REKOMENDACJE

DOTYCZĄCE CYBERBEZPIECZEŃSTWA DLA PROSUMENTÓW OZE

Ministerstwo Cyfryzacji

Ministerstwo Klimatu i Środowiska

CERT.PL NASK

PSE Polskie Sieci Elektroenergetyczne

CERT PSE computer emergency response team

Spis treści

01. Wprowadzenie

Przedstawiamy kompendium podstawowych informacji i dobrych praktyk dotyczących szeroko pojętego cyberbezpieczeństwa. Ich zastosowanie przyczyni się do podniesienia poziomu bezpieczeństwa prosumentów, co może przynieść wymierne korzyści. Rekomendacje zostały wypracowane podczas konsultacji ekspertów CSIRT NASK, Polskich Sieci Elektroenergetycznych S.A., Urzędu Regulacji Energetyki oraz Polskiego Towarzystwa Przesyłu i Rozdziału Energii Elektrycznej oraz przedstawicieli sektora energii, którzy dzieląc się swoim doświadczeniem i wiedzą, zapewnili szeroki zakres tematyczny broszury.

Od 7 lat w Polsce podejmowane są zdecydowane działania na rzecz zdywersyfikowania źródeł pozyskiwania energii i rozwoju sektora energetyki odnawialnej. Przez ten czas ponad siedmiokrotnie wzrosła moc zainstalowana w odnawialnych źródłach energii – do 22,6 GW (koniec 2022 r.). Liczba mikroinstalacji, czyli tych w których moc zainstalowana nie przekracza 50 kW, przekroczyła 1,2 miliona, a ich moc osiągnęła blisko 8,8 GW. Dużą rolę w rozwoju wytwarzania energii w mikroinstalacjach odgrywa rządowy program „Mój Prąd". Jego zadaniem jest wspieranie rozwoju energetyki prosumenckiej, czyli wytwarzania energię na własne potrzeby i przekazywanie nadwyżki do sieci energetycznej. Wytwarzanie energii elektrycznej z odnawialnych źródeł energii niesie za sobą szereg korzyści, zarówno ekonomicznych, w postaci obniżenia rachunków za energię elektryczną, jak i środowiskowych - uniknięte emisji dwutlenku węgla do atmosfery. Korzyści z energetyki prosumenckiej wielokrotnie przewyższają zagrożenia z nią związane. Prosument, przy zastosowaniu się do omawianych niżej zaleceń może zredukować owe zagrożenia do akceptowalnego dla siebie poziomu. Instalacje prosumenckie mogą być bezpieczne, o ile podjęte zostaną odpowiednie działania w kontekście komunikacji tych instalacji z Internetem. Chodzi o zapobieganie występowaniu zagrożeń cyberbezpieczeństwa.

Starając się zapobiegać omawianym zagrożeniom prezentujemy niżej podstawowe wytyczne i rekomendacje. Naturalnie treść oraz poruszane tu kwestie będą ewoluowały wraz ze zmianami i potrzebami zachodzącymi w sektorze energii oraz rozwojem nowych technologii i rozwiązań.

Otoczenie prawne

Najważniejszym krajowym aktem prawnym w zakresie energii jest ustawa z 10 kwietnia 1997r. – Prawo energetyczne[1]. Regulacja określa m. in. zasady kształtowania polityki energetycznej państwa, zasady i warunki zaopatrzenia i użytkowania paliw i energii, zasady działalności przedsiębiorstw energetycznych. Jej uzupełnieniem jest uchwalona dnia 20 lutego 2015 r. Ustawa o odnawialnych źródłach energii[2], zwana dalej ustawą o OZE. Przepisy tej ustawy m.in. określają zasady i warunki

1) T. j. Dz. U. z 2022 r. poz. 1385 ze zm.
2) T. j. Dz. U. z 2022 r. poz. 1378 ze zm.

wykonywania działalności w zakresie wytwarzania energii elektrycznej z odnawialnych źródeł energii. Omawiamy niżej rekomendacje dla prosumentów, których grupa rozrasta się (wraz z postępem prac legislacyjnych) i obejmuje kolejne, nowe kategorie odbiorców. Do 1 kwietnia 2022 za prosumenta uważany był odbiorca, który wytwarza energię na własne potrzeby w mikroinstalacji. W ustawie z dnia 29 października 2021 r. o zmianie ustawy o OZE i niektórych innych ustaw wprowadzono dodatkowe kategorie prosumentów tj. prosumenta zbiorowego i wirtualnego. Prosumentem zbiorowym jest odbiorca końcowy wytwarzający energię elektryczną z odnawialnych źródeł energii na własne potrzeby w mikroinstalacji (do 50 KW), jak również w małej instalacji (do 1 MW). Jego instalacje są przyłączone do elektroenergetycznej sieci dystrybucyjnej za pośrednictwem wewnętrznej instalacji elektrycznej budynku wielolokalowego. Nowelizacja wprowadziła również pojęcie prosumenta wirtualnego, czyli wytwarzającego energię elektryczną wyłącznie z odnawialnych źródeł energii na własne potrzeby w innym miejscu niż miejsce dostarczania energii elektrycznej do tego odbiorcy. Prosument wirtualny nie ma już ustawowego ograniczenia mocy instalacji OZE, którą zamierza wykorzystywać do produkcji energii odnawialnej na własne potrzeby.

Warto zaznaczyć, że zgodnie z polskim prawem za prosumenta uważa się tylko odbiorcę. Odbiorcą natomiast jest każdy otrzymujący lub pobierający paliwa lub energię na podstawie umowy z przedsiębiorstwem energetycznym. Pojęcie prawne odbiorcy zostało zdefiniowane w ustawie - Prawo energetyczne. Istnieje jednak w Polsce pewna grupa osób, dla której wyznacznikiem niezależność energetycznej jest całkowity brak rachunków za prąd. Osoby te nie decydują się na pobieranie ani oddawanie energii do jakiegokolwiek przedsiębiorstwa energetycznego. Często po prostu chcą one spełnić warunek bezemisyjności energii potrzebnej do zasilania ich prywatnego domu. Obecnie takie rozwiązanie jest technicznie możliwe poprzez instalacje OZE typu off-grid. Osoba, która zainstaluje źródło OZE działające wyłącznie w zakresie domowej instalacji elektrycznej, które nie ma wpływu na system energetyczny, nie musi też swojej instalacji zgłaszać. Wybór tej formy niezależności energetycznej jest całkowicie zgodny z prawem. Osoba ta jednak, pomimo że produkuje energię elektryczną na własne potrzeby, wg polskiego prawa nie jest prosumentem.

Przedstawione niżej rekomendacje skierowane są do odbiorców, którzy chcą bezpiecznie wytwarzać energię elektryczną na własne potrzeby niezależnie od zainstalowanej mocy. Choć ze względów praktycznych omawiamy głównie zasady bezpiecznego użytkowania mikroinstalacji, których jest najwięcej, a ich liczba, według szacunków w 2023 roku przekroczy 1,5 mln.

Powiązane regulacje prawne:

- NIS2 – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2555)

- CER – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 w sprawie odporności podmiotów krytycznych (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32022L2557)
- Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560)
- Ustawa z dnia 10 kwietnia 1997 r. – Prawo energetyczne (https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19970540348)
- Ustawa dnia 20 lutego 2015 r. - Ustawa o odnawialnych źródłach energii (https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20220000467)
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/2001 z dnia 11 grudnia 2018 r. w sprawie promowania stosowania energii ze źródeł odnawialnych (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:32018L2001)

Słownik pojęć

Atak ransomware (ang. ransom – okup) – podczas niego dochodzi do zainfekowania urządzeń oprogramowaniem szyfrującym dane w celu żądania okupu za udostępnienie klucza do ich odszyfrowania.

