferanten von EU-Fördermitteln aus und hebt parallel über RED und CRA das Grundschutzniveau vernetzter Produkte an (vgl. Kapitel *7.3.2*).
- **Marktzugang an eine Prüfung binden:** Taiwan macht den Cybersicherheits-Nachweis zum Bestandteil der Typenzulassung (vgl. Kapitel *7.3.3*).
- **Netzanschluss an Sicherheit binden:** Litauen untersagt Herstellern aus Bedrohungsstaaten den Fernzugriff auf Anlagen über 100 kW und erlaubt Netzbetreibern, nicht-konforme Anlagen abzutrennen (vgl. Kapitel *7.3.4*).
- **Selbstregulierung:** Der europäische Branchenverband SolarPower Europe legte 2025 eine vom Prüfunternehmen DNV erarbeitete Analyse zu Cyberrisiken der Photovoltaik für die Netzstabilität vor. Sie enthält eine Risikobewertung, Netzsimulationen und einen Katalog von Mindestanforderungen für Hersteller, Betreiber und Politik. Die Branche hat das Thema damit selbst aufgegriffen.[70]

7.3 Vier Ansätze im Detail

Die vier letztgenannten Ansätze werden nachfolgend näher dargestellt, weil sie für die Schweizer Diskussion unmittelbar anschlussfähig sind.

7.3.1 Deutschland: der Zielkonflikt zwischen Netzsteuerung und Cybersicherheit

Deutschland zeigt den Zielkonflikt zwischen netzdienlicher Steuerung und Cybersicherheit besonders deutlich. Nach §14a des Energiewirtschaftsgesetzes (EnWG) dürfen Netzbetreiber seit dem 1. Januar 2024 bei drohender lokaler Netzüberlastung den Strombezug steuerbarer Verbrauchseinrichtungen wie Wärmepumpen, Wallboxen und Batteriespeicher vorübergehend auf eine Mindestleistung von 4,2 kW drosseln. Im Gegenzug wird das Netzentgelt reduziert.[71]

Als mit dem sogenannten Solarspitzengesetz auch die Abregelung von Photovoltaikanlagen über die bestehenden Wechselrichter vorgesehen wurde, äusserte das Bundesamt für Sicherheit in der Informationstechnik (BSI) erhebliche Bedenken. Es sehe es sehr kritisch, eine netzdienliche Fernsteuerung von Wechselrichtern über die Hersteller zu realisieren. Dass Hersteller, womöglich

[67] Cyber Security Cooperative Research Centre (CSCRC), Rachael Falk / Anne-Louise Brown, «Power Out? Solar Inverters and the Silent Cyber Threat», 2023: https://cybersecuritycrc.org.au/power-out-solar-inverters-and-silent-cyber-threat/
[68] The Department of Home Affairs, Australia, Cyber Security (Security Standards for Smart Device) Rules 2025: https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/security-standards-for-smart-devices
[69] Rijksinspectie Digitale Infrastructuur (RDI), «Onderzoek storingsproblematiek en cyberveiligheid omvormers voor zonnepanelen», Mai 2023: https://www.rdi.nl/documenten/rapporten/2023/05/30/onderzoek-storingsproblematiek-en-cyberveiligheid-omvormers-voor-zonnepanelen
[70] SolarPower Europe, «Solutions for PV Cyber Risks to Grid Stability», 2025: https://www.solarpowereurope.org/insights/thematic-reports/solutions-for-pv-cyber-risks-to-grid-stability
[71] Bundesnetzagentur, «Integration von steuerbaren Verbrauchseinrichtungen (§14a EnWG)»: https://www.bundesnetzagentur.de/DE/Vportal/Energie/SteuerbareVBE/artikel.html

über eine im Ausland betriebene Cloud, direkten Zugriff auf eine so grosse Zahl von Geräten im europäischen Verbundnetz hätten, berge ein erhebliches Gefährdungspotenzial. Neben dem Hersteller selbst könnten Sicherheitslücken auch Dritten unbefugten Zugriff eröffnen. Als Alternative schlug das BSI vor, solche Anlagen möglichst lokal zu betreiben und die netzdienliche Steuerung über intelligente Messsysteme statt über Herstellerclouds zu realisieren.[72] Fachkommentare hielten dem entgegen, dass sich fernsteuerbare Wechselrichter ohnehin über ihr Hersteller-Backend abschalten lassen und der vom BSI befürchtete Zugriff angesichts der Marktdominanz chinesischer Hersteller damit auch ohne das Gesetz längst besteht. [73]

Bemerkenswert für die Schweiz ist zudem, dass Deutschland dieselbe Regulierungslücke kennt. Die BSI-Kritisverordnung[74] greift erst ab 104 MW Anlagenleistung, kleinere Photovoltaikanlagen fallen nicht unter die Vorschriften für kritische Infrastruktur.

7.3.2 Europäische Union

Den bislang deutlichsten Schritt bildet die am 3. Dezember 2025 veröffentlichte «Economic Security Doctrine», die die Abhängigkeit von Solar-Wechselrichtern ausdrücklich als Hochrisiko-Abhängigkeit benennt und dies mit Lieferantenkonzentration, Cyber-Manipulations-Risiken und dem Zugang zu netzrelevanten Betriebsdaten begründet. Als Instrumente nennt sie unter anderem koordinierte Cyberrisikobewertungen und die Zertifizierung unter dem Cyber Resilience Act. Der Herstellerverband ESMC fordert zudem, dass Mitgliedstaaten Hochrisiko-Hardware vom Netzanschluss ausschliessen können.[75]

Im Frühjahr 2026 folgte eine konkrete Massnahme: Die Kommission schränkt EU-Fördermittel, unter anderem der Europäischen Investitionsbank, für Solar-, Wind- und Speicherprojekte ein, die Wechselrichter von Hochrisiko-Lieferanten aus China, Russland, Iran oder Nordkorea einsetzen. Anbieter aus vertrauenswürdigen Partnerländern bleiben förderfähig.[76] Wichtig für die Einordnung: Es handelt sich um eine Förderrestriktion, nicht um ein Marktverbot. Ein weitergehender Schritt in Richtung dauerhafter Marktbeschränkungen ist mit der vorgeschlagenen Revision des Cybersecurity Act (CSA2) angelegt. Eine strukturelle Lücke bleibt: Die für viele dieser Massnahmen grundlegende NIS2-Richtlinie greift primär ab mittlerer Unternehmensgrösse und erfasst kleinere Erzeugungsanlagen wie private Dach-Photovoltaik in der Regel nicht.

Unabhängig davon hebt die EU das Grundschutzniveau vernetzter Produkte an. Die Cybersicherheitsanforderungen der Funkanlagenrichtlinie (RED) gelten seit dem 1. August 2025 und verlangen für internetfähige Funkgeräte Netzschutz, Schutz personenbezogener Daten sowie Betrugsprävention. Ab dem 11. Dezember 2027 tritt der Cyber Resilience Act an ihre Stelle, Meldepflichten für aktiv ausgenutzte Schwachstellen und schwere Vorfälle gelten bereits ab dem 11. September 2026. Der CRA ist technologieneutral und lebenszyklusorientiert und verlangt unter anderem sichere Update-Mechanismen und einen strukturierten Umgang mit Schwachstellen über die gesamte Produktlebensdauer. Da diese Regeln für den Marktzugang gelten und die betroffenen Produkte weitgehend dieselben sind wie in der Schweiz, dürften sie das Sicherheitsniveau auch hierzulande anheben.

