Gehackt: Cyberkriminelle greifen SmartHome mit Solaranlagen an und können das gesamte Stromnetz lahm legen

geschrieben von Andreas Demmig | 11. September 2024

StopTheseThings

Die weit verteilte Mikrostromerzeugung durch Solaranlagen, nicht nur auf Hausdächern, erhöht die Anfälligkeit der Stromnetze. Cyberkriminelle (auch Hacker genannt) testen diese Art von Anfälligkeit oft als eine Art sportliche Herausforderung.

Böswillige staatliche Akteure sind darauf aus, dies als Auftakt zu einem Krieg zu tun. Wenn Sie ein Stromnetz lahmlegen, tappt Ihr (und nun machtloser) Feind buchstäblich im Dunkeln.

Wie das Team von Jo Nova weiter unten berichtet, war es für Hacker (seien es nun einzelgängerische Streber oder uniformierte Typen mit Bürstenhaarschnitt) dank Solaranlagen auf Hausdächern noch nie so einfach, ein ganzes Stromnetz zu (zer-) stören.

Cyberbedrohung der Solar-Wechselrichter: Niederländischer Hacker greift 4 Millionen Module in 150 Ländern an

Jo Nova Blog, 20. August 2024

Was wäre, wenn ein paar Gigawatt Solarstrom ohne Vorwarnung oder eine Wolke am Himmel verschwinden würden?
Stellen Sie sich vor, eine feindliche Macht hätte zur Mittagszeit die Kontrolle über die Hälfte Ihrer nationalen Stromerzeugung und könnte Sie mit einem einzigen Schalter in die Knie zwingen? Oder wie wäre es mit einem Verbrechersyndikat, das bis 17 Uhr ein Lösegeld verlangt?

Steve Milloy: Das kommunistische China bereitet uns auf eine Katastrophe durch Solarmodule vor:

> *„Solarmodule, die den Strom für das Stromnetz bereitstellen und normalerweise mit dem Internet verbunden sind, können „leicht gehackt, aus der Ferne deaktiviert oder für DDoS-Angriffe [Distributed Denial of Service] verwendet werden.“ DDoS ist eine der häufigsten Angriffsarten, die im Grunde versuchen, ein System zu überlasten… Solarmodule wurden in mehreren Szenarien als Schwachstelle herausgestellt, auch aufgrund der Dominanz eines*

> *einzelnen Landes, China, in der Lieferkette.“*

Es ist nur eine Woche ohne Strom…

Daniel Croft, ***CyberDaily (Oktober 2023)***

> Rachael Falk, Geschäftsführerin des Cyber Security CRC, sagte, dass ein Angriff auf das Solarstromnetz einen „Schwarzstart“ auslösen könnte. … *„Dies könnte das gesamte Stromnetz zum Absturz bringen und es könnte eine Woche dauern, bis es sich davon erholt hat“*.

[Frau Falk sagte,] die Bedrohung durch im Ausland hergestellte Solarwechselrichter sei neu, da aufgrund des gestiegenen Interesses an Smart-Home-Technologie nur aktuelle Modelle mit dem Internet verbunden seien.

> *„Traditionell war das Cyberrisiko bei Solarwechselrichtern gering [vor allem der mit geringer Leistung], da sie nicht mit dem Internet verbunden waren. … Mit der zunehmenden Beliebtheit intelligenter Energiesysteme für Privathaushalte hat sich dies jedoch geändert, und die meisten Solarwechselrichter sind heute mit dem Internet verbunden.“*

Sowohl die EU als auch die USA haben in den letzten Wochen einen Weckruf erhalten.

Ein **niederländischer White-Hat-Hacker hat sich** [Firmenangestellter, der seine Erkenntnisse dem niederländischem Institut für die Offenlegung von Schwachstellen meldete] vor ein paar Wochen Zugang zu einem System mit 4 Millionen Panels in 150 Ländern verschafft und dabei einen schwerwiegenden Fehler aufgedeckt. Der Softwarefehler in den amerikanischen Enphase– Wechselrichtern wurde schnell behoben, nachdem er bekannt wurde, aber wie viele andere Schwachstellen bleiben noch offen?

