Chińczycy mogą zdalnie wyłączyć całą fotowoltaikę?

16 maja 2025

Amerykańskie służby energetyczne biją na alarm po odkryciu w chińskich inwerterach fotowoltaicznych i magazynach energii tajemniczych, nieudokumentowanych modułów komunikacyjnych. Te tzw. „ghost devices", niewidoczne w oficjalnej dokumentacji technicznej, mogą stanowić poważne zagrożenie dla bezpieczeństwa energetycznego państw zachodnich, umożliwiając potencjalnie zdalne przejęcie kontroli nad kluczowymi elementami infrastruktury energetycznej.

Sprawa jest tym poważniejsza, że chińscy producenci, na czele z Huawei, dominują globalny rynek inwerterów. Według danych Wood Mackenzie, w 2023 roku Huawei kontrolował ponad 26% światowego rynku inwerterów, a w 2022 roku około 29%. W samej Europie ponad 200 gigawatów mocy zainstalowanej opiera się na chińskich inwerterach, co stanowi ekwiwalent mocy ponad 200 elektrowni jądrowych.

Eksperci, analizując urządzenia podłączone do sieci energetycznych, natrafili na nieautoryzowane moduły komunikacyjne, głównie modemy komórkowe, które nie były wymienione w żadnej dokumentacji technicznej. Najczęściej są to ukryte modemy 4G/LTE, niewymienione w specyfikacjach, ale fizycznie obecne na płytkach PCB urządzeń. Podobne elementy znaleziono również w magazynach energii kilku chińskich producentów.

Odkrycie to budzi poważne obawy o bezpieczeństwo sieci energetycznych. Nieudokumentowane ścieżki komunikacji mogą pozwalać na zdalne obejście firewalli i innych zabezpieczeń stosowanych przez operatorów infrastruktury. W praktyce oznacza to, że atakujący uzyskujący dostęp do interfejsu zarządzania inwerterem może nie tylko aktualizować

oprogramowanie, ale także wyłączyć urządzenie, zmienić jego parametry pracy lub przeprowadzić skoordynowany atak na sieć elektroenergetyczną.

Według ekspertów kontrolowanie nawet 3-4 GW energii generowanej przez instalacje wyposażone w chińskie falowniki mogłoby wywołać zakłócenia na wielką skalę. Potencjalnie, masowe przejęcie kontroli nad inwerterami mogłoby spowodować blackouty lub poważne zakłócenia w dostawach energii.
Image

Realne ryzyko związane z tą sytuacją ujawnił przypadek z listopada 2024 roku, kiedy konflikt handlowy pomiędzy amerykańską firmą Sol-Ark a chińskim producentem Deye skutkował zdalnym wyłączeniem setek inwerterów w USA i innych krajach. Inwertery wyświetliły komunikat informujący, że nie są dopuszczone do użytku w określonych regionach, a do odblokowania wymagały kodu, który mógł być wygenerowany tylko przez producenta. Incydent ten ukazał, jak łatwo zagraniczna firma może zdalnie kontrolować lokalne urządzenia energetyczne.

W odpowiedzi na rosnące zagrożenia, niektóre państwa zaczęły wdrażać ograniczenia dotyczące chińskich technologii w sektorze energii. Litwa zakazała zdalnego dostępu do instalacji OZE powyżej 100 kW dla chińskich producentów i rozważa rozszerzenie tego zakazu na mniejsze instalacje dachowe. Estonia również wyraziła obawy, że kraj może być narażony na „szantaż energetyczny” ze strony Chin, jeśli nie wprowadzi podobnych ograniczeń.

Stany Zjednoczone pracują nad ustawą zakazującą zakupu baterii od wybranych chińskich firm dla Departamentu Bezpieczeństwa Wewnętrznego od 2027 roku, a podobne restrykcje mogą objąć także inwertery. Wielka Brytania przeprowadza zlecony przez rząd przegląd chińskiej technologii wykorzystywanej w krajowym systemie energetycznym.

Z kolei Unia Europejska wprowadza przepisy, które nakładają na chińskich producentów technologii – zwłaszcza w sektorze OZE – obowiązek spełnienia rygorystycznych standardów cyberbezpieczeństwa i transparentności. Dotyczy to między innymi wymogu przechowywania danych w Europie, lokalnej obsługi instalacji oraz szczegółowych planów ochrony danych, jeśli firma pochodzi z kraju uznanego za wysokiego ryzyka.

Problem ukrytych modułów komunikacyjnych w chińskich urządzeniach przypomina o potrzebie większej dywersyfikacji łańcuchów dostaw oraz wprowadzenia skutecznych mechanizmów kontroli sprzętu instalowanego w krytycznej infrastrukturze. Eksperci zalecają zwiększoną transparentność łańcuchów dostaw, rygorystyczną certyfikację urządzeń oraz wdrażanie standardów bezpieczeństwa, które pozwolą chronić infrastrukturę energetyczną przed potencjalnymi zagrożeniami wynikającymi z globalnych napięć geopolitycznych.

Źródło: ZmianyNaZiemi.pl