7.3.3 Taiwan: produktbezogene Prüfung mit erheblicher Prüftiefe

Taiwan verfügt über eines der wenigen produktbezogenen Prüfregime für Solar-Wechselrichter und über das detaillierteste öffentlich dokumentierte. Die Prüfbehörde BSMI veröffentlichte im Oktober 2025 eine technische Prüfspezifikation und verankerte die Cybersicherheits-Nachweise

[72] pv magazine Deutschland, Petra Hannen, «Solarspitzen-Gesetz: BSI warnt vor Zugriff chinesischer Hersteller auf deutsche Photovoltaikanlagen», Januar 2025: https://www.pv-magazine.de/2025/01/20/solarspitzen-gesetz-bsi-warnt-vor-zugriff-chinesischer-hersteller-auf-deutsche-photovoltaik-anlagen/
[73] zfk, Julian Korb, «Wirbel um Überwachung in chinesischen Wechselrichtern»: https://www.zfk.de/energie/strom/wirbel-um-ueberwachung-in-chinesischen-wechselrichtern
[74] BSI-KritisV, Anhang 1, Teil 3 Nr. 1.1.1: https://www.gesetze-im-internet.de/bsi-kritisv/anhang_1.html
[75] pv magazine: «EU security doctrine highlights high-risk dependency on Chinese solar inverters», 16. Dezember 2025: https://www.pv-magazine.com/2025/12/16/eu-security-doctrine-highlights-high-risk-dependency-on-chinese-solar-inverters/
[76] pv magazine, «EU moves to restrict funding for projects using inverters from high-risk suppliers», 23. April 2026: https://www.pv-magazine.com/2026/04/23/eu-moves-to-restrict-funding-for-projects-using-inverters-from-high-risk-suppliers/

mit einer Revision der Typenzulassung vom Mai 2026 verbindlich. Für Solar-Wechselrichter, neben Ladeinfrastruktur, Leistungswandlern und stationären Lithium-Speichern, werden sie ab dem 1. Januar 2028 verpflichtender Bestandteil der Typenzulassung, und der vereinfachte Weg der Konformitätserklärung entfällt dann.[77]

Geprüft werden zwei Einheiten getrennt, der Wechselrichter selbst und die Überwachungseinheit. Für die Überwachungseinheit gelten vier Sicherheitsdimensionen, nämlich physische, System-, Kommunikations- und Authentisierungssicherheit, für den Wechselrichter drei, gestützt auf internationale Standards wie IEC 62443-4-2. Die Prüftiefe ist beachtlich. Verlangt wird die Übergabe des Quellcodes für eine statische Analyse, wobei Schwachstellen mit einem Schweregrad-Wert (CVSS) von 7 oder höher ohne begründete Gegenmassnahme zur Nichtkonformität führen. Hinzu kommt eine Integritätsprüfung des Firmware-Updates, bei der der Wechselrichter eine absichtlich manipulierte Firmware zurückweisen oder in einen sicheren Zustand zurückfallen muss. Für die Überwachungseinheit ist zudem eine Verkehrsanalyse über mindestens 24 Stunden vorgesehen, bei der die tatsächlichen Zieladressen mit den vom Hersteller deklarierten Servern abgeglichen werden.

Analytisch lehrreich sind zwei Grenzen. Erstens handelt es sich um eine Typenprüfung zum Zeitpunkt der Zertifizierung: Die Spezifikation verlangt zwar, dass das Gerät manipulierte Firmware erkennt, schreibt dafür aber kein bestimmtes kryptografisches Verfahren vor, und eine spezifische Nachprüfung bei späteren Firmware-Änderungen sieht sie nicht vor. Zweitens nimmt sie die Informationssicherheit des Managementsystems, also der Cloud-Ebene, ausdrücklich vom Prüfumfang aus; einbezogen wird nur, ob es Benutzerkonten verwalten und Firmware aus der Ferne aktualisieren kann. Damit lässt dieses Prüfregime jene Ebene aus, die nach den Befunden dieser Analyse die grösste Hebelwirkung hat. Die Lehre für die Schweiz und die EU ist entsprechend doppelt: Ein produktbezogenes Prüfregime ist möglich und sinnvoll, es bleibt aber unvollständig, solange es weder eine Lebenszyklus-Komponente noch die zentrale Steuerungsebene erfasst.

7.3.4 Litauen: Sicherheit als Bedingung für den Netzanschluss

Litauen ist am weitesten gegangen. Mit dem am 12. November 2024 verabschiedeten Artikel 73^3 wird Herstellern aus Staaten, die gemäss nationaler Sicherheitsstrategie als Bedrohung gelten und zu denen China zählt, der Fernzugriff auf die Steuerungssysteme von Solar-, Wind- und Speicheranlagen über 100 kW untersagt, konkret das Fernverändern von Leistungsparametern sowie das Ein- und Ausschalten. Verlangt werden unter anderem Mehrfaktor-Authentisierung, sichere Kommunikation, Lieferketten-Kontrollen sowie ein Audit. Für neue Anlagen gilt die Regelung seit dem 1. Mai 2025, Bestandsanlagen mussten bis zum 1. Juni 2026 nachziehen. Die Konformität ist Voraussetzung für den Netzanschluss, und seit Ablauf der Übergangsfrist dürfen Netzbetreiber nicht-konforme Anlagen auch vom Netz trennen.[78] Der Europäische Verband der Solarhersteller unterstützte die Regelung.[79]

Bemerkenswert ist, was das Gesetz nicht verlangt. Chinesische Geräte sind nicht verboten, und bereits installierte Anlagen müssen nicht ersetzt werden. Ihre Betreiber müssen aber zusätzliche Schutzmassnahmen umsetzen.

Die litauische Erfahrung zeigt zugleich, wo der Aufwand anfällt. Für Neuanlagen ist die Konformität vergleichsweise günstig zu erreichen, weil sie bei Beschaffung und Anschluss von Anfang an mitgedacht werden kann. Aufwendig und zeitraubend ist die Nachrüstung des Bestands, bei der sich Umsetzungsstaus bildeten. Für die Schweiz folgt daraus, dass ein solcher Ansatz seine Wirkung vor allem über Neuanlagen entfaltet und der Bestand über Jahre die grössere offene Flanke bleibt.

---

[77] Taiwan, Bureau of Standards, Metrology and Inspection (BSMI): Revision der Typenzulassungsregeln vom Mai 2026: https://www.bsmi.gov.tw/wSite/public/Attachment/f1761016956224.pdf; Zusammenfassung: https://www.gmalabs.com/post/taiwan-bsmi-type-approval-update-new-cybersecurity-files

[78] pv magazine, «Lithuania's grid operators can now disconnect solar plants without cybersecurity measures», Juni 2026: https://www.pv-magazine.com/2026/06/05/lithuanias-grid-operators-can-now-disconnect-solar-plants-without-cybersecurity-measures/

[79] pv magazine, «Lithuania bans remote Chinese access to solar, wind, storage devices», 18. November 2024: https://www.pv-magazine.com/2024/11/18/lithuania-bans-remote-chinese-access-to-solar-wind-storage-devices/

7.4 Regulierung in der Schweiz

In der Schweiz ist der IKT-Minimalstandard für die Strombranche seit dem 1. Juli 2024 verbindlich. Die revidierte Stromversorgungsverordnung (StromVV, Anhang 1a) schreibt Schutzniveaus und Reifegrade vor, deren Erfüllung die Eidgenössische Elektrizitätskommission (ElCom) prüfen kann. Die Einstufung richtet sich nach der Leistungsfähigkeit: Schutzniveau A gilt etwa für Netzbetreiber ab 450 GWh pro Jahr, Schutzniveau B für Netzbetreiber ab 112 GWh pro Jahr sowie für Erzeuger, Speicherbetreiber und Dienstleister, sofern sie Anlagen mit einer Gesamtleistung von mindestens 100 MW betreiben und diese über ein einziges System steuern können.[80] Ergänzend gilt seit dem 1. April 2025 eine Meldepflicht: Cyberangriffe auf kritische Infrastrukturen sind innerhalb von 24 Stunden dem Bundesamt für Cybersicherheit (BACS) zu melden.

