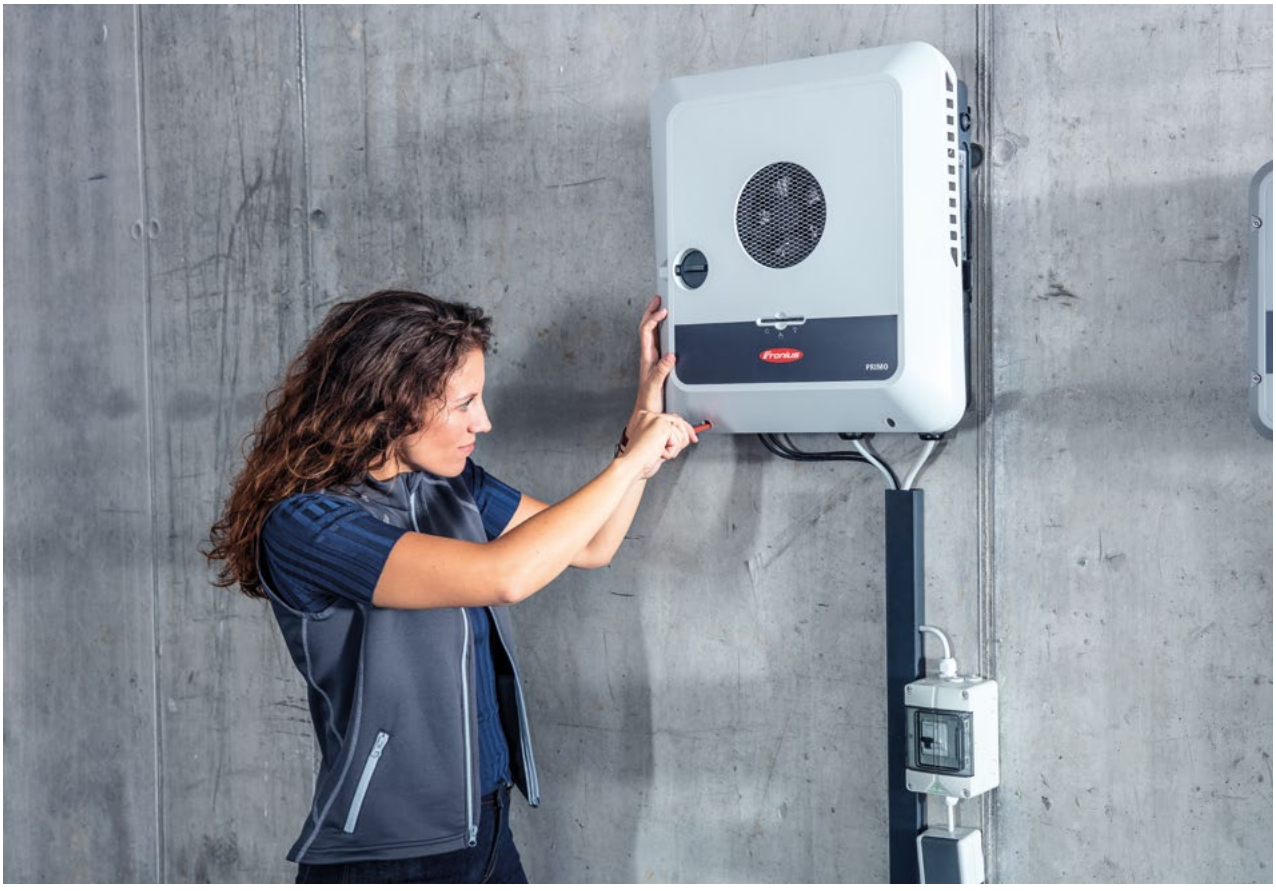
Cyberzagrożenia dla fotowoltaiki. Ryzyko dotyczy danych, kontroli i wojny hybrydowej