Chmura producenta – sieć połączonych serwerów zdalnych, znajdujących się w różnych miejscach, ale działających jak jeden ekosystem. Pełnią one różne funkcje: przechowują dane i umożliwiają zarządzenie nimi, obsługują aplikacje oraz dostarczają zawartość lub usługi u danego producenta. Dzięki temu można uzyskiwać dostęp do nich z dowolnego urządzenia połączonego z Internetem — informacje są dostępne w dowolnym miejscu i czasie.

Datamanager – to centrala komunikacyjna, która przez połączenie internetowe przesyła wartości instalacji fotowoltaicznej bezpośrednio do portalu online.

Energetyka prosumencka – czyli taka, w której osoby wytwarzają energię na własne potrzeby, a jej nadwyżkę przekazują do sieci energetycznej.

Falownik/Inwerter/mikroinwerter/mikrofalownik – urządzenie elektryczne zasilane prądem stałym, zamieniające go (ang. direct current, DC) na prąd przemienny (ang. alternating current, AC) o regulowanej częstotliwości wyjściowej.

Incydent cyberbezpieczeństwa – niepożądane zdarzenie prowadzące do naruszenia bezpieczeństwa systemów informatycznych, sieci, urządzeń lub danych. Może obejmować m.in. ataki hakerskie, kradzieże danych, złośliwe oprogramowanie, przestępstwa związane z cyberprzestępczością, awarie sprzętowe lub oprogramowania oraz błędy ludzkie. Incydent może prowadzić do zagrożenia bezpieczeństwa, poufności,

integralności lub dostępności danych, a także naruszenia prywatności. W przypadku incydentu cyberbezpieczeństwa ważne jest szybkie zareagowanie i podjęcie odpowiednich działań w celu zminimalizowania szkód, odzyskania utraconych danych i zapobieżenia przyszłym atakom.

IoT - (ang. Internet of things) – koncepcja, wedle której jednoznacznie identyfikowalne przedmioty mogą pośrednio albo bezpośrednio gromadzić, przetwarzać lub wymieniać dane za pośrednictwem instalacji elektrycznej inteligentnej KNX lub sieci komputerowej.

Małe instalacje – instalacje o mocy zainstalowanej elektrycznej powyżej 50 kW i poniżej 1 MW.

Mikroinstalacja – instalacja, których moc zainstalowana nie przekracza 50 kW.

MFA – (ang. Multi-Factor Authentication) uwierzytelnianie wieloczynnikowe. Wymaga od użytkowników potwierdzenia tożsamości co najmniej na dwa różne sposoby.

Monitorowanie (stanu instalacji) – monitorowanie pracy inwertera/falownika lub mikroinwerterów oraz pracy całej instalacji fotowoltaicznej. Datamanager, rejestruje parametry wejściowe oraz wyjściowe inwertera, jak np. napięcia, prądy czy moce. Dane te są zbierane, rejestrowane, przechowywane, a następnie prezentowane na stronach internetowych lub w aplikacji mobilnej. Właściciel danej instalacji fotowoltaicznej może przeprowadzać różnego rodzaju analizy: dzienne, miesięczne bądź roczne, a także generować raporty oraz wykresy. Falowniki mają dostęp do Internetu poprzez połączenia przewodowe Ethernet lub bezprzewodowe Wi-Fi. Dzięki temu można na bieżąco archiwizować, analizować i monitorować wszelkie dane dotyczące domowej instalacji fotowoltaicznej.

Optymalizatory pracy paneli – sterują parametrami prądu generowanego przez moduł fotowoltaiczny, aby nie blokował oraz nie był blokowany przez inne moduły/panele fotowoltaiczne.

OZE - Odnawialne źródła energii

OZE typu off-grid – to systemy energetyczne, które nie są połączone z siecią elektroenergetyczną i są zasilane wyłącznie przez źródła energii odnawialnej, takie jak panele słoneczne, turbiny wiatrowe, mikrohydroelektrownie lub biopaliwa.

Phishing – metoda oszustwa, w której przestępca podszywa się pod inną osobę lub instytucję w celu wyłudzenia poufnych informacji (np. danych logowania, danych osobowych, danych karty kredytowej), zainfekowania komputera szkodliwym oprogramowaniem czy też nakłonienia ofiary do określonych działań. Jest to rodzaj ataku

z wykorzystaniem poczty elektronicznej, opartego na metodach i zasadach manipulacji odbiorcy.

Silne hasło – unikalne dla każdego konta, wystarczająco długie i niesłownikowe hasło, które zawiera wielkie i małe litery, cyfry oraz znaki specjalne i jest znane tylko jego użytkownikowi.

Urządzenia IoT – urządzenia, które mogą komunikować się ze sobą i udostępniać dane przez Internet. Urządzenia IoT mogą łączyć się z Internetem i często są wyposażone w czujniki, umożliwiające im gromadzenie danych.

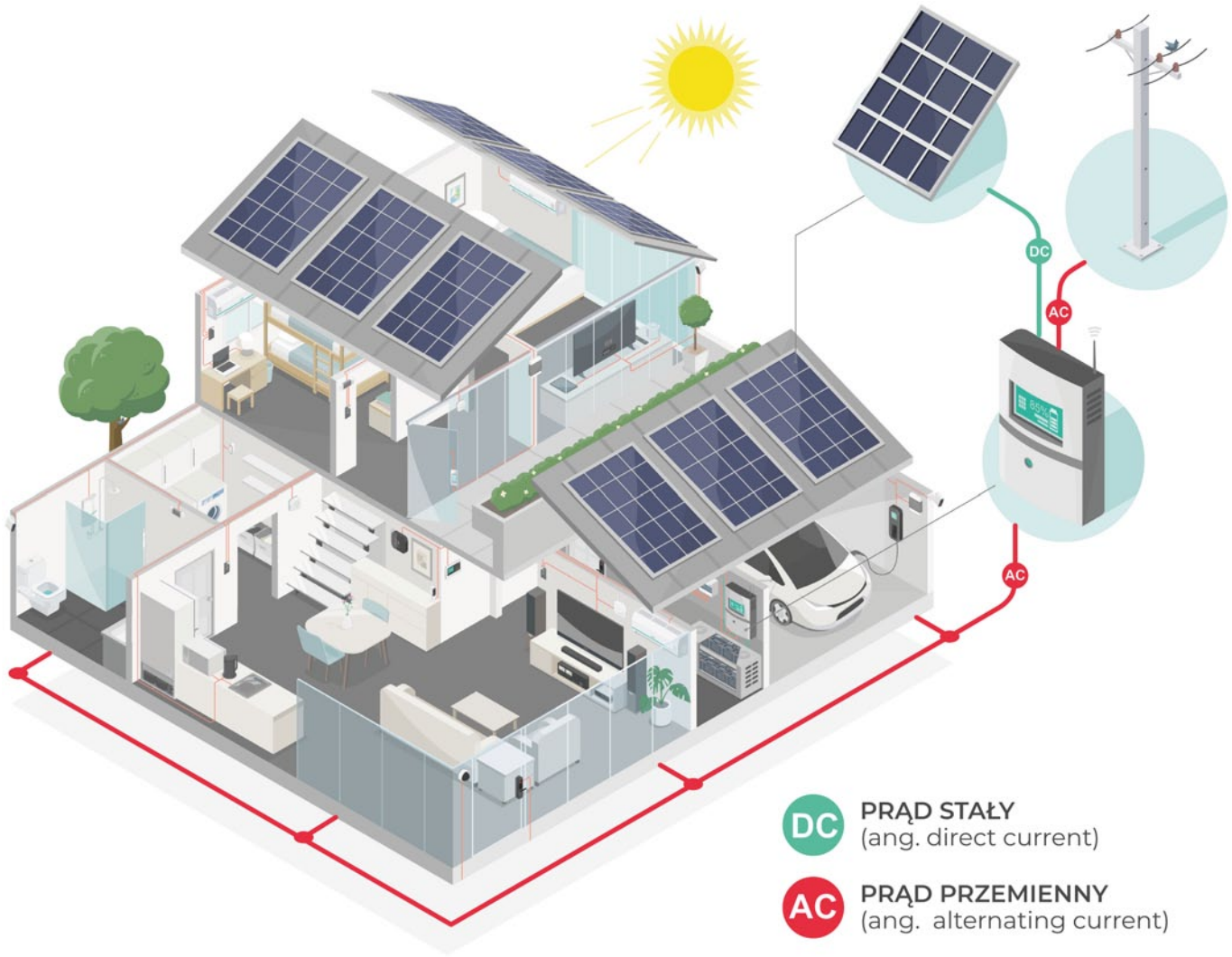
Webserwer (ang. web server) – oprogramowanie lub sprzętowy system komputerowy, odpowiedzialny za przetwarzanie żądań HTTP (Hypertext Transfer Protocol) z przeglądarek internetowych i dostarczanie treści internetowych w odpowiedzi na te żądania.

