Nationales Testinstitut für Cybersicherheit

MEDIENMITTEILUNG
Summarischer Bericht zur Cybersicherheit von Photovoltaikanlagen

Systemrelevante Photovoltaikanlagen: NTC legt umfassende Cybersicherheitsanalyse mit konkreten Empfehlungen vor

Zug, 17. September 2026 – Photovoltaikanlagen sind für die Schweizer Stromversorgung systemrelevant geworden. Ende 2025 waren in der Schweiz rund 338'000 netzverbundene Photovoltaikanlagen installiert. Das Nationale Testinstitut für Cybersicherheit NTC hat vor diesem Hintergrund aus eigener Initiative weit verbreitete Systeme in der Schweiz geprüft. Insgesamt sieben Wechselrichter und vier Energiemanagementsysteme wurden einer tiefgreifenden Analyse unterzogen. Dabei konnten über 50 Befunde identifiziert werden, darunter sieben kritische und sechs hohe. Die Befunde wurden den Herstellern vertraulich gemeldet. Die meisten reagierten rasch, während die Behebung der Schwachstellen bei einigen Produkten noch im Gange ist.

Ergebnisse der Sicherheitsanalyse und zentrale Risikomuster

Um das Sicherheitsniveau der in der Schweiz verbreiteten Photovoltaik-Technik zu beurteilen, hat das NTC im Laufe eines Jahres elf Produkte einer umfassenden technischen Sicherheitsanalyse unterzogen: sieben Wechselrichter und vier Energiemanagementsysteme von insgesamt acht Herstellern, darunter die marktbestimmenden Anbieter.

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 eingeschleusten Programmcode, teils über einen ungenügend geschützten Wartungszugang des Herstellers.

Wiederkehrend traten vier Risikomuster auf: Mängel bei Authentifizierung und Zugriffskontrolle, etwa Standardpasswörter; unsichere Wartungszugänge mit identischen Zugangsdaten für die ganze Geräteflotte; fehlende oder schwache Verschlüsselung der Kommunikation über lokale Schnittstellen; sowie Schnittstellen, die sich nicht deaktivieren lassen. Bei nahezu allen geprüften Wechselrichtern liess sich über die lokale Steuerschnittstelle ohne Anmeldung verändern, wie viel Leistung die Anlage einspeist, bis hinunter auf null.

Das Sicherheitsniveau der einzelnen Produkte ist dabei nicht schlechter als bei anderen weitverbreiteten vernetzten Geräten, die das NTC bereits geprüft hat. Hinweise auf absichtlich eingebaute Hintertüren fanden sich keine, und die meisten Hersteller reagierten rasch auf die gemeldeten Schwachstellen. Was Solaranlagen von anderen vernetzten Geräten unterscheidet, ist nicht die Produktqualität, sondern ihre Rolle: In ihrer Summe sind sie für das Stromnetz systemrelevant. An sonnigen Tagen decken sie zur Mittagszeit regelmässig über die Hälfte des momentanen Stromverbrauchs.

Massgebend für die Netzrelevanz eines Befunds ist dabei nicht seine Schwere allein, sondern seine Reichweite. Die einzelne Solaranlage auf einem Wohn- oder Gewerbedach bleibt für das Stromnetz bedeutungslos: Fällt sie aus oder wird sie manipuliert, ändert dies am Gesamtsystem nichts. Zum Risiko wird die Tatsache, dass viele dieser Anlagen über die Clouds der Hersteller angebunden sind und über diesen Weg zum Beispiel mit Aktualisierungen der Firmware versorgt werden. Sechs der Befunde wirken über eine solche zentrale Instanz auf einen ganzen Gerätebestand und damit potenziell auf Tausende Anlagen gleichzeitig. «Nicht die Schwere einer Schwachstelle allein macht sie gefährlich, sondern ihre Reichweite», sagt Tobias Castagna, Leiter Testexperten beim NTC. «Bei Photovoltaikanlagen kann ein einzelner Befund in einer zentralen Komponente Tausende Anlagen gleichzeitig betreffen – deshalb braucht es hier gezielte, aber machbare Gegenmassnahmen.»