Die entscheidende Lücke betrifft die Kleinanlagen und damit praktisch alle Schweizer Photovoltaikanlagen. Erzeuger unterstehen dem Standard erst ab 100 MW steuerbarer Gesamtleistung über ein einziges System. Der über Hunderttausende Betreiber verteilte Bestand kleiner Anlagen wird von keiner einzelnen verpflichteten Stelle erfasst. Die geltende und kommende EU-Produktregulierung dürfte das Geräteniveau anheben. Die strukturellen und geopolitischen Fragen, also Marktkonzentration und Fernsteuerbarkeit, adressiert sie jedoch nicht.

Dass diese Lücke erkannt ist, zeigt ein Papier der nationalen Netzgesellschaft. Im White Paper «Systemverträgliche Integration Photovoltaik»[81] vom März 2026 hält Swissgrid fest, die Schweizer Energieversorgung sei bereits heute auf Hunderttausende dezentrale Anlagen verteilt. Dies bedinge auch für diese Anlagen und deren Steuerung ein definiertes Schutzniveau gegenüber Cyberangriffen. Gefordert werden verbindliche Mindestanforderungen für Photovoltaikanlagen, die zudem auch bei bestehenden Anlagen effektiv implementiert und kontrolliert werden müssten. Adressiert ist die Empfehlung an Gesetzgeber und Eidgenössisches Starkstrominspektorat (ESTI). Der in diesem Bericht beschriebene Handlungsbedarf wird damit von jener Stelle geteilt, die für die Stabilität des Gesamtsystems einsteht.

Zu beachten ist, was der IKT-Minimalstandard leistet und was nicht. Er richtet sich an Organisationen und verlangt von ihnen, Risiken zu identifizieren, Schutzmassnahmen umzusetzen, Vorfälle zu erkennen und darauf zu reagieren. Auf eine private Anlage, die von einer Person ohne IT-Organisation betrieben wird, ist er nicht sinnvoll anwendbar. Die Lücke bei den Kleinanlagen lässt sich deshalb nicht schliessen, indem man die Leistungsschwelle senkt. Wirksam sind hier andere Instrumente: Anforderungen an das Produkt, Bedingungen für den Netzanschluss oder die Erfassung jener Stelle, die den Zugriff auf viele Anlagen bündelt.

7.5 Einordnung für die Schweiz

Der internationale Trend ist eindeutig: Mehrere Staaten behandeln die verteilte Photovoltaik zunehmend als Frage der kritischen Infrastruktur und nicht nur der Klimapolitik. Die eingesetzten Instrumente reichen von Warnungen (Tschechien, Estland, Deutschland) und behördlichen Stellungnahmen zu Gesetzesvorhaben (Deutschland) über aufsichtsrechtliche Marktprüfungen (Niederlande) und produktbezogene Prüfregime (Taiwan) bis zu Förder- und Beschaffungskriterien (EU) und verbindlichen Netzanschlussbedingungen (Litauen).

Hinzu kommt auf der Durchsetzungsseite ein weiteres Instrument. Mit der Zuschreibung des Angriffs auf das polnische Stromnetz an den russischen Geheimdienst FSB und dem gemeinsamen Sanktionspaket vom 13. Juli 2026 (vgl. Kapitel *6.6*) zeigen die EU und das Vereinigte Königreich, dass eine solche Zuordnung und Sanktionen ergänzend zur technischen und regulatorischen Absicherung eingesetzt werden.[82]

Die Schweizer Regulierung deckt die Netzbetreiber, die grossen Erzeuger und Speicherbetreiber sowie Dienstleister mit entsprechender Steuerungsreichweite ab. Verbindliche

[80] Bundesamt für Cybersicherheit (BACS), IKT-Minimalstandards: https://www.ncsc.admin.ch/ncsc/de/home/infos-fuer/infos-it-spezialisten/themen/ikt-minimalstandards.html
[81] Swissgrid AG, White Paper «Systemverträgliche Integration Photovoltaik», März 2026: https://www.swissgrid.ch/de/home/newsroom/blog/2026/20260330-01.html
[82] OFSI/GOV.UK, Sanktionsmitteilung vom 13.7.2026: https://www.gov.uk/government/news/uk-and-eu-strike-russian-cyber-networks-with-new-sanctions

Cybersicherheitsvorgaben für den Betrieb der einzelnen Kleinanlage fehlen. Die Branchenempfehlung NA/EEA-NE7 enthält seit 2025 zwar ein Kapitel zu Fernzugriff und Firmware-Updates, beschränkt sich dort aber auf Passwortschutz und Updates. Welche dieser Ansätze für die Schweiz in Frage kommen, wird im Kapitel *8 Empfehlungen* aufgegriffen.

7.6 Regulatorischer Ausblick

Das Grundschutzniveau vernetzter Produkte steigt, die strukturellen Fragen bleiben davon jedoch unberührt.

Produktseitig gelten die Cybersicherheitsanforderungen der Funkanlagenrichtlinie RED seit August 2025; in der Schweiz sind sie über die Verordnung über Fernmeldeanlagen umgesetzt, Marktüberwachungsbehörde ist das Bundesamt für Kommunikation BAKOM. Prüfbar werden sie durch die Normenreihe EN 18031, die Zugangskontrolle, sichere Update-Mechanismen und den Umgang mit Zugangsdaten konkretisiert. Ab Dezember 2027 löst der Cyber Resilience Act die RED-Anforderungen ab und erweitert sie auf alle Produkte mit digitalen Elementen, also auch auf Geräte ohne Funkschnittstelle. Parallel entstehen Prüfregime speziell für diese Geräteklasse: die taiwanische Typenzulassung, UL 2941 und die Zertifizierung der SunSpec Alliance (vgl. Kapitel *7.3.3* und *8.3*).

Was diese Regelwerke leisten, ist ein höheres Grundniveau, sie erschweren den unbefugten Zugriff durch Dritte. Sie adressieren jedoch weder die Marktkonzentration noch die Fernsteuerbarkeit durch den Hersteller selbst. Hersteller sowie Betreiberinnen und Betreiber sollten die Empfehlungen im nächsten Kapitel deshalb nicht erst mit dem Inkrafttreten künftiger Pflichten umsetzen, sondern schon heute.

8 Empfehlungen

Die folgenden Empfehlungen ergeben sich aus dem zentralen Befund dieses Berichts: Das massgebliche Risiko ist struktureller Natur, also eine Frage von Cloud-Abhängigkeit, Marktkonzentration und konstruktionsbedingt ungeschützten Steuerprotokollen, und weniger eine Frage mangelhafter Einzelgeräte. Sie sind nach Adressaten gegliedert und bewusst auf hoher Flughöhe gehalten. Dieser Bericht spricht sich nicht gegen die Photovoltaik aus. Die Empfehlungen sollen ihren sicheren weiteren Ausbau ermöglichen. Vorweg ist festzuhalten, dass es die eine, einfache und vollständige Lösung nicht gibt: Alle Ansätze haben Nachteile, und es verbleiben Restrisiken.