Złośliwy kod (ang. malware, malicious software) – program komputerowy zaprojektowany w celu naruszenia prywatności, bezpieczeństwa lub poprawnego funkcjonowania systemu, sieci, urządzenia lub aplikacji. Złośliwy kod może być rozprzestrzeniany drogą internetową, za pośrednictwem zarażonych nośników danych lub wykorzystanie luk w oprogramowaniu systemowym czy aplikacjach. Jego działanie może mieć różne cele: kradzież danych, niszczenie danych lub systemów, szpiegowanie użytkowników, infiltrowanie sieci, wykorzystanie możliwości obliczeniowych zainfekowanych systemów do przeprowadzania kolejnych ataków lub spamowania oraz wymuszanie okupów za odzyskanie zaszyfrowanych danych.

Schemat funkcjonowania prosumenckiej instalacji OZE

Instalacja OZE przetwarza energię odnawialną, czyli energię z odnawialnych źródeł energii. Zgodnie z ustawą o OZE są nimi niekopalne źródła energii obejmujące energię wiatru, promieniowania słonecznego, aerotermalną, geotermalną, hydrotermalną, hydroenergię, fal, prądów i pływów morskich, otrzymywaną z biomasy, biogazu, biogazu rolniczego oraz z biopłynów, w energię elektryczną. Uogólniając, w prosumenckiej instalacji odnawialnego źródła energii można wskazać:

- urządzenia służące do wytwarzania energii takie jak: moduły fotowoltaiczne, śmigła elektrowni wiatrowej lub łopaty turbiny wodnej, silnik gazowy w biogazowni, etc. oraz
- urządzenia przetwarzające pozyskaną energię do postaci umożliwiającej jej zużycie w urządzeniach przyłączonych do instalacji wewnętrznej odbiorcy lub tez wprowadzenie tej energii do sieci elektroenergetycznej w postaci energii elektrycznej o zadanych parametrach, takie jak falowniki (inwertery) PV, prądnice synchroniczne, oraz prądnice asynchroniczne pracujące samodzielnie, lub we współpracy z dedykowanymi inwerterami.



Przykład prosumenckiej instalacji fotowoltaicznej.

Rodzaje instalacji OZE oraz najpopularniejsze instalacje prosumenckie

Instalację odnawialnego źródła energii stanowią opisane przez dane techniczne i handlowe urządzenia lub obiekty budowlane wraz z towarzyszącymi im urządzeniami. Instalacja OZE służy do wytwarzania energii lub biogazu rolniczego (a instalacja może być połączona z magazynem energii elektrycznej lub magazynem biogazu rolniczego).

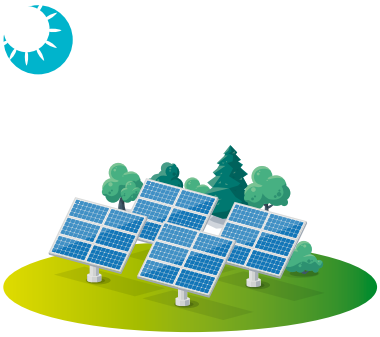
W przypadku prosumentów należy mówić jednak tylko o instalacjach wytwarzających energię elektryczną. Ze względu na moc zainstalowaną elektryczną instalacje OZE dzielimy na:

- mikroinstalacje, o mocy zainstalowanej elektrycznej do 50 kW,
- małe instalacje o mocy zainstalowanej elektrycznej powyżej 50 kW i poniżej 1 MW,
- pozostałe.

Spośród wielu możliwości wykorzystywania odnawialnej energii pierwotnej OZE używamy w Polsce instalacji wykorzystujące następujące jej rodzaje:

- energię wiatru,
- energię promieniowania słonecznego,
- hydroenergię,
- energię otrzymywaną z biomasy,
- energię otrzymywaną biogazu innego niż rolniczy (komunalny, wysypiskowy)
- energię otrzymywaną z biogazu rolniczego.

ENERGIA WIATRU



ENERGIA PROMIENIOWANIA SŁONECZNEGO

HYDROENERGIA

ENERGIA OTRZYMYWANA Z BIOMASY

ENERGIA OTRZYMYWANA Z BIOGAZU INNEGO NIŻ ROLNICZY (KOMUNALNY, WYSYPISKOWY)

ENERGIA OTRZYMYWANA Z BIOGAZU ROLNICZEGO

Źródła odnawialnej energii wykorzystywane w Polsce.

Liczba instalacji wykorzystujących pozostałe energie pierwotne w stosunku od udziału instalacji wykorzystujących energię promieniowania słonecznego jest pomijalnie mały i stanowi zaledwie 0,03%.

Rodzaj wykorzystywanej energii pierwotnej	Liczba prosumentów (koniec 2022 r.)
energia promieniowania słonecznego	**1 193 053**
hydroenergia	**82**
energia wiatru	**57**
energia otrzymywana z biogazu	**44**
energia otrzymywana z biomasy	**43**

Rozkład zarejestrowanych w Polsce instalacji OZE.

Ze względu na liczbę zarejestrowanych prosumentów po omówieniu instalacji wykorzystujących hydroenergię, energię wiatru nasza uwaga zostanie skupiona na instalacjach wykorzystujących energię promieniowania słonecznego.

Małe elektrownie wodne (MEW) jako instalacje prosumenckie zwracają szczególną uwagę ze względu na swoje walory środowiskowe. Podczas ich lokalizacji wskazuje się do wykorzystania przede wszystkim istniejące obiekty piętrzące wodę. To podejście uwydatnia znaczenie środowiskowe tych instalacji. Nie wymaga budowania nowych przegród na rzekach, a jedynie wykorzystywanie już istniejących obiektów. Liczba potencjalnych lokalizacji mikro- i małych- instalacji hydroenergetycznych bazujących na istniejących obiektach piętrzących i lokalizacjach dawnych młynów wodnych szacowana jest na około 8 tys. Jednak małe elektrownie wodne, nawet o wielkości mikroinstalacji, rzadko są wykorzystywane jako instalacje prosumencie. Ich budowa i obsługa jest skomplikowana, a generacja energii często przekracza zapotrzebowanie jednego prosumenta. System automatycznego sterowania mikroinstalacją hydroenergetyczną jest bardzo złożony. Zawiera m. in moduł do pomiaru poziomu wody górnej, położenia łopatek i otwarcia dyszy. Wraz z rozwojem mikroinstalacji wykorzystujących energię wiatru i promieniowania słonecznego również w przypadku MEW zaczęto stosować inwertery. Inwertery dla MEW swoją konstrukcją i oprogramowaniem są zbliżone do inwerterów wiatrowych, jednak różnią się charakterystyką pracy i zabezpieczeniami.