Empfehlungen zur Risikominimierung

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

Auf Basis der mit dieser Untersuchung gewonnenen Erkenntnisse hat das NTC für fünf Adressatengruppen Empfehlungen für Massnahmen zur Reduktion von Cyberrisiken bei Photovoltaikanlagen formuliert:

- **Betreiberinnen und Betreiber von Kleinanlagen:** Wahl eines etablierten Anbieters, Bestätigung individueller Passwörter bei der Übergabe und vertragliche Klärung der Zuständigkeit für Updates
- **Betreiber grösserer Anlagen:** Inventarisierung von Schnittstellen und Fernzugriffen, Netztrennung sowie Sicherheitsanforderungen in Ausschreibungen
- **Installationsbetriebe**: individuelle Zugangsdaten pro Anlage, keine direkte Erreichbarkeit aus dem Internet, Trennung vom übrigen Netz und eine dokumentierte Übergabe
- **Hersteller:** Sicherheit als Konstruktionsprinzip – individuelle Zugangsdaten, signierte Firmware-Updates, zeitlich begrenzte und widerrufbare Wartungszugänge sowie eine werkseitige, nur vor Ort aufhebbare Sperre der netzrelevanten Fernsteuerung
- **Politik und Behörden:** Mindestanforderungen für das Inverkehrbringen von Wechselrichtern und Energiemanagementsystemen, Sicherheitsanforderungen als Bedingung für den Netzanschluss sowie eine benannte Zuständigkeit für das Risiko aus der Summe der Kleinanlagen

Eine einfache und vollständige Lösung gibt es nicht; alle Ansätze haben Vor- und Nachteile, und diese Empfehlungen decken nicht die gesamte Bandbreite möglicher Massnahmen ab. Aber jede der hier genannten Massnahmen, die umgesetzt wird, erhöht die Cybersicherheit.

Die Untersuchung erfolgte auf Initiative des Nationalen Testinstituts für Cybersicherheit NTC, das auch das Prüfteam und einen wesentlichen Teil der finanziellen Mittel aufbrachte. Finanziell unterstützt wurde die Untersuchung durch EnergieSchweiz. Mehrere Organisationen, mehrheitlich aus der Energiebranche, stellten Testgeräte bereit und beteiligten sich an den Kosten.

Das NTC dankt allen beteiligten Organisationen sowie EnergieSchweiz für ihre Unterstützung. Um die Unabhängigkeit der Resultate zu gewährleisten, nahmen weder die Hersteller noch die unterstützenden Organisationen Einfluss auf Auswahl, Prüfumfang oder Ergebnisse; die Hersteller wurden erst im Rahmen der vertraulichen Meldung zur Behebung der Schwachstellen kontaktiert.

Summarischer Bericht Photovoltaik

Medienkontakt:
Andreas W. Kaelin, Geschäftsführer
+41 41 317 00 11, andreas.kaelin@ntc.swiss

Über das Nationale Testinstitut für Cybersicherheit NTC
Das Nationale Testinstitut für Cybersicherheit NTC trägt zur Sicherheit und zur digitalen Souveränität der Schweiz bei, indem es kritische Schwachstellen von digitalen Produkten und Risiken neuer Digitaltechnologien vorausschauend erkennt und deren Mitigation unterstützt. Als gemeinnütziger Verein mit Sitz in Zug folgt das NTC den Prinzipien der Unabhängigkeit und Objektivität. Das NTC testet auf eigene Initiative digitale Produkte und Anwendungen, die in der Schweiz nicht hinreichend getestet werden, jedoch für Wirtschaft und Gesellschaft von grosser Bedeutung sind. Ebenso führt das NTC Cybersicherheitsprüfungen im Auftrag von Betreibern kritischer Infrastrukturen und Behörden durch. https://www.ntc.swiss