8.1 Für Betreiber von Kleinanlagen

Eine einmalige Installation genügt nicht: Anlagen müssen korrekt konfiguriert und regelmässig aktualisiert werden, und im Ereignisfall muss jemand zuständig sein. Wer diese Aufgaben nicht selbst wahrnehmen kann, sollte sie vertraglich übertragen, an den Installationsbetrieb oder einen Dritten. Ein Betriebsangebot allein ist kein Kompetenznachweis. Ob ein Anbieter geeignet ist, zeigt sich daran, ob er die folgenden Punkte von sich aus adressiert und schriftlich zusichert.

Konkrete Punkte für die Einzelanlage:

- Standardpasswörter sofort ändern und automatische Firmware-Updates aktivieren oder Updates zeitnah einspielen.
- Keine Komponente der Anlage aus dem Internet erreichbar machen, insbesondere keine Portweiterleitung einrichten.
- Bewusst entscheiden, ob die Anlage dauerhaft mit der Herstellercloud verbunden sein soll. Diese Verbindung ist technisch nicht zwingend, in der Praxis aber die Voreinstellung, und sie wird selten hinterfragt. Bei vielen Geräten lässt sich die Produktion auch ohne Cloud lokal auslesen. Ein solcher Betrieb ohne Cloud-Anbindung verkleinert die Angriffsfläche, kostet aber Komfort, etwa das bequeme Monitoring über die App. Abzuwägen ist zudem, dass ohne Anbindung keine automatischen Firmware-Updates mehr eintreffen und bekannte Schwachstellen dadurch bestehen bleiben können. Wo das Gerät es zulässt, ist eine Steuerungssperre deshalb oft der bessere Kompromiss: Sie lässt Updates weiterhin zu, aber keine aktive Fernsteuerung (vgl. Kapitel *8.4.2*). Nicht benötigte Fernzugriffe sollten deaktiviert werden.
- Ein Energiemanagementsystem nach überprüfbaren Merkmalen auswählen statt nach Funktionsumfang: lokale Bedienbarkeit ohne dauerhafte Cloud-Verbindung, ein zugesicherter Update- und Supportzeitraum und wo möglich eine unabhängige Prüfung. Ein EMS bündelt die Kontrolle über alle angeschlossenen Geräte an einem Punkt, sodass eine einzige Schwachstelle die gesamte Anlage betrifft.
- Sich bei der Übergabe bestätigen lassen, dass individuelle Passwörter gesetzt sind und die Anlage nicht aus dem Internet erreichbar ist.
- Vertraglich festhalten, wer dafür sorgt, dass Firmware-Updates eingespielt werden, und wer im Ereignisfall zuständig ist.

8.2 Für Betreiber grösserer Anlagen

Für Netzbetreiber und Betreiber grosser gewerblicher und industrieller Anlagen gelten die bewährten Grundsätze aus OT- und IoT-Umgebungen:

- **Anlagenbestand inventarisieren:** Wechselrichter, Energiemanagementsysteme und ihre Schnittstellen samt sämtlicher Fernzugriffe (Hersteller, Installateur, Serviceanbieter, Aggregator) erfassen und aktuell halten. Was nicht bekannt ist, lässt sich nicht absichern.
- **Nicht aus dem Internet erreichbar:** Wechselrichter und Energiemanagementsysteme mit ihren Verwaltungsschnittstellen gehören nicht ins Internet. Ist Fernzugriff nötig, sollte er über abgesicherte Kanäle erfolgen, etwa über ein virtuelles privates Netzwerk (VPN).
- **Netzwerksegmentierung:** Photovoltaik, Energiemanagement und Ladeinfrastruktur einzeln vom übrigen Netz trennen, weil ein kombinierter Zugriff auf Einspeisung und Verbrauch

besonders wirksam ist (vgl. Kapitel *2.6*).

- **Trennung der lokalen Steuerung vom internetseitigen Netz:** Wird Modbus TCP eingesetzt, hängt der Wechselrichter oft im selben Netzsegment wie ein internetverbundenes Energiemanagementsystem. Eine gewöhnliche Netzwerk-Firewall schützt hier nur vor Zugriffen von aussen, nicht aber vor einem bereits im lokalen Netz befindlichen Angreifer, etwa über ein kompromittiertes IoT-Gerät (vgl. Kapitel *5.3.3).* Robuster ist deshalb ein Energiemanagementsystem mit zwei physisch getrennten Netzwerkports, einem für den lokalen Teil (Wechselrichter, ohne Internet) und einem für das internetseitige Netz. Ein bewusster Medienbruch (etwa RS485 statt durchgehend Ethernet) verringert das Risiko, dass ein Gerät versehentlich aus dem Internet erreichbar wird.
- **Das Energiemanagementsystem als Bündelungspunkt behandeln**: Es kontrolliert alle angeschlossenen Geräte und reicht damit weiter als ein einzelner Wechselrichter.
- **Herstellerzugänge vertraglich erfassen:** Umfang, Zweck und Dauer eines privilegierten Fernzugangs schriftlich regeln und ein Widerrufsrecht vorsehen (vgl. Kapitel *5.4.2*).
- **Die zentrale Steuerbarkeit bewusst konfigurieren:** Wo die Anlage keine herstellerseitige Fernsteuerung benötigt, sollte diese eingeschränkt und die Steuerung netzrelevanter Funktionen der regulierten Stelle vorbehalten werden (vgl. Kapitel *3.4* und *8.4.2*).
- **Überwachung und Protokollierung**: Wechselrichter, Energiemanagementsysteme und ihre Fernzugriffe laufend überwachen und die geräteseitige Protokollierung zentral sammeln und auswerten.
- **Einen Update-Prozess betreiben:** Für die eigene Flotte geregelt prüfen, ob neue, insbesondere sicherheitsrelevante Firmware vorliegt, und diese nach Risikoabwägung zeitnah einspielen.
- **Für den Ereignisfall vorsorgen:** Vorab festlegen, wer bei einem Sicherheitsvorfall zuständig ist, samt Kontakten zu Hersteller beziehungsweise Aggregator und den Cybersicherheitsbehörden. Anlagen sollten sich zudem geordnet vom betroffenen Steuerkanal trennen lassen, ohne unkontrolliert gleichzeitig abzuschalten (vgl. Kapitel *8.4.2*).
- **Sicherheit in der Beschaffung:** Sicherheitsanforderungen in Ausschreibungen aufnehmen und Cybersicherheit zu einem Beschaffungskriterium machen.
- **IKT-Minimalstandard freiwillig anwenden:** auch auf Systeme anwenden, die nicht in seinen obligatorischen Geltungsbereich fallen (vgl. Kapitel *7.4).*

8.3 Für Installationsbetriebe

Installationsbetriebe entscheiden in der Praxis über das Sicherheitsniveau der einzelnen Anlage. Bei der Inbetriebnahme entsteht, was später angreifbar ist: Wer die Zugangsdaten setzt, die Schnittstellen konfiguriert und die Anlage ans Netz bringt, legt fest, ob ein Standardpasswort in Kraft bleibt, ob der Wechselrichter aus dem Internet erreichbar ist und ob die lokale Steuerschnittstelle ungeschützt offensteht. Diese Entscheidungen trifft in aller Regel nicht die Betreiberin, sondern der Installationsbetrieb. Das BSI hält es für wahrscheinlich, dass Installation und Einrichtung häufig durch Solarfachfirmen erfolgen, die wenig Expertise in IT-Sicherheit mitbringen.[83] Umso wichtiger ist, dass bei der Inbetriebnahme einige Grundsätze eingehalten werden:

- Für jede Anlage individuelle Zugangsdaten setzen und keine über den Kundenstamm hinweg einheitlichen Passwörter verwenden. Ein flottenweit gültiger Installateur-Code verlagert dasselbe Risiko, das dieser Bericht bei den Herstellern beschreibt, auf die Ebene des Installationsbetriebs (vgl. Kapitel *5.4.2*).
- Keine Komponente der Anlage aus dem Internet erreichbar machen, insbesondere keine Portweiterleitung einrichten.
- Nicht benötigte Schnittstellen deaktivieren, etwa einen ungenutzten WLAN-Hotspot oder eine offene lokale Steuerschnittstelle (vgl. Kapitel *5.3.2*).
- Die Anlage vom übrigen Heim- oder Firmennetz trennen, sodass ein kompromittiertes Gerät im selben Netz den Wechselrichter nicht ohne Weiteres erreicht (vgl. Kapitel *5.3.3*).