Trzecia pod względem liczebności grupa prosumentów (57 instalacji) wykorzystuje mikroinstalacje wiatrowe. Ten typ instalacji warty jest odnotowania, głownie ze względu na swoją komplementarność w stosunku do instalacji fotowoltaicznych. Panele bowiem rozwiązują problem przejścia na czyste źródła energii częściowo, ponieważ produkują energię w wąskim zakresie czasowym. Korzystne zatem jest uzupełnienie „miksu" energetycznego o turbiny wiatrowe, szczególnie, że powstają nowe, oczekiwane przez proekologicznych konsumentów konstrukcje. Dostępne dwa typy turbin: o poziomej oraz pionowej osi obrotu. Najczęściej wybierana jest turbina o poziomej osi obrotu. Jej zalety to mniejsza masa wirnika i niższe koszty inwestycyjne w porównaniu do turbiny z pionową osią obrotu. Natomiast turbina z pionową osią obrotu wydaje

mniejszy hałas od turbiny z poziomą osią obrotu, przy analogicznej mocy. Najpopularniejsze, pośród turbin z pionową osią obrotu, tzw. turbiny z wirnikiem Darrieus'a, są złożone z dwóch lub trzech łopat o stałej cięciwie i symetrycznym profilu. Łopaty są umocowane na pionowym wale, skręcone i wygięte w płaszczyźnie osi turbiny. Turbiny pracują cicho, nie powodują silnych drgań. Z drugiej strony są to turbiny o większej masie i mniejszej wydajności niż turbiny z poziomą osią obrotu. Mikroinstalacje wiatrowe, podobnie jak fotowoltaiczne, wymagają inwertera w celu przyłączenia do sieci. Są przecież narażone na dokładnie takie same cyberzagrożenia.

Najliczniejszą grupą prosumentów są prosumenci wykorzystujący energię promieniowania słonecznego. Ich liczba, wg szacunków MKiŚ, w roku 2023 sięgnie 1,5 miliona. Łączna moc zainstalowana instalacji fotowoltaicznych sięga niemal 9 GW. Niewątpliwie do popularyzacji tego typu instalacji przyczynił się program rządowy „Mój Prąd". Wsparcie państwowe zostało przygotowane przez Ministerstwo Energii we współpracy z ówczesnym Ministerstwem Środowiska i ogłoszone 23 lipca 2019 r. przez Premiera Mateusza Morawieckiego. Program umożliwił uzyskanie dotacji do instalacji fotowoltaicznych. To zwiększyło atrakcyjność instalacji, redukując w początkowym okresie ich stosunkowo wysokie koszty uruchomienia. Koszty te są jednak z roku na rok są coraz mniejsze przy coraz wyższej sprawności paneli.

Zalety instalacji fotowoltaicznych czynią je atrakcyjną technologią prosumencką, niezależnie od oferowanego systemu wsparcia. Do zalet tych należy zaliczyć:

- żywotność instalacji – panele słoneczne powinny działać 40-50 lat. Najstarszy panel fotowoltaiczny ma około 60 lat i wciąż działa.
- niska awaryjność instalacji – gwarancja udzielana na falownik, najbardziej awaryjną część instalacji, trwa zwykle 5 lat. Zdarzają się producenci oferujący nawet 10–letnią gwarancję.
- bezobsługowość instalacji – panele założone pod odpowiednim kątem nie wymagają mycia ani odśnieżania.
- cicha praca instalacji – bezgłośna praca paneli, praca inwertera jest porównywalna z głośnością brzęczenia owada.

W typowej instalacji fotowoltaicznej prosumenckiej panele podłączone są do falownika za pomocą instalacji prądu stałego, a następnie falownik za pomocą wewnątrzbudynkowej instalacji prądu przemiennego przyłączony jest do sieci przedsiębiorstwa energetycznego. Szacuje się, że aktualnie ok. 90% domowych instalacji fotowoltaicznych posiada rozwiązanie z tzw. falownikiem centralnym, tzn. wszystkie panele są przyłączone do jednego urządzenia.

Falowniki występują w różnych wersjach. Sprzedawane są modele jednofazowe (dla instalacji o mniejszych mocach) i trójfazowe. Mogą mieć budowę urządzenia transformatorowego i beztransformatorowego. Można nabyć urządzenia w wariantach wyspowych (falowniki magazynujące nadwyżkę energii w akumulatorach), sieciowych

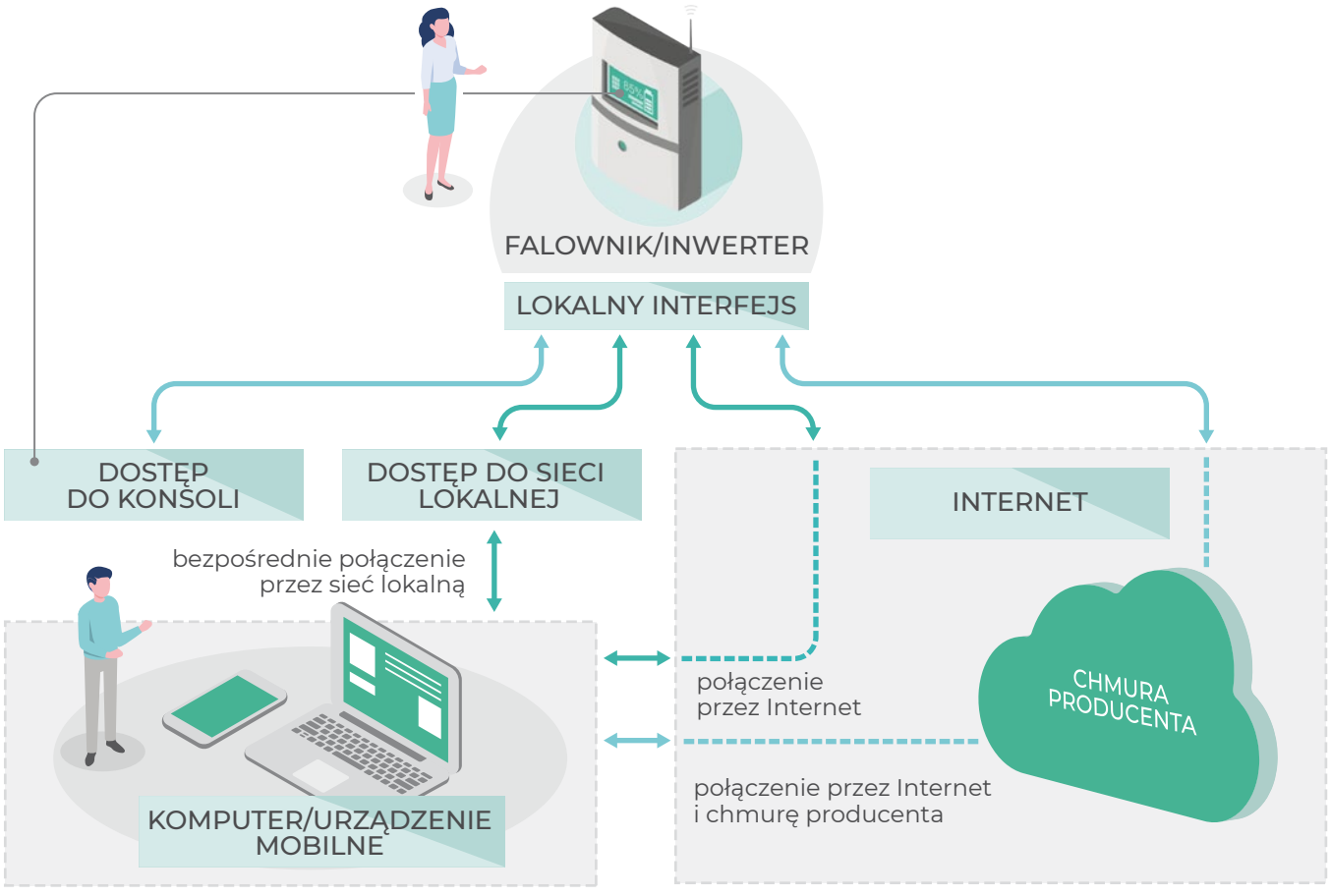
(synchronizujące się z siecią publiczną) i wyspowo-sieciowych (hybrydy łączące obie funkcje). Istnieje jednak pewna grupa instalacji, która pracuje w oparciu o tzw. mikrofalowniki. W takich instalacjach każdy panel (lub grupa paneli) posiada własny mikroinwerter. Te z kolei są przyłączone oddzielnie do instalacji wewnątrzbudynkowej. Mikrofalowniki nie różnią się budową od falowników. Na rynku występują jedynie modele przeznaczone do współpracy z siecią. Nie produkuje się mikrofalowników w wariantach wyspowych ani wyspowo-sieciowych. Mikrofalowniki, podobnie jak falowniki, mogą być przyłączone do Internetu. Komunikacja na zewnątrz jest bezprzewodowa i odbywa się przy zastosowaniu standardów Wi-Fi stosowanych w domowych, bezprzewodowych sieciach komputerowych. Zdarzają się też rozwiązania, w których instalacja z falownikiem centralnym wyposażona jest w tzw. optymalizatory pracy paneli. Urządzenia te, sterują parametrami prądu generowanego przez moduł fotowoltaiczny, aby nie blokował oraz nie był blokowany przez inne moduły/panele fotowoltaiczne. Praca optymalizatorów może być sterowana centralnie lub gdy stanowią system rozproszony, komunikacja pomiędzy nimi następuje przez instalację prądu stałego, łączącego panele z centralnym falownikiem. Aktualnie na rynku oferowane są rozwiązania, w których centralny moduł sterujący można podłączyć do Internetu niezależnie od falownika i wyposażyć w tzw. datamanager/webserwer. W przypadku optymalizatorów w systemie rozporoszonym komunikacja odbywa się przez bezprzewodową, domową sieć komputerową.

