TAGESSPIEGEL
BACKGROUND

Energie & Klima

Netzaufsicht sieht Cybergefahr für die Photovoltaik

Photovoltaikanlagen bieten Hackern ein potenzielles Einfallstor zur Manipulation des Stromnetzes. Das zeigen eine Reihe von Expertenberichten, die auch die Bundesnetzagentur alarmieren. Sie sieht ein steigendes Sicherheitsrisiko und empfiehlt, auch dezentrale PV-Anlagen als kritische Infrastruktur einzustufen.

von **Oliver Ristau**

veröffentlicht am 05.09.2024

Bei der **Photovoltaik** schaut mittlerweile auch das **FBI** genau hin. Anfang Juli *warnte (https://s3.documentcloud.org/documents/24788637/fbiwarning.pdf)* die US-Sicherheitsbehörde, dass der Ausbau der erneuerbaren Energien das Risiko für kriminelle **Cyberattacken** erhöht. Sie identifizierte eine Reihe von Sicherheitslücken, über die Cyberangreifer die Anlagen aus der Ferne steuern können und empfiehlt Gegenmaßnahmen.

Damit ist das FBI nicht allein. Auch die Cybersicherheitsdienstleister **Trendmicro** und **Bitdefender** legten in diesem Jahr Analysen zur Anfälligkeit von PV-Anlagen gegenüber **Cyberangriffen** vor. Zuletzt hatte das niederländische Fachinstitut **DIVD** (Dutch Institute for Vulnerability Disclosure) Sicherheitslücken bei Gateways des US-amerikanischen Herstellers **Enphase Energy**

entdeckt(https://www.divd.nl/newsroom/articles/divd-responsibly-discloses-six-new-zero-day-vulnerabilities-to-vendor/).

Gateways sind die Übergänge ins Datennetz. An dieser Stelle könnten Cyberkriminelle die Kontrolle über die Wechselrichter und die angeschlossenen Solarsysteme übernehmen. Die Gefahr bestehe zwar nur bei unsicheren Netzwerken, so DIVD. Doch das sei **trotzdem für die Sicherheit des Stromsystems im Ganzen gefährlich** – insbesondere je umfangreicher die Energiewende werde. Die Organisation hatte die Probleme vor Veröffentlichung mit Enphase besprochen. Das Unternehmen habe die Sicherheitslücken mittlerweile behoben, so DIVD.

Bundesnetzagentur: „Das Risiko wächst“

Was durchaus im Sinne des Energiemarktes sein kann – nämlich die Steuerung der PV-Anlagen via Internet – stellt ein **zunehmendes Sicherheitsrisiko** dar, das auch der **Bundesnetzagentur** zu denken gibt. „Wiederkehrende Hinweise auf Sicherheitslücken in unterschiedlichen Produkten (PV-Wechselrichter, PV-Batteriesysteme, usw.) sind **Anlass zur Sorge**“, teilte ein BNetzA-Sprecher auf Anfrage mit. Zwar lasse die Heterogenität der Produkte, Hersteller, Softwareversionen und Betreiber die koordinierte Steuerung einer **ausreichenden Menge kleinerer Anlagen** durch Angreifer derzeit noch unwahrscheinlich erscheinen. „Doch das Risiko wächst.“

Im schlimmsten Fall könnten PV-Hacks **Blackouts** oder **Brownouts** auslösen, so die Behörde gegenüber Tagesspiegel Background. Bei letzteren handelt es sich um kontrollierte, regionale Stromabschaltungen. Voraussetzung einer solchen Wirkung sei der Zugriff auf eine elektrische Leistung in einer **ausreichenden Größenordnung**. Wie viel PV-Kapazität Cyberangreifer dafür in ihre Gewalt bringen müssten, wollte der Sprecher nicht konkret benennen. „Das hängt von vielen Parametern ab wie Ort des Anschlusses, Situation im Netz, Tageszeit, Netzzustand und Geschwindigkeit der Steuerung.“

Auch der Branchenverband **Solar Power Europe** (SPE) ist in Sorge. Der Solarsektor, aber auch andere Bereiche der dezentralen Stromerzeugung sind nach seiner Einschätzung unzureichend geschützt. Cyberangriffe nähmen zu und könnten zu einem **Element der modernen Kriegsführung** werden, warnte SPE im Juli (Tagesspiegel Background *berichtete(https://background.tagesspiegel.de/energie-und-klima/briefing/solarparks-verwundbar-fuer-cyberangriffe)*). Bisherige EU-Maßnahmen im Rahmen des Net-Zero Industry Act, der NIS2-Richtlinie, des Cyber Resilience Act (CRA) und der CER-Richtlinie zum Schutz kritischer Einrichtungen reichten nicht aus, warnte die Organisation und forderte eine **Solarsektor-spezifische Sicherheitsstrategie**.