[83] Bundesamt für Verfassungsschutz (BfV) und Bundesamt für Sicherheit in der Informationstechnik (BSI): «Gemeinsamer Sicherheitshinweis: Auskundschaftung schlecht geschützter PV-Anlagen durch staatliche Cyberakteure», 3. Juni 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html

- Zur Übergabe gehören eine Dokumentation der gewählten Konfiguration und eine klare Abrede darüber, wer künftig dafür sorgt, dass Firmware-Updates eingespielt werden, und wer im Ereignisfall zuständig ist.
- In der Beschaffung Produkte bevorzugen, die auch ohne Cloud funktionieren, geschützte lokale Schnittstellen bieten und für die ein Update-Zeitraum zugesichert ist.

Damit diese Punkte in der Praxis eingehalten werden, braucht es die entsprechende Kompetenz im Installationsbetrieb. Cybersicherheits-Grundlagen sollten deshalb fester Bestandteil der Aus- und Weiterbildung sein.

8.4 Für Hersteller

8.4.1 Grundanforderungen

Die Verantwortung für das grundlegende Sicherheitsniveau liegt bei den Herstellern. Zentral sind:

- **Sicherheit als Konstruktionsprinzip:** Sicherheit von Beginn an mitdenken und nicht nachträglich ergänzen («Security by Design»).
- **Sichere Firmware-Updates:** kryptografisch signiert, mit Schutz gegen das Zurückspielen älterer, verwundbarer Versionen.
- **Wartungs- und Servicezugänge absichern:** Die Anmeldedaten müssen gerätespezifisch und nicht rekonstruierbar sein, damit ein einzelnes kompromittiertes Zugangsverfahren nicht die ganze Flotte betrifft. Ein privilegierter Fernzugang sollte zudem zeitlich befristet und für die verantwortliche Stelle widerrufbar sein.
- **Protokollierung sicherheitsrelevanter Ereignisse:** Anmeldungen, Änderungen an netzrelevanten Parametern, Firmware-Wechsel und Zugriffe über Wartungskonten müssen im Gerät protokolliert und auslesbar sein.
- **Gesicherte Cloud-Schnittstellen:** durchgängige Authentisierung und Autorisierung in allen APIs.
- **Umgang mit gemeldeten Schwachstellen:** ein strukturierter Responsible-Disclosure-Prozess mit einer erreichbaren Meldestelle und einer Behebung innert angemessener Frist.
- **Sicherer Zustand bei Support-Ende:** Endet die Herstellerunterstützung, etwa durch Geschäftsaufgabe, Marktrückzug, Sanktionen oder einen Vertriebsstreit, muss das Gerät lokal funktionsfähig bleiben und darf nicht fernabschaltbar oder blockierbar sein.
- **Sicherung und Wiederherstellung:** Konfiguration und netzrelevante Einstellungen müssen gesichert und wiederhergestellt werden können, und der Hersteller sollte einen geprüften Grundstand der Firmware so bereitstellen, dass eine Anlage auch ohne seine Mitwirkung wieder in Betrieb genommen werden kann.
- **Reichweite des eigenen Fernzugangs begrenzen:** Auch ein legitimer Zugang soll nicht die gesamte Geräteflotte gleichzeitig steuern oder aktualisieren können. Das ist durch getrennte Netze, Steuerserver und Cloud-Anwendungen technisch sicherzustellen (vgl. Kapitel *8.5.2*).
- **Eine abgesicherte lokale Schnittstelle anbieten:** Für die lokale Steuerung fehlt ein verbreiteter sicherer Standard, und eine Verschlüsselungspflicht würde die Kopplung mit gängigen Energiemanagementsystemen brechen. Hersteller sollten deshalb zusätzlich eine authentisierte und verschlüsselte Variante anbieten, wie es einzelne bereits tun (vgl. Kapitel *3.3*), und die Schnittstelle ab Werk deaktivieren, solange sie nicht benötigt wird.

Ein Teil dieser Anforderungen ist keine Empfehlung, sondern Produktrecht: Für Geräte mit Funkschnittstelle gelten seit August 2025 die Cybersicherheitsanforderungen der Funkanlagenrichtlinie RED, die für diese Produkte durch den CRA ab Dezember 2027 abgelöst werden, der dann für alle Produkte mit digitalen Elementen gilt (vgl. Kapitel *7.3.2*). Die Befunde dieser Analyse zeigen, dass diese Anforderungen in der Praxis nicht durchgängig erfüllt sind. Herstellern wird deshalb empfohlen, nicht auf das Mindestmass für die Konformitätserklärung zu zielen, sondern die dahinterliegenden Prinzipien umzusetzen: sichere Voreinstellung und Sicherheit als Konstruktionsprinzip.

8.4.2 Werkseitige Steuerungssperre für netzrelevante Funktionen

Über die Grundhygiene hinaus wird empfohlen, geräteseitig zu begrenzen, was sich aus der Ferne verändern lässt. Neu ist der Grundsatz nicht: Die Leitlinien des US-amerikanischen NIST für Wechselrichter (NIST IR 8498)[84] empfehlen, nicht in jeder Einsatzart benötigte Fähigkeiten ab Werk zu deaktivieren und nur bewusst freizuschalten.

Wirksam ist eine solche Begrenzung nur an einem Punkt, der den Inhalt der Befehle unterscheiden kann und nicht umgehbar ist. Eine gewöhnliche Netzwerk-Firewall erfüllt das Erste nicht, weil Betriebsdaten und Steuerbefehle über dieselbe Verbindung zum selben Endpunkt laufen. Durchsetzbar ist sie im Wechselrichter selbst oder in einem vorgeschalteten Energiemanagementsystem (vgl. Kapitel *8.2*), letzteres allerdings nur, wenn der Wechselrichter keinen eigenen Weg zur Herstellercloud offen hat und unauthentisierte lokale Schreibzugriffe verweigert. Die Empfehlung unterscheidet drei Klassen von Fähigkeiten, für die jeweils ein anderes Regime gilt: den Fernzugriff im Auslieferungszustand, die netzrelevanten Parameter und die Einspeise-Sollwerte.

Auslieferungszustand: Aus der Ferne zulässig sind ausschliesslich das Auslesen von Betriebsdaten und kryptografisch signierte Firmware-Updates. Die Anlage muss ohne diesen Kanal vollständig weiterlaufen, mit unverändertem Verhalten gegenüber dem Netz.

Die schweizerische Branchenempfehlung NA/EEA-NE7[85] empfiehlt demgegenüber, die Funktion für Firmware-Updates aus der Ferne wo möglich zu deaktivieren und Updates nur vor Ort durchzuführen. Die Überlegung ist nachvollziehbar, weil der Update-Kanal tatsächlich der mächtigste Fernzugriff ist. Bei einem Bestand von hunderttausenden Kleinanlagen führt sie aus Sicht des NTC jedoch zum grösseren Risiko: Ohne funktionierenden Update-Kanal bleiben bekannte Schwachstellen über Jahre offen. Das deutsche BSI rät dringend dazu, regelmässig zu prüfen, ob neue Softwareversionen vorliegen, und mindestens solche, die Sicherheitslücken beheben, nach Risikoabwägung schnellstmöglich zu installieren.[86] Dieser Bericht folgt dieser Linie, verbindet sie aber mit Anforderungen an die Update-Kette selbst: kryptografische Signatur, Schutz gegen das Einspielen älterer Versionen und eine feststellbare Version, deren Änderungen am Netzverhalten dokumentiert sind.