02. Cyberzagrożenia

Omówienie stosowanych sposobów dostępu sieciowego do instalacji jest kluczowe dla zdefiniowania cyberzagrożeń oraz rekomendacji obrony przed nimi. To właśnie dostęp może umożliwić wystąpienie zagrożenia. Warto jednak zaznaczyć, że nie omawiamy w tym poradniku ryzyk związanych z dostępem fizycznym. W przypadku małych instalacji prosumenckich najczęściej spotykanym urządzeniem, z dostępem sieciowym, będzie falownik (inwerter). To on może zostać zaatakowany lub np. w przypadku niepoprawnej konfiguracji atakujący może uzyskać do niego dostęp.

Zasadniczo można wyróżnić trzy sposoby dostępu do danych inwertera:

- system samowystarczalny umożliwiający dostęp z sieci lokalnej – poprzez webserwer wbudowany w inwerter lub aplikację (w tym mobilną) komunikującą się bezpośrednio z falownikiem.
- skonfigurowanie instalacji, aby była osiągalna z Internetu poprzez np. modem, czy router. Najczęściej wtedy wykorzystywany jest stały adres IP oraz otwierany port dostępu do inwertera. Jest to stosunkowo rzadkie rozwiązanie w małych instalacjach.
- stałe połączenie instalacji przez Internet z chmurą producenta. Ten sposób zyskuje na popularności wśród prosumentów.



Sposoby dostępu do danych inwertera.

Korzyści i ryzyka związane z podłączeniem przydomowych instalacji OZE do Internetu

Każdy z przedstawionych wyżej sposobów podłączenia może przynieść korzyści dla użytkownika. To użytkownik podejmuje decyzję o sposobie podłączenia swojej instalacji OZE i oceniania korzyści (funkcjonalność) oraz ryzyka (bezpieczeństwo) z tym związane, w tym ochronę swoich danych.

Najbezpieczniejszym dla użytkownika rozwiązaniem jest podłączenie instalacji OZE wyłącznie za pomocą sieci lokalnej, odseparowanej od Internetu. Wtedy instalacja i przetwarzane dane nie podlegają ryzykom towarzyszącym korzystaniu z Internetu. Z drugiej strony, podłączenie umożliwiające zdalny dostęp jest wygodne zarówno dla właściciela jak i producenta.

Obecnie większość sprzedawanych produktów umożliwia połączenie z wykorzystaniem chmury producenta. Wymaga to zapewnienia stałego dostępu internetowego dla inwertera. Takie rozwiązania prawdopodobnie będą w przyszłości wypierały rozwiązania z dostępem lokalnym oraz wskazywały tylko taki sposób połączenia.

Korzyści wynikające z podłączenia instalacji do Internetu:

- zdalne monitorowanie stanu własnej instalacji przez stronę internetową lub aplikację mobilną;
- możliwość pobierania i korzystania z automatycznych aktualizacji udostępnianych przez producenta;
- korzystanie z usług zagregowanych w ramach rozwiązań dostarczanych przez producentów urządzeń;
- możliwość uzyskania wydłużonej gwarancji oferowanych przez niektórych producentów.

Zagrożenia związane z podłączeniem instalacji do Internetu:

Z podłączeniem instalacji do Internetu wiążą się również ryzyka, które należy uwzględnić w przypadku stosowania tego typu rozwiązań. W przypadku udanego ataku, mogą to być:

- potencjalne utracone korzyści finansowe z tytułu generacji energii elektrycznej w instalacji lub potencjalnie zwiększone koszty zużycia energii elektrycznej będące efektem przejęcia starowania nad instalacją
- ujawnienie innych danych użytkownika instalacji
- uzyskanie dostępu do sieci domowej właściciela, a w konsekwencji możliwość przeprowadzenia ataku na inne urządzenia podłączone do tej sieci (komputery, smartfony, tablety, urządzenia zaliczane do kategorii IoT);
- uszkodzenie urządzenia, np. poprzez wgranie wadliwego oprogramowania wbudowanego (firmware), lub jego zaszyfrowanie, skutkujące koniecznością poniesienia nakładów finansowych na zakup nowego i przestoju w pracy.

Jak dochodzi do ataku?

Wektorami ataków są elementy wykazujące słabości, podatne na działanie cyberprzestępców. Atakujący wykorzystując wektory ataku może uzyskać dostęp do systemu, sieci lub urządzeń. Potencjalna dostępność wektorów ataku może być tym większa, im bardziej złożony jest system. Skuteczne wykorzystanie wektora ataku może prowadzić do wystąpienia ryzyk opisanych w poprzednim rozdziale.

W odniesieniu do prosumenckich instalacji OZE posiadających połączenie sieciowe można wyróżnić następujące wektory ataku:

- wykorzystanie słabych lub powtarzalnych haseł. Przykładowo do konta w chmurze producenta, czy na wbudowanym panelu,
- nadmierna ekspozycja urządzeń na połączenia internetowe lub brak świadomości o niej, w przypadku korzystania z rozwiązań lokalnych, niedostatecznie zabezpieczona lokalna sieć Wi-Fi,
- niedostatecznie zabezpieczone kanały konfiguracji urządzeń, np. wbudowanego w inwerter hotspotu Wi-Fi,
- brak dostatecznej izolacji od sieci domowej urządzeń wchodzących w skład instalacji OZE,
- występowanie podatności w oprogramowaniu urządzenia – brak dostępnych aktualizacji bezpieczeństwa lub ich niezwłocznej instalacji,
- w przypadku korzystania z chmury, podatność w serwisie internetowym producenta,
- przejęcie konta w wyniku innego ataku, np. phishingu. W szczególności w przypadku korzystania z chmury producenta.
- zainfekowanie sieci przeprowadzone w wyniku nieświadomych działań zaatakowanej firmy/serwisanta konfigurującego i utrzymującego instalację np. przez zainfekowany komputer, z którego wgrywana jest aktualizacja oprogramowania.