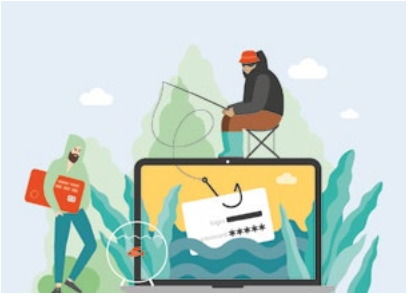
Szybki rozwój technologii oraz postępująca cyfryzacja to nie tylko ułatwienia i nowe możliwości, ale także nowe zagrożenia. Ryzyka związane z cyberzagrożeniami nie omijają też branży fotowoltaicznej. Potencjalne problemy dotyczą m.in. kontroli nad instalacjami fotowoltaicznymi, bezpieczeństwa danych czy nawet wrogich działań w ramach wojny hybrydowej. Szczególnie pod tym względem istotne jest odpowiednie zabezpieczenie falowników, które pełnią kluczową rolę w systemach fotowoltaicznych. Coraz większe znaczenie cyberbezpieczeństwa w sektorze energii odnawialnej dostrzega również Unia Europejska, co już skutkuje i będzie skutkowało zmianami prawnymi w tej dziedzinie.



W marcu br. marka Fronius Polska Solar Energy zainicjowała nową kampanię informacyjną **„Falownik ma znaczenie”**, w ramach której koncentruje uwagę na znaczeniu doboru falownika dla systemu fotowoltaicznego. Aktualnie coraz większe znaczenie ma w tym kontekście kwestia odpowiedniego zabezpieczenia instalacji i danych przed rosnącymi cyberzagrożeniami.

Inteligentne falowniki potrafią coraz więcej

W elektrowniach fotowoltaicznych istotną rolę pełnią falowniki, które stanowią podstawę systemów tego rodzaju. W praktyce falownik określa i kontroluje zachowanie instalacji fotowoltaicznej, a jednocześnie pełni ważną rolę we wspieraniu sieci elektroenergetycznej. Falownik ma znaczenie także z punktu



widzenia bezpieczeństwa danych czy kontroli zdalnego dostępu.

– Nie każdy zdaje sobie sprawę z tego, jak ważną obecnie rolę w systemach energii odnawialnej pełnią falowniki, które z biegiem lat stały się bardziej inteligentne. Chodzi zarówno o stabilizację sieci energetycznej i liczne funkcje sieciowe, jak i zarządzanie przepływem energii na poziomie lokalnym. Do tego dochodzą również inne kwestie – np. umożliwienie przez falownik efektywniejszego wykorzystania magazynów energii, dostarczanie odpowiednich danych czy w niektórych krajach także reagowanie na aktualny popyt na energię – mówi dr inż. Maciej Piliński, Dyrektor Solar Energy w firmie Fronius Polska.

Jak podkreślają eksperci europejskiej firmy branży PV, wagę inteligentnych falowników dobrze pokazuje to, że są one bezpośrednio lub pośrednio powiązane z niemal każdym elementem systemu fotowoltaicznego i jego otoczenia – operatorami sieci i przedsiębiorstwami użyteczności publicznej, innymi podmiotami zarządzającymi, agregatorami technicznymi, lokalnymi systemami zarządzania energią EMS czy pompami ciepła. Nowoczesny falownik zapewnia liczne kanały komunikacji, generując równocześnie wiele różnych danych dotyczących przepływów energii. Poszczególne kanały służą do wspierania, monitorowania, konfigurowania i aktualizacji oprogramowania, a interfejsy API pozwalają na zdalne sterowanie i optymalizowanie zużycia energii w instalacji. Konkretne dane związane m.in. z telemetrią urządzeń, lokalizacjami i kontami klientów są obecnie przechowywane i przetwarzane z wykorzystaniem platform w chmurach obliczeniowych.

Ochrona danych i kontrola dostępu mają kluczowe znaczenie

Inteligentne systemy w instalacjach fotowoltaicznych są obecnie narażone na różne cyberzagrożenia. Okazuje się, że ryzyko dotyczy bardzo różnych aspektów, w tym m.in. punktów danych w sieci sterującej i serwisowej oraz punktów danych usług rynkowych. Potencjalne zagrożenia mogą odnosić się np. do przejęcia kontroli nad systemami i doprowadzenia do zakłócenia działania lokalnych sieci energetycznych. Niewykluczona jest nawet całkowita awaria sieci (tzw. blackout).