Netzrelevante Parameter: Netzrelevante Parameter werden bei der Inbetriebnahme gesetzt und sind danach gesperrt. Gemeint sind die Werte, die das Verhalten der Anlage gegenüber dem Netz bestimmen: z.B. die Ländereinstellung als Ganzes, die Schutzeinstellungen für Spannung und Frequenz, die Zuschalt- und Wiederzuschaltbedingungen, das Blindleistungs- und Wirkleistungsverhalten in Abhängigkeit von Spannung und Frequenz sowie das Verhalten bei Netzfehlern. Den Umfang gibt Anhang E der Branchenempfehlung NA/EEA-NE7 vor. Zugleich sind sie ein besonders wirksamer Angriffsvektor (vgl. Kapitel *6.3*, Typ B). Denselben Schutz verlangt Swissgrid ohne Bezug auf einen Angriff: Das Verhalten der Anlagen bei einer Netztrennung und ihre Bedingungen für die Wiederzuschaltung sollen direkt in der Anlage festgelegt werden, um in der anspruchsvollen Phase des Netzwiederaufbaus eine grosse Unsicherheitskomponente zu reduzieren. Diese Werte sind also nicht nur deshalb zu schützen, weil sie sich manipulieren lassen, sondern auch, weil sich der Netzbetrieb auf sie verlässt.

Der besondere Schutz dieser Werte wird auch international empfohlen:

- Die NIST-Empfehlungen für Wechselrichter empfehlen ab Werk deaktivierte Schnittstellen, Software nur aus verifizierten Quellen und eine Trennung der Regelfunktionen von den Kommunikationsschnittstellen. Ein Passwort allein gilt dort für Zugriffe mit Wirkung auf kritische Infrastruktur als nicht mehr angemessen.
- Die Untersuchung von Secura empfiehlt, kritische Parameter unveränderbar zu halten und

[84] National Institute of Standards and Technology NIST: Cybersecurity for Smart Inverters – Guidelines for Residential and Light Commercial Solar Energy Systems, NIST IR 8498, Dezember 2024: https://doi.org/10.6028/NIST.IR.8498
[85] VSE: Branchenempfehlung «Netzanschluss für Energieerzeugungsanlagen an das Niederspannungsnetz NA/EEA-NE7 – CH 2025»: https://www.strom.ch/de/dokument/netzanschluss-fuer-energieerzeugungsanlagen-das-niederspannungsnetz-naeea-ne7-ch-2025-0
[86] Bundesamt für Verfassungsschutz (BfV) und Bundesamt für Sicherheit in der Informationstechnik (BSI), «Gemeinsamer Sicherheitshinweis: Auskundschaftung schlecht geschützter PV-Anlagen durch staatliche Cyberakteure», 3. Juni 2026: https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2026/2026-262584-1032.html

Fernkonfiguration nur mit lokaler Zustimmung zuzulassen.[87]

Für die Schweiz besteht dazu keine einheitliche Vorgabe. Entscheidend wäre, dass eine solche Sperre nicht allein auf einer Authentisierung beruht. Ein Berechtigungsnachweis, der zentral verfügbar ist, lässt sich über viele Anlagen gleichzeitig einsetzen, und genau diese Gleichzeitigkeit ist die Wirkung, die dieser Bericht als systemrelevant beschreibt. Naheliegend ist deshalb, die Aufhebung der Sperre an eine lokale Autorisierung am Gerät zu binden, sodass sie sich nicht über einen zentral verfügbaren Zugang bei vielen Anlagen gleichzeitig auslösen lässt, etwa durch eine physische Handlung vor Ort. Die Sperre gilt für alle Schreibpfade auf diese Werte, also Bedienoberfläche, lokale Kommunikationsschnittstellen, Cloud-Anbindung und Wartungszugang. Dasselbe Prinzip verfolgt die Plombierung von Zählern und Schutzeinrichtungen seit langem. Gemeint ist dabei der Schutz vor unbefugter Veränderung und nicht Unveränderlichkeit als solche. Ändern sich die Anschlussbedingungen, muss eine Anpassung im Bestand möglich bleiben.

Einspeise-Sollwerte: Gesperrt, aber vor Ort freischaltbar, sobald die Anlage an einem Netzdienst teilnimmt. Eine blosse Begrenzung des Sollwertbereichs genügt nicht, weil die Abregelung auf null gerade der vorgesehene Netzdienst ist und zugleich dem Angriffsmuster Typ A entspricht. Zwei Bedingungen gehören dazu:

- Ist die Fähigkeit freigeschaltet, sollte sie nicht über die Herstellercloud laufen, sondern über den Netzbetreiber oder den vertraglich gebundenen Aggregator (vgl. Kapitel *8.5.1*).
- Fällt die Steuerverbindung aus oder bleibt sie aus, fällt das Gerät nach einer Haltezeit auf einen bei der Inbetriebnahme festgelegten Zustand zurück. Die Haltezeit verhindert, dass eine Störung der Kommunikation bei vielen Anlagen gleichzeitig einen Leistungssprung auslöst.
  Dieselbe Anforderung wird auch ohne Angriffsszenario erhoben. Swissgrid empfiehlt, neue Anlagen «fail-safe» zu bauen: Sie sollen auch ohne externe Steuerung und ohne funktionierende Kommunikation sicher weiterbetrieben werden können, wozu die Netzbetreiber Vorgaben für einen im Voraus festgelegten Zustand erarbeiten sollen. Auslöser ist dort der gewöhnliche Kommunikationsunterbruch, also derselbe Fall, den die vorstehend beschriebene Haltezeit adressiert. Die Empfehlung setzt damit die Annahme eines Angreifers nicht voraus.[88]

Damit ist der abgesicherte Zustand die Voreinstellung, und jede zusätzliche Fernsteuerbarkeit wird zu einer bewussten, sichtbaren und örtlich getroffenen Entscheidung. Gegen manipulierte Firmware schützt sich ein Gerät damit nicht, denn Code auf dem Gerät kann jede geräteseitige Sperre umgehen. Gegen den Hersteller selbst und gegen eine kompromittierte Update-Kette wirken deshalb nur die Integrität dieser Kette, eine Nachprüfung bei wesentlichen Firmware-Änderungen (vgl. Kapitel *8.5.3*), Diversifizierung und unabhängige Prüfbarkeit.

Abschliessend zum Verhältnis dieser Empfehlung zur energiepolitischen Stossrichtung: Die Branche bewegt sich in Richtung mehr Steuerbarkeit. Swissgrid hält in ihrem White Paper zur Integration der Photovoltaik fest, Flexibilität sei für Photovoltaikanlagen künftig keine Option, sondern eine Voraussetzung. Die hier vorgeschlagene werkseitige Steuerungssperre steht dazu nicht im Widerspruch. Sie verlangt keinen Verzicht auf Flexibilität, sondern nur, dass deren Freischaltung vor Ort erfolgt und die netzrelevante Steuerung anschliessend über die regulierte Stelle läuft.