Wektory ataku mogą powstać w wyniku:

- niezamierzonych błędów konfiguracyjnych i programistycznych różnych stron
- braku regularnych aktualizacji oprogramowania
- niedbałości lub nadmiernego optymizmu instalatorów lub właścicieli
- nieznajomość obszaru cyberbezpieczeństwa
- celowych działań na różnych etapach: produkcji, dostawy sprzętu, oprogramowania

Wykorzystanie wektora jest jednym z etapów cyberataku. Może zostać przeprowadzone w wyniku działań:

- motywowanych finansowo, np. celem żądania okupu za przywrócenie instalacji do pracy

- motywowanych aktywistycznie czy politycznie, np. wpływ na pracę instalacji dla medialnego wykorzystania tego działania lub wzmocnienia określonego przekazu
- wrogich lub nawet wojennych, np. wyłączenie znacznej liczby instalacji w celu spowodowania niedostępności energii elektrycznej dla użytkownika

03. Cyberbezpieczeństwo instalacji OZE

Bezpieczeństwo instalacji OZE można podnosić przez wykonywanie konkretnych czynności oraz ostrożne postępowanie w sytuacjach podwyższonego ryzyka. Istotna jest świadomość występowania potencjalnych zagrożeń związanych z posiadaniem i korzystaniem z urządzeń komunikujących się poprzez sieć internetową. Ważne jest przestrzeganie ogólnych zasad "cyberhigieny" oraz aktywne podejmowanie działań w celu ograniczenia ryzyka możliwości uzyskania nieautoryzowanego dostępu do urządzeń i wykorzystywanej sieci.

Bezpieczeństwo haseł

Większość systemów, w których można monitorować i konfigurować parametry pracy instalacji OZE posiada zabezpieczenie w postaci hasła, lub pary loginu i hasła. Dodatkowo, należy pamiętać, że podczas korzystania z sieci Wi-Fi do podłączenia instalacji do Internetu, często wykorzystujemy kolejne hasło. Gdy korzystamy z rozwiązania chmurowego lub nasz system jest dostępny z Internetu słabość stosowanego hasła może być bezpośrednim wektorem ataku. Dlatego bezpieczeństwo właśnie tego składnika jest kluczowe w ochronie przed atakującymi.

Atakujący stosują najpopularniejsze hasła (np. 12334, abcd, qwerty, admin12 itp.) lub wykorzystają publicznie dostępne informacje, aby uzyskać dostęp do kont użytkowników. Wszystkie zasady dotyczące bezpieczeństwa haseł można znaleźć pod adresem https://cert.pl/hasla. W kontekście OZE najważniejsze z nich to:

- Zmiana domyślnego hasła ustawionego przez producenta lub firmę wdrożeniową.
- Nowe silne i łatwe do zapamiętania hasło, wg. wytycznych opisanych poniżej. Unikanie haseł przewidywalnych: dat, nazwiska i imienia czy imienia czworonoga.
- Różne hasła do innych celów.
- Zapisywanie haseł i ich przechowywanie w bezpieczny sposób, np. w menedżerze haseł. Nieujawnianie hasła.
- Używanie uwierzytelniania wieloskładnikowego (MFA – Multi-Factor Authentication). W przypadku interfejsu lokalnego dla OZE jest to bardzo rzadko spotykane rozwiązanie, ale coraz częściej jest ono dostępne w przypadku korzystania z chmury producenta.

W celu stworzenia silnego, łatwego do zapamiętania hasła, można używać zasady pełnych zdań. Warto unikać znanych cytatów czy powiedzeń. Można jednak je modyfikować, aby służyły jako inspiracja. Tak stworzone hasło powinno składać się z przynajmniej pięciu słów:

WlazłKostekNaMostekIStuka

Inną wartą polecenia metodą jest budowanie hasła z opisu wyimaginowanej sceny, której obraz jest łatwy do zapamiętania i jednoznacznego opisania. Należy zwrócić uwagę, że scena opisująca hasło, powinna zawierać jakiś element nierealistyczny albo abstrakcyjny:

zielonyParkingDla3malychSamolotow

Kolejnym pomysłem na generowanie silnego hasła jest użycie słów z kilku języków. Siła tego hasła wynika wprost z zasad łamania haseł opartych o całe zdanie. Metoda słownikowa najczęściej bierze pod uwagę słowa/zwroty z jednego języka:

DwaBialeLatajaceSophisticatedKroliki

Galwaniczny123$
zaq1@WSXcde3$RFV
admin.1admin.1admin.1admin.1

WlazlKostekNaMostekIStuka
zielonyParkingDla3malychSamolotow
DwaBialeLatajaceSophisticatedKroliki

Przykłady słabych i mocnych haseł.

Jak rozpoznawać popularne ataki?

Informacje o aktualnych zagrożeniach można znaleźć na stronie: https://cert.pl/zagrozenia. Wśród nich wielokrotnie przewija się phishing, który jest jednym z najpopularniejszych typów ataków. Phishing to działanie socjotechniczne, wykorzystujące techniki i metody manipulacyjne dla osiągnięcia oczekiwanego rezultatu. Najczęściej chodzi o wiadomość e-mail, SMS czy wiadomości na komunikatorach internetowych. Przestępcy internetowi próbują oszukać użytkownika i spowodować, aby podjął działanie zgodnie z zamierzeniami przestępców. Takie ataki mogą być szczególnie groźne w przypadku korzystania z chmury producenta. Atakujący mogą sklonować stronę logowania pa-

nelu do sprawdzania stanu pracy instalacji, a następnie nakłaniać użytkowników do podania danych na fałszywej stronie.

Podstawowe zasady ochrony przed zagrożeniem to:

- Sprawdzenie nazwy domeny odwiedzanego portalu. Domena to nazwa zawierająca się między https://, a pierwszym kolejnym znakiem /
- Nieuleganie presji czasu i autorytetu – oszuści próbują skłonić ofiarę do szybkiego, nieprzemyślanego działania, często bazując na emocjach.
- Ignorowanie wszelkich próśb o podanie hasła, nawet jeżeli komunikat wygląda oficjalnie, wymaga natychmiastowej reakcji i grozi dezaktywacją konta.
- Sprawdzenie pochodzenia wiadomości. Często adres mailowy nadawcy jest zupełnie niewiarygodny, czy też nie jest tożsamy np. z podpisem pod treścią maila.
- Poza próbą wyłudzenia dostępu do danych ataki phishingowe są coraz częściej wykorzystywane do zainfekowania urządzeń, np. w celu ich zaszyfrowania i żądania okupu (ataki ransomare).

Bezpieczeństwo urządzeń

Smartfony, tablety, laptopy lub komputery stacjonarne mogą być celem cyberataków. Bezpieczeństwo tych urządzeń często ma bezpośredni wpływ na bezpieczeństwo instalacji OZE ponieważ są narzędziem do odczytu parametrów pracy czy zmian konfiguracyjnych. W celu ich ochrony:

- Należy aktualizować oprogramowanie – nowe wersje zawierają poprawki i nowe funkcje, które chronią przed najnowszymi zagrożeniami. Jeśli pojawi się monit o zainstalowanie aktualizacji, warto upewnić się, czy faktycznie zostały one zaktualizowane.
- Warto korzystać z aktualnego oprogramowania antywirusowego.
- Należy blokować urządzenie, gdy nie jest używane. Warto wprowadzić kod PIN, hasło lub odcisk palca jako hasło dostępu do urządzenia. Utrudni to atakującemu wykorzystanie urządzenia, jeśli zostanie ono zgubione lub skradzione.
- Używanie tylko oficjalnych sklepów z aplikacjami (np. Google Play lub Apple App Store), zapewniających ochronę przed złośliwym oprogramowaniem. Nie warto pobierać aplikacji z przypadkowych źródeł, do których jesteśmy zachęcani w mediach społecznościowych. Ważne jest unikanie aplikacji, których reputacji nie znamy.

Zgłaszanie incydentów

Zgłaszanie informacji o podejrzanych działaniach w cyberprzestrzeni może znacznie zmniejszyć potencjalne szkody powodowane przez cyberataki. Dlatego w razie podejrzenia ataku lub jego próby należy zgłosić się do zespołu reagowania na incydenty bezpieczeństwa CSIRT NASK.