– Rozwój technologiczny i cyfryzacja niosą ze sobą, poza oczywistymi korzyściami, także nowe zagrożenia dla cyberbezpieczeństwa. Realia są takie, że w ramach inteligentnej sieci urządzenia generujące energię mogą być wykorzystane w celu destabilizacji podłączonej sieci, jeżeli atakujący jest w stanie przejąć kontrolę nad krytyczną liczbą takich urządzeń. Z kolei lepsza łączność pomiędzy siecią internetową a inteligentnymi falownikami tworzy pewne możliwości manipulowania zasobami, co może prowadzić do utraty danych, przerwy czy nawet pełnego zatrzymania dostaw prądu. Lista możliwych zagrożeń jest oczywiście szersza, bo niebezpieczeństwo wiąże się też np. z możliwymi zmianami ustawień wyzwalania częstotliwości i/lub napięcia dla falowników – wyjaśnia Maciej Piliński.

Potencjalne ryzyka dotyczą również punktów danych usług rynkowych, co wiąże się także z możliwymi stratami finansowymi. Manipulacja danymi pomiarowymi może mieć skutki finansowe m.in. dla klientów zarządzających flotami instalacji czy farm PV, a manipulacja kontami klientów grozi wyciekiem danych osobowych, w tym adresów, danych kont czy informacji geolokalizacyjnych.

– Sytuacja geopolityczna na świecie jest niestabilna, a sektor energetyczny ma znaczenie strategiczne. Obecnie świat musi liczyć się nawet z konfliktem o globalnym charakterze. Mówiąc wprost, w ewentualnych działaniach w ramach tzw. wojny hybrydowej celem ataku mogą być również instalacje fotowoltaiczne, które odgrywają coraz większą rolę w systemach energetycznych krajów Europy. Dlatego cyberbezpieczeństwo i zapewnienie odpowiedniej kontroli nabiera aktualnie szczególnie dużej wagi – podkreśla Dyrektor Solar Energy w firmie Fronius Polska.

Jak zwiększyć cyberbezpieczeństwo?

Sprawa cyberbezpieczeństwa inteligentnych systemów związanych z energetyką została zauważona również na poziomie Unii Europejskiej. Przykładem może być Cyber Resilience Act (CRA), czyli wprowadzone już w życie unijne rozporządzenie określające obowiązki producentów produktów cyfrowych w kontekście m.in. projektowania z myślą o bezpieczeństwie.

W podobnym kierunku idzie także nowa dyrektywa NIS2, która modyfikuje przepisy dotyczące kwestii cyberbezpieczeństwa i odporności biznesowej. Termin na wdrożenie NIS2 upłynie 17 października 2024 r.

– Jako Fronius spełnimy warunki nowych unijnych regulacji z wyprzedzeniem, najprawdopodobniej już w czerwcu br. Dyrektywa NIS2 to ruch w dobrym kierunku, ale może być niewystarczający. Z naszej strony kładziemy od dawna duży nacisk na odpowiednie zabezpieczenie falowników pod kątem cyberzagrożeń. Przykładowo, przechowujemy oddzielnie dane klientów i dane systemowe, by ograniczyć ryzyko. Same dane przechowujemy na serwerach zlokalizowanych na terenie Unii Europejskiej. Nasi pracownicy regularnie uczestniczą też w szkoleniach w zakresie cyberprzestępczości, a nasze starania potwierdza też uzyskanie certyfikatu ISO 27001 w zakresie bezpieczeństwa informacji – dodaje Maciej Piliński.

W tak ważnym dla bezpieczeństwa sektorze priorytetem powinna być autonomia na poziomie europejskim i niezależność wobec krajów spoza wspólnoty. Temu służyć mógłby np. szeroki obowiązek przechowywania, wykorzystywania i przekazywania danych nt. energii na terenie UE, a także zabezpieczenia przed sterowaniem spoza Europy. Z punktu widzenia kontroli nad systemami PV kluczowe może być pytanie, gdzie znajduje się centrum sterowania pozwalające potencjalnie na kontrolowanie milionów europejskich elektrowni PV.