8.5 Für Politik und Regulierung

8.5.1 Zuständigkeit

Die Verantwortungslücke für Kleinanlagen schliessen: Vorgaben bestehen, aber sie greifen zu kurz. Die Cybersicherheitsanforderungen der Funkanlagenrichtlinie erfassen nur Geräte mit Funkschnittstelle und beruhen auf der Erklärung des Herstellers und die Branchenempfehlung zum Netzanschluss beschränkt sich auf Passwortschutz und Updates. Wirksam sind Instrumente, die

[87] Secura, «Cybersecurity threats and measures for the solar power sector», 2024: https://www.energy-innovation.nl/documents/1299/2024-Secura_Report-Cybersecurity_threats_and_measures_for_the_solar_power_sector.pdf
[88] Swissgrid AG, White Paper «Systemverträgliche Integration Photovoltaik», März 2026: https://www.swissgrid.ch/de/home/newsroom/blog/2026/20260330-01.html

nicht am einzelnen Betreiber ansetzen. Regulatorische Eingriffe sind hier voraussichtlich nötig, weil diese Absicherung nicht von selbst entsteht. Als Ansätze bieten sich Modelle an, die andere Staaten bereits nutzen: Netzanschlussbedingungen für die Steuerbarkeit von Anlagen (wie in Litauen) oder Beschaffungs- und Förderkriterien (wie auf EU-Ebene). Keiner dieser Wege ist perfekt (vgl. Kapitel *7*). Dieser Handlungsbedarf ergibt sich nicht nur aus den technischen Befunden. Der NDB weist ausdrücklich darauf hin, dass die Schweiz als Ziel an Attraktivität gewinnt, wenn die Nachbarstaaten ihre kritische Infrastruktur stärker schützen und die Schweiz nicht gleichzieht (vgl. Kapitel *2.5*).

Steuerhoheit über netzrelevante Funktionen sichern: Ziel ist nicht ein Verbot der Cloud, sondern eine klare Antwort auf die Frage, wer einer Anlage netzrelevante Befehle erteilen darf. Diese Befugnis sollte bei einer Stelle liegen, die selbst reguliert ist und für die Netzstabilität einsteht: beim Verteilnetzbetreiber oder bei einem vertraglich gebundenen Aggregator, der dem IKT-Minimalstandard untersteht. Dasselbe Modell empfiehlt der europäische Branchenverband, der zwischen kritischen und nicht-kritischen Funktionen unterscheidet: Starten, Stoppen und das Verändern von Wirk- und Blindleistung nur über die regulierte Stelle, Überwachung und Software-Updates auch über andere Kanäle, sofern sich diese im Verdachtsfall unterbrechen lassen.[89] Für die Schweiz ist dieser Grundsatz im Ansatz bereits angelegt: Der Verteilnetzbetreiber darf die Flexibilität einer Anlage nur netzdienlich nutzen.[90] Swissgrid weist zugleich auf die praktischen Lücken hin:[91] Es fehlen eine standardisierte Kommunikation zwischen Anlage beziehungsweise Energiemanagementsystem und Verteilnetzbetreiber, eine standardisierte Kaskadierung zwischen den Netzbetreibern sowie die technische Umsetzung der gesetzlichen Regel, wonach die garantierte netzdienliche Flexibilität alle übrigen Steuersignale übersteuert. Wer die Steuerhoheit verbindlich regeln will, muss deshalb auch die Schnittstelle dafür schaffen. Ohne sie bleibt der Weg über die Herstellercloud der einzige, der in der Praxis funktioniert. Zu klären bleibt, ob eine dauerhafte Anbindung an eine Herstellercloud netzseitig überhaupt erforderlich ist und, falls ja, welche Anforderungen diese Infrastruktur erfüllen muss. Der blosse Hosting-Standort genügt dafür nicht (vgl. Kapitel *5.4.5*). Geräteseitig umsetzbar wäre die Vorgabe, dass Wechselrichter eine Steuerungssperre für netzrelevante Funktionen ab Werk aktiv haben (vgl. Kapitel *8.4.2*). Diese Richtung deckt sich mit der Position des deutschen BSI (vgl. Kapitel *7.3.1*).

Eine Zuständigkeit für das Summenrisiko benennen: Für die einzelne Kleinanlage ist niemand verantwortlich, und für das Risiko, das erst aus der Summe vieler Anlagen entsteht, fehlt eine benannte Stelle. Zu klären ist, welche Stelle dieses aggregierte Risiko beobachtet, im Ereignisfall koordiniert und die Wirksamkeit der produkt- und anschlussseitigen Massnahmen überwacht.

Für den Ereignisfall vorsorgen: Neben der Vorbeugung braucht es die Fähigkeit, einen laufenden Missbrauch zu erkennen und geordnet zu beenden. Einen zentralen Notausschalter gibt es nicht, und eine defensive Massenabschaltung würde selbst die Stabilität des Netzes gefährden. Ein kompromittierter Steuerkanal lässt sich nur gefahrlos trennen, wenn die Anlagen dann in einen sicheren, netzkonformen Zustand fallen (vgl. Kapitel *8.4.2*) und eine benannte Stelle das Lagebild führt und die Beteiligten koordiniert. Die Fähigkeit dient vor allem der Abwehr anhaltender Kompromittierung und der Bewältigung nach einem Vorfall, nicht der Verhinderung des ersten, in Sekunden ablaufenden Angriffs.

8.5.2 Reichweite eines einzelnen Zugriffs

Reichweite eines einzelnen Zugriffs begrenzen: Netzrelevant ist nicht die Schwere einer Schwachstelle, sondern ihre Reichweite. Daraus folgt eine Massnahme, die unabhängig von Marktanteilen und Produktqualität wirkt: Kein einzelner Punkt soll eine ganze Geräteflotte gleichzeitig verändern können. In der klassischen Erzeugung ergab sich diese Grenze von selbst, weil ein Kraftwerk selten mehr als rund 1,5 Gigawatt umfasst und sein Leitsystem nur dieses eine Kraftwerk erreicht. Mit Herstellerclouds und Aggregatoren entfällt sie. Der europäische

[89] SolarPower Europe / DNV: «Solutions for PV Cyber Risks to Grid Stability», 2025: https://www.solarpowereurope.org/insights/thematic-reports/solutions-for-pv-cyber-risks-to-grid-stability
[90] Art. 17c StromVG (SR 734.7) und Art. 19a StromVV (SR 734.71). Zur Einordnung: VSE, «Potenzial und Limiten der neuen Flexibilitätsregulierung», Dezember 2025: https://www.strom.ch/de/perspective/potenzial-und-limiten-der-neuen-flexibilitaetsregulierung
[91] Swissgrid AG, White Paper «Systemverträgliche Integration Photovoltaik», März 2026: https://www.swissgrid.ch/de/home/newsroom/blog/2026/20260330-01.html

Branchenverband schlägt deshalb vor, sie ausdrücklich vorzugeben und technisch zu unterlegen:[92]

- eine Obergrenze für die Erzeugungsleistung, die sich über ein einziges Steuerungssystem ansprechen lässt: wer mehr betreibt, muss dafür getrennte Systeme ohne gemeinsame Ausfallursachen verwenden
- eine Segmentierung des herstellereigenen Fernzugangs, sodass sich nicht die gesamte Flotte auf einmal steuern lässt
- technische Vorkehrungen gegen die gleichzeitige Aktualisierung aller Geräte, damit Zeit für ein Eingreifen bleibt, wenn ein Update fehlerhaft oder manipuliert ist
- geräteindividuelle Zufallsverzögerungen für ausgewählte Steuerbefehle. Welche Befehle betroffen sind und wie lange verzögert wird, ist über Normen und in Abstimmung mit dem Netzbetrieb festzulegen

Diese Massnahmen verlangen keinen Verzicht auf Fernsteuerung und keine Veränderung der Marktanteile. Sie begrenzen nur, wie viel ein einzelner Befehl bewirken kann. Drei Vorbehalte gehören dazu: Der Schwellenwert ist offen und müsste erst festgelegt werden. Die Umsetzung liegt in der Architektur des Herstellers und ist von aussen kaum überprüfbar, bleibt ohne Nachweispflicht also eine Selbstdeklaration. Und sie begrenzt die Reichweite, nicht die Abhängigkeit selbst: Ein segmentierter Fernzugang verschafft im Ereignisfall Zeit zum Eingreifen, lässt den Hersteller aber weiterhin Kontrolle über jedes einzelne Segment behalten.