Cyberataki mogą być trudne do wykrycia. Dlatego najlepiej niezwłocznie prosić o wskazówki lub wsparcie, gdy wiadomość lub kontakt wydaje się podejrzany lub niezwykły. Ataki powinno się zgłaszać jak najszybciej - nie zrobi tego za nas nikt inny. Zgłoszenia rejestruje się na: https://incydent.cert.pl

Rekomendacje techniczne zmniejszające ryzyko ataku

Poza przestrzeganiem na co dzień zasad „cyberhigieny" równie ważna jest świadomość możliwości posiadanego systemu i konkretne techniczne działania zmniejszających ryzyko wystąpienia ataku. Poniżej znajduje się zbiór porad i wskazówek technicznych. Ich wdrożenie wymaga posiadania podstawowej wiedzy teletechnicznej. Rekomendujemy zatem, aby skorzystać z pomocy osoby posiadającej taką wiedzę i umiejętności.

Zweryfikuj złożoność haseł i uprawnienia kont

Po zalogowaniu do aplikacji służącej do odczytu parametrów pracy OZE należy wejść w ustawienia kont użytkowników. Szczegółowe informacje jak to zrobić będą dostępne w instrukcji użytkowania wykorzystywanego systemu. Jeśli taka możliwość się nie pojawia należy skontaktować się z firmą instalującą system i skonsultować opisane niżej czynności.

Czy używane hasło do logowania spełnia zasady cyberhigieny (patrz rozdział 3 - Bezpieczeństwo haseł)?

Jeśli nie, należy zmienić hasło dla użytkownika na nowe zgodnie z wytycznymi.

Czy na co dzień używane jest konto umożliwiające konfigurację systemu?

Jeśli tak, a system umożliwia zarządzanie uprawnieniami, należy stworzyć nowe konto, które będzie mogło jedynie monitorować parametry pracy bez możliwości jego konfiguracji. Na co dzień warto używać jedynie konta z ograniczonymi uprawnieniami.

Sposób połączenia z siecią

Ważną kwestią jest sposób komunikacji urządzeń OZE z siecią lokalną lub z Internetem. Znajomość sposobu połączenia i wynikające z niego ryzyka to kluczowa informacja dla bezpieczeństwa instalacji (patrz rozdział 2 - Wektory ataków).

Aby ustalić sposób połączenia należy odpowiedzieć na następujące pytania: Czy urządzenie jest podłączone do sieci Wi-Fi? Czy urządzenie jest podłączone kablem RJ45 (Ethernet)? Jeśli odpowiedź nie jest jednoznaczna, należy skontaktować się z firmą instalującą system. Jeśli do komunikacji z Internetem wykorzystywane jest Wi-Fi lub kabel Ethernet prawdopodobnie używane jest internetowe łącze domowe. W takim przypadku można sprawdzić, które z domowych urządzeń są publicznie widoczne z Internetu[1)].

1) Weryfikacji można dokonać używając np. strony internetowej me.shodan.io. Uwaga: Należy to zrobić znajdując się w sieci, podlegającej weryfikacji. Jeśli zostaną wyszukane nieznane usługi, należy sprawdzić konfigurację sieci lub skonsultować się z firmą instalującą system.

Jeśli urządzenie podłączone jest do sieci Wi-Fi kluczowe jest zadbanie o jej bezpieczeństwo. Przede wszystkim należy korzystać wyłącznie z sieci zabezpieczonej, do której dostęp jest chroniony silnym hasłem utworzonym zgodnie z rekomendacjami w rozdziale 3 - Bezpieczeństo haseł oraz wyłącznie z bezpiecznych algorytmów tj. WPA3 lub WPA2 (wiele urządzeń może nie wspierać jeszcze WPA3). Warto również wyłączyć mechanizm WP czy zadbać o aktualizację oprogramowania routera. Szczegółowe informacje jak sprawdzić i skonfigurować ustawienia routera powinny być dostępne w instrukcji użytkowania lub po kontakcie z firmą montującą router.

Dodatkowym aspektem zwiększającym bezpieczeństwo w przypadku wykorzystania sieci domowej jest odpowiednia izolacja urządzeń. W przypadku używania Wi-Fi warto podłączyć urządzenia związane z OZE do osobnej podsieci, nie używanej do żadnego innego celu. Na niektórych sprzętach nazwano ją np. “sieć gościa”. W bardziej zaawansowanych rozwiązaniach można do tego celu wykorzystać logicznie wydzielone podsieci tzw. VLANy, jednak ich szczegółowe omówienie nie jest zakresem tego poradnika.

Sprawdzenie aktualizacji

Zadbanie o regularną instalację aktualizacji oprogramowania jest podstawowym i najważniejszym działaniem, które można wykonać dla ochrony urządzeń podłączonych do sieci domowej lub komunikujących się przez Internet. W tym celu należy zweryfikować, czy urządzenie posiada możliwość automatycznej instalacji aktualizacji. Jeśli to jest możliwe i pozwala na to konfiguracja sieci, należy włączyć te funkcjonalność. Natomiast jeśli ta opcja jest niedostępna należy:

- regularnie sprawdzać aktualność oprogramowania;
- korzystać tylko z zaufanych źródeł zawierających aktualizacje;
- w przypadku aktualizacji z nośników zewnętrznych, zawsze wcześniej sprawdzać nowe nośniki pod kątem bezpieczeństwa;
- jeśli istnieje taka możliwość, aktualizację przeprowadzać bezpośrednio z wykorzystaniem aplikacji dostarczanej przez producenta falowników.

Na co zwrócić uwagę wybierając instalację OZE oraz firmę instalującą lub serwisującą instalacje?

1. Zadbaj o swoja wiedzę i śledź zmiany w prawie

Merytoryczne przygotowanie do inwestycji pozwoli Ci podejmować przemyślane decyzje i ułatwi komunikację z wykonawcą. Na bieżąco sprawdzaj zmiany w prawie. Zapoznaj się z podstawowymi informacjami dotyczącymi planowanej instalacji oraz opiniami użytkowników.

2. Zweryfikuj ofertę wybranej firmy fotowoltaicznej

Dobry wykonawca gwarantuje profesjonalne doradztwo i kompleksową usługę, obejmującą audyt fotowoltaiczny oraz przygotowanie projektu instalacji fotowoltaicznej. Projekt powinien uwzględniać konkretne warunki techniczne i zapotrzebowanie budynku na energię elektryczną.

3. Podpisz umowę z wykonawcą instalacji fotowoltaicznej

Uwzględnij wszystkie aspekty współpracy. Nieporozumienia dotyczą głównie kosztów i terminów. W dokumencie muszą znajdować się też szczegóły dotyczące samej instalacji fotowoltaicznej, np. moc systemu fotowoltaicznego. Pamiętaj: zanim podpiszesz umowę, dokładnie ją przeczytaj.

4. Zapytaj o gwarancję

Producenci udzielają gwarancji na moduły fotowoltaiczne (min. 10 lat), na zachowanie mocy (średnio 80% pierwotnej mocy znamionowej po 25 latach) oraz na falownik (zwykle 5 lat z możliwością przedłużenia). Ważna jest także gwarancja na wykonane prace od instalatora (od 3 do nawet 15 lat). Pamiętaj, nawet w przypadku rozwiązania firmy zachowasz gwarancje przyznane przez producenta.

5. Co sprawdzić i czego dowiedzieć się w firmie wykonującej instalację przed rozpoczęciem inwestycji?

- Czy udostępniane aktualizacje są bezpłatne i w jaki sposób są udostępniane?
- Czy instalowanie aktualizacji wymaga połączenia inwertera z Internetem?
- Czy aktualizacje oprogramowania będą dostępne w okresie gwarancyjnym i pogwarancyjnym?
- Czy aktualizacje mogą być wykonywane automatycznie?
- Kto jest odpowiedzialny za przeprowadzanie aktualizacji i czy jest to bezpłatne?
- Czy dla działania instalacji konieczny jest dostęp do Internetu?
- Do której sieci podłączono inwerter, jeśli potrzebuje dostępu do Internetu?
- Co się stanie, gdy instalacja utraci połączenie z Internetem?
- Jakie funkcjonalności są niedostępne dla użytkownika offline?
- Czy można monitorować parametry pracy instalacji będąc offline?
- Czy oferowane jest wsparcie w konfiguracji instalacji w przypadku wymiany routera Wi-Fi?