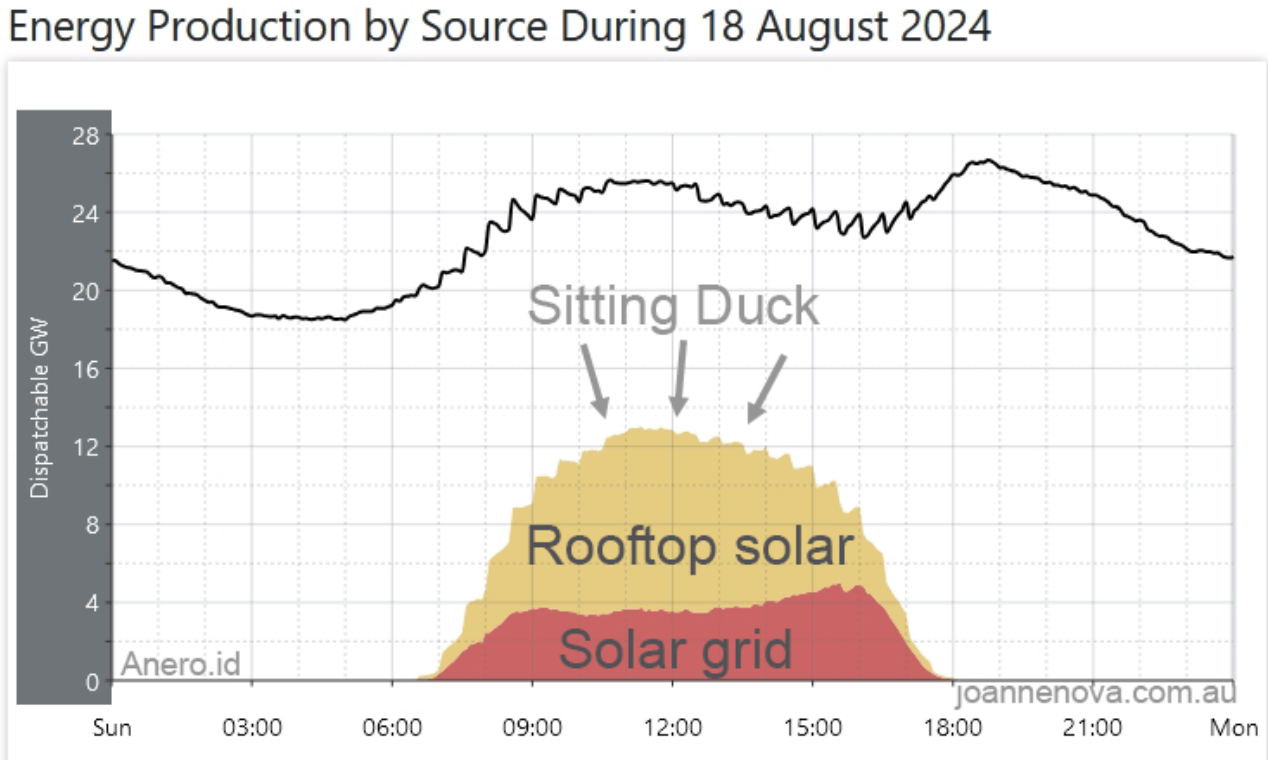
Erst vor zwei Wochen behauptete eine andere Gruppe namens Bitdefender, dass 20 % der weltweiten Solarmodule und 195 Gigawatt Leistung seit Monaten durch Cyberkriminalität gefährdet seien. Die Solarmanagement-Software für Dächer von Solarman und Deye (beides chinesische Solarhersteller) wird von 2 Millionen „Solaranlagen“ und 10 Millionen Geräten verwendet. Hacker hätten die Kontrolle über die Wechselrichter übernehmen können (was „die Art und Weise verändern könnte, wie die Wechselrichter mit dem Netz interagieren). Sie könnten auch eine ganze Menge Daten stehlen, darunter GPS-Standorte und -Produktion in Echtzeit. Was wäre, wenn sie Einzelpersonen ins Visier nehmen könnten?

> **Diese Probleme wurden** offenbar schon im Mai gemeldet, sind jetzt aber auch gepatcht. (Ich schätze, niemand würde Probleme erwähnen, für die es keine Patches gibt, oder?) **SecurityBrief** enthält die

grausamen Einzelheiten.