Diversifizierung rechtzeitig fördern: Der Wechselrichter-Markt konsolidiert sich stark. Für die Cybersicherheit ist das unmittelbar relevant, denn ein heterogenes Herstellerfeld ist selbst ein Schutzfaktor: Unterschiedliche Hersteller, Plattformen und Firmware-Stände erschweren es, viele Anlagen mit einem einzigen Angriff zu erreichen. Umgekehrt entsteht mit jeder weiteren Marktkonsolidierung ein grösserer «Single Point of Failure». Ziel sollte deshalb sein, dauerhaft Hersteller in mehreren Weltregionen zur Auswahl zu haben, und nicht die Bevorzugung einer bestimmten Herkunft. Instrumente sind etwa Beschaffungskriterien, die Mehr-Anbieter-Strategien belohnen. Der Punkt berührt Beschaffungs- und Handelsrecht und ist nur begrenzt einseitig umsetzbar. Das Zeitfenster könnte sich verengen, weil mehrere Anbieter zwar noch Kapazität haben, aber Marktanteile verlieren. Wie sich das entwickelt, ist offen. Diversifizierung senkt das Risiko eines einzigen, herstellerübergreifenden Exploits, löst aber das strukturelle Kernproblem nicht: Bei einer Schwelle von unter zwei Prozent des europäischen Bestands (vgl. Kapitel *6.5)* bleibt praktisch jeder marktrelevante Hersteller allein systemrelevant. Laut Secura genügt in den Niederlanden der Angriff auf einen einzelnen Hersteller; zwei kommen dafür nach Marktanteil in Frage (vgl. Kapitel *5.4*). Diversifizierung ist deshalb eine sinnvolle Ergänzung, aber kein Ersatz für die übrigen hier genannten Massnahmen.

8.5.3 Überprüfung und Nachrüstung des Bestands

Produktprüfung mit Lebenszyklus-Komponente: Ein produktbezogenes Cybersicherheits-Prüfregime für Wechselrichter und Energiemanagementsysteme ist möglich und sinnvoll. Taiwan zeigt mit Quellcode-Analyse, Verkehrsanalyse und Firmware-Integritätsprüfung, wie tief eine solche Prüfung gehen kann. Entscheidend ist jedoch, dass ein solches Regime nicht bei einer einmaligen Typenprüfung stehen bleibt: Nötig sind ein vorgeschriebenes kryptografisches Update-Verfahren und eine Nachprüfung bei wesentlichen Firmware-Änderungen. Zu beachten ist die Grenze jeder Produktprüfung: Sie adressiert die Angreifbarkeit durch Dritte, macht aber nicht unabhängig vom Hersteller selbst. Gegen das Szenario des Insider- oder Staatsakteurs, der die legitime Update-Kette kontrolliert, wirken nur Diversifizierung und eine technische Begrenzung dessen, was die Cloud fernsteuern darf (vgl. Kapitel *5.2*).

Nicht alles davon setzt neues Recht voraus. Für Wechselrichter mit Funkschnittstelle liesse sich die Konformität mit den Cybersicherheitsanforderungen der Funkanlagenrichtlinie und der zugehörigen Norm EN 18031 bereits heute im Rahmen der Marktüberwachung prüfen (vgl. Kapitel 7.4 Regulierung in der Schweiz). Produktbezogene Prüfregime für diese Geräteklasse entstehen

[92] SolarPower Europe / DNV: «Solutions for PV Cyber Risks to Grid Stability», 2025: https://www.solarpowereurope.org/insights/thematic-reports/solutions-for-pv-cyber-risks-to-grid-stability

zudem international: Neben der taiwanischen Typenzulassung bestehen mit UL 2941[93] und der Zertifizierung der SunSpec Alliance Programme[94], an die sich eine schweizerische oder europäische Anforderung anlehnen könnte.

Die bestehende Anlagenkontrolle für die Cybersicherheit nutzen: Photovoltaikanlagen sind nach der Niederspannungs-Installationsverordnung kontrollpflichtig. Ein unabhängiges Kontrollorgan prüft die Anlage nach der Erstellung, der Sicherheitsnachweis geht an die Netzbetreiberin, und die Kontrolle wiederholt sich periodisch. Damit besteht ein obligatorisches Verfahren, das die Anlage im installierten Zustand erfasst und dessen Ergebnis bei einer regulierten Stelle landet. Es setzt dort an, wo Produktanforderungen und Vorgaben an die einzelne Betreiberin nicht hinreichen. Es wird empfohlen, das zugehörige Prüfprotokoll um wenige eindeutig feststellbare Punkte zu ergänzen: z.B. geänderte Standardpasswörter, keine Erreichbarkeit aus dem Internet, deaktivierte nicht benötigte Schnittstellen und der Zustand der Steuerungssperre (vgl. Kapitel *8.4.2*). Swissgrid schlägt denselben Weg für die betrieblichen Einstellungen vor und verlangt für die Cybersicherheit gesondert Mindestanforderungen, die auch kontrolliert werden müssen, ohne ein Verfahren dafür zu nennen.[95] Nötig ist dafür eine Anpassung der Vorgaben, allerdings an einem eingespielten Verfahren statt in einem neuen Regime, und prüfbar bleibt nur, was sich ohne Interpretationsspielraum feststellen lässt.

Den Bestand nicht vergessen: Alle vorstehenden Massnahmen wirken vor allem über Neuanlagen. Einzig die periodische Anlagenkontrolle erreicht auch den Bestand, allerdings langsam. Der bestehende Anlagenpark bleibt über Jahre die grössere offene Flanke (vgl. Kapitel *7.3.4*). Umsetzbar wäre dort eine vorgeschaltete Kommunikationseinheit, die mit bestehenden Wechselrichtern zusammenarbeitet und die Steuerung dem Netzbetreiber zuordnet. Sie überträgt damit auf den Bestand, was Kapitel *8.5.1 Zuständigkeit* vorschlägt.

Gemeinsam ist all diesen Empfehlungen eine Richtung: Die Photovoltaik soll weiterwachsen, aber die Kontrolle über hunderttausende netzrelevante Geräte darf nicht bei wenigen Stellen liegen, deren Eingriffe technisch unbegrenzt und von aussen nicht überprüfbar sind. Das Zeitfenster dafür ist offen. Es schliesst sich mit jeder Anlage, die heute gebaut wird und in zwanzig Jahren noch am Netz hängt.

[93] UL Solutions: UL 2941, Outline of Investigation for Cybersecurity of Distributed Energy and Inverter-Based Resources, 2023; Zertifizierungsprogramm seit Februar 2026: https://www.ul.com/services/cybersecurity-distributed-energy-and-inverter-based-resources
[94] SunSpec Alliance: DER Device Cybersecurity Certification: https://sunspec.org/certifications/
[95] Swissgrid AG, White Paper «Systemverträgliche Integration Photovoltaik», März 2026: https://www.swissgrid.ch/de/home/newsroom/blog/2026/20260330-01.html