- Czy serwisant może uzyskać zdalny dostęp do instalacji, na jakich zasadach może się do niej podłączać?
- Jakie są zasady przetwarzania danych w chmurze producenta?
- Jak długo są przetrzymywane dane w chmurze producenta?
- Czy można uzyskać kopię danych z chmury producenta w dowolnym czasie?
- Czy w przypadku wystąpienia incydentu bezpieczeństwa w chmurze producenta do której podłączone są urządzenia użytkownik zostanie o tym poinformowany?
- Czy jest możliwość wieloskładnikowego uwierzytelniania podczas logowania (w szczególności do aplikacji internetowej)?
- Kto może modyfikować parametry pracy systemy w przypadku wystąpienia takiej potrzebny i w jaki sposób powinien to zrobić?
- Czy do instalacji można się podłączyć radiowo? Przykładowo, czy posiada ona wbudowany hotspot. Jeśli, tak w jaki sposób jest on zabezpieczony?
- Jeśli inwerter posiada wbudowany hotspot Wi-Fi to czy musi być on stale włączony?
- Czy instalator/użytkownik zmienił hasło dostępowe do systemu na unikalne?

6. Wskazówki i porady.

Lista pytań ułatwiających ocenę kompetencji firmy wykonującej instalację fotowoltaiki:

- Czy firma wykonuje audyt fotowoltaiczny i przygotowuje projekt instalacji fotowoltaicznej?
- Czy może przedstawić do wglądu rekomendacje/zdjęcia/opinie z wcześniejszych realizacji firmy?
- Czy wykonawca montuje instalację fotowoltaiczną samodzielnie, czy z podwykonawcami?
- Z jakich komponentów będzie składać się instalacja PV? Czy pochodzą od autoryzowanego producenta i mają odpowiednie certyfikaty?
- Czy moc instalacji jest wystarczająca, aby w przyszłości zamontować pompę ciepła lub klimatyzację?
- Czy firma zadba o dobór zabezpieczeń elektrycznych do instalacji fotowoltaicznej i instalację uziemiającą?
- Czy firma dokonuje odbioru instalacji i jaki jest zakres odbioru (np. pomiar uziemienia instalacji, pomiar wydajności instalacji)?
- Jakie są warunki gwarancji na wykonanie usługi montażu instalacji fotowoltaicznej?
- Czy firma posiada ubezpieczenie OC?

- Czy firma zapewnia serwis? Jakie są warunki serwisowania instalacji PV?
- Jaka będzie ostateczna cena zakupu i montażu paneli fotowoltaicznych oraz forma płatności?
- Co dokładnie zawiera oferta na zakup i montaż instalacji fotowoltaicznej? Czy firma pomaga w formalnościach, np. we wnioskowaniu o dofinansowanie?
- Kiedy rozpoczną się i zakończą prace instalacyjne, w tym montaż paneli fotowoltaicznych?

Jak odróżnić fachowca od amatora? Dobry instalator fotowoltaiki:

- ma uprawnienia do przygotowania projektu instalacji fotowoltaicznej (uprawnienia elektryczne lub certyfikat instalatora OZE),
- dysponuje uprawnieniami Stowarzyszenia Elektryków Polskich (SEP) typu D oraz E do montażu paneli słonecznych oraz opcjonalnie certyfikatem z Urzędu Dozoru Technicznego (UDT),
- odpowiada na pytania techniczne (np. o komponenty instalacji, przewody, systemy montażowe, uziemienie, zabezpieczenia przeciw zwarciom prądowym),
- pomaga w doborze miejsca zainstalowania falownika,
- wykonuje audyt fotowoltaiczny,
- opracowuje spersonalizowany projekt instalacji fotowoltaicznej,
- gwarantuje wybór prawidłowej mocy instalacji fotowoltaicznej oraz odpowiednich komponentów systemu PV,
- oferuje komponenty instalacji PV od cenionych producentów,
- pomaga przy dokumentacji technicznej i zgłoszeniowej,
- samodzielnie montuje moduły fotowoltaiczne, bez udziału podwykonawców,
- przeprowadza testy końcowe i pomiary elektryczne.

Zwróć szczególną uwagę jeżeli instalator fotowoltaiki:

- nie widnieje w rejestrach CEIDG i KRS,
- nie istnieje w Internecie,
- nie ma opinii od poprzednich klientów,
- nie informuje o całkowitej cenie zakupu i montażu instalacji fotowoltaicznej,
- oferuje zbyt niskie lub niewiarygodnie wysokie ceny,
- jest dostępny od zaraz,
- nie wykonuje audytu fotowoltaicznego,

- zawyża lub zaniża moc instalacji fotowoltaicznej,
- chce zamontować panele słoneczne w niekorzystnym miejscu,
- jest mało konkretny i nie potrafi odpowiedzieć na techniczne pytania, operuje wyłącznie ceną,
- nie oddzwania i nie odpowiada na wiadomości, nie dotrzymuje umówionych terminów.

Najważniejsze zapisy w umowie montażu instalacji fotowoltaicznej:

- data i miejsce zawarcia umowy,
- dane osobowe obu stron (koniecznie NIP i REGON firmy),
- przedmiot umowy,
- ostateczny koszt zakupu i montażu instalacji fotowoltaicznej,
- termin rozpoczęcia i zakończenia montażu instalacji fotowoltaicznej,
- szczytowa moc instalacji fotowoltaicznej określona w jednostce kWp,
- spis podzespołów fotowoltaicznych wykorzystywanych w ramach instalacji, ze wskazaniem producenta,
- sposób wykonania montażu instalacji fotowoltaicznej,
- termin i forma wypłaty wynagrodzenia,
- okres i warunki gwarancji na wykonane prace montażowe,
- obowiązki zlecającego i wykonawcy,
- własnoręczne podpisy obu stron,
- czytelna forma zapisu bez tzw. „drobnych druczków".

04. Podsumowanie

Odnawialne Źródła Energii to ciągle rozwijający się zbiór technologii, który pozwoli na realizację polityki klimatycznej oraz energetycznej w skali Unii Europejskiej oraz Rzeczypospolitej Polski. Dobrze wykorzystywana instalacja optymalizuje koszty utrzymania gospodarstw domowych. To z kolei niewątpliwie przekłada się na korzyści odbiorców końcowych, w tym prosumentów.

Rozwój OZE na przestrzeni ostatnich lat jest niezwykle dynamiczny. Równie sprawnie następuje postęp w rozwoju technologii, w tym wykorzystywanej przez

cyberprzestępców. Warto więc zadbać o stosowną ochronę i przestrzegać zasad cyberbezpieczeństwa na etapie wyboru, budowy i eksploatowania instalacji pozyskujących energię z odnawialnych źródeł. Ważne jest świadome podejście do zagadnienia bezpieczeństwa oraz stosowanie tzw. dobrych praktyk. Takie przeświadczenie powinno towarzyszyć przyszłemu prosumentowi już na wstępnie - czyli w fazie wyboru technologii, potem instalacji, a następnie jej konfigurowania.

Wskazówki opisane w zaprezentowanym dokumencie oraz podstawowe zasady tak zwanej „cyberhigieny", pozwolą zminimalizować ryzyko oraz zoptymalizować korzyści płynące z korzystania z odnawialnych źródeł energii. W przypadku wykrycia cyberataku lub innych niepokojących oznak należy dokonywać zgłoszeń pod adresem: https://incydent.cert.pl.

Dodatkowo w celu ciągłego podnoszenia świadomości z obszaru cyberbezpieczeństwa, zachęcamy do śledzenia publikacji w rzetelnych i zweryfikowanych źródłach, takich jak:

- https://www.gov.pl/web/cyfryzacja/wiadomosci
- https://www.gov.pl/web/baza-wiedzy/aktualnosci
- https://www.nask.pl/pl/aktualnosci
- https://cert.pse-online.pl/
- https://cert.pl/