Welche Bedrohungen auch immer in den Niederlanden bestehen, Australien ist eine leichte Beute.

Sogar zur Mittagszeit im Winter wird manchmal die Hälfte des australischen Stroms aus Solarmodulen gewonnen. Das sind 12 Gigawatt Solarstrom von insgesamt 25 Gigawatt. (Und **in WA ist es ähnlich** .) Hier im Crashtest-Dummy für erneuerbare Energien **stammen ganze 58 % der mit dem Internet verbundenen Solarwechselrichter von Unternehmen mit Sitz in China**. (Und der Rest hat seinen Sitz woanders, aber wer weiß, vielleicht werden sie auch in China hergestellt, wo 70 % der Solarwechselrichter der Welt herkommen?)



Solarenergie macht einen großen Teil des australischen NEM aus, sogar im Winter. Die schwarze Linie stellt die Gesamterzeugung dar. Das NEM umfasst NSW, QLD, Vic, Tasmanien und SA. **(Quelle: Anero.id)**

Cyberexperte Falk warnte uns also im Oktober letzten Jahres vor einem Schwarzstart-Desaster – und wie weit sind wir gekommen? Im Januar überarbeiteten wir unsere Cybersicherheitspläne, **vergaßen dabei aber irgendwie immer noch Smart-Home-Geräte** wie Solarwechselrichter und die Steuerung unserer nationalen kritischen Infrastruktur. Aber keine Sorge, im Februar bekamen wir die Nachricht, dass wir Standards Australia damit beauftragen würden, **einen „Fahrplan“ zu entwickeln** . (Das wird sie aufhalten!) In der Zwischenzeit arbeiten wir weiterhin mit Hochdruck an Solaranlagen.

> Wir können uns immer darauf verlassen, dass die Regierung ~~nichts erledigt~~, … dem Feind hilft …!?

White-Hat-Hacker macht auf Schwachstellen in europäischen Solarmodulen aufmerksam

Von Nikolaus J. Kurmayer | *Euraktiv*

Ein ethischer Hackerangriff auf Solarmodule in den Niederlanden hat deren Anfälligkeit für Cyberangriffe offenbart und die Industrie dazu veranlasst, strengere Sicherheitsbewertungen zu fordern.

Ein niederländischer White-Hat-Hacker könnte über eine Hintertür die Kontrolle über Millionen intelligenter Solarpanelsysteme erlangt haben, **berichtet das Investigativportal FollowTheMoney** .

Die Ergebnisse bestätigen einen **Bericht einer niederländischen Agentur aus dem Jahr 2023** , in dem festgestellt wurde, dass Konverter – wesentliche Teile von Solarmodulen, die den Strom für das Stromnetz umformen und normalerweise mit dem Internet verbunden sind – „leicht gehackt“ werden können …

In einem **Bericht der EU-Agentur für Cybersicherheit vom 24. Juli** heißt es, die Union sei auf einen konzertierten Angriff auf ihre Energieinfrastruktur, sei er von einem ausländischen Staat oder böswilligen Insidern durchgeführt, schlecht vorbereitet.

Wie viel wird das kosten?

Wir müssen **Wechselrichter testen und ggf. austauschen und die Software reparieren** :

Ein Bericht des Cyber Security Cooperative Research Centre in Perth empfiehlt, alle in Australien verkauften Solarwechselrichter zu prüfen und festzustellen, welche Schwachstellen behoben werden müssen. Der Bericht fordert außerdem, dass für Solarwechselrichter und IoT-Geräte generellere Cybersicherheitsbewertungen eingeführt werden sollten. Außerdem wird empfohlen, Solarwechselrichter mit festgestellten schwerwiegenden Cyber-Schwachstellen aus dem Einzelhandel in Australien zu verbannen.

Jo Nova Blog

> Hacked Off: CyberCrims Attack Rooftop Solar To Bring Down Entire Grid

Übersetzt durch Andreas Demmig

Ergänzung:

Wenn die mit dem Internet verbundenen Wechselrichter eine Schwachstelle sein können, kann das mit den Wechselrichtern der Windkraftanlagen noch heftiger sein, da größere Leistung.