Kleine, verteilte Anlagen als Kritische Infrastruktur

Die BNetzA schlägt zur Risikominderung vor, Sicherheitskriterien für die **Kritische Infrastruktur** auch auf die **dezentrale Energieerzeugung** auszuweiten. Die Ampel-Koalition arbeitet an einem **Kritis-Dachgesetz**, das auch Energieinfrastrukturen abdecken wird. Das Gesetz zur Umsetzung der EU-Richtlinie **NIS2** soll derweil regeln, wie Deutschland den Schutz von Unternehmen – auch des Energiesektors – gegen Cyberangriffe verbessert. Aus dem entsprechenden Gesetzentwurf geht hervor, dass die im **Energiewirtschaftsgesetz** verankerten Sicherheitsanforderungen nicht mehr nur für Netzbetreiber gelten sollen, sondern auch für Betreiber von **Energieanlagen** und deren **Zuliefererketten** (Tagesspiegel Background *berichtete(https://background.tagesspiegel.de/energie-und-klima/briefing/cybersicherheit-soll-standard-werden)*).

Unter die Vorgaben für Kritische Infrastruktur fallen bisher lediglich größere Energieerzeugungseinheiten ab einer Leistung von **104 Megawatt**. Dazu zählen neben großen Kraftwerken auch Direktvermarkter, die beispielsweise **Photovoltaikanlagen bündeln** und dabei eine Leistung in der Größenordnung von 104 MW erreichen. Die Betreiber müssen laut Paragraf 11 (1b) des Energiewirtschaftsgesetzes „einen angemessenen Schutz gegen

Bedrohungen für Telekommunikations- und elektronische Datenverarbeitungssysteme […] gewährleisten, die für einen sicheren Anlagenbetrieb notwendig sind“. Die BNetzA habe dazu in Abstimmung mit dem **Bundesamt für Sicherheit in der Informationstechnologie** (BSI) einen **Sicherheitskatalog erarbeitet**, teilte das BSI auf Anfrage mit. Der besteht aus einer Reihe von Sicherheitsnormen und -vorkehrungen, die alle per Zertifikat nachzuweisen sind.

Künftig sollten die „technischen und organisatorischen Maßnahmen der IT-Sicherheitskataloge nicht nur von Betreibern großer Anlagen, sondern auch von Herstellern und Inverkehrbringern von **PV-Anlagen, PV-Batterie-Systemen, Home-Energy-Management-Systemen, Wärmepumpen oder Ladesäulen** eingehalten“ werden, findet die Behörde. Das gelte auch „für digitale Energiedienste wie virtuelle Kraftwerksbetreiber, Fernwartungsdienstleister und Energiehandelsplattformen“. Damit würden vor allem Hersteller verpflichtet werden, ihre Produkte cyberfest zu machen.

Mit PV-Hack die USA steuern

Dass dies bisher vielfach nicht der Fall ist, hat Anfang August das Cybersecurity-Unternehmen Bitdefender in einer *Analyse(https://www.bitdefender.com/blog/labs/60-hurts-per-second-how-we-got-access-to-enough-solar-power-to-run-the-united-states/)* öffentlich gemacht. Diese hatte ernste Sicherheitsgefahren bei Wechselrichtern des chinesischen Herstellers **Deye** in Kombination mit der Monitoring- und Steuerungsplattform **Solarman** festgestellt. Die Cyberspezialisten haben darüber laut eigenen Angaben auf ausreichend große PV-Kapazitäten Zugriff bekommen, „um die USA zu steuern“.

Zuvor hatte das Sicherheitsunternehmen Trendmicro auf **Sicherheitsprobleme von PV-Produzenten** *hingewiesen(https://www.trendmicro.com/de_de/about/newsroom/press-releases/2024/20240124-solarenergie-und-cybersecurity-sicherheitsrisiken-bei-dezentraler-stromerzeugung.html)*. Von den untersuchten Produkten der Hersteller Enphase, Outback, Phocos,

Sol-Ark und Victron seien lediglich bei zweien keine Sicherheitslücken festgestellt worden. Vor Veröffentlichung ihrer Ergebnisse hatten Bitdefender und Trendmicro die Hersteller informiert, die die Probleme demnach mittlerweile gelöst haben.

Zu den größten Risikoquellen zählen **leicht zu erratende Passwörter** und eine **fehlende Verschlüsselung** bei der Datenübertragung. Laut Trendmicro kann aber auch die Sicherheitsarchitektur der großen Cloudanbieter wie beispielsweise **Amazon**, **Microsoft** und **Alibaba** zum Problem werden. Denn viele zentrale **PV-Daten** fließen über deren Server. Wer also in der Lage ist, solche Großrechner zu knacken, könnte Zugriff auf eine Anlagengröße erhalten, die am Ende zu Brown- und Blackouts führen kann.